



Canadian Securities
Administrators

Autorités canadiennes
en valeurs mobilières

**Joint Canadian Securities Administrators/Investment Industry
Regulatory Organization of Canada**
Consultation Paper 21-402
Proposed Framework for Crypto-Asset Trading Platforms

March 14, 2019

PART 1 – Introduction and purpose

The emergence of “digital assets” or “crypto assets” continues to be a growing area of interest for regulators globally. Innovations like distributed ledger technology (**DLT**) and crypto assets are relatively new and are transforming the landscape of the financial industry. Interest in crypto assets among investors, governments and regulators globally has increased significantly since the creation of bitcoin in 2008 and continues to grow. Early in 2018, at its peak, the total value of crypto assets was estimated, by one source, at more than US\$800 billion.¹ While the value has since fallen, trading volumes remain significant. Today, there are over 2000 crypto assets² that may be traded for government-issued currencies or other types of crypto assets on over 200 platforms³ that facilitate the buying and selling or transferring of crypto assets (**Platforms**). Many of these Platforms operate globally and without any regulatory oversight.

Although DLT may provide benefits, global incidents point to crypto assets having heightened risks related to loss and theft as compared to other assets. Regulators around the world are currently considering important issues surrounding the regulation of crypto assets including the appropriate regulation of Platforms. The Canadian Securities Administrators (the **CSA**) and the Investment Industry Regulatory Organization of Canada (**IIROC**, and together with the CSA, **we**), have been engaged with regulators globally, through IOSCO and other innovation initiatives, to seek input on a variety of regulatory approaches that exist in this area.

Platforms, depending on how they operate and the crypto assets they make available for trading may be subject to securities regulation. The CSA, through its Regulatory Sandbox⁴, is in discussions with several Platforms that are seeking guidance on the requirements that apply to them. We have heard directly from some Platform operators and their advisers that a regulatory framework is welcome, as they seek to build consumer confidence and expand their businesses across Canada and globally.

Currently there are no Platforms recognized as an exchange or otherwise authorized to operate as a marketplace or dealer in Canada. As such, the CSA has urged Canadians to be cautious when buying crypto assets.⁵

Platforms facilitate the buying and selling of crypto assets and perform functions similar to one or more of exchanges, alternative trading systems (**ATSs**), clearing agencies, custodians and dealers. Depending on their structure, they may also introduce novel features which create risks to investors and our capital markets that may not be fully addressed by the existing regulatory framework. Where securities legislation applies to Platforms we are considering a set of tailored regulatory requirements for them to address the novel features and risks (the **Proposed Platform Framework**).

¹ <https://coinmarketcap.com/charts/>.

² Coinmarketcap.com listed 2098 different crypto assets as of March 1, 2019. See: <https://coinmarketcap.com/all/views/all/>.

³ Coinmarketcap.com listed 241 Platforms as of March 1, 2019. See: <https://coinmarketcap.com/rankings/exchanges/3>.

⁴ The CSA Regulatory Sandbox is an initiative of the CSA to support businesses seeking to offer innovative products, services and applications in Canada.

⁵ The CSA has previously issued investor alerts reminding investors of the [inherent risks associated with crypto asset futures contracts](#) and [the need for caution when investing with crypto asset trading platforms](#).

We endeavor to facilitate innovation that benefits investors and our capital markets, while ensuring that we have the appropriate tools and understanding to keep pace with evolving markets. The purpose of this joint CSA/IIROC Consultation Paper (the **Consultation Paper**) is to seek feedback from the financial technology (**fintech**) community, market participants, investors and other stakeholders on how requirements may be tailored for Platforms operating in Canada whose operations engage securities law. We intend to use this feedback to establish a framework that provides regulatory clarity to Platforms, addresses risks to investors and creates greater market integrity.

Throughout the Consultation Paper, investors participating on Platforms may be referred to as either **investors** or **participants**.

PART 2 – Nature of crypto assets and application of securities legislation⁶

Crypto assets differ in their functions, structures, governance and rights. Some crypto assets, commonly referred to as “utility tokens”, are created to allow holders to access or purchase goods or services on a DLT network being developed by the creators of the token. As set out in [CSA Staff Notice 46-307 Cryptocurrency Offerings](#) and [CSA Staff Notice 46-308 Securities Law Implications for Offerings of Tokens](#), staff of the CSA have found that most of the offerings of utility tokens have involved a distribution of securities, usually as investment contracts. Other crypto assets are tokenized forms of traditional securities or derivatives and may represent an interest in assets or have their value may be based on an underlying interest. If crypto assets that are securities and/or derivatives are traded on a Platform, the Platform would be subject to securities and/or derivatives regulatory requirements.

We note that it is widely accepted that at least some of the well established crypto assets that function as a form of payment or means of exchange on a decentralized network, such as bitcoin, are not currently in and of themselves, securities or derivatives. Instead, they have certain features that are analogous to existing commodities such as currencies and precious metals.

However, securities legislation may still apply to Platforms that offer trading of crypto assets that are commodities, because the investor’s contractual right to the crypto asset may constitute a security or derivative. We are evaluating the specific facts and circumstances of how trading occurs on Platforms to assess whether or not a security or derivative may be involved. Some of the factors we are currently considering in this evaluation include:

- whether the Platform is structured so that there is intended to be and is delivery of crypto assets to investors,
- if there is delivery, when that occurs, and whether it is to an investor’s wallet over which the Platform does not have control or custody,
- whether investors’ crypto assets are pooled together with those of other investors and with the assets of the Platform,
- whether the Platform or a related party holds or controls the investors’ assets,

⁶ As defined in National Instrument 14-101 *Definitions*.

- if the Platform holds or stores assets for its participants, how the Platform makes use of those assets,
- whether the investor can trade, or rollover positions held by the Platform, and
- having regard to the legal arrangements between the Platform and its participants, the actual functions of the Platform and the manner in which transactions occur on it
 - who has control or custody of crypto assets,
 - who the legal owner of such crypto assets is, and
 - what rights investors will have in the event of the Platform's insolvency.

Consultation question

1. Are there factors in addition to those noted above that we should consider?

The CSA wishes to remind market participants that any person or company advertising, offering, selling or otherwise trading or matching trades in crypto assets that are securities or derivatives, or derivatives that are based on crypto assets to persons or companies in Canada, or conducting such activities from a place of business in Canada is subject to securities legislation in Canada. Further, as noted above, although some crypto assets may be commodities, securities legislation may still apply to Platforms that offer trading of such crypto assets because the investor's contractual right to the crypto asset/commodity may constitute a security or derivative. Further, in most jurisdictions in Canada, the provisions of securities legislation relating to fraud, market manipulation and misleading statements apply not just to the trading of securities and derivatives but also to trading of the underlying interest of a derivative (e.g. the commodity).

The Proposed Platform Framework referred to in this Consultation Paper considers how existing regulatory requirements may be tailored for Platforms and should not be construed as acceptance by the CSA that securities and/or derivatives legislation may not apply to any particular offering involving crypto assets.

PART 3 – Risks related to Platforms

The operational models and the risks related to Platforms may vary from one platform to another; however, the risks are not entirely different than those applicable to other types of regulated entities such as marketplaces and dealers. The introduction of crypto assets and the operational models of Platforms, however, raise different and in some cases heightened, areas of risk. Key areas of risk include:

- **Investors' crypto assets may not be adequately safeguarded** – Many Platforms have control of their participants' crypto assets (e.g. they keep participants' crypto assets in a single account on the distributed ledger under the Platform's private key or the Platform holds its participants' private keys on their behalf). Platforms may not have necessary processes and controls in place to segregate participants' assets from their own and to safeguard those assets, including maintaining and safeguarding any private keys associated with wallets held by the Platform. There are also current challenges associated with auditing the internal controls surrounding custody of participants' assets.

- **Processes, policies and procedures may be inadequate** – Platforms may not have sufficient processes, policies and procedures in place to establish an internal system of controls and supervision sufficient to prudently manage the risks associated with their business, including business continuity risks, key personnel risks and regulatory compliance risks.
- **Investors’ assets may be at risk in the event of a Platform’s bankruptcy or insolvency** – Platforms may not segregate participants’ assets from their own or may use participants’ assets to fund operating costs and other expenses. As a result, Platforms may not hold sufficient assets to cover investor claims and return investors’ assets in the event of bankruptcy or insolvency. In addition, Platforms may operate in jurisdictions that have limited asset protection and insolvency regimes.
- **Investors may not have important information about the crypto assets that are available for trading on the Platform** – Each crypto asset has its own functions, associated rights and risks. Platforms may not provide sufficient or clear information about the crypto assets for participants to make informed investment decisions. Examples of information may include the standards that the crypto asset had to meet before being admitted for trading on the Platform and any potential difficulties in liquidating the crypto asset.
- **Investors may not have important information about the Platform’s operations** – Platforms may not provide sufficient information about the functions they perform and their fees. For example, some Platforms do not deliver crypto assets to a wallet controlled by the participant unless requested, but participants may not be aware of this or the risks associated with the Platform retaining custody of their crypto assets, including that they may not be able to access their crypto assets.
- **Investors may purchase products that are not suitable for them** – Exchanges and other regulated marketplaces do not interact directly with retail investors; instead they interact through regulated intermediaries (i.e. registered dealers). In contrast, Platforms may offer investors (including retail investors) direct access to the Platform without the use of a regulated intermediary that performs know-your-client and suitability assessments. As a result, participants may purchase crypto assets, many of which can be complex, high risk and volatile products, that are not suitable investments for them.
- **Conflicts of interest may not be appropriately managed** – There may be conflicts of interest between the Platform’s operator and participants who access the Platform, including the inherent conflicts of interest where Platforms act as market makers and trade as principal.
- **Manipulative and deceptive trading may occur** – Platforms may be susceptible to manipulative and deceptive trading given the market volatility, lack of reliable pricing information for crypto assets, the fact that they trade 24 hours daily and the fact that trading on many Platforms is not currently monitored.
- **There may not be transparency of order and trade information** – Information relating to the price and volume of orders and trades may not be publicly available or sufficient to support efficient price discovery.
- **System resiliency, integrity and security controls may be inadequate** – Platforms have significant cybersecurity risks. DLT is a nascent technology and Platform operators may not have sufficient experience or possess the necessary skills to ensure that systems function properly and there is adequate protection against cyber theft of participants’ crypto asset investments.

Consultation question

2. What best practices exist for Platforms to mitigate these risks? Are there any other substantial risks which we have not identified?

PART 4 – Regulatory approaches in other jurisdictions

In developing the Proposed Platform Framework, we considered the approaches taken by securities and financial regulators in other jurisdictions. We found that in many jurisdictions the existing regulatory requirements will apply to regulate Platforms within those jurisdictions. Some jurisdictions may tailor requirements or provide exemptions. This means that the regulatory requirements applicable to exchanges, ATSS (in the U.S. or Canada), multilateral trading venues (in Europe) and other regulated markets may apply to a Platform.

In the U.S., the Securities and Exchange Commission (**SEC**) issued a statement indicating that, if a platform offers trading of digital securities and operates a marketplace, it must be registered with the SEC as a national securities exchange, registered with the Financial Industry Regulatory Authority as a broker-dealer operating an ATS, or be exempt from registration.⁷ The Commodity Futures Trading Commission (**CFTC**) has indicated that bitcoin and certain other crypto assets are encompassed in the definition of “commodity”. In the context of retail commodity transactions in crypto assets, for example on Platforms, the CFTC has consulted with market participants on its approach to the proposed interpretation of the term “actual delivery”.⁸

In European jurisdictions, the regulatory framework under the Markets in Financial Instruments Directive (**MiFID**) applies when crypto assets qualify as financial instruments. The European Securities and Markets Authority (**ESMA**) recently published a report with their advice on initial coin offerings and crypto assets where they identify the risks in the crypto asset sector.⁹ In the report, ESMA indicates that where crypto assets qualify as transferable securities or other types of MiFID financial instruments, the existing regulatory framework will apply. ESMA also noted that the existing requirements may not address all the risks, and in some areas, the requirements may not be relevant in a DLT framework.

In Singapore, Platforms that trade crypto assets that are securities may be approved exchanges or be recognised market operators and, in both cases, are subject to regulation by the Monetary Authority of Singapore.¹⁰

⁷ SEC Statement on Potentially Unlawful Online Platforms for Trading Digital Assets (March 7, 2018):

<https://www.sec.gov/news/public-statement/enforcement-tm-statement-potentially-unlawful-online-platforms-trading>.

⁸ CFTC, Retail Commodity Transactions Involving Virtual Currency, Proposed Interpretation, 82 Fed. Reg. 60335 (December 20, 2017): <https://www.cftc.gov/sites/default/files/idc/groups/public/@Irfederalregister/documents/file/2017-27421a.pdf>.

⁹ ESMA Advice – Initial Coin Offerings and Crypto-Assets (January 9, 2019):

https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf.

¹⁰ Monetary Authority of Singapore, A Guide to Digital Token Offerings (last updated November 30, 2018):

<http://www.mas.gov.sg/~media/MAS/Regulations%20and%20Financial%20Stability/Regulations%20Guidance%20and%20Licensing/Securities%20Futures%20and%20Fund%20Management/Regulations%20Guidance%20and%20Licensing/Guidelines/A%20Guide%20to%20Digital%20Token%20Offerings%20last%20updated%20on%2030%20Nov%202018.pdf>

In Hong Kong, Platforms that are trading products that are not within the remit of the Hong Kong Securities and Futures Commission (**HKSFC**) can apply to use HKSFC's Regulatory Sandbox, particularly if they will, in the future, seek to offer trading of products that are within the remit of the HKSFC. This will allow the HKSFC to engage in an exploratory stage where it observes the Platform's operations and considers the effectiveness of proposed regulatory requirements for Platforms and whether Platforms are appropriate to be regulated by the HKSFC. If the decision is made to license the Platform, additional restrictions may apply.¹¹

In Malaysia, the *Capital Markets and Services (Prescription of Securities) (Digital Currency and Digital Token) Order 2019* came into force on January 15, 2019 and specifies that all digital currencies, tokens and crypto assets are classified as securities, placing them under the authority of the Securities Commission Malaysia.¹²

Many financial regulators are proactively conducting inquiries into the activities of Platforms to determine if they are carrying on activities that require them to comply with their requirements.

Consultation question

3. Are there any global approaches to regulating Platforms that would be appropriate to be considered in Canada?

PART 5 – The Proposed Platform Framework

5.1 Overview of the Proposed Platform Framework

The Proposed Platform Framework will apply to Platforms that are subject to securities legislation and that may not fit within the existing regulatory framework. It will apply both to Platforms that operate in Canada and to those that have Canadian participants.¹³

In developing the Proposed Platform Framework, the CSA considered that some of the Platforms are hybrid in nature and may perform functions typically performed by one or more of the following types of market participants: ATSS¹⁴, exchanges¹⁵ (exchanges and ATSS are both types of marketplaces¹⁶), dealers, custodians and clearing agencies. Specifically:

¹¹ HKSFC Conceptual framework for the potential regulation of virtual asset trading platform operators (November 1, 2018): https://www.sfc.hk/web/EN/files/ER/PDF/App%20-%20Conceptual%20framework%20for%20VA%20trading%20platform_eng.pdf

¹² Securities Commission Malaysia media release (January 14, 2019): <https://www.sc.com.my/news/media-releases-and-announcements/sc-to-regulate-offering-and-trading-of-digital-assets>

¹³ The CSA may consider exemptive relief from the applicable requirements if the Platform is located outside of Canada and is regulated by a foreign regulator in a manner that is similar to domestic oversight.

¹⁴ ATS is defined in every jurisdiction other than Ontario in s. 1.1 of National Instrument 21-101 *Marketplace Operation* (**NI 21-101**), and in Ontario in ss. 1(1) of the *Securities Act* (Ontario).

¹⁵ An exchange is a marketplace that may, among other things, lists the securities of issuers; provides a guarantee of a two-sided market for a security on a continuous or reasonably continuous basis; sets requirements governing the conduct of marketplace participants; or disciplines marketplace participants. Securities legislation enables securities regulatory authorities to recognize exchanges or exempt an exchange from recognition.

¹⁶ Marketplace is defined in every jurisdiction other than Ontario in s. 1.1 on NI 21-101, and in Ontario in ss. 1(1) of the *Securities Act* (Ontario).

- like an exchange or ATS, they may be a market or facility where orders of multiple buyers and sellers are brought together and matched;
- like an exchange, they may facilitate the creation or “listing” of a crypto asset;
- like an ATS or exchange, they may decide which crypto assets will be eligible for trading;
- like an exchange, they may offer a guarantee of a two-sided market and conduct regulatory activities;
- like a dealer, they may perform know-your-client and suitability reviews to grant access to investors (retail and institutional) and they may trade as principal;
- like a dealer or a custodian, they may self-custody investor’s assets or otherwise have control over investors’ assets; and
- like a clearing agency, they may enable the clearing and settlement of trades.

Application of marketplace requirements

The Proposed Platform Framework is based on the existing regulatory framework applicable to marketplaces and incorporates relevant requirements for dealers facilitating trading or dealing in securities. It is tailored to take into account the functions that may be performed by each Platform. Specifically, a Platform that brings together orders of buyers and sellers of securities and uses non-discretionary methods for these orders to interact is a marketplace.

As a marketplace, a Platform will be subject to requirements that will address many of the risks outlined in Part 3 of the Consultation Paper, such as those set out in NI 21-101, National Instrument 23-101 *Trading Rules* (NI 23-101 and, together with NI 21-101, the **Marketplace Rules**) and National Instrument 23-103 *Electronic Trading and Direct Access to Marketplaces* (NI 23-103).

Application of dealer requirements

In addition to marketplace functions, the Platform may also perform dealer functions, for example, providing custody of crypto assets and permitting direct access to trading by retail investors. As a result, the Proposed Platform Framework will include requirements that address the risks relating to these additional functions. Many of these requirements already exist in regulatory frameworks applicable to dealers.

Some entities will not fall within the definition of a marketplace. For example, an entity that is trading crypto assets that are securities but always trades against its participants and does not facilitate trading between buyers and sellers may be regulated as a dealer only and therefore not be subject to the Marketplace Rules and the Proposed Platform Framework. For example, firms that are currently registered in the category of exempt market dealer and that are currently permitted under securities legislation to facilitate the sale of securities, including crypto assets, in reliance on available prospectus exemptions in National Instrument 45-106 *Prospectus Exemptions* can continue to offer this service as long as they do not fall within the definition of “marketplace”.

Registered firms introducing crypto asset products and/or services are required to report changes in their business activities to their principal regulator and the proposed activities may be subject to review to assess whether there is adequate investor protection.

Investment dealer registration and IIROC membership

Like the Marketplace Rules, the Proposed Platform Framework contemplates Platforms both becoming registered as investment dealers and becoming IIROC dealer and marketplace members (**IIROC Members**)¹⁷. IIROC currently oversees all investment dealers as well as trading activity on debt and equity marketplaces in Canada and, accordingly,

- has a comprehensive body of rules governing the business, financial and trading conduct of IIROC Members which are tailored to the different types of products and services offered by IIROC Members;
- has established programs to assess compliance with both IIROC's rules applicable to dealers (**IIROC Dealer Member Rules**) and the Universal Market Integrity Rules (**UMIR**) that govern trading on a marketplace;
- has experience with dealers and marketplaces that trade a variety of securities and has developed tailored compliance programs and applied tailored rules for marketplaces; and
- operates in a regulatory capacity in every province in Canada.

Recognition as an exchange

A Platform that intends to carry on business as an exchange should contact the relevant securities regulatory authority to discuss whether recognition as an exchange is appropriate or, if such Platforms offer direct retail access or trade as principal, the Proposed Platform Framework is more appropriate to address risks arising from these activities.

Derivatives requirements

The CSA plans to consult on the appropriate regulatory framework to apply to marketplaces that trade over-the-counter derivatives, including platforms that offer derivatives with exposure to a crypto asset (e.g. a derivatives trading facility or swap execution facility that facilitate transactions in bitcoin-based derivatives). In the interim, if a Platform is trading or dealing in crypto assets that may be classified as derivatives, to the extent that the Platform has similar functions or operations to those contemplated in this Consultation Paper, it may be appropriate to apply requirements to those Platforms that are similar to the requirements contemplated by the Proposed Platform Framework. We anticipate, however, that such requirements may need to be specifically tailored to reflect the requirements that currently apply to derivatives or are otherwise appropriate to apply to those products and marketplaces.¹⁸

5.2 Proposed Platform Framework - Key areas for consultation

While the Proposed Platform Framework builds on an existing regulatory regime that was designed for a wide variety of market participants, we recognize that the existing regulatory requirements, and particularly the Marketplace Rules, were designed for marketplaces trading traditional securities (such as equities and debt). The CSA supports innovation in our capital markets while

¹⁷ We note that IIROC membership may not be appropriate in all cases, depending on the facts and circumstances.

¹⁸ We would also like to remind market participants of the requirements relating to commodity futures exchange contracts in securities and commodity futures legislation.

protecting investors and promoting fair and efficient capital markets. We are therefore considering a set of requirements tailored to Platforms' operations that appropriately addresses the new risks introduced.

Below, we seek feedback on a number of areas that will assist in determining appropriate requirements for Platforms.

5.2.1 Custody and verification of assets

It has been reported that crypto assets with a value of almost US\$1 billion were stolen in 2018 from Platforms that operate globally.¹⁹ The ownership of crypto assets is evidenced by private keys which are required to execute crypto asset transactions. As the loss or theft of a private key may result in the loss of assets, the safeguarding of private keys is especially critical.

The operational model of many Platforms involves the Platform having custody of its participants' assets including private keys or the Platform holding the crypto assets in its own wallet with the Platform's private key. As a result, appropriate custody controls are a necessary part of managing risks to investors. To the extent that the Platform holds or has control over investors' assets, a significant risk is that investors' assets are not sufficiently accounted for or protected by the Platform. As a result, the Platform might not have sufficient crypto assets or cash to satisfy demand or could be vulnerable to theft. This risk increases substantially if there is insufficient insurance to cover the full amount of the theft.

When looking at the operations of a Platform, we will assess whether a Platform's risk management policies and procedures are appropriate to manage and mitigate the custodial risks. Expectations will be guided by the operational model of the Platform. For example, if the trades on a Platform do not occur on the distributed ledger, and instead the Platform keeps track of changes in ownership on its own internal ledger, we will evaluate whether the Platform has a robust system of internal controls, including records, that ensures that a participant's crypto assets are accurately accounted for by the Platform and appropriately segregated from assets belonging to the Platform.

Traditional custodians that hold assets for clients typically engage an independent auditor to perform an audit of the custodian's internal controls and prepare an assurance report. There are different types of assurance reports; however, it is common for custodians to engage external auditors to issue system and organization controls reports such as SOC 1 Reports²⁰ and SOC 2 Reports²¹ regarding the suitability of internal controls in financial reporting and controls surrounding the custody of investors' assets. The auditor will issue a report pertaining to the design of the controls (**Type I Report**), and a report assessing whether such controls are operating as intended over a defined period (**Type II Report**). We anticipate that these reports will play an important role in the authorization and oversight of the Platform, reporting of transactions, internal risk management and verification of the existence of investors' assets. We contemplate requiring that Platforms obtain SOC 2, Type I and II Reports for their custody system and, if they use third-party custodians, to ensure that they have SOC 2, Type I and II Reports.

¹⁹ <https://www.reuters.com/article/us-crypto-currency-crime/cryptocurrency-theft-hits-nearly-1-billion-in-first-nine-months-report-idUSKCN1MK1J2>.

²⁰ Report on controls at a service organization relevant to participant entities' internal control over financial reporting.

²¹ Report on controls at a service organization relevant to security, availability, processing integrity, confidentiality or privacy.

We understand, however, that there have been challenges with crypto asset custodians and Platforms obtaining SOC 2, Type II Reports, in part due to the novel nature of crypto asset custody solutions and the limited period of time that Platforms have been in operation to allow for the testing of internal controls. Nevertheless, we contemplate that Platforms seeking registration as an investment dealer registration and IIROC membership that plan to provide custody of crypto assets will not only need to satisfy existing custody requirements but will also be expected to meet other yet-to-be determined standards specific to the custody of crypto assets.

Consultation questions

4. What standards should a Platform adopt to mitigate the risks related to safeguarding investors' assets? Please explain and provide examples both for Platforms that have their own custody systems and for Platforms that use third-party custodians to safeguard their participants' assets.
5. Other than the issuance of Type I and Type II SOC 2 Reports, are there alternative ways in which auditors or other parties can provide assurance to regulators that a Platform has controls in place to ensure that investors' crypto-assets exist and are appropriately segregated and protected, and that transactions with respect to those assets are verifiable?
6. Are there challenges associated with a Platform being structured so as to make actual delivery of crypto assets to a participant's wallet? What are the benefits to participants, if any, of Platforms holding or storing crypto assets on their behalf?

5.2.2 Price determination

Fair and efficient capital markets are dependent on price discovery. The wide availability of information on orders and/or trades is important to foster efficient price discovery and investor confidence. As with traditional marketplaces, Platforms will be required to foster price discovery for the crypto assets they offer for trading. It is important for regulators and for the participants on the Platform to understand how prices on a Platform are determined. In addition, where the Platform or an affiliate acts as a market maker and provides quotes, the mechanisms for determining those quotes are expected to be available to participants. When trading as a market maker against its participants, a Platform will also be required to provide participants with a fair price.

Consultation questions

7. What factors should be considered in determining a fair price for crypto assets?
8. Are there reliable pricing sources that could be used by Platforms to determine a fair price, and for regulators to assess whether Platforms have complied with fair pricing requirements? What factors should be used to determine whether a pricing source is reliable?

5.2.3 Surveillance of trading activities

The existing types of marketplaces have different regulatory responsibilities. Exchanges are responsible for conducting market surveillance of trading activities on the exchange and enforcing market integrity rules. All of the existing equity exchanges have retained IIROC to monitor trading activity and enforce market integrity rules. ATSS, by contrast, are not permitted to conduct market surveillance or enforcement activities and are required to engage a regulation services provider (**RSP**). IIROC currently acts as an RSP to all equity and fixed income marketplaces.

If IIROC were retained as an RSP by a Platform, IIROC would conduct market surveillance for that Platform. We understand that some of the types of manipulative and deceptive trading activities that may occur on Platforms that trade crypto assets are similar to those on marketplaces trading traditional securities. A unique challenge associated with market surveillance on Platforms is the fact that crypto assets trade on a global basis, on and off Platforms, outside regular trading hours, and may be illiquid and highly volatile. This, and the fact that there is currently no central source for pricing, may affect the price of a crypto asset trading on a Platform. This may also make it difficult to obtain reliable reference data that is needed to conduct effective surveillance.

To reduce the risks of potentially manipulative or deceptive activities, in the near term, we propose that Platforms not permit dark trading or short selling activities, or extend margin to their participants. We may revisit this once we have a better understanding of the risks introduced to the market by the trading of crypto assets.

Some Platforms have indicated that they intend to set rules and monitor the trading activities of their marketplace participants rather than retaining an RSP. This may raise conflicts of interest issues that will need to be addressed.

Consultation questions

9. Is it appropriate for Platforms to set rules and monitor trading activities on their own marketplace? If so, under which circumstances should this be permitted?
10. Which market integrity requirements should apply to trading on Platforms? Please provide specific examples.
11. Are there best practices or effective surveillance tools for conducting crypto asset market surveillance? Specifically, are there any skills, tools or special regulatory powers needed to effectively conduct surveillance of crypto asset trading?
12. Are there other risks specific to trading of crypto assets that require different forms of surveillance than those used for marketplaces trading traditional securities?

5.2.4 Systems and business continuity planning

System resiliency, reliability and security controls are important for investor protection. System failures may result in investors being unable to access their crypto assets and may have an impact on market efficiency and investor protection. Marketplaces are required to have adequate internal and information technology controls over their trading, surveillance and clearing systems and information security controls that relate to security threats and cyber-attacks.²² Marketplaces are also required to maintain business continuity and disaster recovery plans to provide uninterrupted provision of key services.²³ To ensure that marketplaces have adequate internal and technology controls in place over their trading, surveillance and clearing systems and that their systems function as designed, marketplaces are required to engage an entity with relevant experience both in information technology and in the evaluation of related internal controls to conduct an independent systems review (**ISR**).²⁴

Technology and cyber security are key risks for Platforms. For these reasons they will also be required to comply with the systems and business continuity planning requirements applicable to existing marketplaces in NI 21-101. One key difference between Platforms and traditional marketplaces is that there is a greater risk for participants when a Platform provides custody of investors' crypto assets and does not have the appropriate internal controls.

In the normal course, all marketplaces are required to have an ISR conducted for other critical systems including order entry, execution or data. These requirements are in place to manage risks associated with the use of technology and to ensure that minimum standards are maintained. In some cases, we have granted temporary exemptions from the ISR requirements, provided the marketplace did not pose a significant risk to the capital markets and certain reports and information are provided to regulators.

Consultation question

13. Under which circumstances should an exemption from the requirement to provide an ISR by the Platform be considered? What services should be included/excluded from the scope of an ISR? Please explain.

5.2.5 Conflicts of interest

Platforms may have certain conflicts of interests, similar to other marketplaces. They may also raise a number of unique conflicts. For example, they may provide advice to their participants, which raises a conflict because the Platform may be providing advice on the same crypto assets that they have made eligible for trading on the Platform.

Another conflict relates to proprietary trading. Like dealers, it is possible that some Platforms trade for their own account against their participants, including retail investors. This raises conflicts of interest and a number of risks, including that the Platform's participants may not know that the

²² Part 12 of NI 21-101.

²³ Ibid.

²⁴ Ibid.

Platform operator also trades on the marketplace against the investor and the risk that investors may not receive a fair price when trading against the Platform operator.

To address these risks, we contemplate that Platforms will be required to identify and manage potential conflicts of interest and will be required to disclose whether they trade against their participants, including acting as a market maker, and the associated conflicts of interest. Disclosure will assist investors in assessing whether they want to participate on the Platform. To the extent Platforms are required to become IIROC Members, they will also be subject to requirements in the UMIR aimed at mitigating the risks associated with trading against their participants.²⁵

Consultation questions

14. Is there disclosure specific to trades between a Platform and its participants that Platforms should make to their participants?
15. Are there particular conflicts of interest that Platforms may not be able to manage appropriately given current business models? If so, how can business models be changed to manage such conflicts appropriately?

5.2.6 Insurance

Some Platforms have custody of investors' assets. This makes them attractive targets for cyber-attacks and theft by insiders. Accordingly, insurance will also be an important safeguard. Dealers are required to maintain bonding or insurance against specific risks and in specified amounts.²⁶ This requirement may not address the specific operational risks of Platforms.

Many Platforms currently operate without any insurance covering investors' assets. We note that there may be significant difficulty and costs for a Platform to obtain insurance, in part due to the limited number of crypto asset insurance providers, and the high risk of cyber-attacks. Therefore, some Platforms have indicated that they are considering limited coverage that only extends to certain crypto assets, crypto assets in "hot wallets" or "cold wallets", loss as result of hacking, or loss from insider theft.

Consultation questions

16. What type of insurance coverage (e.g. theft, hot-wallet, cold-wallet) should a Platform be required to obtain? Please explain.
17. Are there specific difficulties with obtaining insurance coverage? Please explain.
18. Are there alternative measures that address investor protection that could be considered equivalent to insurance coverage?

²⁵ These include UMIR 5.3 *Client Priority*, UMIR 8.1 *Client Principal Trading* and UMIR 4.1 *Frontrunning*.

²⁶ s. 12.3 of NI 31-103.

5.2.7 Clearing and settlement

All trades executed on a marketplace are required to be reported and settled through a clearing agency.²⁷ A regulated clearing agency improves the efficiency of marketplaces and brings stability to the financial system.

Without exemptive relief, this requirement would also apply to Platforms that are marketplaces. However, currently there are no regulated clearing agencies for crypto assets that are securities or derivatives. As indicated above, we understand that on some Platforms, transaction settlement occurs on the Platform's internal ledger and is not recorded on the distributed ledger. We are considering whether an exemption from the requirement to report and settle trades through a clearing agency is appropriate. In these circumstances, Platforms will still be subject to certain requirements applicable to clearing agencies and will therefore be required to have policies, procedures and controls to address certain risks including operational, custody, liquidity, investment and credit risk.²⁸ We plan to revisit such exemptions in the future, as the space continues to develop and evolve.

Some Platforms may operate a non-custodial (decentralized) model where the transfer of crypto assets that are securities or derivatives occurs between the two parties of a trade on a decentralized blockchain protocol (e.g. smart contract). These types of Platforms will be required to have controls in place to address the specific technology and operational risks of the Platform.

Consultation questions

19. Are there other models of clearing and settling crypto assets that are traded on Platforms? What risks are introduced as a result of these models?
20. What, if any, significant differences in risks exist between the traditional model of clearing and settlement and the decentralized model? Please explain how these different risks may be mitigated.
21. What other risks are associated with clearing and settlement models that are not identified here?

5.2.8 Applicable regulatory requirements

Platforms that are marketplaces are subject to existing marketplace regulatory requirements, including those summarized at **Appendix B**. Some of these requirements may not be relevant for Platforms and others may need to be tailored to address specific risks.

Platforms may perform additional functions typically performed by dealers and clearing agencies. We are also considering how the requirements summarized at **Appendices C** and **D** may apply. Leveraging the existing regulatory frameworks will ensure that Platforms are treated similarly to

²⁷ Part 13 of NI 21-101.

²⁸ If not already addressed by rules applicable to IIROC Members, to the extent they apply.

other marketplaces, but with appropriately tailored requirements that are relevant for the functions they perform.

Please note that Appendices B, C and D provide only an overview of certain requirements and therefore they should not be relied upon as exhaustive lists of the requirements applicable to marketplaces, dealers and clearing agencies.

Consultation question

22. What regulatory requirements, both at the CSA and IIROC level, should apply to Platforms or should be modified for Platforms? Please provide specific examples and the rationale.

PART 6 – Providing Feedback

The CSA Regulatory Sandbox is an initiative of the CSA to support business seeking to offer innovative products, services and applications in Canada. The CSA Regulatory Sandbox is a part of the CSA's 2016-2019 Business Plan's objectives to gain a better understanding of how fintech innovations are impacting capital markets and assess the scope and nature of regulatory implications.²⁹

We invite interested parties to make written submissions on the consultation questions identified throughout this Consultation Paper. A complete list of the consultation questions referred to throughout this paper is provided in **Appendix A**. We also welcome you to provide any other comments on the appropriate regulation of Platforms. The information provided will assist us in refining the Proposed Platform Framework and our understanding of this area of innovation.

Please submit your comments in writing by **May 15, 2019**. Please send your comments by email in Microsoft Word format. Address your submission to IIROC and all members of the CSA as follows:

British Columbia Securities Commission
 Alberta Securities Commission
 Financial and Consumer Affairs Authority of Saskatchewan
 Manitoba Securities Commission
 Ontario Securities Commission
 Autorité des marchés financiers
 Financial and Consumer Services Commission (New Brunswick)
 Superintendent of Securities, Department of Justice and Public Safety, Prince Edward Island
 Nova Scotia Securities Commission
 Securities Commission of Newfoundland and Labrador
 Superintendent of Securities, Northwest Territories
 Superintendent of Securities, Yukon
 Superintendent of Securities, Nunavut

²⁹ CSA Business Plan, 2016-2019: https://www.securities-administrators.ca/uploadedFiles/General/pdfs/CSA_Business_Plan_2016-2019.pdf

Please deliver your comments **only** to the addresses below. Your comments will be distributed to IIROC and the other CSA members.

The Secretary
Ontario Securities Commission
20 Queen Street West
22nd Floor, Box 55
Toronto, Ontario M5H 3S8
Fax: 416-593-2318
comments@osc.gov.on.ca

Me Anne-Marie Beaudoin
Corporate Secretary
Autorité des marchés financiers
800, square Victoria, 22e étage
C.P. 246, tour de la Bourse
Montréal (Québec) H4Z 1G3
Fax : 514-864-6381
Consultation-en-cours@lautorite.qc.ca

IIROC
Victoria Pinnington
Senior Vice President, Market Regulation
Investment Industry Regulatory Organization of Canada
Suite 2000, 121 King Street West
Toronto, Ontario M5H 3T9
vpinnington@iiroc.ca

Certain CSA regulators require publication of the written comments received during the comment period. We will publish all responses received on the websites of the Autorité des marchés financiers (www.lautorite.qc.ca), the Ontario Securities Commission (www.osc.gov.on.ca), and the Alberta Securities Commission (www.albertasecurities.com). Therefore, you should not include personal information directly in comments to be published. It is important that you state on whose behalf you are making the submission.

PART 7 – Questions

Please refer your questions to any of the following CSA and IIROC staff:

Amanda Ramkissoon
Fintech Regulatory Adviser, OSC LaunchPad
Ontario Securities Commission
aramkissoon@osc.gov.on.ca

Ruxandra Smith
Senior Accountant, Market Regulation
Ontario Securities Commission
ruxsmith@osc.gov.on.ca

<p>Timothy Baikie Senior Legal Counsel Market Regulation Ontario Securities Commission tbaikie@osc.gov.on.ca</p>	<p>Serge Boisvert Senior Policy Advisor Exchanges and SRO Oversight Autorité des marchés financiers serge.boisvert@lautorite.qc.ca</p>
<p>Marc-Olivier St-Jacques Senior Policy Advisor Supervision of Intermediaries Autorité des marchés financiers marco.st-jacques@lautorite.qc.ca</p>	<p>Denise Weeres Director, New Economy Alberta Securities Commission denise.weeres@asc.ca</p>
<p>Katrina Prokopy Senior Legal Counsel, Market Regulation Alberta Securities Commission katrina.prokopy@asc.ca</p>	<p>Sasha Cekerevac Senior Analyst, Market Structure Alberta Securities Commission sasha.cekerevac@asc.ca</p>
<p>Dean Murrison Director, Securities Division Financial and Consumer Affairs Authority of Saskatchewan dean.murrison@gov.sk.ca</p>	<p>Zach Masum Manager, Legal Services, Capital Markets Regulation British Columbia Securities Commission zmasum@bcsc.bc.ca</p>
<p>Ami Iaria Senior Legal Counsel, Capital Markets Regulation British Columbia Securities Commission aiaria@bcsc.bc.ca</p>	<p>Peter Lamey Legal Analyst, Corporate Finance Nova Scotia Securities Commission peter.lamey@novascotia.ca</p>
<p>Chris Besko Director, General Counsel The Manitoba Securities Commission chris.besko@gov.mb.ca</p>	<p>Wendy Morgan Deputy Director, Policy Financial and Consumer Services Commission (New Brunswick) wendy.morgan@fcnb.com</p>
<p>Victoria Pinnington Senior Vice President, Market Regulation IIROC vpinnington@iiroc.ca</p>	<p>Sonali GuptaBhaya Director, Market Regulation Policy IIROC sguptabhaya@iiroc.ca</p>

APPENDIX A

Consultation Questions

1. Are there factors in addition to those noted in Part 2 that we should consider?
2. What best practices exist for Platforms to mitigate the risks outlined in Part 3? Are there any other significant risks which we have not identified?
3. Are there any global approaches to regulating Platforms that are appropriate to be considered in Canada?
4. What standards should a Platform adopt to mitigate the risks related to safeguarding investors' assets? Please explain and provide examples both for Platforms that have their own custody systems and for Platforms that use third-party custodians to safeguard their participants' assets.
5. Other than issuance of Type I and Type II SOC 2 Reports, are there alternative ways in which auditors or other parties can provide assurance to regulators that a Platform has controls in place to ensure that investors' crypto-assets exist and are appropriately segregated and protected, and that transactions with respect to those assets are verifiable?
6. Are there challenges associated with a Platform being structured so as to make actual delivery of crypto assets to a participant's wallet? What are the benefits to participants, if any, of the Platforms holding or storing crypto assets on their behalf?
7. What factors should be considered in determining a fair price for crypto assets?
8. Are there reliable pricing sources that could be used by Platforms to determine a fair price, and for regulators to assess whether Platforms have complied with fair pricing requirements? What factors should be used to determine whether a pricing source is reliable?
9. Is it appropriate for Platforms to set rules and monitor trading activities on their own marketplace? If so, under which circumstances should this be permitted?
10. Which market integrity requirements should apply to trading on Platforms? Please provide specific examples.
11. Are there best practices or effective surveillance tools for conducting crypto asset market surveillance? Specifically, are there any skills, tools or special regulatory powers needed to effectively conduct surveillance of crypto asset trading?
12. Are there other risks specific to trading of crypto assets that require different forms of surveillance than those used for marketplaces trading traditional securities?
13. Under which circumstances should an exemption from the requirement to provide an ISR by the Platform be appropriate? What services should be included/excluded from the scope of the ISR? Please explain.

14. Is there disclosure specific to trades between a Platform and its participants that Platforms should make to their participants?
15. Are there particular conflicts of interest that Platforms may not be able to manage appropriately given current business models? If so, how can business models be changed to manage such conflicts appropriately?
16. What type of insurance coverage (e.g. theft, hot-wallet, cold-wallet) should a Platform be required to obtain? Please explain.
17. Are there specific difficulties with obtaining insurance coverage? Please explain.
18. Are there alternative measures that address investor protection that could be considered that are equivalent to insurance coverage?
19. Are there other models of clearing and settling crypto assets that are traded on Platforms? What risks are introduced as a result of these models?
20. What, if any, significant differences in risks exist between the traditional model of clearing and settlement and the decentralized model? Please explain how these different risks could be mitigated.
21. What other risks could be associated with clearing and settlement models that are not identified here?
22. What regulatory requirements (summarized at Appendices B, C, and D), both at the CSA and IIROC level, should apply to Platforms or should be modified for Platforms? Please provide specific examples and the rationale.

APPENDIX B

Summary of Regulatory Requirements Applicable to Marketplaces

Marketplaces are subject to the Marketplace Rules and NI 23-103. These include high-level principles relating to access to the marketplaces and trading on the marketplaces. A summary of the regulatory requirements is included below. Please note that this summary should not be relied upon as being an exhaustive list of the requirements applicable to marketplaces.

1. Market integrity

The Marketplace Rules and NI 23-103 have a number of requirements covering market integrity. For example, NI 21-101 requires a marketplace to take reasonable steps to ensure it operates in a way that does not interfere with fair and orderly markets.³⁰ NI 23-101 and securities legislation in some jurisdictions also prohibit any person or company from engaging in transactions that they know, or should know, result in market manipulation or are fraudulent. NI 23-103 also has requirements for marketplaces aimed at maintaining market integrity. For example, marketplaces are required to assess, on a regular basis, whether they require risk management and supervisory controls, policies and procedures, in addition to those of their participants. Marketplaces are also required to assess on a regular basis the continuing adequacy and effectiveness of these controls, policies and procedures.³¹

While the Marketplace Rules and NI 23-103 establish the high-level principles for marketplaces that trade in Canada, the specific requirements applicable to participants on a marketplace are included in the UMIR, which are administered by IIROC.

2. Transparency of operations

Marketplaces are required to make transparent, on their websites, a description of how their orders are entered, interact and are executed, the hours of operation, their fees (including fees for facilitation, routing and mark-ups, if applicable), their affiliates' fees, access requirements, conflicts of interest policies and procedures, and referral arrangements between the marketplace and service providers.³² The purpose of these requirements is to ensure that market participants understand how the marketplace works, as well as the associated risks, its features and its fees.

3. Transparency of orders and trades

Except in certain circumstances, marketplaces must make transparent their order and trade information for securities traded on a marketplace by providing it to an information processor.³³ The information processor collects, consolidates and disseminates their data, and also sets the requirements for the order and trade information that must be provided to it by marketplaces.

³⁰ s. 5.7 of NI 21-101.

³¹ Part 4 of NI 23-103.

³² s. 10.1 of NI 21-101.

³³ Part 7 of NI 21-101 and Part 8 of NI 21-101 for equity and fixed income securities, respectively.

4. Transparency to regulators

Marketplaces are required to provide certain information to the securities regulators, so that they understand the business of the marketplace and the risks it introduces to the market. Such information is described in the exhibits included in Forms 21-101F1 *Information Statement Exchange or Quotation and Trade Reporting System* and 21-101F2 *Information Statement Alternative Trading System*, for exchanges and ATSS respectively, and relates to: governance, marketplace operations, outsourcing arrangements, systems, custody, the types of securities traded, how access to services is provided, and fees. These forms must be filed prior to the commencement of the operations and must be kept up to date. Changes to the information included in these forms must also be reported to the securities regulators, either in advance, if the change is significant, or subsequent to its implementation if it is not.

In addition, marketplaces report their trading activities on a quarterly basis.³⁴ The quarterly reports are provided to the securities regulators in electronic form. The information reported is included in Form 21-101F3 *Quarterly Report of Marketplace Activities* and includes trading activity information (value, volume and number of trades) by category of security, information about orders and order types, and information about the most traded securities.

5. Listing securities

Exchanges may list securities of an issuer.³⁵ They are required to comply with the fair access requirements in NI 21-101 (and in their recognition orders), which include the requirement to establish written standards for granting access to each of their services,³⁶ including listings. Since exchanges have listings requirements in the form of rules, they must ensure that these rules require compliance with securities legislation³⁷ and that they provide appropriate sanctions for violations of the rules.³⁸

6. Fair access

Marketplaces must not unreasonably prohibit or limit access by a person or company to services offered by the marketplace. A marketplace must establish written standards for granting access to each of its services and must keep records of each access grant or denial of access.³⁹ It must neither permit unreasonable discrimination among participants, issuers and marketplace participants nor impose any burden on competition that is not reasonably necessary and appropriate.⁴⁰ Lastly, a marketplace must not prohibit, condition or otherwise limit a marketplace participant from trading on any marketplace.⁴¹

7. Conflict of interest

A marketplace must establish, maintain and ensure compliance with policies and procedures that identify and manage any conflicts of interest arising from the operation of a marketplace or the

³⁴ Part 3 of NI 21-101.

³⁵ An issuer is listed when there is a formal arrangement between the exchange and the issuer to have the issuer's securities listed, and the exchange has and enforces listing requirements.

³⁶ para. 5.1(2)(a) of NI 21-101.

³⁷ para. 5.3(b) of NI 21-101.

³⁸ para. 5.4(b) of NI 21-101.

³⁹ s. 5.1 of NI 21-101.

⁴⁰ ss. 5.1(3) of NI 21-101.

⁴¹ s. 5.1 of NI 21-101.

services it provides, and any conflicts that owners of the marketplace may have.⁴² These policies must be disclosed on the marketplace's website.

8. Outsourcing

A marketplace that outsources key services or systems to a service provider must have policies and procedures relating to the selection of the service provider, must maintain access to the books and records of the service provider, must ensure that the securities regulatory authorities have access to data that is maintained at the service provider and must review, on a regular basis, the performance of the service provider.⁴³ The outsourcing requirements seek to ensure that the marketplace retains responsibility and control over the outsourced services or systems.⁴⁴

9. Confidential treatment of trading information

A marketplace must not release the order or trade information of any of its participants. This requirement protects each marketplace participant's trading history and strategy. There is an exception to this requirement in limited situations, where data is used for capital markets research and provided certain conditions are met.⁴⁵

10. Recordkeeping requirements

Marketplaces are required to keep books, records and other documents that are reasonably necessary for the proper recording of its business in electronic form.⁴⁶

11. Systems and business continuity planning

Marketplaces are required to have adequate internal and information technology controls over their trading, surveillance and clearing systems and information security controls that relate to security threats and cyber attacks. A marketplace is also required to maintain business continuity and disaster recovery plans. A marketplace is required to develop, maintain and test a business continuity plan to ensure uninterrupted provision of key services. A marketplace is required to engage a qualified third party to conduct an independent system review to assess whether it has adequate internal and information technology controls and if they function as designed.⁴⁷

12. Clearing and settlement

All trades executed on a marketplace must be reported and settled through a clearing agency.⁴⁸ Marketplace participants have a choice as to the clearing agency that they would like to use for the clearing and settlement of their trades, provided that the clearing agency is appropriately regulated in Canada.

⁴² s. 5.11 of NI 21-101.

⁴³ s. 5.12 of NI 21-101.

⁴⁴ Ibid.

⁴⁵ s. 5.10 of NI 21-101.

⁴⁶ Part 11 of NI 21-101.

⁴⁷ Part 12 of NI 21-101.

⁴⁸ Part 13 of NI 21-101.

APPENDIX C

Summary of Regulatory Requirements Applicable to Dealers

Registration is required if a person or company is in the business of or is holding itself out as being in the business of, trading securities. We have generally found Platforms that intermediate trades of securities between buyers and sellers to be “in the business” of trading securities and subject to the registration requirements set out in National Instrument 31-103 *Registration Requirements, Exemptions and Ongoing Registrant Obligations*, and, where applicable, IIROC Dealer Member Rules and UMIR.

Although the details of the specific requirements applicable to different categories of dealers vary, the summary below captures the basic requirements applicable to a dealer. Please note that this summary should not be relied upon as an exhaustive list of the requirements applicable to dealers.

1. Proficiency

Dealers are in the business of buying and selling securities and derivatives on behalf of the clients and are implicitly or explicitly holding themselves out as having a certain level of knowledge or expertise. Accordingly, individuals registered as dealing representatives are expected to have the education, training and experience that a reasonable person would consider necessary to perform their activities competently, including understanding the structure, features and risks of each security the individual recommends.⁴⁹

Similarly, firms are required to employ individuals as ultimate designated persons (**UDP**) and chief compliance officers (**CCO**) who meet certain additional educational and experience requirements and who will have responsibilities respecting promoting compliance with securities legislation and establishing and monitoring policies and procedures designed to assess compliance by the firm and its dealing representatives with securities legislation.⁵⁰

2. Books and records

Dealers may hold the assets of and conduct transactions on behalf of a multitude of clients. Accordingly, it is important that they maintain books and records that accurately reflect their business activities, financial affairs and client transactions. These books and records requirements help dealers ensure that they are able to prepare and file financial information, determine their capital adequacy, and generally demonstrate compliance with the capital and insurance requirements, among other securities law requirements.⁵¹ Maintaining proper books and records allows dealers to document information about their relationships with their clients and with other entities, as well as, to report to their clients the trades they have transacted on behalf of their clients.⁵²

3. Compliance system

⁴⁹ The proficiency requirements for registered individuals at investment dealers are set out in IIROC Dealer Member Rule 2900 *Proficiency and Education*. The requirements for registered individuals at dealers other than investment dealers are included in Part 3 of NI 31-103.

⁵⁰ s. 11.2 and 11.3 of NI 31-103, respectively.

⁵¹ s. 11.5 of NI 31-103.

⁵² s. 14.12 and 14.14 of NI 31-103.

Given the significant role registered dealers play vis-à-vis their clients and to the capital markets, dealers are required to establish, maintain and apply policies and procedures that establish a system of controls and supervision sufficient to provide reasonable assurance that the firm and each individual acting on its behalf complies with securities legislation and to manage the risks associated with its business in accordance with prudent business practices.⁵³ An effective compliance system includes internal controls and day-to-day monitoring and supervision elements that are appropriately documented. These elements are intended to ensure the integrity of the practices of the dealer, as well as the appropriate segregation of key duties and functions, and includes employee proficiency and training.

As part of a compliance system, a registered firm must appoint both a CCO and an UDP. The CCO is responsible for monitoring, updating and reviewing policies and procedures a registered firm must have as part of its compliance system. The UDP promotes compliance with securities legislation and sets the tone for firm-wide compliance. Investment dealers are also required to appoint a Chief Financial Officer.

4. Financial condition and required capital

Dealers may have access to the assets of a multitude of clients and the insolvency of a dealer could have serious implications for clients and confidence in the capital markets. Accordingly, firms are subject to ongoing financial requirements.⁵⁴

Registered firms are required to calculate regulatory capital to ensure that it is not less than zero. The minimum capital for an exempt market dealer and a restricted dealer is \$50,000 (unless an alternative minimum is imposed). Investment dealers are required to maintain risk adjusted capital, calculated in accordance with IIROC requirements, that is greater than zero.⁵⁵

5. Insurance

Similarly, because of the significance of the financial condition of registered dealers to their clients and the capital markets, registered dealers must also maintain bonding or insurance that contains certain specific clauses and coverage. The amount of insurance coverage depends on the category of dealer involved.⁵⁶

6. Financial reporting

Securities regulators monitor the financial condition of registered firms by requiring them to prepare and deliver to regulators annual and interim financial information, and to abide by requirements in IIROC Dealer Member Rule 16 *Dealer Members' Auditors and Financial Reporting*.

7. KYC and suitability

⁵³ s. 11.1 of NI 31-103.

⁵⁴ The financial requirements for investment dealers are found in IIROC Dealer Member Rule 17 *Dealer Member Minimum Capital, Conduct of Business and Insurance* and Form 1. The financial requirements for dealers other than investment dealers are in s. 12.1 of NI 31-103.

⁵⁵ Part 12, Division 1 of NI 31-103.

⁵⁶ The insurance requirements for dealers other than investment dealers are included in s. 12.3 of NI 31-103. The insurance requirements for investment dealers are in IIROC Rule 400 *Insurance*.

Know-your-client and suitability obligations require dealers to collect information to establish the identity of their clients, to understand their investment needs and objectives, overall financial circumstances, and risk tolerance and to then take reasonable steps to use that information to ensure a proposed transaction is suitable to the client. In order to make that suitability assessment, the dealer also needs to understand the features and risks of the security or derivative to be transacted (the know-your-product requirement).⁵⁷ In addition, dealers also have separate, specific obligations under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* and the associated regulations, including the requirement to verify the identity of clients for certain activities and transactions.

8. Conflicts of interest

Dealers are faced with many potential conflicts of interest between their and their clients' interests. Accordingly, securities legislation requires that a dealer take reasonable steps to identify conflicts of interests that exist and may exist between itself and its clients. Among other requirements, a dealer must identify conflicts of interest that should be avoided and respond appropriately to other conflicts of interest given the level of risk each conflict raises (e.g. through control and/or disclosure of the conflict of interest).⁵⁸

9. Custody

As dealers may have access to clients' assets, there are a number of requirements and prohibitions regarding custody of client cash and securities. Investment dealers, as IIROC members, must comply with the custodial requirements of IIROC.⁵⁹ Depending on the location where such assets are held, investment dealers may have to provide additional capital to reflect increased risk.⁶⁰ Exempt market dealers must comply with the requirements regarding holding client cash and securities set out in NI 31-103 which prohibits them from holding client assets and acting as custodians themselves.⁶¹ Instead, client assets of exempt market dealers are normally held by a custodian that is a separate legal entity.

10. Best execution and fair pricing

Investment dealers are required to establish, maintain and follow written policies and procedures that are reasonably designed to achieve best execution when acting for a client.⁶² What constitutes "best execution" varies depending on the particular circumstances and, for transactions that are executed over the counter, such as transactions in fixed income securities, the expectation is that dealers have policies and procedures to ensure that prices to their clients for these securities are fair and reasonable, both for the pricing of principal transactions and for commissions that may be charged by the dealer.

11. Handling Complaints

⁵⁷ The suitability requirements for dealers other than investment dealers are included in Part 13 of NI 31-103. The requirements for investment dealers are in IIROC Rule 1300 *Supervision of Accounts*.

⁵⁸ s. 13.4 of NI 31-103.

⁵⁹ IIROC Dealer Member Rule 2000 *Segregation Requirements*, Dealer Member Rule 17 *Dealer Member Minimum Capital, Conduct of Business and Insurance* and Dealer Member Rule 2600 *Internal Control Policy Statements*.

⁶⁰ IIROC Form 1 General Notes and Definitions, (d) "acceptable securities locations".

⁶¹ s. 14.5.2 of NI 31-103.

⁶² IIROC Dealer Member Rule 3300 *Best Execution of Client Orders*.

Dealers are required to document complaints and to effectively and fairly respond to them. These procedures should include monitoring of complaints, to allow the detection of frequent and repetitive complaints made with respect to the same matter, which may, on a cumulative basis, indicate a serious problem. Registered firms are required to be a member of the Ombudsman for Banking Services and Investments,⁶³ except in Québec where the dispute resolution service is administered by the Autorité des marchés financiers.

⁶³ Part 13, Division 5 of NI 31-103.
#5450795

APPENDIX D

Requirements Applicable to Clearing Agencies

A clearing agency is defined in securities legislation as a person or company that, among other activities, provides centralized facilities for clearing and settlement of transactions in securities or, in some jurisdictions, derivatives.

National Instrument 24-102 *Clearing Agency Requirements* (NI 24-102) sets out certain requirements in connection with the application process for recognition as a clearing agency or exemption from the recognition requirement. Please note that this summary should not be relied upon as being an exhaustive list of the requirements applicable to clearing agencies.

NI 24-102 also sets out the ongoing requirements applicable to recognized clearing agencies. This includes the requirement to meet or exceed applicable principles as set up in the April 2012 report *Principles for financial market infrastructures* published by the Committee on Payments and Market Infrastructure and the International Organization of Securities Commissions (PFMI). The PFMI cover all areas associated with activities carried out by a clearing agency: systemic risk, legal risk, credit risk, liquidity risk, general business risk, custody and investment risk and operational risk. Clearing agencies are required to:

- have appropriate rules and procedures on how transactions are cleared and settled, including when settlement is final;
- minimize and control their credit and liquidity risks;
- have rules that clearly state their obligations with respect to the delivery of securities traded; and
- identify, monitor and manage the risks and costs associated with the delivery of crypto assets, including the risk of loss of these crypto assets.

INCLUDES COMMENT LETTERS

**THROUGH A DIGITAL GLASS DARKLY:
CRYPTOCURRENCIES AND THE REGULATORY CHALLENGE**

*Allan C. Hutchinson**

As a social process that places great stock in its stability and predictability, law does not deal as easily or as well with change as it might wish. In a modern world that is in a constant and extensive state of flux, law is being placed under considerable stress in its efforts to fulfill its task as a primary regulator of social and economic behaviour. This challenge is particularly acute in the realm of technology and its profound ramifications for social and economic behaviour. The innovative Techno-Age not only offers fresh ways of handling old problems, but also throws up entirely new problems; traditional ways of thinking about and responding to these old and new problems and their optimal resolution are no longer as tenable as many once thought. One such example is the burgeoning world of cryptocurrencies – this peer-to-peer digital network presents a profound challenge to the status quo of the financial services sector, to the established mode of state-backed fiat currency, and to the regulatory authority and reach of law. Taken together, these related challenges demand the urgent attention of jurists, lawyers and law reformers. It is the future and relevance of legal regulation as much as cryptocurrency that is at stake.

In this article, I want to propose an approach to regulating cryptocurrency that recognises and retains its innovative and transformative potential, but also identifies and deals with some of its less appealing qualities and implications. In so many ways, the term ‘cryptocurrency’ is misleading, especially from a legal and definitional point of view. By characterizing itself as a currency, it begs the very question that needs to be answered – what is the nature of cryptocurrency and, as such, how should it be regulated, if at all? I maintain that cryptocurrency is sufficiently special and different in its dynamics and character that it warrants a regulatory approach that is equally special and different in approach and implementation. Although secondary aspects of cryptocurrency’s workings and structure lend themselves to similar and selective regulation to currencies, commodities or securities, the primary ambit and operation of cryptocurrency deserves its own *sui generis* regulation. So, rather than be content with canvassing possibilities, I will plumb for a particular style, scheme and substance of regulation. This is a tall order, but it is necessitated by both the unique challenges and opportunities that cryptocurrency and its enabling blockchain technology present.

This article has four main parts. In the first part of the article, I sketch the beginnings of cryptocurrency, the forces that gave rise to it, the working of this technological innovation, and the challenges it now faces. The second part looks to the regulatory challenge more generally by considering the tools available, the normative ends of regulatory schemes, and the fit of different regulatory initiatives with different activities. In the third part, I explore the different categories of existing regulatory schemes – property, securities, currency and commodities -- that might be relied upon to deal with cryptocurrency. The fourth part works towards suggesting a regulatory

* Distinguished Research Professor, Osgoode Hall Law School, York University, Toronto, Canada. I am grateful to Peter Blaha, Joshua Harriott, Dale Lastman, Jennifer Leitch, Taylor Trottier, **, and other friends and colleagues for critical assistance and intellectual support.

approach that respects and enhances the essential character of cryptocurrency, but also wrestles with its shortcomings as a more general and transformative mode of digital trading. Throughout the article, my overriding and constructive ambition is to grapple with and confront the basic challenge of any regulatory scheme -- to regulate something in such a way that, after regulation, that something is essentially the same and better than it was rather than having it become something different and worse.

A. GOING SECRET

1. Banking on It

Trade and commerce are as old as civilisation itself. The need to exchange goods and services is a continuing and vital social feature. However, influenced by innovators and entrepreneurs, how this has been done has changed significantly and frequently over the centuries. Bartering was once the most common forms of commerce. However, the idea and practice of utilising ‘money’ as a medium of exchange recommended itself as a convenient and reliable system that could overcome the inefficiencies and limitations of a bartering system; it would serve to broaden, deepen and diversify trading practices.¹ At first, there was commodity money (e.g., salt), but this soon gave way to the issuance of representative or paper money. Whether state-backed or not, the overall function of such money is to provide a commodity that can be saved and held with confidence, whose value will remain stable, and that it can be retrieved when needed and used as a reliable medium of exchange. After a long run, the almost exclusive reliance on paper money is now under threat by the rise of digital money or cryptocurrencies.

As representative or paper money became the convenient currency of commerce, the first banks began to appear. Indeed, modern banking still resembles the early institutions of the Medici family in 15th Century Florence. Their role was to act as a trusted intermediary between buyer and seller by facilitating trade and sharing the risks that are inherent in the use of money as a unit of account, a repository of value, and a medium of exchange. In performing that task, banks (and other financial institutions) have themselves become lucrative and powerful trading bodies; they make money on handling other people’s money. The core business of banks is to hold accounts for customers, facilitate the uses of that account for payments and deposits, and to extend credit to borrowers. As well as user fees, banks make money on the difference between loan/credit interest charged and deposit/account interest paid by borrowers. As the old joke goes, bankers were happy if they could follow the 3-6-3 rule – interest paid at 3% on money deposited, interest earned at 6% on money lent, and on the golf-course at 3:00. Although they have now branched out and their activities are more diverse and widespread, the basic institutional logic remains much the same.

At the heart of the bank’s power is their valued and valuable activity of creating and validating a ledger that keeps a trustworthy record of all transactions so that double-spending (i.e., that people would use the same resources or money more than once to buy goods or services) and other fraudulent and dubious practices were avoided. Most importantly, although originating as

¹ NOBLE HOGGSON, *BANKING THROUGH THE AGES* (1926) and FREDERIC MISHKIN, *THE ECONOMICS OF MONEY, BANKING, AND FINANCIAL MATTERS* (2007).

trusted facilitators and guaranteed ledger-keepers of trade and commerce, a bank-centric approach to financial services has become both a major drain on the economy and financial transactions generally and a de-stabilizing institutional force. The convoluted and costly nature of this intermediary role is considerable. With sometimes 5 or 6 intermediate dealers between buyer and seller, the banking system adds up to 8% to all transactions made and it takes up to a week to clear and settle most transactions. Indeed, the payment card industry (e.g., Visa, Mastercard, and Diners Club) processes about \$20 trillion in volume and generates almost \$300 billion in fees each year.

Although there remains a crucial role for banks and bank-like institutions, those institutions have developed and grown to such an extent that they threaten the original basis for their existence -- to facilitate efficient exchange and provide trusted security in handling money. Apart from a continuing history of bank failures and collapses,² financial institutions and banks have become self-serving entities who any real lack of transparency and utilize informational asymmetry to their advantage. Indeed, banks foster and benefit from the false idea that they are not simply one more economic corporate entity, but that they occupy a special and semi-public role that sets them aside from the usual profit-making priorities of other market actors. In short, the whole financial services industry tends to serve its own as much as the public's interests. Although they have turned to technology and e-commerce to perform their roles, they have not embraced more fully the possibilities of a truly digital and transformed style of banking. As such, the rise of cryptocurrencies is not only a response to the dominating role of banks (and governments), but also presents a genuine threat to the centralising role of banks in the burgeoning world of trade and commerce.

2. Blocking Efforts

Imagine a way of transacting one's life and business in which everyone that you dealt with was part of the same bank. All the people that you deal with are account-holders of that same bank; this will reduce a number of risks and costs that presently weigh upon your capacity to act speedily, safely and cheaply in making payments for goods and services. But not only that, imagine that you and all the other account-holders were also the exclusive managers and owners of the bank; there was no middleperson to orchestrate or benefit from your efforts. Moreover, imagine that there is the added attraction of being able to be both account-holder and manager in a largely confidential and semi- or pseudo-anonymous manner; other account-holders that you transact with would not be able to know your business or spending habits (or you theirs). This arrangement would mean that many issues of trust could be handled better, risks could be more contained, and costs could be further reduced.

² For example, between 2008 and 2012 alone, over 450 U.S. banks failed. See K. CONNORS, *THE HISTORY OF BANKING: THE HISTORY OF BANKING AND HOW THE WORLD OF FINANCE BECAME WHAT IT IS TODAY* (2017) and ANDREW ROSS SORKIN, *TOO BIG TO FAIL: THE INSIDE STORY OF HOW WALL STREET AND WASHINGTON FOUGHT TO SAVE THE FINANCIAL SYSTEM--AND THEMSELVES* (2010).

This scenario is one way to think about cryptocurrencies. They came into being on 3rd January, 2009 under the genius and guidance of the fabled Satoshi Nakamoto. He or she (or perhaps they, as Nakamoto's identity remains unknown) set out to develop a scheme that was intended to be an entirely borderless, decentralised, unmediated (without banks), pseudo-anonymous, self-regulating and politically-neutral medium. In particular, it needed to be capable of solving the double-spending problem that made the existence of ledger-maintaining banks desirable. This originally involved the still-dominant mode of cryptocurrency entitled 'Bitcoin'. In the intervening decade or so, there have been more than 1000 different types of cryptocurrency created and put into use. Over half of them are still trading actively on unregulated or registered exchanges. At present, there are approximately 17.5 million bitcoins in circulation. While it initially traded at approximately US\$0.003 per bitcoin, it is currently valued at approximately US\$3800, with a market capitalization of over US\$67 Billion.

At its most basic, therefore, cryptocurrency is a self-contained and decentralised system that allows for peer-to-peer transactions in a digital space that is free from outside control, safe from exploitive meddling, and is unrestricted by national borders. Anyone can join by downloading the free software and becoming part of the process; there are presently millions of computer-users in 90 or so jurisdictions. Because it does not have an underlying or anchoring asset, its price is determined purely by the supply and demand for bitcoins. The appeal of such a system of transacting and banking is obvious to people of very different backgrounds (both poor and rich) and with very different interests for doing so (both legal and illegal).³ The challenge is to devise a cryptocurrency process that operates in a secure, inexpensive, confidential and dependable way. In short, that it will work better than the existing banking system

Nakamoto offered "a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions."⁴ What does this mean for the ordinary person? The task was to generate a system that cut out the role of the middle-person by replacing institutions, like banks and credit card distributors, with a process whereby a universal ledger was established and validated by individual users who would be incentivised to maintain, run and authenticate the system through their own computers. People would transact using bitcoins; these are digital markers. They are held in a personal e-wallet on a computer that is encrypted and can only be opened by the owner through a private key or password. These bitcoins can be used in much the same way as any currency to buy and sell products and services from other bitcoin users. In that sense, the bitcoin cryptocurrency is a closed and consensus-based digital system in that is only usable by and through other members on the system. Of course, as the number of bitcoin users increases, so will the utility and reach of the system. Today, there are over four million bitcoin users globally with over 20 million e-wallets between them; over 20,000 transactions are made daily. However, the combined total of their crypto-holdings account for only about 3% of the combined assets of the world's leading central banks.

³ The best and most accessible account of the workings of bitcoin and blockchain is PAUL VIGNA AND MICHAEL CASEY, *THE AGE OF CRYPTOCURRENCY: HOW BIT COIN AND THE BLOCKCHAIN ARE CHALLENGING THE GLOBAL ECONOMIC ORDER* (2016). See also ARVIND NARAYANAN ET AL., *BITCOIN AND CRYPTOCURRENCY TECHNOLOGIES: A COMPREHENSIVE INTRODUCTION* (2016) and CRAIG K. EWELL ET AL., CONG. RESEARCH SERV., R43339, *BITCOIN: QUESTIONS, ANSWERS, AND ANALYSIS OF LEGAL ISSUES 1* (2015).

⁴ Satoshi Nakamoto, [Bitcoin: A Peer-to-Peer Electronic Cash System](https://bitcoin.org/bitcoin.pdf), <https://bitcoin.org/bitcoin.pdf>.

The whole process of cryptocurrency is contained within a software program that keeps a corroborated and immutable record of all transactions made -- blockchain.⁵ Every time someone enters a new transaction and pays by or is paid with bitcoin, that transaction is checked and measured against all the existing transactions ever made with bitcoin. It is only then that the transaction can be recorded and e-stamped as being unique and, therefore, legitimate. This process takes a few minutes (as compared to the week or so that it takes banks to clear and settle transactions). Because there is no central server or controlling third-party, this distributed process allows all users to be involved in and, therefore, responsible for guaranteeing that each and every transaction that has ever occurred is unrepeated: the blockchain can only be added to, not revised retroactively. If one or series of computers are compromised, there are still large numbers of users with a complete record.⁶ Further, all transactions are open to view, but only by way of the encrypted and pseudonymous e-addresses of users. This overcomes the double-spend problem, ensures the trusted integrity of the overall system, reduces payments to third-party intermediaries, and preserves users' confidentiality.

However, there are, at least, two particular challenges with this cryptocurrency process – who controls the supply of bitcoins? And how are users incentivised to do the necessary authenticating work? Nakamoto had the ingenious idea of linking these two issues together. When the first bitcoin was released in January 2009, a secured stash of 21 million bitcoins was also created. The stash was programmed to be released over a 130-year span. This release is scaled so that the amount of bitcoin made available in each block was reduced to 25 per 10 minutes after 2012 and then halved every four years after that. This means that the total supply of the 21 million bitcoins will not be exhausted until 2140. Also, bitcoins are divisible into smaller units known as *satoshis*; each satoshi is worth 0.00000001 (10^{-8}). As well as providing incentives for security and performance, this arrangement also ensures that the value of bitcoins is not vulnerable (at least within the digital universe)⁷ to devaluation by unanticipated releases of more bitcoins or by intervening governmental and corporate policies. Secondly, in order to earn bitcoins, users or 'miners' have to do the essential work of confirming the legitimacy of existing bitcoin transactions as they happen by solving randomly-generated and complex mathematical problems. If successful, these miners are rewarded by obtaining a block of the 50 coins that are released every 10 minutes; they can also charge an optional fee (as low as 0.00001 bitcoin).

An unfortunate side-effect of this is that 'mining' has become a far from simple or cheap activity. Indeed, it has been deliberately made mathematically more difficult as the regular supply

⁵ For an expansive look at the broader potential of blockchain technology, see DON TAPSCOTT AND ALEX TAPSCOTT, *BLOCKCHAIN REVOLUTION: HOW THE TECHNOLOGY BEHIND BITCOIN IS CHANGING MONEY, BUSINESS, AND THE WORLD* (2016). For example, it is now being used by some American states as part of their election process. See Coingeek, [Denver to apply blockchain technology in upcoming elections](https://coingeek.com/denver-to-apply-blockchain-technology-in-upcoming-elections/), <https://coingeek.com/denver-to-apply-blockchain-technology-in-upcoming-elections/> (March, 2019).

⁶ There is the problem of the so-called 51% attack. This when a group might ambush the network by commandeering over half the computer network, take control and approve illegitimate transactions. This is becoming increasingly expensive and is now likely prohibitive so at about \$1.5 billion. See Osato Avan-Nomayo, [Bitcoin 51% Attack is Unrealistic](https://bitcoinist.com/bitcoin-51-percent-attack-study/), <https://bitcoinist.com/bitcoin-51-percent-attack-study/>.

⁷ There is, of course, the vulnerability of the boom-and-bust cycle of bitcoin valuation in terms of traditional fiat currencies. See *infra* pp. **-**.

of bitcoins reduces. As well as attracting a techno-geek clientele that has access to sophisticated and expensive computers, the search for bitcoins requires a huge investment in electrical resources to be done properly. This has had a couple of very significant effects. First, big business has become involved in mining and begun to squeeze out the small and local enthusiasts who were in on the ground-floor of the cryptocurrency start-up; as few as 10 groups or so now dominate mining. This development has changed the overall thrust of the cryptocurrency market and turned it into as much a vehicle for investment or speculation as an alternative mode of banking and transacting. Secondly, in order to facilitate the use of cryptocurrencies as an investment tool and to allow the less technically-sophisticated to enter the cryptocurrency sector, a secondary market has developed in which bitcoin can be exchanged for traditional fiat currency. There now exist a variety of sites and institutions, like that Bitstamp, Binance and Kraken, that work as cryptocurrency exchanges. This turn of events has not only largely transformed how cryptocurrencies are viewed and used, but also has created a new set of problems and challenges for those who maintain that regulation is demanded.

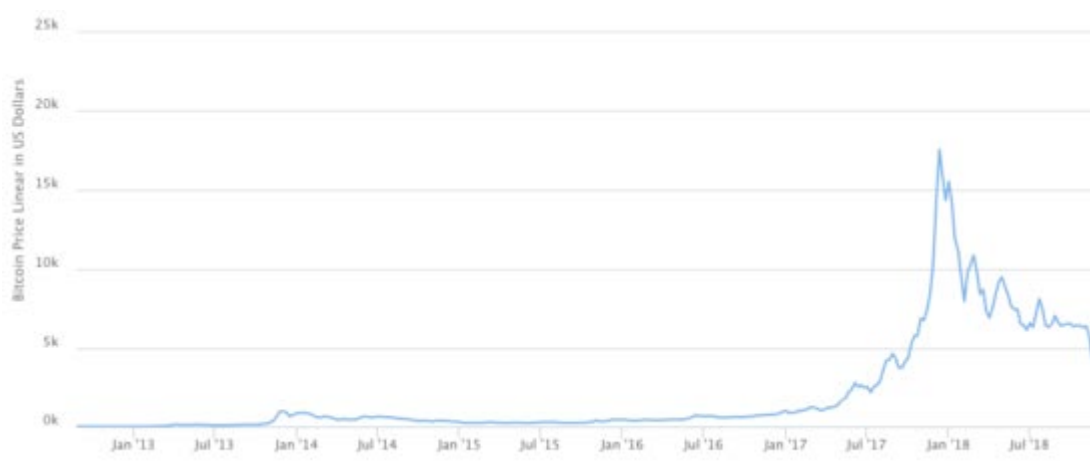
Bitcoin is the dominant, but by no means only mode of cryptocurrency. There are over 1000 different kinds of cryptocurrency that can be acquired and traded. Utilised for a variety of purposes and with varying degrees of technological similarities to bitcoin, they tend to be closed or permissioned schemes that require certified membership to participate and that are overseen by the controlling entity; Paypal is an example. In the past few years, these Initial Coin Offerings (ICOs) have generated more than \$4 billion in revenue. Although they are an adjunct to cryptocurrency rather than an integral part of it, these sites are the public and often troubled face of cryptocurrency. Moreover, these sites have become the profitable intermediaries that cryptocurrency was intended to challenge and do away with.

3. Booming and Busting

One of the major bones of contention about cryptocurrency is that it is perceived by a number of respected commentators and critics as a fad or flash in the pan. While it has a certain innovative and trendy appeal, it is condemned because, in failing to respect the cautionary logic of basic economics, it will soon fall victim to its own surreal success. In more technical terms, it is seen as a hyper-mode of speculative investing in an untethered asset or commodity that has no state-backing; the basic bitcoin has no intrinsic value to anchor it in reality so its over-inflated pricing is a boom waiting to go bust if and when its users' confidence wobbles or wanes. As such, it is very vulnerable to a 'pumps and dumps' cycle of valuation. In many ways, therefore, crypto-sceptics predict that the cryptocurrency market will end in tears and trouble like The Dutch Tulip Mania of 1634-37, the British South Sea Bubble of 1720 or even Bernie Madoff's Ponzi scheme of 2008.⁸ There is some basis for these claims in that the price of bitcoin raced to a high of \$19,783 in December 2017 and then proceeded to crash to \$3,756 a year later; it is a much more volatile entity than gold, fiat currency or most stocks and shares. However, for all the dooms-saying, there is, as it were, another side to the coin.

⁸ Nouriel Roubini, Blockchain Isn't About Democracy and Decentralisation, <https://www.theguardian.com/technology/2018/oct/15/blockchain-democracy-decentralisation-bitcoin-price-cryptocurrencies> and Paul Krugman, Transactions Costs and Tethers: Why I'm a Crypto-Sceptic, <https://www.nytimes.com/2018/07/31/opinion/transaction-costs-and-tethers-why-im-a-crypto-skeptic.html>.

Despite its admitted volatility as a partial result of its more than 200-times smaller market than global stock markets (\$300 billion to \$75 trillion), cryptocurrencies have not been the disastrous investment that some have forecast. The collapse that many have predicted has not happened, at least for now. Despite the boom-and-bust effects of 2018, the value of bitcoin has tended to stabilise to a more modest, if still high price in the mid-\$3,500. This price is not to be scoffed at. Anyone who invested in 2009 would be still benefitting enormously from a very high rate of return on their investment today, even if they did not reap the extravagant rewards of late 2018. Most revealingly, on an average basis, someone who invested in bitcoin in the last few years would still be doing much better than someone who invested in the stock market; they would have increased their initial investment thousands-fold.



Bitcoin price since 2009 to 2018. The historical chart shows the changes of price of Bitcoin (BTC).

No one is pretending that cryptocurrency does not come with its own share of perils and pitfalls. It would a naïve and foolish investor who did not invest in bitcoin without a strong sense of anticipated adventure that could offer great losses as well as great rewards; the higher the possible rewards, the greater the actual risk. It is ironic, in light of cryptocurrency's anti-establishment posture, to expect government to protect such speculators in this off-the-grid region. That said, the problem with all this for defenders of cryptocurrency is that it was never intended to be one more vehicle for high-risk speculation; the basic idea of cryptocurrency in its purer Nakamoto-form was to be an alternative mode of doing business that did not rely on fiat currency and banks. At its inception in 2009, there was no sense or expectation that it would become a speculative vehicle for investing: it was about finding a truly trustworthy and unmediated medium that did not have the very problematic history of banks, central and otherwise.⁹ Indeed, insofar as bitcoin became a target for wealthy investors, it seemed to be exactly the kind of traditional financial wheeling-and-dealing that cryptocurrency was intended to abandon and set itself apart

⁹ See Satoshi Nakamoto, [Bitcoin Open Source Implementation](http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source), <http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source> (February, 2009).

from. In other words, the primary function of cryptocurrency as a medium of exchange has been supplemented, if not supplanted by its secondary use as an investment vehicle.

This distinction between primary and secondary markets in cryptocurrencies is hugely significant in thinking about law and regulation. Whereas the primary market of cryptocurrency exchange is separate and apart from the traditional financial markets, the secondary market is more fully a part of it. Transactions that occur through and on blockchain are to the side of traditional markets in terms of the self-selected participants involved, the contained purposes for which cryptocurrency can be used, and the internal process utilized for recording transactions. Governed by consensus and encrypted security, cryptocurrency is an alternative to, not an adjunct of the traditional market. However, the secondary market – coin exchanges, ICOs, and other related trading activities – is intended to function as a limb of the traditional market that facilitates interactions between cryptocurrencies and fiat currencies. Inside cryptocurrency, bitcoin rules. But, on the edges of the traditional market, the dollar rules.

B. THE REGULATORY CHALLENGE

1. Beyond The Technical

Regulation comes in many shapes and sizes. Society is constructed and constituted by the different modes of regulation that are adopted or in place. These can span a broad spectrum from criminalisation and command-and-control laws through delegated authority and market competition to self-regulation and tax incentivization. Indeed, there has been a general move away from the traditional command-and-control model to less coercive and more cooperative types of regulation. Of course, there is no one tried-and-trusted formula by which to determine what kind of regulation best suits what kind of activity. The prevailing rationales are seen to be about correcting for market failures and power caused by informational asymmetries, lack of competition, interest group capture, and the like; the goal is treated as being the need to create regulatory processes that encourage transparency, efficiency, confidence, and accountability.¹⁰ However, these choices of appropriate tacks and tools are not simply technical matters or considerations; they involve formative values and bigger choices that raise matters of deeper normative commitments.

As such, it is a mistake to view regulation as being the exclusive domain of technicians and bureaucrats. For example, centralized regulatory devices or decentralized ones are not to be considered as ends in themselves, but as means to achieve larger and more encompassing objectives. Nor is it simply a matter of calibrating regulatory responses in terms of market efficiency; this already builds upon a hidden and set of normative values and assumptions: it assumes that an efficient market is self-evidently the gold-standard of regulatory schemes. The choice of regulatory design or instruments, therefore, is framed by broader and more contested issues that go to the heart of the civil compact — who should be responsible for ordering social

¹⁰ See, for example, ROBERT BALDWIN AND MARTIN CAVE, UNDERSTANDING REGULATION: THEORY, STRATEGY, AND PRACTICE ch.4 (1999); John Braithwaite, Rewards and Regulation, 29 J.L. & SOC'Y 12 (2002); and I.A. MOOSA, GOOD REGULATION, BAD REGULATION (2015).

practices?; who needs to be protected and from whom?; what kind of society do we want to move away from and towards?; and how are we going to get that done? At bottom, the choice of regulatory processes, organisations and tools is a matter of politic engagement and ideological alignment.

In light of these considerations, it would be wrong to begin with the notion, as many do, that cryptocurrencies are presently unregulated. While there is no outside or independent regulatory bodies over cryptocurrency that claim to be acting in the broader public interest, a more accurate description would be to say that cryptocurrency is self-regulated through its blockchain code. This is the so-called *lex cryptographica*.¹¹ Although this is a mode of regulation, it is not a public or governmental set of intervening rules that require or only incentivise cryptocurrency to act in certain ways. It consists of the code and protocols that comprise the network itself. By necessity, these software designs determine the nature of people's interaction within the network by channeling and constraining what can and cannot be done and how it can be done; there is no network without a code to realize and sustain it. As such, the technology of blockchain is a kind of regulation. In the same way that, there is no game of chess without the rules of chess, there is no cryptocurrency without the architectural imperatives of blockchain technology.

If there is to be a move away from this self-regulated world of cryptocurrency (as with any other self-regulated activity), there is a range of questions and challenges that must be addressed:¹²

- *Context* – What are the existing conditions and parameters of the activity to be regulated that might recommend or constrain the nature and type of regulation to be introduced?;
- *Stakeholders* – What are the identities and competing interests of the various actors that participate in the activity to be regulated?;
- *Objectives* -- What is the need for and purpose of interventions from a social, economic and/or political perspective?; and
- *Tools* – What modes of intervention are available and likely to be effective in addressing the behavior to be regulated?

These challenges do not recommend or lend themselves to easy answers. However, they do offer a framework for thinking about and organising an appropriate scheme of regulation. Any scheme of regulation that is to have any chance of success must be able to confront and have responses to them.

¹¹ See PRIMAVERA DE FILIPPI AND AARON WRIGHT, BLOCKCHAIN AND THE LAW: THE RULE OF CODE 32 (2018) and LAWRENCE LESSIG, CODE: VERSION 2.0 (2006). Whether this amounts to 'law' is, of course, an open question. For an introduction to the perennial preoccupation of jurists and legal theorists with these definitional challenges, see H.L.A. Hart, *Definition and Theory in Jurisprudence*, 70 L.Q.R.. 37 (1954) and Allan Hutchinson, *Coming Home (Again): A Jurisprudential Exploration* 1 SORBONNE L.J. 56-84 (2018)

¹² I have relied upon and modified the ideas in ALBERTO ASQUER, REGULATION OF INFRASTRUCTURE AND UTILITIES 31-32 (2018).

Accordingly, any effort to design a useful, fair and responsible process of regulation for cryptocurrencies must begin by taking a stand on the broader political matters that underpin both cryptocurrency and regulation generally. It is only when that is done by way of preface that the proposed nuts and bolts of regulation can be taken seriously. No scheme of regulation (including self-regulation) is perfect or even close to it; what works at any particular time and place will be a matter of normative contestation and institutional design. As the economist Andrei Shleifer put it, there is a need to seek a “trade-off between dictatorship and disorder.”¹³ As such, the regulatory challenge is not only both political and technical, but also involves an acknowledgement of their mutually-sustaining relationship.

2. A Political Beginning

The origins of cryptocurrency are important and revealing. Although there is no one universal or accepted creation-story, its genesis is clearly to be found in a techno-generation reaction to prevailing conditions and alliances. There are two main culprits in this story – the banks and the government. Brought to a head by the financial and global crisis of 2008, the banking sector was under great suspicion and opprobrium as it sought and received government bail-outs. For some, this was further evidence that there needed to be some attempt made to break out of the cycle of boom-and bust that both fueled and, in some cases, felled the financial establishment. Indeed, in developing his radical ideas, Satoshi Nakamoto offered his digital peer-to-peer bitcoin innovation as a riposte to both the government’s and banks’ untrustworthiness and exploitive behaviour in handling currency and people’s finances.¹⁴

Although perhaps more than a little romantic and nostalgic in its intentions, there was an attempt to make good on the original promise of the internet to act as a democratic medium that had been betrayed or sullied by the new techno-aristocracy of the Googles, Amazons and Facebooks of the early 21st Century. As some of cryptocurrency’s early advocates insisted, it was birthed by cyberpunks as a direct challenge to the hegemony of the financial establishment and Big Brother. This has persuaded some that cryptocurrency is or was part of a radical anarcho-libertarian movement that was motivated to take back and reinvigorate popular control over those institutions that now exerted enormous and self-serving economic and social power. While there is no doubt much to this depiction, it is also unnecessary to frame all supporters of cryptocurrency as being aligned with such a political orientation and momentum. Indeed, whatever its specific roots and realities, the world of cryptocurrency is now treated as a semi-alternative haven for many disparate actors from the oppressive practices of the financial and fiscal establishment. It has befriended and galvanised supporters from across the political spectrum; it has its advocates from both the political right and left as well those in the middle-of-the road.¹⁵

¹³ Andrei Shleifer, Understanding Regulation, 11 EUROPEAN FINANCIAL MANAGEMENT 439 at 51 (2005).

¹⁴ See Nakamoto, supra note **.

¹⁵ A good summary of views can be found in Bitcoin And Other Cryptocurrencies Are Useless, THE ECONOMIST, August 30th, 2018 and Nigel Dodd, The Social Life of Bitcoin, CULTURE & SOCIETY (2017). The fact that Steve Bannon, President Trump’s former Chief of Staff, considers it an aspect of “disruptive populism” and that “it takes control back from central authorities” is not necessarily a strike against it for those not on the far-ish right. Also, there can be little doubt that the wider possibilities of blockchain technology have been embraced by all manner of political activists. See generally Tapscott and Tapscott, supra note **.

After almost a decade of life, cryptocurrency has begun to experience the trials and tribulations of coming-of-age in the larger world of financial services. Whatever the original motivations for its creation, real or mythical, bitcoin and its relatives have come to feel and occasionally succumb to the pressures of Big Business – mining has been taken over by large and highly-funded corporations; Wall Street (and even government) has begun to co-opt the technological innovation of cryptocurrency; exchange markets have prospered as a means to turn cryptocurrency into fiat currency; and investment and wealth has become the seeming measure of cryptocurrency's success, not innovation and freedom. In short, what began as an effort to offer a genuine alternative to traditional banking and finance has itself become vulnerable and almost hostage to those very same forces and institutions. Also, government has become suspicious of the global reach and subversive qualities of cryptocurrency; the fact that cryptocurrency has no borders has made it more resistant to the state's territorial sovereignty. Taken together, the banks' and government's anxiety and desire to protect their own turf threaten to stifle the enormous potential of cryptocurrency as a viable and valuable alternative mode of banking and finance.

Within such an environment, it is not surprising that there are both sceptics and true believers. Those who cling to the almost New Techno-Age-appeal of cryptocurrency are confronted by the hard-nosed economic realists who foresee a further and avoidable crisis waiting to happen. Those who forecast its imminent collapse are confounded by the real-world persistence of cryptocurrency as an alternative mode of exchange. As is often the case, this heated and polarised debate is in need of a cooler and more measured assessment. If cryptocurrency is not the salvation that its supporters claim, nor is it the devil incarnate that its opponents suggest. The truth lies somewhere in the middle or, at least, in a mix of the two.

This elusive space or mixture can be found in the notion that people of different political affiliations can agree that a shift of financial power from a concentrated centre to a more dispersed margin and from institutional intermediaries to individual users is no bad thing. Cryptocurrency offers one way to help bring that about. It has the potential to transform as well as destabilize the whole banking and financial system. However, in the process of any makeover, there is a genuine need to avoid throwing out the baby with the bathwater. The strengths of the traditional system of banking and currency regulation must be retained at the same time that its failings are being overcome. Accordingly, any effort to regulate cryptocurrency must be clear in its political assumptions and ambitions – the shared notion of putting ordinary people and their interests at the heart of any regulated society, not those of many civil or state-controlled institutions that tend to put their own interests ahead of others. This is a democratic and popular mandate that can garner broad political support.

3. Legitimizing Regulation

In order to achieve that political goal, it will be necessary for supporters of cryptocurrency to shelve or suspend their varying degrees of antagonism toward government. The reality of contemporary politics dictates that the choice is not between regulation and no regulation, but between different kinds of regulation, strong or lite; there is no real possibility of the continuing status quo of self-regulation (or, at least, self-regulation in its present mode) unless there is a willingness for cryptocurrency insiders to put their own house in some decent order. Ironically, while cryptocurrency was created as a strike against government, it will require something of

government's imprimatur if cryptocurrency is to resist heavy-handed regulation and the encroachment of banks and other financial intermediaries.¹⁶ However, the opposition to any kind of regulation comes from two very different sources.

The first are those anarcho-libertarians who were in at the introduction of digital peer-to-peer innovation. These die-hards view any kind of government intervention as a sell-out and entirely unacceptable. For them, to agree to any regulation would be considered to be the equivalent to make a deal with the devil. However, these true believers seem at their happiest when they are on the outside looking in: they are perpetual and habitual renegades who need an establishment to rail against. As such, in their world of constant opposition, no plan of regulatory action or compromise will ever be acceptable. The second are a group of traditionalists who maintain that regulation will only add further legitimacy to the very dubious and scam-like arrangement that is cryptocurrency. This is also a dubious and impractical stance. There are many things that are allowed and regulated in today's society that it would likely be better off to do without. Gambling is an obvious one. Although there is little to no redeeming social value to it, gambling is not only allowed, but is heavily regulated. Indeed, government often is not only the major regulator of gambling activity, but is also its major beneficiary by way of taxes and fees.

Others have been more open to regulation-lite. Ironically (in light of its laissez-faire origins), some self-styled cryptocurrency purists have welcomed the prospect of more invasive regulation; they claim that it will allow cryptocurrency to get back to its original purposes as a legitimate and alternative mode of private ordering and be consistent with its technology's potential as an unburdened and experimental medium for innovative entrepreneurialism. Although a tad idealistic and naive, there is substantial appeal to such an undogmatic and pragmatic anti-establishment ethic. After all, one of the great attractions of cryptocurrency is that it will "dispel much of the enormous cost that a bank-centric model of payments imposes."¹⁷ Yet, how to regulate crypto-currencies, even with a light and sensitive touch, is by no means obvious. There are some deep and perilous shoals to be navigated in the already treacherous cross-waters of technology and high finance. In particular, the central challenge will be to generate and implement ways of regulating cryptocurrencies that curb its secretive and illicit excesses, but preserve its innovative and decentralised strengths as an alternative market to so-called fiat money. This is no easy task.

In designing and implementing a regulatory regime, therefore, it is important to take a broader institutional view. To ban or gut the cryptocurrency system, like China and other countries are doing, would be a serious mistake (as would ignoring it entirely). Indeed, over-regulating would play into the hands of the very institutions that are most threatened by and have most to lose from the existence of an entirely borderless, decentralised, unmediated, self-regulating and neutral medium – the established structures and private financial institutions. The challenge, therefore, is to split the debilitating alliance of banks and government in their control over currency and financial services. By so doing, it might be possible to enlist government support for ensuring that

¹⁶ The widespread use of the internet was preceded by and perhaps facilitated by government regulation of the internet. See JACK GOLDSMITH AND TIM WU, WHO CONTROLS THE INTERNET? ILLUSIONS OF A BORDERLESS WORLD ** (2006).

¹⁷ Vigna and Casey, *supra* note ** at 295.

the alternativeness of cryptocurrency schemes is secured and the suffocating hold that the banks and similar institutions have over the financial services sector is released or loosened. This can only be done if some of the excesses of a self-regulated digital peer-to-peer process are dealt with. In particular, there is no reason why criminals and others should be able to utilise blockchain technology of cryptocurrency to hide and/or launder funds, evade taxes, circumvent currency restrictions, and the like. Nor are there any serious reasons as to why users of cryptocurrency should be able to shield their transactions from being open to similar kinds of taxation as other similar financial dealings.

Accordingly, if cryptocurrency is to survive and even thrive, it must accept that regulation is not only around the corner, but might be helpful. To resist that conclusion would be a form of institutional suicide. Of course, realizing that ambition will not be simple or straightforward. At a minimum, regulators will have to abandon typical command-and-control and top-down approaches to regulation. Indeed, the effort to meet the challenge of regulating cryptocurrency presents an opportunity to match cryptocurrency's innovative technological achievement with an equally innovative regulatory approach. This will involve developing and implementing a regulatory regime that is matched to the unique openings and deep pitfalls of a digitalised financial world. Whatever route is taken, there is a clear and looming notion that some regulation of cryptocurrency is both wise and timely.¹⁸ After all, despite the prognostications of some economic commentators, the world of crypto-currency is a reality. The move away from self-regulation towards a more cryptocurrency-sensitive style of regulation can only contribute to improving its chances of survival and even growth.

Of course, any legal intervention will not occur in a vacuum. There are a whole range of regulatory regimes and options that are already in play to cover a wide range of activities and actors. A first step, therefore, in working towards a suitable regulatory scheme for cryptocurrency is to canvass the existing regulatory landscape and evaluate whether they can or should be used to tackle the specific challenges of cryptocurrency regulation. This will demand attention to the context, stakeholders, objectives and tools of such regulation. It is to that comparative and difficult task that I now turn.

C. REGULATORY REGIMES

1. Sameness and Difference

The task of determining whether something is or is not like something else is a staple tool of legal analysis. But, as quotidian as it, this does not make it a simple task; the whole process is fraught with complexities and challenges. For example, in deciding whether two people have a relationship that would be sufficient to allow one person to be described as a 'child' of another is deceptively difficult. Imagine I am out with my young grand-daughter, teenage step-daughter and her friend; we meet someone who asks me 'are these your children?' There is no easy answer; much will depend on who asked, why they asked, and what follows from my answer. So my

¹⁸ For instance, at the recent G20 Summit in Argentina in December 2018, member countries announced that they would be taking concerted action to regulate the cryptocurrency. See *infra*, pp.**-**.

answer might be all, none or a couple of them – am I responsible for them while out with them?; are they part of my family?; are they my dependents?; do we look alike?; and are they my blood relative? In short, it depends on why it is important to determine who is a child of someone and, as importantly, what follows from deciding if a person is or is not a child of someone. These two matters – context and consequence – are pivotal to any effort to provide and apply definitions or analogies.

These taxonomic challenges apply acutely to the question of whether cryptocurrency is sufficiently like other entities or activities that it warrants the same or a similar type and style of regulation. While it seems reasonable to assume that cryptocurrency is ‘property’, it is a matter of some uncertainty about what category of property it falls into. For present purposes, there are three possible options that might profitably be explored –is cryptocurrency a currency?; is cryptocurrency a security?; and is cryptocurrency a commodity? In order to resolve those questions, it is necessary to pay close attention to the context for making the inquiry (i.e., whether and how to regulate) and the consequences of so finding (i.e., the particulars of the regulatory scheme to be applied). As such, context and consequence are related issues that give rise to important and competing analyses.

So, what is cryptocurrency? The answer is that it is a little bit of this and a little bit of that. It has characteristics that permit it to be thought of as a currency, a commodity or a security. As such, it might feasibly be understood to be any or all of them. However, it is important to recognize what flows as a regulatory matter from treating them as either property, a currency, a security or a commodity. As I have suggested, cryptocurrency does not lend itself well to an exclusive treatment as a currency, a security or a commodity. Consequently, the optimal approach is not to force cryptocurrency into one of these categories and apply the relevant regulatory tools and processes as if it were fully and centrally part of that categorization. Instead, it is much better and more productive to think about cryptocurrency as demanding a different and separate regulatory approach and apparatus that fits and responds to its specific and, in some ways, unique characteristics. This might well entail borrowing and blending aspects from all three regulatory regimes and perhaps adding new approaches to boot. By so doing, it might be possible to achieve an integrated set of regulatory solutions that are sufficiently efficacious and balanced that it will accommodate a broad range of political interests.

2. Is It Property?

Like most other legal concepts, the idea of ‘property’ is not a fixed or transcendental entity. It is a functional device that shifts and changes to meet the demands of different and changing social, economic and political conditions. As such, it is more a site for contestation as it is a solution to it. From this less formalistic standpoint, property is not about things, but about the relationship between persons and things.¹⁹ So understood, it is a metaphysical notion as much as

¹⁹ See Wesley Hohfeld, Fundamental Legal Conceptions as Applied in Judicial Reasoning, 23 YALE L.J. 16 (1913) and C.B. MACPHERSON, PROPERTY: MAINSTREAM AND CRITICAL POSITIONS (1978). There is debate about whether the cryptocurrency is a non-private space and, therefore susceptible to the ‘tragedy of the commons’. See Garrett Hardin, The Tragedy of The Commons, 162 SCIENCE 1243(1968). However, this is a distraction as cryptocurrency is neither public (it is entirely controlled by private actors) nor private (it is open to anyone who joins); it is a hybrid space.

a physical entity. The status of property, therefore, can attach to ‘things’ that may be tangible (e.g., land) or intangible (e.g., ideas). Consequently, whatever the physical status of cryptocurrency, the question of whether bitcoins can be counted and treated as property will not solely be resolved by determining what pieces of computer code actually are. Whether they are or are not like other kinds of property in some essentialist sense will not be the crucial determinant. Instead, the focus is upon why something is to be treated as property and what follows from that designation will be central to any definitional inquiry.

Although there is much debate by judges and jurist over the nature of digital information as property, there is a growing consensus that cryptocurrency (or, at least, the bitcoin itself as opposed to the overall blockchain process or any related activity) is best treated as private property for various legal and regulatory purposes.²⁰ In traditional terms, a bitcoin can be controlled by one person and its use can be exclusively reserved to one person; it is a valuable digital asset that can be held or transferred as the owner sees fit . Like information, it can be shared with and used by others. As such, but unlike information and more like money, it can only be used by one person at one time; it cannot be used simultaneously by others. While control is exercised by the use of an encrypted key or password rather than through physical possession of the bitcoin itself, this is insufficient in itself to defeat the argument that is it best understood as private property. Accordingly, the main issue is not so much whether bitcoin is property: it is. More importantly, the focus of debate is about how should such property be regulated as a legal matter.

The designation of cryptocurrency as property, therefore, might end one particular debate, but it opens up other and more important debates about what follows from that determination. There is no rigid formula for deciding that question; it is not a one-size-fits-all resolution. For instance, when it comes to matters of taxation, there are different applications of taxing measures that might be adopted in different jurisdictions even though there is general agreement on the status of cryptocurrency as property.²¹ Or the fact that it is to be classified as property might be sufficient for one purposes (e.g., the crime of money laundering), but not for another (e.g., the sale of securities).²² This means that, although cryptocurrency is to be recognised and understood as property, it is necessary to take the next step and explore what particular legal regime might best be suited to its regulation – is cryptocurrency to be treated as a currency, a security, or a commodity? And, of course, these questions do not lend themselves to straightforward or ordained answers; they are normative and contested as much as technical and objective.

3. Is it A Currency?

²⁰ See, for example, *OBG Ltd. v. Allan*, [2008] 1 A.C. 1; *Kremen v. Cohen*, 337 F.3d 1024 (U.S. C.A. 9th Cir., 2003); and *Tucows.Com Co. v. Lojas Renner S.A.*, (2011) 336 D.L.R. (4th) 443 (Ont. C.A.). See generally Joshua A. T. Fairfield, *BitProperty*, 88 S. CAL. L. REV. 805 (2015) and Petter Hurich, *The Virtual is Real: An Argument for Characterizing Bitcoins as Private Property*, 31 BANKING & FINANCE L. REV. 573 (2016).

²¹ Compare the approach of the American IRS with that of the Canadian CRA. See IRS, Notice 2014-21 *5-6 (Mar 25, 2014), online at <http://www.irs.gov/pub/irsdrop/n-14-21.pdf> and **.

²² See, for example, *United States v. Ulbricht*, 31 F. Supp. 3d 540 (S.D.N.Y 2014) (cryptocurrency is money for the purposes of laundering).

The most obvious place to begin the classificatory exercise is with the question of whether cryptocurrency is a currency. The fact that it is called ‘cryptocurrency’ should in itself not be dispositive of the issue of whether it is a currency and should be regulated as a currency for legal purposes. There are a number of clear ways in which cryptocurrency does function as a currency. It is a medium of exchange, a unit of account and store of value. Because it is not backed by any underlying asset, its value is determined by supply and demand alone. In this way, cryptocurrency is very similar to standard fiat currencies, like the US dollar, the Euro or the British pound. However, despite its similarities to fiat currency, there are very significant differences that recommend that cryptocurrency is of a very dissimilar kind and warrants a distinct regime of regulation. Only one country, Japan, to date has designated cryptocurrency as ‘legal tender’ and, therefore, susceptible to direct and equivalent regulation as a fiat currency. As always, it is a matter of context and consequences.

The major difference between cryptocurrency and fiat currency is that the latter is state-backed and its supply is determined by government. Indeed, the very nature of cryptocurrency is that it is intended to be and work as an alternative form of currency; it is a private and decentralized medium and, as such, immune to government’s monetary policy. Although it is personal chattel, albeit of a non-physical form than coins or notes, it has a different property-like status than fiat currency. Also, it moves across geographical and state-defining borders; it is an international medium that eludes control by any one national (e.g., the American and Canadian dollar) or bloc government’s (e.g., the Euro) central bank. While it is convertible into fiat currency, it is not itself fiat currency.²³ However, distinguishing cryptocurrency from fiat currency does not in itself exempt its users from tax obligations; the use, sale and holding of cryptocurrency are amenable to appropriate and relevant tax principles and rules. Indeed, in some jurisdictions, like Canada and the United States, it has been specifically determined that, although cryptocurrency functions in much the same way as fiat currency and money generally, only coins issued by the national mint and under the authority of law should be treated as legal tender and, therefore, regulated as official currency.²⁴

In short, while cryptocurrency and fiat currency have important family resemblances and, as it were, cryptocurrency is not not a currency, their underlying origins, operation and rationale are more than sufficiently different to warrant a different approach and method in terms of their regulation. Indeed, the scheme and purposes of the existing regulatory structures seem ill-designed to confront and contain the challenges of cryptocurrencies: they are premised entirely on the idea that currency is a state-backed and state-controlled entity and that the state has an unfettered monopoly in such matters.²⁵ While there are lessons to be learned from the history and practice

²³ See, for example, Reuben Grinberg, Bitcoin: An Innovative Alternative Digital Currency, 4 HASTINGS SCI. & TECH. L.J. 159, 160 (2011); Kevin Tu and Michael Meredith, Rethinking Virtual Currency Regulation in The Bitcoin Age, 90 Wash L Rev 271 (2015); and Oleg Stratiev, Cryptocurrency and Blockchain: How to Regulate Something We Do Not Understand, 33 BANKING & FINANCE L. REV. 173 (2018).

²⁴ See <https://www.irs.gov/pub/irs-drop/n-14-21.pdf> and https://www.canada.ca/en/revenue-agency/services/forms-publications/publications/t4037/capital-gains-2016.html#P279_29831.

²⁵ In the United States, the Constitution extends to the federal government an exclusive right to issue currency and coin money. See U.S. CONST. art. I, § 8 and also the Stamp Act of 1862. In Canada, ‘currency and coinage’ is in the exclusive control of the federal government. See Constitution Act 1867, s.91(14) and the Currency Act in 1985 and the Bank of Canada Act in 1985.

of currency regulation by governments, they do not offer a very useful or framework for regulating cryptocurrency. Cryptocurrency is its own kind of currency and should be regulated as such.

4. Is It A Commodity?

Deciding whether cryptocurrency is or is not a commodity is much like the discussion about whether it is or is not a currency. There is no black and white answer, but only a shifting series of gray responses. For some purposes, it does share important characteristics with and function as a commodity, but for others it does not. Indeed, when it is appreciated that currencies have been classified for some legal and regulatory purposes as a commodity, the difficulty of pinning down whether cryptocurrency is or is not a commodity can be understood becomes clearer. Indeed, throughout history and across societies, many commodities (e.g., gold and salt) have served as a currency. In short, the question of whether cryptocurrency is a commodity depends on the context for asking and answering it and the consequences that flow for such a determination.

The general understanding of what is a ‘commodity’ is broad and diffuse. At one level, commodities are simply goods and articles that can be commercially traded. This has traditionally included metals, energy, livestock, and agricultural products. Cryptocurrency does not square up easily with these kinds of property. However, recent understandings of what counts as a commodity have expanded to include mortgages, foreign currencies, and communication bandwidths. Like all commodities, cryptocurrency can also be bought or sold like a commodity; the price of bitcoin is based on supply and demand. The volatility of cryptocurrencies is very much like that of commodities; commodities investors invest in futures contracts rather than purchase the commodity. A connecting thread seems to be that commodities, like gold or pig-bellies, have value not only as an investment device, but also as a usable product; cryptocurrency does not. Moreover, because the value of cryptocurrency is not backed by anything other than itself, it differs from traditional commodities. Nevertheless, even though its initial and perhaps primary purpose is to act as a medium of exchange, currency can be treated as a commodity because it can be purchased and sold as an investment and, thereby, benefit from ups-and-downs in currency exchange rates.

In comparing cryptocurrency and commodities, the main practical issue is with the use of commodities as a speculative investment by way of future trading: most regulatory efforts are devoted to monitoring and constraining such activities. However, cryptocurrency is not like other commodities in that, when functioning as a currency, it is exchanged directly and momentarily. Also, unlike more usual futures commodity trading, the user of cryptocurrency as a currency is an exclusive owner; they have more than a contractual option to trade the underlying asset in question. That said, it can also, like currency, be utilized as an investment tool to hedge risk and speculate. When used in this way and traded for future consideration, it does potentially fall within the regulatory authority of the U.S. Commodity Futures Trading Commission (CFTC), a federal regulatory agency. Indeed, the CFTC has always insisted that that bitcoin and other digital currencies are commodities and, therefore, within its regulatory reach: this stance has been

confirmed by the courts.²⁶ Furthermore, the Canadian Revenue Agency has characterized cryptocurrency as a commodity, not a government-issued currency for the purposes of taxation.²⁷

From a regulatory standpoint, the issue has become one of jurisdictional competence and priority. The central rivalry over the nature and identity of cryptocurrency is between the CFTC (as a commodity) and the Securities Exchange Commission (as a security). The decision whether to allocate regulatory responsibility to one, the other or both has significant consequences for the focus and substance of any regulations imposed. However, rather than opt for one or even both bodies as the regulatory agency of choice, a more preferable approach might be to treat cryptocurrency as property of its own kind, a little bit currency and a little bit commodity. This would allow the development of a regulatory scheme that is specifically designed for cryptocurrency and its peculiarities rather than squeeze it into a regulation scheme that clearly did not have in mind even the possibility of there being cryptocurrencies when its rules and regulations were developed. Accordingly, the more telling question is not whether cryptocurrency is a commodity (or anything else for that matter), but what is the most suitable and effective kind of regulation for cryptocurrency.

5. Is It A Security?

Perhaps the most settled definitional issue is that cryptocurrency can and should be considered to be a security. Appropriate regulatory agencies have determined that, whatever else they might be as well, bitcoin and other cryptocurrencies count as securities. However, this determination has limited and specific scope. Rather than treat cryptocurrency as a security at all times and for all purposes, the general consensus among securities regulators has been that the initial establishment of a cryptocurrency scheme or a cryptocurrency exchange comes within their regulatory mandate. In other words, the use of digital coin within the bitcoin process of exchange is not a practice to be regulated by securities agencies, but the venue for and practices of converting these coins into fiat currency through initial coin offerings (ICOs), initial token offerings (ITOs), or by selling securities of cryptocurrency investment funds is.²⁸

²⁶ CFTC, Retail Commodity Transactions Involving Virtual Currency, Proposed Interpretation, 82 Fed. Reg. 60335 (December 20, 2017), <https://www.cftc.gov/sites/default/files/idc/groups/public/@Irfederalregister/documents/file/2017-27421a.pdf>. See *CFTC v. McDonnell* in the Eastern District of New York (August, 2018) where it was held that bitcoin and other cryptocurrency fell within the definition of a ‘commodity’ under the Commodity Exchange Act of and, therefore, fell within the regulatory jurisdiction of the CFTC. See also *In re Coinflip, Inc.*, CFTC No. 15-29, 2015 WL 5535736 (Sept. 17, 2015) where then court on an expansive definition of commodity so that markets can be properly policed and traders appropriately protected. See also Nicole Swartz, *Bursting the Bitcoin Bubble: The Case to Regulate Digital Currency as a Security or Commodity*, 17 TUL. J. TECH. & INTELL. PROP. 319 (2014) and Hadar Jabotinsky, *The Regulation of Cryptocurrencies - Between a Currency and a Financial Product*, SSRN-id119591 (March, 2018).

²⁷ See https://www.canada.ca/en/revenue-agency/services/forms-publications/publications/t4037/capital-gains-2016.html #P279_2983.

²⁸ See, for example, https://www.sec.gov/news/public-statement/statement-clayton-2017-12-11#_ftnref8 and Canadian Securities Administrators, “CSA Staff Notice 46-307: Cryptocurrency Offerings”, 40 OSCB 7233 (Toronto: OSCB, 24 August 2017) at 7231 [CSA Staff Notice] and SEC Statement on Potentially Unlawful Online Platforms for Trading Digital Assets (March 7, 2018), <https://www.sec.gov/news/publicstatement/enforcement-tm-statement-potentially-unlawful-online-platforms-trading>.

Although the meaning of what counts as a security for the purposes of regulation is not entirely fixed, it has long been accepted that there are several main elements to this categorization – the entity in question must involve an investment of money in a common enterprise with the expectation of profits that will be solely from the efforts of others.²⁹ While this definition encompasses the secondary and later market of cryptocurrency as an investment exercise, it does not apply too well to the original use of cryptocurrency itself as a medium of exchange; there is no real or necessary expectation of profits through the efforts of others. This becomes more apparent when the consequences of deciding that cryptocurrency is or is not a security for regulatory purposes are considered.

The effect of classifying something as a security and bringing it within the purview of the appropriate regulatory agency is that an array of governing principles and rules will apply. These include dealer registration, full disclosure, no insider trading, record keeping, auditing, investor protection and the like. The purpose of these requirements is to ensure that investors are appraised of all relevant information and that the market is able to price the securities appropriately. As regards, the secondary market of coin offerings and investment funds (e.g., Coinbase and Poloniex), these regulations seem to be warranted, even if some more subtle tweaking of those rules and their application would be beneficial and helpful. Similarly, these regulations do not adapt well to the regulation of the cryptocurrency itself; there is no investment or capital market that is in need of regulation and there is no form of asset representation other than the cryptocurrency unit itself. In this sense, the use of cryptocurrency as an exchange medium is more aptly thought of as a piece of personal property that functions more as currency than a security.

It is revealing that some of the most well-known fiascos around cryptocurrency involve the failure of these secondary organizations. In early 2014, Mt. Gox placed exchanges in the glare of publicity and alerted people to the risks of an unregulated market around cryptocurrency; losses were around \$400M. More recently, the collapse the Canadian cryptocurrency exchange, Quadriga CX has revived concerns about the unruly operation of such institutions; unexplained losses remain at around \$200M. Both of these affairs speak to the need for more serious regulation of the secondary market around cryptocurrency.³⁰ However, this leaves unresolved issues of how to deal with the primary operation of cryptocurrency. Efforts by the New York state Department of Financial Services to impose a BitLicense framework are a beginning.³¹ But more is needed if cryptocurrency is to be used as a reliable and responsible zone of digital trading.

²⁹ See SEC v. W.J. Howey Co., 328 U.S. 293, 301 (1946). This definition has been adopted by the supreme court of Canada in Pacific Coast Coin Exchange of Canada v. Ontario (Securities Commission), [1977] 80 DLR (3d) 529, [1978] 2 SCR 112. See also Swartz, supra, footnote ** and Thomas Witteveen, Future Crypto-Concerns for Canadian Securities Regulators, 33 BANKING AND FINANCE L. REV. 265(2018).

³⁰ See Jake Adelstein and Nathalie-Kyoko Stucky, Behind the Biggest Bitcoin Heist in History: Inside the Implosion of Mt. Gox, <http://www.thedailybeast.com/articles/2016/05/19/behind-the-biggest-bitcoin-heist-in-history-inside-the-implosion-of-mt-gox.html> and Allan Hutchinson, The Lesson Of Quadriga Are Not As Obvious as Many Think, <https://www.theglobeandmail.com/business/commentary/article-lessons-of-quadriga-fiasco-not-as-obvious-as-many-think/>.

³¹ New York State Department of Financial Services (July 17, 2014). "NYDFS Releases Proposed BitLicense Regulatory Framework for Virtual Currency Firms. See <https://web.archive.org/web/20140923054843/http://www.dfs.ny.gov/about/press2014/pr1407171.html>.

D. A SEPARATE REGIME

1. A Special Agency

The problem to be faced in regulating cryptocurrency is the general issue of the ‘governance paradox’³² – How do you regulate an innovative scheme that demands some regulation, but know that any regulation will transform the very features of that scheme that makes it what it is as well as what makes it unique and useful? More specifically, how do you regulate an off-the-grid, decentralized and distributed scheme without making it into an on-the-grid, centralized and undistributed scheme? This is the challenge to be met in devising any kind of proposal to create a regulatory regime for cryptocurrency. Consequently, in doing so, it will be important to remember that regulation is not a technical end in itself, but a means to a larger and more substantive end -- the shared notion of putting ordinary people and their interests at the heart of any regulated society, not those of many civil or state-controlled institutions that tend to put their own interests ahead of others.

As I have been at pains to demonstrate, cryptocurrency is its own kind of activity and, therefore, should be regulated as such. It is an item of property that a little bit currency, a little bit security, and a little bit commodity. While it is conceivable that a patchwork quilt of regulatory agencies might be tasked with regulating cryptocurrency in the hope that this will produce a thorough and comprehensive scheme of regulation, this is highly unlikely. Indeed, the chances are that this will produce the worst of all worlds. Not only will administrative agencies vie for control, they will be doing so as a result of competing ambitions and by way of conflicting devices. This is a recipe for regulatory disaster; it will result in a heavy-handed, ill-suited and untidy mish-mash of regulations. Instead, it seems much more practical and useful to develop a regulatory approach to cryptocurrency that is as special and different in approach and implementation as cryptocurrency is in nature and operation. Of course, this might well entail borrowing and blending aspects from different and existing regulatory regimes and perhaps adding new approaches to boot. By so doing, it might be possible to achieve an integrated and coherent set of regulatory solutions that are sufficiently efficacious and balanced that they will advance the main goal of regulating cryptocurrency so that it is a better version of itself, not a lesser one.

The first move towards this goal is to establish an agency that will have primary and sole responsibility for regulating cryptocurrency in all its manifestations. In the spirit of cryptocurrency’s decentralised philosophy, such a body should not be a typical and traditional government agency, like the SEC or CFTC. While it will be essential to include government representatives, they need not and should not comprise the majority of members. This would be a certain kind of quasi-autonomous non-governmental organisation (a QUANGO).³³ The idea is that this would be separate from government, but have ties to and representation from government. It would occupy that important, but neglected space between public authority and private autonomy. Working as a go-between for the cryptocurrency community and the broader society, its members would have a degree of tenure and, even if government appointees, have an arms-length relation

³² KEVIN WERBACH, *THE BLOCKCHAIN AND THE NEW ARCHITECTURE OF TRUST* 133-38 (2018).

³³ Alan Pifer, *The Quasi Nongovernmental Organization* (Carnegie Corporation, 1967). For instance, while more popular in the United Kingdom, these organizations might include bodies like the US Federal Reserve. See PAUL KRUGMAN, *THE AGE OF DIMINISHED EXPECTATIONS: US ECONOMIC POLICY IN THE 1990s* 99 (1997).

to government. The ambition here would not be to produce neutral or apolitical recommendations, but to balance the often competing interests of its various constituencies.

Of course, it is important for both the legitimacy and efficacy of such an agency that it be populated by a full range of stakeholders from both inside and outside the cryptocurrency community. These might include software developers, miners, coin-holders, financial services representatives, cryptocurrency exchange operators, CFTC and SEC representatives, and the like. Also, in the spirit of the cryptocurrency community, the members would strive to attain rough consensus in its deliberations and policy initiatives. By populating such a regulatory body in this way, it might be possible to generate the kind of technological expertise, regulatory experience, and political savvy that is needed to pull off its ambitious mandate of regulating cryptocurrency in a way that holds true to its transformative possibilities and opportunities. This would entail the usual regulatory responsibilities of developing standards for registration, certification, sound practices, security, database management and the like.

This endeavour to create such a cryptocurrency quango, populate it representatively and define appropriately its mandate can draw upon the efforts of some organizations that already exist, even if they are in a somewhat embryonic state. For instance, there is the fledging ICO Governance Foundation (IGF). This is a decentralized, global and non-profit organization whose mission is to establish a protocol-based community that regulates ICOs in capital markets; it seeks to create and enforce global standards for disclosures as part of a voluntary registry.³⁴ Also, there is the Virtual Currency Association (VCA). An initiative of the Winklevoss twins, it is similar to the IGF in its non-profit and independent structure, but has a broader self-created mandate: it seeks to establish a global standards and best practices for the U.S. virtual currency industry, specifically virtual commodity exchanges and custodians. As a self-regulatory organization, it models itself on other similar groups, like the National Futures Association, and plans to work with established regulators, like the SEC or CFTC.³⁵

Both the IGF and VCA are non-public initiatives that offer some flavour of what a new cryptocurrency agency might look like or, at least incorporate. Rather than liaise with government bodies, the agency being proposed would combine the IGF and VCA with those public bodies and create a new quango that would replace them all. Although these kind of quangos are more common in the United Kingdom and Canada than in the US, they have much potential in cryptocurrency context. Although not without risks and flaws (i.e., if not properly constructed, they are open to government- and/or industry-capture), such a quango-like agency would be an important step in kick-starting an appropriate regulatory process for cryptocurrency.

2. A Balancing Mandate

³⁴ Miko Matsumura, ICO Governance: A Protocol-Based Self-Regulation of Token Sales in Decentralized Capital Markets, November 27, 2017. See https://icogovernance.org/wp-content/uploads/2017/12/Governance_of_Token_Sales_in_Decentralized_0.91.pdf.

³⁵ Cameron Winklevoss, A Proposal for a Self-Regulatory Organization for the U.S. Virtual Currency Industry (March 13th, 2018). See <https://medium.com/gemini/a-proposal-for-a-self-regulatory-organization-for-the-u-s-virtual-currency-industry-79e4d7891cfc>.

While the mandate of a Cryptocurrency Agency would be broad and comprehensive, it would be for the members to decide how to exercise and fulfil it. Nevertheless, there are certain issues that will have to be addressed and confronted. The crux of the matter will involve some evaluation of those characteristics that go the heart of the cryptocurrency enterprise and those that do not. It is only by engaging in this important exercise that it might be possible to address properly, if not entirely resolve fully the ‘governance paradox’ – to regulate, but not to negate the basic structure of the cryptocurrency process. To do this, tough decisions will have to be made about what is core and what is not. Also, it will be important to approach the regulatory task with the enigmatic Satoshi Nakamoto’s admonition to early bitcoin users about the blockchain technology – “there’s no reliance on recourse. It’s all prevention.”³⁶

The primary characteristics of cryptocurrency are that it is it was intended to be an entirely borderless, decentralised, unmediated (without banks), pseudonymous, self-regulating and politically neutral medium. To be blunt, which of these characteristics, if any, can be interfered with or altered without eviscerating the whole cryptocurrency project? One way to come at this is to ask how it might be possible to deal with one of its main perceived failings – its use for illegal and even criminal activity. Insofar as there are a variety of legal provisions in play in the financial sector that are intended to prevent or punish activities like money laundering, tax, evasion, terrorist funding, currency limitations, and the like, there are no compelling reasons why cryptocurrency should be exempt from their reach or application. Indeed, it seems a reasonable complaint by established members of the financial services sector, especially banks, that cryptocurrency should not escape the prevailing legal frameworks for detecting and deterring such activities; ordinary people and traders would be harmed by such an exemption. It was surely not a central purpose of the Nakamoto and his colleagues to develop a process to facilitate such activities.³⁷

If that all is the case, the challenge becomes how to prevent such activities while, at the same time, allowing the use of cryptocurrency to continue in its primary and defining initial format. While anonymity is a positive good, it is also a negative charge in that it allows criminal activities to proceed and go unchecked. At present, it is not so much that transactions are entirely anonymous, but that they are ascribable to a particular account by way of a cryptic pseudonym or password; the particular coin-holder is known, but not their real world identity. Indeed, the whole benefit of blockchain technology is that not only does it record and confirm all transaction, but it also does by knowing who transferred coins to who. The crunch issue, therefore, is whether it is possible to abandon or modify the semi- or pseudo-anonymity of present cryptocurrency transactions without irreparably changing their basic structure? Although purists will argue that it is not possible, I maintain that the answer to this is that it can be. In other words, cryptocurrency can remain cryptocurrency without being crypto.

³⁶ Satoshi Nakamoto, Re: Bitcoin P2P e-cash paper, <https://www.mail-archive.com/cryptography@metzdowd.com/msg10006.html> (November 17th, 2008).

³⁷ A question of relative importance is whether cryptocurrency is any more or less vulnerable to criminal activities than other trading or banking process. Although the predominant view seems to be that it is, some argue that cryptocurrency is less vulnerable because all transactions are viewable and, as such, cryptocurrency might be more capable of protecting against criminal activity than cash or fiat currency. See Tapscott and Tapscott, supra, note ** at 275-77.

The underlying integrity of cryptocurrency is founded on the notion of it bringing into existence a non-hierarchical system that is bottom-up, not top-down in its operational philosophy and regulatory structure. Moreover, because it was intended to challenge the hegemony of the banks and offer a viable alternative to them and other financial sector actors, its primary dynamic was motivated by a desire to create a decentralized, unmediated, self-generating and distributed process. If the characteristic of anonymity was to be cut back or reduced, it is not obvious that the *raison d'être* of the whole process of cryptocurrency trading would be fatally impaired. Indeed, ensuring that the process was less open to criminal or illegal use might actually enhance the wider reputation and attractiveness of the process and encourage more people to become participants. Divested of the stigma of illegality, cryptocurrency might better slip out of the relative shadows into a brighter and less marginal future.

Of course, achieving this, without doing substantial damage to the overall cryptocurrency process, is not a simple task. It will take a series of subtle and targeted interventions. In keeping with a commitment to regulation-lite, it will be useful to move well beyond the command-and-control mentality of traditional regulatory efforts. Instead, the cryptocurrency situation would best be handled, at least initially, with a range of more 'nudge-like' initiatives.³⁸ Indeed, regulation of cryptocurrency seems to be one of those activities that would benefit from a more-carrots-than-sticks approach. As such, a Cryptocurrency Agency might adopt measures like best practices, incentivization, voluntary registration and the like. If these proved ineffective, then a sterner and more directive set of interventions might be considered.

A particular and related challenge in regulating cryptocurrency is that, unlike in other similar areas and activities, there is no central authority or organizing lynchpin when it comes to cryptocurrency. Because cryptocurrency is a truly decentralized and distributed process, no one entity is fully tasked with the responsibility to make or implement decisions that are prescribed by a regulatory agency. Even if a gentler and more suggestive approach is adopted, there is the continuing problem of how such recommendations will be introduced across the cryptocurrency board. This is where a more innovative mind-set can intervene in ways that are both effective and consensual. The regulatory impulse might be able to influence the so-called *lex cryptographica* and engineer the kind of changes, like a scaling back of the system's semi-anonymous characteristics, that might be demanded.³⁹ In short, it might be possible to nudge and chivy the software guardians of the blockchain to design and build code that incorporates the kind of values and incentives that would be thought to best advance the goals of a more fairly and lightly regulated cryptocurrency world. These latter-day heirs to Nakamoto might be acting in the benevolent spirit of that originating genius.

Mindful that the blockchain code used is the heartbeat of cryptocurrency, the idea would be to take steps that would incentivise the code-makers to alter the operating software so that the identities of coin-holders could be retrieved and stored. As holders' pseudonyms must presently be recorded and known in order to allow the blockchain to validate transactions, it would be a relatively small step to develop a data-store of the real identity of the pseudo-anonymous users of cryptocurrency. There is no need for all other holders to be aware of a holder's identity: conditions

³⁸ RICHARD THALER AND CASS SUNSTEIN, **

³⁹ See *supra*, pp. **-**.

and constraints can be in place that preserve the limited confidentiality of such a data-store. Moreover, limited access in limited circumstances might be granted to certain existing government agencies, like those entrusted to handle taxation and money-laundering; such a scheme might be judicially-administered so as to balance and protect persons' individual rights. This overall kind of regulatory approach would allow a blend of the *lex cryptographica* with what might be termed the *lex traditionis* for the mutual benefit of each. Importantly, this would also permit the blockchain to remain its own regulator by continuing and developing an internal mode of algorithmic governance.⁴⁰

Another approach that is attuned to and based upon the particular characteristics of a blockchain-enabled cryptocurrency system is the use of 'smart contracts'. These are self-executing agreements that require no third-party intermediary for enforcement and are based upon the autonomous code of existing blockchain technology. As such, they offer similar advantages to cryptocurrency generally – heightened cyber-security and lower transaction costs.⁴¹ They are already used within or on top of the bitcoin network to facilitate a number of transactions, like escrow accounts, payment channels, multi-party security, and others. These innovative digital contracts can be utilized to regulate the use of cryptocurrency by organizing and verifying the operation of the data-store. Also, they could be customized to allow a tax-at source protocol that levied and transferred a certain sum upon each transaction to the appropriate tax authority; this would prevent the kind of extended litigation that is presently wending its way through the courts.⁴²

Accordingly, the challenge of regulating an enterprise that has no central hub, is entirely technology-driven, creates its own enforced practice of trust, and prides itself on its reliance on distributed consensus can be achieved. Of course, these suggestions are only the beginning of a continuing and, through the cryptocurrency quango, an almost open-source of regulation. The most important feature is that the means and target of such regulation is compatible with both the nature and spirit of cryptocurrency and its blockchain protocols. Also, although some will resist this possibility, such regulation can make cryptocurrency a better and safer place to trade, transact and do business.

3. Across Borders

A distinctive feature of cryptocurrency is that, among others, it is a borderless process that operates in its own public domain. There are two dimensions to this problem in regard to regulation. The first is the border between the primary sphere of cryptocurrency as a trading process and its secondary province as an investment device. The second is the task of recognising that cryptocurrency is intended be a global innovation that does not acknowledge national boundaries and so can more easily evade the regulatory reach of any one jurisdiction. While the

⁴⁰ See generally DE FILIPPE AND WRIGHT, *supra*, note ** at 193-204 and WERBACH, *supra*, note ** at 157-60.

⁴¹ See MICHAEL CASEY AND PAUL VIGNA, *THE TRUTH MACHINE: THE BLOCKCHAIN AND THE FUTURE OF EVERYTHING* 2018) and Tapscott and Tapscott, *supra*, note **. The primary smart-contract platform is Ethereum that is public, not permissioned site and has its own cryptocurrency: 'ether' is the most common and valuable cryptocurrency after bitcoin.

⁴² See, for example, **.

former regulatory challenge is easier to meet, the latter will require more concerted and cooperative efforts.

There seems to be a strong consensus within and outside the cryptocurrency community that some form of regulation is need for the secondary market of coin exchanges, initial coin offerings (ICOs), and other related trading and investment activities. Because these entities and occurrences function as part of the traditional market by facilitating various interactions between cryptocurrencies and fiat currencies, it is appropriate to recommend the introduction and enforcement of a regulatory regime that requires much the same set of principles and rules as the traditional market itself. The existing approaches of SEC and CFTC can be borrowed and amended in ways that a cryptocurrency regulatory agency would see fit.⁴³ As things stands, the usual requirements of registration, adequate record-keeping candid disclosure, auditing, client transparency principles, ‘know your customer’ rules, insurance, conflicts checks, and the like seem to be apposite and pertinent. Although some will contend that these requirements will be unduly onerous and stymie innovation, they do seem to be recommended on the same basis as existing securities and futures regulation – the protection of investors and other stakeholders.

A telling example of what can happen in an unregulated environment and what regulation might do to improve matters is offered by the recent collapse of the Canadian crypto-exchange, QuadrigaCX. When the creator and sole operator of the company, Gerald Cotten, died in mysterious circumstances, there was apparently no way to access his laptop or off-line USBs (so-called ‘cold wallets’) on which a suspected C\$200 million of assets from almost 100,000 clients were stored: no one knew or could replicate his encrypted key. There were also suggestions that the funds had been embezzled. To make matters worse, there were no enforced regulations about registration, auditing, record-keeping and the like in effect: Cotton was running a truly off-the-grid operation. Ironically, this state of affairs confirms the hyper-security of cryptocurrency. Nevertheless, even if speculative users of QuadrigaCX were naïve in much the same way as investors in Bernie Madoff’s too-good-to-be-true scheme,⁴⁴ they were entitled to some regulatory supervision and protection that might have avoided such a fiasco.

The other challenge is how to handle and respond to the borderless ambitions and actual operations of cryptocurrency. As with tax evasion and dubious banking, the possibility of simply moving off-shore to avoid unwanted regulations is real. This should not discourage jurisdictions from taking the regulatory task seriously; many crypto-enthusiasts will remain local in their trading and business, especially in the United States. At present, there is a patchwork of national procedures for such monitoring. Some countries, like China, have taken a no-cryptocurrency position, while others, like Malta and Japan, are enthusiastically open for business. Obviously, this is not a desirable situation: a multi-national approach is a much better option.

⁴³ In Europe, the regulatory framework under the Markets in Financial Instruments Directive (MiFID) has been held to apply when crypto-assets qualify as transferable securities or other types of financial instruments. See ESMA Advice – Initial Coin Offerings and Crypto-Assets (January 9, 2019), https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf.

⁴⁴ See DIANA HENRIQUES, *THE WIZARD OF LIES: BERNIE MADOFF AND THE DEATH OF TRUST* (2017). On the QuadrigaCX debacle, see Mystery as Quadriga crypto-cash goes missing, <https://www.bbc.com/news/technology-47454528> and Hutchinson, supra, note **.

At the recent G20 Summit in Argentina in November 2018, the member countries agreed that they would be taking concerted action to regulate cryptocurrency. With guarded praise for its technological innovations that have led to significant benefits to the global economy, a call was made for some substantial and serious regulation to deal with money laundering, terrorist funding, excessive risk speculation, and the coordination of cross-border taxation. The basic plan is to rely on the standards created by the Financial Action Task Force (FATF), established by the G7 in 1989.⁴⁵ However, the G20 is unlikely to exercise a light touch in regulating crypto-currency. In combatting criminal and terrorist activity, there will likely be a more heavy-handed approach. Innately suspicious of any effort to evade public scrutiny and oversight, governments will find it difficult to forebear from introducing a raft of restrictive and intrusive measures. However, as I have recommended, that impulse should be resisted. When it comes to cryptocurrency, the more that is done in plain sight will be better than pushing it further to the shadowy margins.

E. Conclusion

If the effort to regulate cryptocurrency is to be successful, it will be important that the cryptocurrency community is not the only one open to some changes and enhancements. It is also vital that the legal and regulatory community approach this task as an occasion to change and challenge its own traditional ways of doing things. The style, tools and substance of legal regulation must adapt to cryptocurrency as much as cryptocurrency must adjust to regulatory interventions. On both sides, there are beneficial and mutually-reinforcing opportunities for transformation and improvement. A heavy-handed approach would be counter-productive and work to the advantage of the very established financial institutions that are most threatened by the efficient innovation of an entirely borderless, decentralised, unmediated, self-regulating and politically-neutral medium for doing business and trading. By adopting lighter and more sensitive modes of regulatory policy, both cryptocurrency (and other new technological inventions) and law can evolve and serve better the interests of the broader public.

⁴⁵ Financial Action Task Force, Public Statement: Mitigating Risks from Virtual Assets, [http://www.fatf-gafi.org/publications/fatfrecommendations/documents/regulation-virtual-\[assets-interpretive-note.html](http://www.fatf-gafi.org/publications/fatfrecommendations/documents/regulation-virtual-[assets-interpretive-note.html)

**Joint Canadian Securities Administrators/Investment Industry
Regulatory Organization of Canada
Consultation Paper 21-402
Proposed Framework for Crypto-Asset Trading Platforms March 14, 2019**

Draft Wording in Regard to Disclosure of Digital Assets

A. The Disclosable Digital Assets

Disclose each and every entity, effect and asset, and each and every item of property, resources, estate, holdings, possessions, effects, goods, valuables, belongings, chattels, worldly goods, worldly possessions, capital, funds, wealth, principal, money, riches, means, fortune, finance, reserves, rights, savings, and/or securities, held in any and every digital form, including but not limited to:

A.1 Cash, Currencies, Fiat Currencies in particular any holdings or contracts (including futures contracts), options, and derivatives of, for and/or pertaining to cash and currencies including but not limited to those denominated in: Pound Sterling (GBP), United States Dollar (USD), Euro, Japanese Yen, Australian Dollar, Canadian Dollar, Swiss Franc, Brazilian Real, Chinese Renminbi;

A.2 Cryptocurrencies, in particular any holdings or contracts (including futures contracts), options, and derivatives of, for and/or pertaining to leading or other cryptocurrencies, altcoins, and/or tokens, including but not limited to: Bitcoin, Ethereum, Litecoin, Zcash, Dash/Darkcoin, Ripple, Monero, Bitcoin Cash, NEO/AntShares, Cardano, EOS;

A.3 De- or non-materialised data, datasets and/or databases, and/or all other technologies and means, holding or having ascribable financial and/or tradeable value;

A.4 Each and every instance of physical digital storage media and devices holding or having ascribable financial and/or tradeable value including but not limited to servers, cloud services, wallets, USB stubs and/or pen drives and/or other devices, CDs, DVDs, electromagnetic, optical and/or quantum media;

A.5 Banking, accounting and each and every paper or computer record scheduling or referring to such, including account numbers and names and all other identifying and access details, with guidance and explanation as to transaction and instruction entries, listings and references;

(each of the above referred to for ease of reference as a/the '**Disclosable Digital Entity**', collectively the '**Disclosable Digital Assets**').

B. The Access Methodologies

Disclose for each such **Disclosable Digital Entity** and for all **Disclosable Digital Assets** all data, techniques, methodologies, software, hardware, information and materials needed to identify, access, analyse, process, value, transfer, decrease or increase the value of, buy, sell, trade, store, deposit, maintain, report on and/or generally deal reliably and completely with each and every such **Disclosable Digital Entity**, including but not limited to:

B.1 Safe Deposit Boxes, Bank Accounts, Physical Storage Means, Hardware Wallets, USB Key Storage Devices, User IDs, Passwords, PIN Codes, Public and Private Encryption Keys, Security Tokens, Procedures or Techniques, Signing Protocols, Two-Factor Authentication Protocols, Devices and Materials;

B.2 All Relevant Trading, Storage and/or Other Exchanges Information;

B.3 Relevant Software and who developed it, test records, audits carried out, independent expert assessments as to its reliability, privacy and security, prevention of being compromised, completeness and correctness;

B.4 Anything signed by, or requiring signature by, a Digital Signature and/or any other written or non-written authorisation, verification or validation means or methodology; (individually, for ease of reference, the '**Access Entity**', collectively the '**Access Methodologies**').

C. Confirmation and/or Means of Repository and Access

C.a Disclose and Confirm whether or not any such **Access Entity** and/or all **Access Methodologies** are held by one or more **Trusted Third Parties** (e.g. bank, accountants, solicitors, Digital Repository*) and, if so, disclose all details of said one or more **Trusted Third Parties**, including but not limited to:

C.a.1 Full contact details – address, telephone number, email address(es), fax number;

C.a.2 Associated Access and Retrieval procedures, processes and protocols, including any security parameters or data involved (e.g. presentation of photo ID, passports, tokens, fobs);

C.a.3 Each and every responsible officer, agent and/or executive;

C.a.4 Physical Location, Directions, Opening Times and the like;

C.a.5 Reference Number(s), Repository Identification, File Titles and any other Descriptors;

C.a.6 All quantitative and qualitative data relating thereto.

C.b If any **Access Entity** and/or all **Access Methodologies** are **not** held by one or more Trusted Third Parties:

C.b.1 (i) Immediately deliver up the details of each such **Access Entity** and/or all **Access Methodologies** not so held to _____ (the '**Matter TTP**') [insert desired/proposed Thrusted Third Party e.g. bank, accountants, solicitors, Digital Repository*], without alteration, redaction, in complete and functional form and state so that the **Matter TTP** is able to gain, achieve, complete and/or generally deal reliably and completely with any and all analysis, reporting, operational and transactional access to each and every **Disclosable Digital Entity** and all **Disclosable Digital Assets**.

C.b.2 (ii) Provide along with such delivering-up a complete and detailed schedule of all things being so delivered-up.

D. Existing Assessments and/or Valuations of Digital Assets

Disclose for each such **Disclosable Digital Entity** and for all **Disclosable Digital Assets** any and all existing assessments and/or valuations and/or demands, notices or other assessments of liability for taxes and/or other investigations, analyses, appraisals, or estimations thereof including those carried out by, or on behalf of, or at the commission of, any tax and/or other fiduciary, state or regulatory authorities including but not limited to:

D.1 Privately or Publicly Appointed Lawyers, Accountants, Insurers and/or Other Investigators and/or Experts;

D.2 In the UK, HMRC;

D.3 In the USA, the IRS;

D.4 In Europe, any national, central or state or European Union fiscal or taxation entity;

D.5 Globally, any national, central or state or Regional or Inter-Governmental investigative, fiscal or taxation entity;

D.6 Any Law Enforcement agency or entity.

* Are there such things? If so, which, where? If not, should we not set one up...?
Possibly relevant, but maybe not:

<https://researchguides.library.wisc.edu/c.php?g=177944&p=1169874>
<http://www.rsp.ac.uk/start/before-you-start/what-is-a-repository/>

Dr Stephen Castell CITP CPhys FIMA MEWI MIOd
Chairman, CASTELL Consulting
PO Box 334, Witham, Essex CM8 3LP, UK
Tel: +44 1621 891 776 Mob: +44 7831 349 162
Email: stephen@castellconsulting.com
<http://www.CastellConsulting.com> <http://www.e-expertwitness.com>

Sunday, March 17th, 2019

© 2019 Dr Stephen Castell and *CASTELL Consulting*

March 19, 2019

I have a degree in Computer Science and I've started 3 companies in the technology and distributed systems software space.

I'd like to comment on the first three questions, the first following an observation stating that crypto assets are commodities and not securities:

"1. Are there factors in addition to those noted above that we should consider?"

2. What best practices exist for Platforms to mitigate these risks? Are there any other substantial risks which we have not identified?

3. Are there any global approaches to regulating Platforms that would be appropriate to be considered in Canada?"

My comment is as follows:

These token schemes are all centrally controlled, sometimes anonymously, and were foisted on the public so the people who created the tokens could make millions.

The tokens are presented as "coins" or "money" and the public is given promises that they can get rich selling the tokens to someone else at a higher price in the future, when the "coins" might be "worth millions".

At their core, they are all zero sum pyramid schemes. The only potential "value" they have is their utilization for illegal transactions.

One of the primary ways the people who created these tokens got people to use them is pushing use cases of smuggling, drug purchases, ransomware and the like, along with explaining that governments would not be able to track individual users or block transactions between parties.

Everyone who started a token scheme began by giving a large number of their tokens to themselves. They then attempted to create a market for the tokens where they could exchange those tokens for money by getting other people involved in their scheme by giving them tokens or allowing them to print their own tokens by utilizing their own computing resources. Many of these attempts have been successful.

The token systems themselves are generally controlled by 2 different parties.

The first centrally controlling entity is the small set of developers behind the software that runs the token scheme. They have the ability to block or reverse transactions, determine which token ledger is the true ledger, increase or decrease the number or rate of token issuance and change transaction parameters by changing the software that manages the token ledger and associated transaction processing.

The second controlling party is the party that runs the computers that actually process transactions. In Bitcoin, this is any group that controls a majority of hashing process power. They have the ability to block transactions, roll back transactions and double spend tokens.

The first group, the developers, are the true central control and they generally state that if the group processing transactions acts in a manner the developers don't like, the developers will roll back the transactions of the transaction processors and block the ones who act in a manner they disagree with.

I've never understood how any government can see any of these schemes as legitimate. None of them are any different from me selling people casino chips marked with my name, calling them money and saying they will go up in value because I will only issue 100 casino chips. Then I would process transactions between individuals, keeping a ledger of who owns what by not by name, print fake prices of the casino chips to show people the price going up and promote them as the "new form of money".

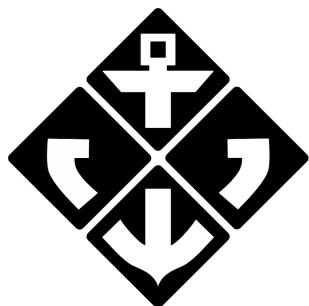
The technology behind the tokens is slow, wasteful and insecure.

Insecure because you must have trust in the transaction processors and developers who maintain the system.

Since, at their core, the systems are designed to facilitate illegal transactions and get people to buy worthless assets for money, the average person buying into these schemes will lose their money. As a zero sum game, it is impossible for them not to.

The best approach to dealing with all these schemes is to enforce the existing laws against running pyramid schemes.

Eric Swildens



Atlantic Blockchain Company

Author : [Keegan Lee Francis](#)
Date : April 9th 2019
Website : www.atlantic-blockchain.com

Consultation Questions

1. There are additional questions that have yet to be asked
 - a. Is “The Platform” jointly owned, or run, by anonymous individuals, as is the case with several Decentralized Autonomous Organizations
 - b. Does “The Platform” facilitate illegal activity or serve a **copyright resistant** use case?
 - c. Does “The Platform” implement any profit sharing mechanisms based on the performance and usage of the platform?
 - d. Does “The Platform” implement dividend based profits from other securities held, or traded on “The Platform”.
 - e. Does “The Platform” perform any locking mechanisms such as “staking”, “lending” or “collateralization”.

2. There are additional best practices not covered in the document.
 Exchanges should not allow fake volume to be generated. Although exchanges profit from the mechanism of creating fake volume (**90% of volume is fake**), it should not be a practice that is permitted on an exchange, or it should be openly transparent that fake volume is taking place. A common measure of success in a crypto project, is the amount of volume its associated asset has on exchanges. It is common for the project administrator to generate fake volume (at their own expense, and the profit of the exchange) in pursuit of generating sufficient “hype” to “moon” the price of their coin. Fake volume may be a signal for investors to buy an investment, identifying fake volume is one way to mitigate risk.

Overall, this section was well put together, and rather exhaustive in the list of risks.

3. Wyoming is currently leading the regulatory framework battle of digital assets in a number of ways. Firstly, Wyoming has initiated a new classification of digital assets,

creating three new classifications for assets based on blockchains. A “Digital Security”, or investment contract, a “Digital Consumer Asset”, or utility tokens, and “Virtual Currencies” such as Bitcoin, Ethereum, and Monero.

This is a sensible, and reasonable approach for the regulation of blockchain assets. Each of these assets can then acquire property rights for holding, trading, and managing these three asset classes. With respect to investment contracts, the digitization of securities would allow for more advanced lending schemas to take place. For example, an entity holding stock in a company could use this stock as collateral for additional lending, without needing to involve the company that the stock actually pertains to.

Wyoming has enacted bill [HB-70 Utility ICO bill](#) which exempts Utility Tokens from being classified as securities, which is a common barrier for blockchain businesses to overcome.

Wyoming accepts state tax in Bitcoin and other cryptocurrencies, all the while, waving property tax for entities mining Bitcoin.

Wyoming has four rather progressive and utilitarian bills that just recently came into law.

- **Special Purpose Depository Institutions:** This is to create institutions to service blockchain companies that cannot access traditional banking services. However, these institutions are prohibited from providing loans and must maintain 100 percent of its deposits in its reserves. They must also comply with applicable federal laws.
- **Commercial Filing System:** This blockchain bill authorizes the Secretary of State to create a blockchain-based commercial filing system for business entity registration submissions and reports, certain financial statements, and other similar types of filings.
- **Corporate Stock Certificate Tokens:** This bill allows businesses in Wyoming to issue ‘certificate tokens’ on a blockchain rather than stock certificates. This way, they can choose whether to list certified or uncertified blockchain shares.
- **Digital Assets – Existing Law:** This classifies digital assets by type (virtual currencies or digital securities) and specifies how each one should be treated in the context of existing commercial laws. Wyoming banks can also opt to become custodians of digital assets under the terms of this bill

4.

Standards:

- a. Multisignature wallets: The decentralized/multi ownership models for private keys. There are many schemas of “weighted” keys wherein a predefined threshold of “votes” are required in order to act upon a wallets funds. For example. A multisig wallet held between 3 people could be configured such that any 2 of the 3 individuals have the sufficient power to move/act upon the funds. Any 1 of the individuals would not have sufficient power to act upon the funds.

Furthermore, any one of the 3 aforementioned individuals, could also be a multi signature account, that requires approval/action from multiple parties. This is tiered ownership, and would enforce rigorous, and robust ownership models that are resistant to centralized control.

One example of a platform wherein these dynamic ownership models is possible, is within the EOS blockchain, where multiple key types exist, as well as the ability to create tiered and multi-weight ownership models.

In the example of the QuadrigaCX case of January 2019. One individual held 100% of the operational keys for the exchange, resulting in a multitude of problems when the untimely death of that individual occurred.

- b. A “Dead Man’s switch” is a mechanism that would allow for a living individual, who becomes deceased, to safely and securely transfer their responsibility to a trusted 3rd party. An “analog” version of this mechanism would simply be a will, containing the private keys for assets, that is sealed, held, and kept safe by a trusted 3rd party, such as Estate Lawyers. This analog approach may work for some situations, but may not work with systems that have dynamically changing keys. With systems that change keys on a regular basis, this would be infeasible to keep up with on an analog level. A digital approach would be required, and even recommended for owners of exchanges, and large amount of individuals’ investments.

I would draw attention back to the QuadrigaCX example of January 2019, to illustrate the practicality for such a system.

5. There exists platforms that fall under the category of a “DEX” or “Decentralized Exchange”. These are blockchains that do not have any form of centralized control, and therefore no centralized ownership. By definition, these exchanges lack an authority that speaks for, or represents, the ownership of all assets tracked, and held by the blockchain. Another term used to refer to these platforms is DA(O/C) (Decentralized Autonomous Organization/Company).

These platforms are built, and used by participants of the system. Any interaction taken by any of the users of the system are permanently recorded by the system, in the traditional blockchain like fashion. All assets that are created, destroyed, and traded on the platform are publicly accounted for at all times, perfectly, transparently, and without error.

6. The **benefits** of an exchange not assigning a private key to each and every users’ accounts are as follows:

- a. The platform and users avoid **blockchain** transaction fees for every transfer/exchange that takes place on their platform.
- b. The platform is centralized, and can therefore leverage the speed of a centralized system for facilitating trades and exchanges on the platform. This is crucial with financial markets where seconds and microseconds matter deeply within the markets. The users of the platform benefit from the speed at which the exchanges can take place.

The **challenges** that an exchange faces by holding crypto assets are as follows:

- a. There is an expectation for exchanges to keep up with blockchain events that result in “rewards”, “dividends”, or “additional profits”. These events include, but are not limited to, “Hard Forks”, “Airdrops”, “Dividends”. This becomes difficult for the exchange to manage, as additional programming and logic may be required to accurately and appropriately distribute the rewards that correspond to a user’s account balance.
 - b. Private key management inside an exchange is difficult as private keys are the aspect of a blockchain that determines the ownership of an asset. If an exchange has allowed for private key ownership by its users, then every exchange that takes place on the platform must happen on an address to address level (decentralized and slow), rather than an account to account (centralized and fast) level.
7. This is a very broad question. I am assuming the asker of the question is looking for any and all aspects upon which an experienced crypto-investor is evaluating an investment.
- a. Github Activity/Commits - This is a good indication of “progress” being made on the core underlying technology of a particular blockchain / coin / investment. This would be analogous to market activity, or development updates by a company traded on a regular stock exchange.
 - b. Social Media - Reddit, Facebook, Telegram, Discord, Twitter, LinkedIn. Are there founding members, or representatives, on these platforms? Do they respond quickly and appropriately to questions and critiques? Do they have a good history of entrepreneurship and have they conducted a history of successful business based or technical endeavours?
 - c. Founders / Team - Do they exist? Are they real people? Find the teams information, and make sure that the owner of the website did not put stock photos of “professionals” on the website. If they exist, is the team reputable?
 - d. What does the asset do - Does the asset actually solve a real world problem? Or is it a problem that can be solved better, without a blockchain. If the asset is for a blockchain that a centralized system can solve better, then the asset is worth \$0 and should be valued as such.
 - e. Does the asset produce dividends - It is now becoming more common for blockchain enterprises to build into their token, the ability to distribute a portion of the profits gained from the blockchain itself. The daily / monthly / yearly dividend amount should rightfully be factored into the equation as to the price of the asset.

- f. Does the underlying technology make sense - The underlying blockchain must be able to scale in order to handle the supposed use case. If the underlying technology does not scale well (cannot meet tx/s demand) then it doesn't matter how good the idea is, if mass adoption of the idea takes place, and the platform cannot handle the load, the entire system is virtually useless. Once a blockchain is started, it is technically difficult and complicated to "pitch fork" the assets to a different blockchain.
8. I am unaware of any reliable and unbiased pricing sources. There are plenty of sites that will tell you information about the asset, the team, and the market associated with the asset, but then fail to give a reasonable estimate of fair market value.
9. I believe it is reasonable for platforms to set and enforce their own rules. It is their system, they should be able to define their rules as they like, as long as they are compliant with their local regulations. Platform rules are some of the ways that platforms can differentiate themselves from their competitors. Some exchanges have games or competitions that take place on the platform where they give away prizes for particular actions taken by the users. (Ex. Referrals)
10. A Market Integrity Requirement should be that all reasonable effort should be given to identifying and preventing fake volume on the exchange. Such traffic is misleading and difficult for investors to interpret.
11. On private exchanges (exchanges owned by private companies) there does not exist a way for regulatory bodies to conduct surveillance on the exchanges that take place on the platform. There is no way to tell WHO is making the exchanges, only that the exchanges are taking place. Most exchanges have opened their "order books" through a public API (Application Programming Interface) for programmers to query and receive real time information about what trades are taking place on the network. This is the foundation for any and all "trading bots" that automated investors have implemented. The skills that are required for polling and analyzing this information is intermediate/advanced knowledge of any popular programming language such as JavaScript, Python, GoLang, etc, coupled with economic analysis tools.
12. A common strategy for trading crypto assets, is to base your trades off of secondary information such as the amount of people googling the word "bitcoin". In the past, there has been positive correlation between the price of Bitcoin and the volume of searches with the word "Bitcoin" in the query. The same methodology can be applied to search for trends in global social media platforms such as Reddit, Facebook, Twitter, and Instagram. This strategy is commonly referred to as identifying market "hype".
13. N/A

14. If the Platform is in possession of significantly large amounts of the asset that corresponds to the platform (example is Binance or BNB coin), then any large transfers and the details/conditions of such assets should be made publicly available as to inform users that there could be price fluctuations due to large amounts of such assets entering the marketplace.
If there exists mechanisms within platforms that allow for users to “set the price” or publish a “price feed” for a particular asset, then this information should be made publicly available as to guard against this privileged user manipulating the price in their favour. (example is BitShare with SmartCoins or User Issued Assets).
15. A platform is not able to manage conflicts of interest if there is no central aspect of authority or control. The best example of this is BitShares or EOS wherein they are defined as DAO's and lack any centralized authority. This opens up the opportunity for bad actors to take advantage of the lack of authority and manipulate sub-systems as they see fit.
16. Any and all insurances would be nice for an exchange to have, however, I don't anticipate these insurances being reasonably priced such that the exchanges would benefit from obtaining them. At the moment, cryptocurrency in general is dangerous, volatile, and towing a rather bad reputation as a safe-haven for hackers. Making an insurance policy for exchanges that exchanges actually want to purchase would be more trouble, and more expensive than it is worth.
17. Articulated in 16
18. Proof of distributed authority, Key Management Systems, & Dead Man's Switch.
Articulated in 4a, 4b.
19. There exists other models of clearing and settling crypto assets. I've spoken about several of the exchanges that make this possible. BitShares and EOS both make all trades and exchanges publicly accessible on a public ledger. Everything, including the account name (which does not necessarily disclose the identity of the account holder) is published on the ledger which is publicly available. The risk of such a system is it inherits some of the properties of blockchain technology, one notable property is that the exchange is permanent and irreversible, whereas with a centralized exchange, there is someone you can call (support staff) if something doesn't go the way you planned.
20. The risks are as follows:
 - a. Permanent - All transactions that take place on DLT's are permanent and irreversible. (Some exceptions exist)
 - b. Anonymous - All transactions that take place on DLT's are more or less completely anonymous, or difficult to ascertain the identity of the two parties.

- c. Identity Fraud - It is much easier to fraud your identity in a digital ecosystem, than that of a modern established securities exchange. Such an implication opens the door to money laundering and other financial crime.
21. Black Swan events are market crashes that cause unintended side effects. There exist coins that are referred to as “Collateralized Stable Coins” which are massively complex systems of collateral that back an asset. The underlying asset that collateralized the stable coin is what upholds the value of stable coins. If the underlying asset crashes significantly, then there is a risk that a cascade of smart-contract triggers are fired, executing large amount of clearings and settlements. **Collateralized Stable Coins are a modern phenomenon worth grasping fully, and completely.** Stable coins have massive potential and geopolitical implications for the disruption of modern currency, more so than Bitcoin. What Satoshi Nakamoto purposed in 2008, is not what Bitcoin is today. Bitcoin behaves more like a stock or commodity, much like digital gold, as opposed to its intended purpose, a peer to peer digital cash/currency. Bitcoin is slow, and volatile, which currency is not. Stablecoins made the advent onto the world stage in 2014, but didn’t hit mass adoption (in the cryptosphere) until 2017/18.
22. N/A

Consultation Paper 21-402 Proposed Framework for Crypto-Asset Trading Platforms Feedback

Addressed to:

- British Columbia Securities Commission
- Alberta Securities Commission
- Financial and Consumer Affairs Authority of Saskatchewan
- Manitoba Securities Commission
- Ontario Securities Commission
- Autorité des marchés financiers
- Financial and Consumer Services Commission (New Brunswick)
- Superintendent of Securities, Department of Justice and Public Safety, Prince Edward Island
- Nova Scotia Securities Commission
- Securities Commission of Newfoundland and Labrador
- Superintendent of Securities, Northwest Territories
- Superintendent of Securities, Yukon
- Superintendent of Securities, Nunavut

https://www.osc.gov.on.ca/en/SecuritiesLaw_csa_20190314_21-402_crypto-asset-trading-platforms.htm

https://www.bcsc.bc.ca/Securities_Law/Policies/Policy2/PDF/21-402_CSA_IROC_Consultation_Paper_March_14_2019/

1. Are there factors in addition to those noted above that we should consider?

In recent years we have seen a rise of Decentralised Exchanges (<https://www.tzero.com/> , <https://ripple.com/> , <https://client.wavesplatform.com> , etc.), Gateways (<https://tether.to/> , <https://xrpcharts.ripple.com/#/manage-gateway?base> , etc.), as well as “Non-Custodial Exchanges” (<https://shapeshift.io> , etc.).

It is important to distinguish between a Centralised Exchange (QuadrigaCX), a Decentralised Exchange (t0), a Non-Custodial Exchange (Shapeshift), a Custodial Wallet (Coinbase), a Non-Custodial Wallet (Blockchain.info), a crypto payment processor (BitPay), and a Gateway (Tether) and their roles in the cryptocurrency ecosystem. It is also important to note a high degree of cross-pollination in the space – Coinbase for example is a Custodial Wallet and a Centralised Exchange, BitStamp is a Centralised Exchange and a Gateway, Ripple is a Decentralised Exchange, a payment rail and a cryptocurrency network, etc. There are also solutions out there that integrate with external services (for example – a Non-Custodial Wallet might offer Shapeshift integration for easy conversion between cryptocurrencies).

All in all, there are a lot of services out there that don't resemble QuadrigaCX and have their own important considerations to keep in mind when attempting to create regulations for exchanges. It is important to consult with experts in the crypto space to understand the full ecosystem and how regulating one part of it might have negative impact on the others.

2. What best practices exist for Platforms to mitigate these risks? Are there any other substantial risks which we have not identified?

First, it is important to both secure users' crypto assets, as well as their fiat (CAD, USD, etc.) assets as well. At the moment, it is nigh-impossible for crypto exchanges to secure banking relationships in Canada. To my knowledge, both of the historical major Canadian Crypto Exchanges (QuadrigaCX, CaVirtEx) had to resort to third party payment processors, offshore bank accounts and deal with partners from the online gambling space that charge high processing fees. The same is true for other crypto businesses (ATM operators, etc.) – nobody is able to secure a bank account at any of the major banks due to their affiliation with the cryptocurrency space. If Canadian Cryptocurrency Exchanges and other businesses are to keep their client fiat deposits safe, they need to be able to access the Canadian banking infrastructure and keep their funds in Canadian banks without risking their accounts getting frozen. **The biggest unsolved problem in the crypto space is transacting with legacy banking space.**

Secondly, securing crypto funds can be a technical challenge, but it's not insurmountable. It can be compared to securing user records – you need proper procedures, safeguards and accountability. The use of cold storage multisignature addresses distributed between multiple parties is the first step. Even the basic 2-of-3 address guarantees the funds remain secure in case one party loses their keys, becomes malicious or the like. It is important for crypto exchanges to have a clear record of where the funds are kept, who has access to those keys (not necessarily publicly disclosed, but notarised in some way might be preferable), as well as have the proper procedures in place to ensure the keys don't get compromised.

Thirdly, the cryptocurrency space has a concept in place for ensuring unprecedented accountability – Proof of Solvency (<https://tpbit.blogspot.com/2016/01/full-proof-of-solvency-pondering-tether.html>). This approach has been widely discussed after the collapse of MtGox, but hasn't become the industry norm unfortunately. With this approach, Cryptocurrency Exchanges could create a mathematically verifiable proof that they do indeed hold enough funds to cover all of their clients' deposits. It does expose their balances to their competitors, but also gives insight to everyone else, allowing anyone to bring any discrepancies to public attention straight away.

Number four, there is a conceptual idea that has been proposed a long while back called Voting Pools (<https://tpbit.blogspot.com/2016/08/avoiding-bitfinex-scenarios-with-voting.html>). It is a schema where multiple Exchanges would come together and secure one another's funds. The set of exchanges would cross-audit one another and be responsible for counter-signing any outgoing transactions – one exchange acting by itself would not be able to move funds, even their own! Provided the exchanges were not colluding with one another (as one would expect from competitors), this would prevent any loss of funds should one exchange be compromised. Implementation of Voting Pools has so far only

been theoretical, and this schema might have issues dealing with traditional banking space, but in theory it should work pretty well for crypto assets.

3. Are there any global approaches to regulating Platforms that would be appropriate to be considered in Canada?

One approach that SHOULD NOT be emulated is the BitLicense (<https://en.wikipedia.org/wiki/BitLicense>) used by the New York State. That approach is so draconian very few cryptocurrency exchange would wish to apply for it. Similarly any cryptocurrency owner from the New York State is being hampered by its implementation, since any exchange servicing them, even if they are not located in New York State, have to go an extra mile to onboard them. Some cryptocurrency businesses opt to blacklist anyone from the New York State rather than try to comply with it. Implementing anything close to that in Canada would have disastrous effects on the Canadian cryptocurrency space.

4. What standards should a Platform adopt to mitigate the risks related to safeguarding investors' assets? Please explain and provide examples both for Platforms that have their own custody systems and for Platforms that use third-party custodians to safeguard their participants' assets.

First, a Platform needs to safeguard its fiat assets. This should be a problem that's not uncommon in non-cryptocurrency financial institutions, so not much needs to be added. That is, of course, provided the traditional banking sector will treat cryptocurrency platforms as they would any other businesses – something that's not a guaranteed in the current Canadian cryptocurrency world. Having access to high-quality banking from “the Big Five” should not be a problem for Canada's biggest cryptocurrency exchanges, but it has been in the past.

Given a proper banking is in place, the rest is a problem with some known solutions in the cryptocurrency space – Proof of Solvency (<https://tpbit.blogspot.com/2016/01/full-proof-of-solvency-pondering-tether.html>). With credible banking statement for fiat deposits, the Platform would need to prove its crypto holdings (very simple), and create a record of the amounts owed to all of their clients (a bit more complicated). The balances can be verified on regular basis to ensure ongoing liquidity.

Main drawback of this approach would be disclosing full internal balances to third parties. Some cryptocurrency exchanges might be fine with that, while others might wish to resort to trusted auditors keeping tabs on the accounts and recording any past audits in case they need to be checked.

Biggest problem that still remains unaddressed however is the question of who has access to the address keys. Ideally, you would have various key holders declare their ownership of the keys in a notarised fashion (declaring them publicly, while effective, might leave the key holders as targets). Provided there is enough redundant key owners to ensure the business remains functional in an event

of some owners losing access to their keys or those keys becoming compromised, and that those entities are known to some third party auditors, this should be enough.

Given all of these, there is no difference between the Platform managing their own keys or using a third-party custodian – only the party responsible shifts. You need the same safeguards either way.

5. Other than the issuance of Type I and Type II SOC 2 Reports, are there alternative ways in which auditors or other parties can provide assurance to regulators that a Platform has controls in place to ensure that investors' crypto-assets exist and are appropriately segregated and protected, and that transactions with respect to those assets are verifiable?

See previous answer on Proof of Solvency, private key distribution, etc.

6. Are there challenges associated with a Platform being structured so as to make actual delivery of crypto assets to a participant's wallet? What are the benefits to participants, if any, of Platforms holding or storing crypto assets on their behalf?

The main challenge comes from the Hot Wallet – Cold Wallet divide. Cryptocurrency exchanges want to keep some of the coins on hand to handle small-scale withdrawals fast, but need to keep the bulk of the deposits in a separate, more secure storage for safe keeping. Moving coins from the hot wallet into the cold wallet is simple, moving them the other way is always more risky – you are usually dealing with larger sums of money, having to deal with more secure transaction signing and a lot less automation of the process.

Benefits of the Platform holding its customers' assets mainly come with saving costs and increasing speed of trading. If the customer is a professional trader, they want to be able to trade rapidly with minimal costs. Having to move the coins each time a trade happens means paying on-chain transaction fees and having to wait long confirmation times. Currently, you can't achieve high-frequency, low-latency trading on a blockchain.

Moreover, holding multiple customers' assets allows the Platform to aggregate multiple trades easier and ensure even large orders can be cleared in a simple fashion without potentially triggering a lot of small, on-chain trades.

7. What factors should be considered in determining a fair price for crypto assets?

Traditionally, the fair price for a crypto asset is the current market rate on a given exchange or in aggregate. A lot of exchanges publish their market data via an API, and there are some aggregators of

multiple markets (most notable being <https://coinmarketcap.com/>). As long as the method for determining the price are known in advance and verifiable via an external API, it isn't really an issue.

8. Are there reliable pricing sources that could be used by Platforms to determine a fair price, and for regulators to assess whether Platforms have complied with fair pricing requirements? What factors should be used to determine whether a pricing source is reliable?

See previous question. In general, either using the spot price at a given exchange or taking a price from a third party API are used. The market data can be easily gathered and aggregated for any future audits as needed.

9. Is it appropriate for Platforms to set rules and monitor trading activities on their own marketplace? If so, under which circumstances should this be permitted?

No comment.

10. Which market integrity requirements should apply to trading on Platforms? Please provide specific examples.

No comment.

11. Are there best practices or effective surveillance tools for conducting crypto asset market surveillance? Specifically, are there any skills, tools or special regulatory powers needed to effectively conduct surveillance of crypto asset trading?

No comment.

12. Are there other risks specific to trading of crypto assets that require different forms of surveillance than those used for marketplaces trading traditional securities?

No comment.

13. Under which circumstances should an exemption from the requirement to provide an ISR by the Platform be considered? What services should be included/excluded from the scope of an ISR? Please explain.

No comment.

14. Is there disclosure specific to trades between a Platform and its participants that Platforms should make to their participants?

There are a few potential issues with a Platform trading with its participants.

First of all, there is insider knowledge. The Platform and a fair number of their employees will usually know well in advance any assets that will be listed on it, meaning they can trade on that knowledge

ahead of time. This is usually limited to really big players in the industry being able to sway the market (for example – world’s biggest exchanges listing some new cryptocurrency).

Secondly, the Platform does know about any cryptocurrency deposits that are taking place in advance of their customers being credited the amounts. For example, seeing a large amount of bitcoins being deposited into an exchange might signal a large sell order coming when that deposit is confirmed an hour later. This can give the Platform some time to trade with that knowledge before their client can create that sell order.

Similarly, there is a possibility of front running. An exchange, seeing a large order being put in could front run its own order to take a bit of profit from their customer.

Finally, there is an issue of fake volumes and no fee trading. It is possible for an exchange to trade on its own platform without charging itself any fees to either create fake volume, or try to play the market more efficiently than its clients.

If a Platform engages in any of those practices, those should be disclosed to their customers (if not outright forbidden).

15. Are there particular conflicts of interest that Platforms may not be able to manage appropriately given current business models? If so, how can business models be changed to manage such conflicts appropriately?

No comment.

16. What type of insurance coverage (e.g. theft, hot-wallet, cold-wallet) should a Platform be required to obtain? Please explain.

Ideally, full coverage of their liabilities to their customers, both in crypto and fiat.

17. Are there specific difficulties with obtaining insurance coverage? Please explain.

No comment.

18. Are there alternative measures that address investor protection that could be considered equivalent to insurance coverage?

Hot wallet theft could be mitigated by maintaining more than 100% balances in cold storage wallet. This would mean the exchange would have to be able to cover all of its liabilities using only its cold wallet by having its assets be greater than its liabilities.

19. Are there other models of clearing and settling crypto assets that are traded on Platforms? What risks are introduced as a result of these models?

No comment.

20. What, if any, significant differences in risks exist between the traditional model of clearing and settlement and the decentralized model? Please explain how these different risks may be mitigated.

The main problem with decentralised clearing, if done via the means of smart contracts at least, is that the assets might become irrevocably lost due to a software bug from the smart contract development or deployment (see Parity wallet for an example of what could happen - <https://blog.zeppelin.solutions/on-the-parity-wallet-multisig-hack-405a8c12e8f7>).

21. What other risks are associated with clearing and settlement models that are not identified here?

No comment.

22. What regulatory requirements, both at the CSA and IIROC level, should apply to Platforms or should be modified for Platforms? Please provide specific examples and the rationale.

No comment.

Piotr Piasecki

INVESTOR ADVISORY PANEL

May 13, 2019

The Secretary
Ontario Securities Commission
20 Queen Street West
22nd Floor, Box 55
Toronto, Ontario M5H 3S8
Fax: 416-593-2318
comments@osc.gov.on.ca

Me Anne-Marie Beaudoin
Corporate Secretary
Autorité des marchés financiers
800, square Victoria, 22e étage
C.P. 246, tour de la Bourse
Montréal (Québec) H4Z 1G3
Fax : 514-864-6381
Consultation-en-cours@lautorite.qc.ca

Victoria Pinnington
Senior Vice President, Market Regulation
Investment Industry Regulatory Organization of Canada
Suite 2000, 121 King Street West
Toronto, Ontario M5H 3T9
vpinnington@iiroc.ca

Consultation Paper 21-402: Proposed Framework for Crypto-Asset Trading Platforms

The members of the Ontario Securities Commission's Investor Advisory Panel (IAP) wish to thank the Canadian Securities Administrators (CSA) and the Investment Industry Regulatory Organization of Canada (IIROC) for this opportunity to comment on how regulatory requirements may be tailored for crypto-asset trading platforms (Platforms) operating in Canada.

The IAP is an initiative by the Ontario Securities Commission to enable investor concerns and voices to be represented in its rule and policy making process. In this capacity, we welcome the proposed regulatory framework for crypto-assets and the focus that has been placed on investor protection in key areas such as custody and verification of assets, price determination, market surveillance, systems and business continuity planning, conflicts of interest, crypto-asset insurance, and clearing and settlement.

The regulatory imperative in light of crypto-assets' uncertain nature

As the consultation paper notes, every crypto-asset is unique, with its own features, attributes, use and value. Consequently, it is difficult to determine whether all crypto-assets are securities. Yet even if a crypto-asset does not fall within the definition of a security, the investor's contractual right to the crypto-asset may constitute a security or derivative; and we believe many investors who trade crypto-assets hold them as if they were securities and would look to the CSA and IIROC if their investments went missing.

For this reason, the IAP fully supports the creation of a sound regulatory framework to govern the exchanges and marketplaces on which investors may trade crypto-assets. We believe it is incumbent upon securities regulators to fashion rules that help protect investors with this emerging asset class while also regulating these new types of marketplaces that are emerging.

We are mindful that overzealous regulation could, inadvertently, encourage these exchanges to go underground and thereby deprive retail investors of any protection and transparency. However, we believe an appropriate and proportionate level of smart regulation can be implemented that will allow innovative firms to succeed in their development stages while adequately protecting investors – and this, in turn, will serve to increase the confidence investors and other market participants have in crypto-assets and the Platforms.

Safeguards for investors

To accomplish these important goals, we strongly support the development of robust rules in the following areas:

Transparency and disclosure

There should be transparency and disclosure of key information so that investors know what they are buying and holding. Key information about each crypto-asset should be provided, including features, attributes, use, value, risk factors, and method of valuation. At the same time, key information about the platform also should be provided, such as operations behind a trade (including how orders are entered and executed and the applicable fees), the order and trade information for crypto-assets traded on the Platforms, and corporate governance.

This level of disclosure will help investors make better-informed decisions to determine:

- Whether crypto-assets are suitable investments compared to other investment vehicles;

- The investor's preferred crypto-asset(s), given the wide range of features, attributes, use, value and risk factors that are available; and
- The Platform that would be the most suitable place to conduct trades and store the assets.

A robust regulatory framework for custodians

The custodian of the asset(s) must itself be subject to a robust regulatory framework covering both custody and verification of assets. Custodians must be required to follow industry best practices for keeping assets secure, including:

- Maintaining a majority of the crypto-assets in offline cold storages;
- Stringent withdrawal protocols including fragmentation of private keys and quorum of designated individuals to transfer crypto-assets;
- Regular back-ups of key information;
- Appropriate operational policies and procedures around the technology that establishes checks and controls against various risks, such as insider theft and hacks; and
- Verification of assets and reporting by an independent third-party.

Protection from insolvency

Safeguards are needed to protect investors in case of insolvency of any of the parties to the transaction. Client assets must be segregated from the Platform's assets and provided with a layer of protection to ensure the client assets can be returned in case the Platform becomes insolvent. Also, in the event of insolvency, technology controlling custody of crypto-assets must allow appropriate parties to retrieve the clients' property.

Third-party verification

All Platforms must have appropriate operational policies and procedures regarding conflict of interest, fair access, insider theft, etc. Perhaps more importantly, independent third parties must provide verification of such internal processes and procedures.

Traditionally, the steps of a trade execution process have been divided among various parties, such as exchange/ATS, dealer, custodian, and clearing agency. One of the dangers with crypto-asset trading is that the Platforms are involved in all aspects of the trade and, therefore, a greater risk of delay in detecting insider fraud exists.

This concern is heightened by the fact that the Platforms generally do not need the majority of their crypto-assets to carry out their day-to-day operations. Instead, crypto-asset balances are often shifted from one user account to another user account, all

within the Platform's internal ledger. In other words, the balance does not actually move from wallet to wallet, but all transactions generally occur within the Platform's own wallets. In practice, this means that even if a Platform is missing crypto-assets, this fact may not be evident to an investor, as there would be no impact on the day-to-day operations of the Platform.

Introducing independent third parties into the process as verifiers will increase the probability of detecting insider fraud earlier. For example, auditors can verify that the assets are actually segregated and that proper controls and processes are being followed.

Regulatory approaches in other jurisdictions

The third consultation question asks whether there are other jurisdictions whose regulatory framework Canada should consider. With regard to crypto-assets, we believe Australia and Japan provide models worth examining, as follows:

Australia

It is our understanding that Australia imposes two different registration requirements for Platforms:

- If the Platform facilitates the trading of crypto-assets that are considered securities, the exchange needs a market license from the Australian Securities and Investment Commission.
- If the Platform converts fiat currencies into digital currencies or vice versa, it must also be registered with the Australian Transaction Reports and Analysis Centre, regardless of whether the crypto-assets are securities.

Obligations imposed on such Platforms include anti-money laundering requirements, customer due diligence, know your customer measures, reporting of suspicious and other reportable transactions, and record keeping.

Japan

To operate in Japan, Platforms must be registered with the Financial Services Agency. In addition, a self-regulatory body has been created called the Japanese Virtual Currency Exchange Association.

It is currently in the process of developing rules and regulations.

Various obligations imposed on Platforms in Japan include establishing security systems to protect information, providing information regarding fees and other terms to their customers, and segregating customers' crypto-assets from the Platform's crypto-assets. The Platforms also are required to have certified public accountants or accounting firms

review and verify the segregation of crypto-assets. We believe these robust regulatory requirements are worth considering, in the context of this CSA/IIROC joint initiative.

Conclusion

As the evolving crypto-asset space continues to involve new investors and other market participants, securities regulators must strive to follow international best practices and understand how technological changes and new innovations need to be regulated and incorporated into the securities regulatory framework.

This will require regulators to continually build knowledge and capacity to stay on top of technological innovation and understand its potential impact on investor outcomes and vulnerabilities.

Again, thank you for the opportunity to participate in this consultation. Please let us know if you require clarification of our comments or any further information.

Sincerely,



Neil Gross
Chair, Investor Advisory Panel

FAIR

Canadian Foundation *for*
Advancement *of* Investor Rights
Fondation canadienne *pour* l'avancement
des droits *des* investisseurs

May 13, 2019

The Secretary
Ontario Securities Commission
20 Queen Street West
22nd Floor, Box 55
Toronto, Ontario M5H 3S8
Fax: 416-593-2318
comments@osc.gov.on.ca

Me Anne-Marie Beaudoin
Corporate Secretary
Autorité des marchés financiers
800, square Victoria, 22e étage
C.P. 246, tour de la Bourse
Montréal (Québec) H4Z 1G3
Fax : 514-864-6381
consultation-en-cours@lautorite.gc.ca

IIROC
Victoria Pinnington
Senior Vice President, Market Regulation
Investment Industry Regulatory Organization of Canada
Suite 2000, 121 King Street West
Toronto, Ontario M5H 3T9
vpinnington@iroc.ca

RE: Joint CSA/IIROC Consultation Paper 21-402 Proposed Framework for Crypto-Asset Trading Platforms

FAIR Canada is pleased to offer comments on Joint CSA/IIROC Consultation Paper 21-402 proposed framework for crypto-asset trading platforms (“CP 21-402”) that is intended to establish a framework that provides regulatory clarity to platforms that facilitate the buying and selling or transferring of crypto assets (“Platforms”) to address risks to investors and creates greater market integrity.

FAIR Canada supports the proposed framework for the regulation of crypto-asst trading platforms as described in CP 21-402.

The proposed framework is based on the existing regulatory framework applicable to marketplaces and incorporates relevant requirements for dealers facilitating trading or dealing in securities. It is tailored to take into account the functions that may be performed by each Platform. Specifically, a Platform that brings together orders of buyers and sellers of securities and uses non-discretionary methods for these orders to interact is a marketplace. This may require registration of the Platform as an exchange, or if not as an alternative trading system (“ATS”). Certain derivatives requirements may also apply if a Platform trades assets that should be classified as derivatives. As noted in CP 21-402, “some Platforms are hybrid in nature and may perform functions typically performed by one or more of the following types of market participants: ATS, exchanges, dealers, custodians and clearing agencies.”

The proposed framework contemplates Platforms becoming registered as investment dealers and becoming IIROC dealer and marketplace members. This poses challenges and raises questions regarding IIROC’s capacity to surveil and supervise these Platforms if multiple applicants become registered. CP 21-402 states that a Platform will be required to provide fair prices, and asks what factors should be considered. This may be challenging with respect to cryptocurrencies that trade on multiple Platforms around the world, whose prices vary widely, and are very volatile.

FAIR Canada is supportive of the proposed framework to the extent that it thoroughly identifies risks and provides a robust framework of requirements that addresses the need for strict risk controls on markets in order to protect the interests of investors in crypto assets.

We thank you for the opportunity to provide our comments and views in this response. We welcome its public posting and would be pleased to discuss this letter with you at your convenience. Feel free to contact Ermanno Pascutto at 647-256-6693 / ermanno.pascutto@faircanada.ca or Douglas Walker at 647-256-6690 / douglas.walker@faircanada.ca.

Sincerely,



Ermanno Pascutto
Executive Director
Canadian Foundation for Advancement of Investor Rights

FAIR Canada is a national, charitable dedicated to putting investors first. As a voice for Canadian investors, FAIR Canada is committed to advocating for stronger investor protections in securities regulation. Visit www.faircanada.ca for more information.



May 13, 2019

Delivered Via Email

British Columbia Securities Commission
Alberta Securities Commission
Financial and Consumer Affairs Authority of
Saskatchewan
Manitoba Securities Commission
Ontario Securities Commission
Autorité des marchés financiers
Financial and Consumer Services Commission
(New Brunswick)

Superintendent of Securities, Department of
Justice and Public Safety, Prince Edward
Island
Nova Scotia Securities Commission
Securities Commission of Newfoundland and
Labrador
Registrar of Securities, Northwest Territories
Registrar of Securities, Yukon Territory
Superintendent of Securities, Nunavut

Delivered to

The Secretary
Ontario Securities Commission
20 Queen Street West
22nd Floor, Box 55
Toronto, Ontario M5H 3S8
comments@osc.gov.on.ca

IIROC
Victoria Pinnington
Senior Vice President, Market Regulation
Investment Industry Regulatory Organization
of Canada
Suite 2000, 121 King Street West
Toronto, Ontario M5H 3T9
vpinnington@iiroc.ca

Me Anne-Marie Beaudoin
Corporate Secretary
Autorité des marchés financiers
800, Square Victoria, 22e étage
C.P. 246, tour de la Bourse
Montréal (Québec) H4Z 1G3
consultation-en-cours@lautorite.qc.ca

Dear Sirs/Mesdames,

**RE: Joint CSA/IIROC Consultation Paper 21-402 Proposed Framework for Crypto-Asset Trading
Platforms**

We are writing in response to CSA Consultation Paper 21-402. We appreciate the opportunity to comment on this topic. Our comments are limited to a discussion of why we believe IIROC should oversee crypto-asset platforms. We feel those directly involved in crypto asset platforms are best to speak to the consultation questions.

Investors view crypto-assets as an investment. The Bank of Canada Staff Analytical Note – Bitcoin Awareness and Usage in Canada: An Update¹ noted that 58% of individuals surveyed viewed Bitcoin as an investment. Investors have approached our advisors asking if we can trade cryptocurrencies for them. It is reasonable for investors to expect crypto-assets to be regulated or sold by investment dealers.

We support the CSA & IIROC's efforts to regulate crypto-asset platforms because the markets for crypto-assets in Canada are effectively not regulated. Investors can be easily confused because the securities markets are regulated but crypto assets are not. Investors can incorrectly believe their assets are protected by CIPF or CDIC. Investors may also believe their assets are held in a secure fashion, when there is currently no such requirement. This creates an environment where investor confidence and protection can deteriorate.

The approach taken by the CSA and IIROC is the best approach for investor protection. IIROC Dealer Member rules include custody rules that ensure assets are held in a secure location or appropriate insurance or capital is retained. The CSA and IIROCs approach will ensure crypto assets are held in a safe manner.

The one comment we have regarding the consultation questions is that it would be best for custody requirements and internal control reporting requirements to remain as is. Crypto-asset custodians are now able to obtain assurance over their internal controls² which will help align current custody rules with the realities of crypto-assets. Ensuring client assets are secure is the most important aspect of regulating crypto assets.

If you have any questions or further inquiry, please feel free to contact us.

Sincerely,
Jason Jardine, CPA, CA
Manager, Regulatory & New Initiatives
Leede Jones Gable Inc.

¹ <https://www.bankofcanada.ca/wp-content/uploads/2018/07/san2018-23.pdf> - page 18

² See <https://www.coindesk.com/crypto-custodian-bitgo-one-ups-gemini-with-advanced-security-exam>

May 14, 2019

CSA Consultation Paper 21-402:

Attention:

The Secretary
Ontario Securities Commission
comments@osc.gov.on.ca

Corporate Secretary
Autorite des marche financier
Consultation-en-cours@lautorite.gc.ca

Victoria Pinnington
SVP IIROC
vpinnington@iiroc.ca

cc.

Vic Fedeli
Minister of Finance
Government of Ontario
vic.fedelico@pc.ola.org

Bill Morneau
Minister of Finance
Government of Canada
bill.morneau@parl.gc.ca

Proposed Framework for Crypto-Asset Trading Platforms

“The Future Canadian Framework for Digital Assets Needs to be a Federal Government Responsibility”

The initiative of the Canadian Securities Administrators (CSA) and Investment Industry Regulatory Organization of Canada (IIROC) to issue the 21-402 Consultation Paper on the **Proposed Framework for Crypto-Asset Trading Platforms** is a welcome and professional step to ensure Canada remains globally competitive in the new era of digital assets. For this global initiative to be timely, competitive and successful there needs to be an expansion of this project under a Government of Canada mandate with an appropriate funding budget.

The Canadian public capital markets have existing regulatory and technology stacks that took many years to develop and refine into successful operations. These regulations and software systems allow Canadian registered investment dealers and public stock exchanges to be innovators in creating, financing and trading new investment opportunities in all economic sectors including emerging growth areas such as cannabis, esports and blockchain.

The Canadian capital markets operate within a relatively closed system based on Canadian dollars using compatible proprietary software systems that are integrated with the Canadian Banking system. These

systems continue to be automated and optimized and are expected to formidable competitors with many aspects of the new era of digital assets.

There is direct potential competition between of existing capital markets and banking systems and the new era of global digital assets. To nurture innovation a complete “blue sky” review of how Canada can be a global leader in digital assets is recommended. Digital assets creation and trading through the global internet will likely be as significant as the global trade of hard assets and products in the future.

The 21-402 Consultation paper provides useful questions on key areas for additional research based on the existing systems. Each of these questions is worthy of creating a task force of specialists that can recommend possible best practices.

A concern is the CSA and IIROC should not be the regulated authorities to lead the digital assets initiative. The CSA and IIROC can be important contributors to the discussion, but a federal framework, and not provincial securities regulators and may provide broader and more timely leadership on this issue.

It is noted that Singapore has chosen to develop regulations under the authority of the Monetary Authority of Singapore. The Bank of Canada has also conducted extensive research on digital assets from the perspective of applications with fiat currencies. Indeed, many believe that the digital asset marketplace will only truly succeed when government backed digital currencies are available to complete transactions.

It would be a bold stroke for Canada to become the first G7 country to issue a fully backed digital currency using the latest generation of technology. Just as the CSA has created a regulatory sandbox, perhaps the Bank of Canada should launch a digital currency sandbox. A test phase where perhaps \$1 Billion in digital Canadian dollars are issued to qualified investors to allow a new era of innovation for Canadian digital assets and new business models.

Canadian leadership on bold global topics has recent precedent. Many would say the Cannabis Act developed by the Canadian government has sparked a long overdue end to global prohibition on a therapeutic plant that has many beneficial medical claims and may be less toxic than alcohol.

The lawyers and policy advisors can discuss jurisdictional issues and develop assigned responsibilities for different aspects of digital assets global economy. The visionary goal will be to create the **Digital Assets Act of Canada** to define and attain best global practices for digital assets both from a technology and regulatory aspect.

Appropriate federal government budgets can then be assigned to create the **Digital Asset Act of Canada** best practices template for Canada and potentially the world. At this time the CSA, IIROC and provincial regulators all have limited resources and expertise and should remain focused on optimizing existing jurisdictional systems.

A federal taskforce to address all the Digital Assets issues would likely be more focused, better funded and better able to interact with other global leaders than the CSA coalition and the IIROC SRO that is funded by an existing subset of private Canadian registrants in the capital markets ecosystem. Developing new federal legislation can utilize existing principles but also consider new approaches to regulation.

To summarize, the intent and questions raised in the CSA 21-402 Consultation Paper are appropriate. It is however the view of the author that the regulatory authority and limited resources of the CSA and IIROC should not be utilized to develop Digital Assets best practices.

Federal task forces should be established to develop best practices with the possible goal of creating new legislation for the Digital Asset Act of Canada. As appropriate assigned representatives from the CSA and IIROC can provide independent expertise but the CSA and IIROC should not have jurisdictional authority.

A case could be made that registrant funded CSA and IIROC should not even consider assuming the liability risk of developing standards for globally traded digital assets.

These comments are the personal views of the author based on over 30 years of experience in all aspects of the buy, sell and corporate dimensions of the capital markets including senior roles with IIROC Investment Dealers and Canadian banks.

Best Regards,

James S. Hershaw
CFA MBA BSC
Director Capital Markets & CCO
Crowdmatrix (Exempt Market Dealer)
416-420-9122
sandy@crowdmatrix.co



BRANE CAPITAL

Brane Inc.

Info@Brane.Capital
(416) 500-2477
Ottawa / Toronto

The Secretary
Ontario Securities Commission
20 Queen Street West
22nd Floor, Box 55
Toronto, Ontario M5H 3S8 Fax: 416-593-2318
comments@osc.gov.on.ca

Me Anne-Marie Beaudoin
Corporate Secretary
Autorité des marchés financiers
800, square Victoria, 22e étage
C.P. 246, tour de la Bourse
Montréal (Québec) H4Z 1G3
Fax : 514-864-6381
Consultation-en-cours@lautorite.qc.ca

IIROC
Victoria Pinnington
Senior Vice President, Market Regulation
Investment Industry Regulatory Organization of Canada Suite 2000,
121 King Street West
Toronto, Ontario M5H 3T9
vpinnington@iiroc.ca

May 14, 2019

To Whom It May Concern:

Re: Joint Canadian Securities Administrators/Investment Industry Regulatory Organization of Canada - Consultation Paper 21-402 - Proposed Framework for Crypto-Asset Trading Platforms

We would like to thank the Joint Canadian Securities Administrators (CSA) and the Investment Industry Regulatory Organization of Canada (IIROC) for preparing the Proposed Framework for Crypto-Asset Trading Platforms and for inviting industry stakeholders to participate in this process.



Brane Inc. is a Canadian-based fintech company focused on blockchain technology and digital asset custody. We are developing products and solutions that will make this technology accessible, secure and useful for the global investment community.

We have two business divisions: (1) digital asset custody services, and (2) staking and validation activities on blockchain networks that rely on proof-of-stake consensus protocol, commonly referred to as PoS mining. Founded almost two years ago, through our experience with our PoS mining division, we have come to understand custodianship and its related issues. Accordingly, we have developed highly effective, operating custody solutions appropriate for institutional investors. Custodianship has grown to become our primary business focus, and our answers are from the perspective of this line of business. However, we also believe that our answers are equally applicable from the perspective of our PoS mining division.

We cannot provide comments on ALL the questions as we are not necessarily positioned to provide insight in certain areas, such as those relating to trading activities, self-dealing, market making and clearing. In these cases, we cannot give meaningful answers, however, we will have some overarching comments to make. Our answers are from the perspective of our custody services business – that of the custodianship of digital assets (including crypto assets).

General comments:

We appreciate the extent to which the CSA and IIROC have provided guidance and the consideration they have given to crafting Consultation Paper 21-402 (the ‘Paper’), particularly with respect the questions being asked, and we very much appreciate the opportunity to respond.

There is a common theme throughout the Consultation Paper that the risks associated with Crypto-asset Trading Platforms (‘Platforms’) “... are not entirely different than those applicable to other types of regulated entities such as marketplaces and dealers”. This would tend to support the overall position of the paper that existing regulatory requirements may be tailored for Platforms. This is a position with which we strongly agree. We believe that, in most cases, the existing regulatory framework can be extended and applied to Platforms and other industry participants in most jurisdictions.

We do, however, wish to point out that there are additional risks, not addressed within the paper, that are applicable to crypto assets and related blockchain technology. These risks are not specific to Platforms but are applicable to the safeguarding of all crypto assets. We refer to these risks as follows:

- *Centralization Risk* – private keys ensure absolute security on the blockchain, but they *also centralize the risk of a security failure*.
- *Rapid/Binary Outcomes* – if a private key is compromised, related crypto assets can be transferred immediately and can never be recovered.



- *Failure persistence* – unlike networks, for which security can be restored after a hack, security of compromised private keys can never be reinstated. Mistakes and breaches will haunt users forever.

This risk landscape is less forgiving than anything that is currently regulated or that regulatory bodies have ever seen. In the context of digital asset custody, they combine to form what we refer to as “operator risk”. Blockchain technology can provide high levels of cybersecurity, however the centralized nature of private key security results in the potential for a single point of failure. Platforms, and almost all other industry-related entities, ultimately ensure that private keys can be reconstituted by entrusting one individual or functional area (such as the IT department) or systems component (such as a designated HSM) with access to all private keys. Should the operator fail, as with Quadriga CX, or the security infrastructure be breached, as has happened a number of times over the past decade, assets will suffer total loss and be rendered irretrievable. The manner in which Platforms presently operate amplifies operator risk and it is our opinion that regulators should take steps to ensure that Platforms minimize or eliminate operator risk, to protect the interests of investors.

We suggest that, because of these risk considerations, existing best practice processes and regulations that govern capital markets today need to be applied in the context of cryptoasset trading Platforms. This would include segregation of assets and duties, regular audits, obtaining appropriate and sufficient insurance coverage, transparent reporting and compliance with applicable regulations. While it is important for regulators and industry participants to comprehend what is new about this technology, consideration should initially be given to understanding what existing rules and best practices can be applied, and how, to entities working with this new asset class.

We expect that the trend towards decentralization initiated by the adoption of blockchain technology and crypto assets certainly will result in an amplification of risk (financial and otherwise) layered on top of a diffusion of accountability. Tracking all of the risks and accountability will become more and more difficult unless rules and guidelines are well developed now. Without such guidelines, identifying clear delineation of responsibilities will become very difficult – making the mitigation of related risks nearly impossible over time.

Specific Answers and Comments to Questions Posed in the Consultation Paper:

PART 2 – Nature of crypto assets and application of securities legislation

1. Are there factors in addition to those noted above that we should consider?

We believe that it will be in the best interests of investors to prohibit pooled crypto assets or ‘floats’. Most Platforms pool assets, citing reasons of practicality and expense. The recent hack of the world’s largest Platform – Binance – demonstrates the vulnerability of participants’ assets when such concessions are made. In this instance, the Platform’s entire hot wallet of Bitcoins, worth over \$40 million, was stolen, facilitated in part by the pooling of client crypto assets.



More generally, we recommend that control and custody of crypto assets be clearly defined. For example, what the custodian does with those funds must be tightly controlled and clearly delineated.

At present, most Platforms provide, or plan to provide, a number of services related to the trading of crypto assets, including acting as an ATS, clearing and settlement, price determination and custodian. Given the risks we have highlighted above, particularly with respect to that of operator risk, we suggest that the combination of all of these functions present conflicts of interest. In order to clearly delineate fiduciary responsibility, we recommend that the provision of all crypto asset trading market related activities in a single entity, or group of related entities, be prohibited and, in particular, we recommend that Platforms should not be permitted to conduct custody services of crypto assets.

Investors in the crypto asset space should be concerned with the concentration of risk over time in entities that, perhaps, could be classified as “too big to fail”. As traditional assets become “tokenized” and crypto assets become more commonplace as mediums of exchange, the failure of any one entity that is permitted to operate as “all things to all people” could be catastrophic to a broad spectrum of the investing public and could impact those who have no interest in, nor any direct exposure, to this asset class. Restricting potential fiduciary conflicts of interest should mitigate this exposure.

We highlight the special nature of separate custody as it clarifies to whom the custodian has fiduciary responsibility. Traditionally, custodianship of client assets invested with registrants and/or investment funds has been provided by qualified and, in the case of investment funds, independent custodians (as defined in NI 31-103 and NI 81-102). Crypto assets should likewise require involvement of a qualified and independent custodian in the provision of that service (either as a qualified custodian itself, or through partnership with one).

PART 3 – Risks related to Platforms

2. **What best practices exist for Platforms to mitigate these risks? Are there any other substantial risks which we have not identified?**

Of the ten risks noted in the Paper (pp 4-5), we highlight the first three and the last (addressing safeguarding of assets, inadequate policies and procedures, investors’ risk of loss due to insolvency, and inadequate system resiliency and security controls) in our response. We believe that there are a number of ERMs and ISMSs that are respected currently that provide models for application in the space today.

Mature processes and procedures exist today for traditional markets that are equally applicable to Platforms – such as ERM frameworks, ISMSs, control frameworks (COSO and COBIT), etc. – and should be mandatory for such Platforms.



For example, the standards promulgated by the International Organization for Standardization ('ISO') and National Institute of Standards and Technology ('NIST') with respect to cybersecurity frameworks and ISMSs are well developed and are applicable to systems and processes used by Platforms. We suggest that any participant in the crypto asset space be independently certified under one or more of these standards.

As already noted, above, we agree with the statement on page 4 that, for Platforms, "... the risks are not entirely different than those applicable to other types of regulated entities such as marketplaces and dealers". We also highlight the additional risks that we previously described. In addition, we believe that these unique technology-related risks significantly amplify the risks the risks noted in the Paper in the context of Platforms.

We also draw attention to the additional risk of "operator risk" with respect to Platforms. Even if Platforms take reasonable steps to address system resiliency, integrity and security controls, most process and system-based solutions will retain an element of centralizing operator risk, in that some individual, or small group of individuals, within the Platform's organization will retain the ability to reconstitute private keys that would permit access to client funds or accounts. This is particularly true of HSM-based solutions, which are primarily used by Platforms in their operations. Although this can expose crypto assets to loss through fraudulent or criminal actions, it also exposes participants to the risk of loss in other ways, such as the recent failure of Quadriga CX, in which private keys were lost altogether.

We believe that, in order to properly safeguard participants' crypto assets, Platforms should not be permitted to provide custody services to participants if they also provide a platform of exchange of such crypto assets.

PART 4 – Regulatory approaches in other jurisdictions

3. Are there any global approaches to regulating Platforms that would be appropriate to be considered in Canada?

We agree with the statement (pg 6) that "... the existing regulatory requirements will apply to regulate Platforms within those jurisdictions." Having said that, it is our opinion that the critical consideration when applying these regulations is the intent of both the Platform and its participants. Accordingly, sweeping regulations – such as Order 2019 in Malaysia which specifies that all digital currencies, tokens and crypto assets be classified as securities – are too broad to be considered in this fashion in Canadian (and other North American) markets. For example – Starbucks accepting crypto payments – should not be a regulated transaction.

Clearly Canadian regulations will be influenced, in part, by actions taken in the United States, particularly by the SEC. While not perfect, the recently re-tabled Token Taxonomy Act of 2019 is an example. We do not, however, recommend that Canadian regulators adopt a "wait and see" approach as that could very well result in unnecessary delays in the development of a domestic regulatory approach with



respect to Platforms. We encourage the CSA, IIROC and other Canadian regulatory bodies to continue to lead the development of a regulatory and oversight framework.

PART 5 – The Proposed Platform Framework

- 4. What standards should a Platform adopt to mitigate the risks related to safeguarding investors' assets? Please explain and provide examples both for Platforms that have their own custody systems and for Platforms that use third-party custodians to safeguard their participants' assets.**

We encourage the development of verified ERMs, ISMSs, and financial and systems controls – including audit oversight and reporting (such as SOC 1 and SOC 2 Type I and Type II reports) – regardless of the use of self-custody or 3rd party custodians. In either case, the custodian at a minimum should be ISO 27001 - and ISO 27017 certified if cloud-based technology is being applied. Additional certifications should also be considered, such as NIST (minimum Level 3).

- 5. Other than the issuance of Type I and Type II SOC 2 Reports, are there alternative ways in which auditors or other parties can provide assurance to regulators that a Platform has controls in place to ensure that investors' crypto-assets exist and are appropriately segregated and protected, and that transactions with respect to those assets are verifiable?**

We believe that it is appropriate for regulatory authorities to require SOC 1 and SOC 2 (Type I and II) reports of Platforms and custodians. With respect to the scope of SOC 2 reports – regulators will need to be aware of the scope of the SOC 2 reports being prepared and ensure that such scope is appropriate in all cases. As such, it would be prudent for regulators to either establish minimum scope requirements or review the scope proposed by a Platform on a case by case basis.

We anticipate and encourage the development of industry best practices. This would address full documentation and stringent testing of systems and processes. At Brane Inc., our entire design approach to systems engineering is rooted in risk mitigation and regulatory compliance, and the application of industry-leading solutions for processes and systems. However, simply developing processes and systems is insufficient from the perspective of stakeholder requirements; the safety and security of these systems must be demonstrable. Independent certifications and SOC 2 reports are two means by which assurance can be provided, but additional approaches should also be used. A potential example of an additional approach, which we use, is the application of “formal verification” which is used for software and hardware in certain industries (such as aerospace and military). In this context, formal verification proves (or disproves) the correctness of intended algorithms underlying a system or automated process using formal mathematical methods and it is helpful in proving the correctness of systems such as cryptographic protocols. We encourage the adoption of formal verification



methods by the industry to provably demonstrate the effectiveness of internally developed systems and processes.

Any industry oversight and self-regulation will take time to mature. It may therefore be necessary for regulators to establish minimum scope standards – to minimize the risk of industry-led establishment of best practices becoming insufficient. A potential example is the pervasive use of HSMs (hardware security modules) across the industry. HSMs are very secure and have been used for years in traditional banking services, but they cannot be used to manage risk nor distribute it in any way, leading to the operator risk we have described above. The previously mentioned hack of Binance involved the theft of API keys, underscoring the weakness of HSMs as a custody tool. HSMs may be appropriate for lower value, high volume-high speed transactions on which the storage of information is ephemeral but they are not appropriate for the long-term storage of high value crypto assets.

Functionality inherent in blockchain technology may be of assistance to regulators. All transactions utilizing Platforms are completed “on chain” – that is the transaction, including the wallets involved, are recorded on the blockchain. This permits regulators to monitor directly all transactions “real time” as they occur, rather than relying on compliance with any reporting regulations. Certain blockchain networks that support the use of smart contracts could permit the active participation of regulators to enforce compliance with regulatory requirements as transactions occur (rather than monitoring the actions of exchanges and traders after the fact via compulsory reporting). The technology required to support this is not yet fully mature, but it is an approach the regulators should be considering as the framework is developed.

6. Are there challenges associated with a Platform being structured so as to make actual delivery of crypto assets to a participant’s wallet? What are the benefits to participants, if any, of Platforms holding or storing crypto assets on their behalf?

We are not in a position to comment on the first part of this question, although we support delivery of crypto assets to participants’ wallets. Although it is possible that trading of cryptocurrency could occur on chain only on a P2P basis, this approach is not presently practical and lacks any degree of oversight. Regulatory oversight of Platforms would provide necessary governance, oversight and protection for investors.

With respect to the second part of this question, we believe that self-custody on the part of Platforms is potentially dangerous on an institutional scale, due to operator risk and the unique technology risks noted previously. As a minimum, Platforms that wish to store crypto assets on behalf of participants should be required to comply with custodian requirements that ensure custodianship is undertaken by qualified custodians, utilizing acceptable controls and processes, and which do not allow for pooling of assets.

We reiterate our previous comment that permitting Platforms to be all things to all participants provides them with too much power today and sets up the creation of a



high degree of systemic risk in the future as crypto assets become more prevalent as a medium of exchange.

We have no specific comments with respect to Questions 7 through 12 inclusive.

- 13. Under which circumstances should an exemption from the requirement to provide an ISR by the Platform be considered? What services should be included/excluded from the scope of an ISR? Please explain.**

We do not foresee a circumstance in which an exemption from an ISR would be appropriate or should be permitted. As we commented previously, the establishment of the scope of the ISR requires careful consideration on the part of regulators but should – at the minimum – consider and include normal industry best practices and the unique risks we have discussed throughout our response, particularly operator risk.

We have no specific comments with respect to Question 14.

- 15. Are there particular conflicts of interest that Platforms may not be able to manage appropriately given current business models? If so, how can business models be changed to manage such conflicts appropriately?**

As we have noted throughout this response, we believe that there are several potential conflicts of interest with which Platforms will have difficulty managing given current business models. This difficulty derives from operator risk and is a primary reason for our recommendation that Platforms be denied self-custody of participants' crypto assets. We have further discussed these conflicts of interest in the "General comments" section, above and in our response to Question 1.

- 16. What type of insurance coverage (e.g. theft, hot-wallet, cold-wallet) should a Platform be required to obtain? Please explain.**
- 17. Are there specific difficulties with obtaining insurance coverage? Please explain.**

We recommend that full crime insurance coverage that addresses all fiat funds and crypto assets, regardless of the method of storage, be required. Platforms and custodians that operate in a transparent manner and with good oversight should be capable of obtaining full crime coverage.

We, as a custodian, have not had particular difficulty obtaining crime coverage however we can comment that the market for underwriting the risks associated with crypto assets is limited and some underwriters' understanding of the technology and the industry remains limited.



18. Are there alternative measures that address investor protection that could be considered equivalent to insurance coverage?

While it should not be considered equivalent to insurance coverage, the maintenance of participants (and Platform) crypto assets across multiple wallets distributes the related risk and responsibility of security – reducing the amount of insurance coverage required and making insurance coverage more readily obtainable.

19. Are there other models of clearing and settling crypto assets that are traded on Platforms? What risks are introduced as a result of these models?

Similar to the key points discussed throughout our response, all models of clearing and settling crypto assets presently utilized by Platforms introduce a centralized point of failure – covering ownership, settlement, price discovery, and safekeeping. Permitting Platforms to continue to conduct all the services they presently provide could result in future systemic risk.

20. What, if any, significant differences in risks exist between the traditional model of clearing and settlement and the decentralized model? Please explain how these different risks may be mitigated.

While Platforms are better able to comment on the significant risk differences, we believe that, over time, settlement will most likely trend towards on-chain settlement only as crypto assets become more readily accessible and assets regularly used, resulting in a natural mitigation of clearing and settlement.

We have no specific comments with respect to Questions 21 and 22.

We encourage the CSA and IIROC to continue to engage with members of the industry as it develops regulatory and legislative guidance.

We would be happy to provide additional information or answer any questions that you might have in relation to our submission.

Yours truly,

T. Paul Rowland, CPA, CA,
CPA (Illinois), CGMA

Chief Financial Officer & Corporate Secretary

May 14, 2019

British Columbia Securities Commission
Alberta Securities Commission
Financial and Consumer Affairs Authority of Saskatchewan
Manitoba Securities Commission
Ontario Securities Commission
Autorite des marches financiers
Financial and Consumer Services Commission (New Brunswick)
Superintendent of Securities, Department of Justice and Public Safety, Prince Edward Island
Nova Scotia Securities Commission
Securities Commission of Newfoundland and Labrador
Superintendent of Securities, Northwest Territories
Superintendent of Securities, Yukon
Superintendent of Securities, Nunavut

To Whom it May Concern:

**Re: Consultation Paper 21-402 Proposed Framework for Crypto-Asset Trading Platforms
Feedback**

As you may be aware, 4C is planning to establish a clearing agency, which would operate as a central counterparty and depository, for certain digital assets (including but not limited to crypto-currencies) and approved blockchain-based security tokens for Ontario-based participants. Omega Securities Inc., an existing alternative trading system, is working with 4C and intends to offer a regulated marketplace on which Ontario-based investment dealers and approved institutions could trade such investments.

With this background, the following are our comments on the above consultation paper.

1. We are very supporting of the regulators' initiative with this consultation paper in order to obtain marketplace feedback on a regulatory framework for crypto-asset trading platforms.
2. We are also encouraged to see the CSA and IIROC working together, as we think that the solution for the marketplace needs to include all of the regulators.
3. A regulatory framework is welcomed but it may take some time to formalize. In the meantime, in order to foster innovation in the digital asset space, we encourage the CSA and IIROC to engage in active dialogue with market participants and be willing to grant exemptions where appropriate in the meantime.
4. We think the regulatory frameworks for trading platforms that custody client assets and those that simply match orders should be different. Capital adequacy requirements for trading platforms should also be considered with care, and should be modest where client assets are not being custodied.
5. The CSA paper talks about creating "tailored regulatory requirements" for platforms that are determined to be marketplaces – but fails to provide details on how this tailoring will apply. We would encourage the CSA to release further information with respect to, for example, which parts of NI 21-101 should apply and which should not.
6. We would like the regulators to provide guidance with respect to expected timelines regarding when the framework is expected to be established, in order to provide clarity to the marketplace.

7. Regarding your consultation Question 1 – We suggest you consider who is the counterparty to the transaction. Responses could be, among others, the platform, another client and/or a central counterparty. The reply may well drive the appropriate regulatory model.
8. Consultation Question 2 – Consider the concept of a central information processor similar to ATS rules for order and trade transparency. Best practices for dealers and marketplaces are different. So this will depend on whether or not the platform is holding client assets or simply matching trades.
9. With respect to SOC reports, we think SOC II Type I reports would be appropriate for initial operation and SOC II Type II reports for ongoing operations after an initial period of say, one year. Exemptive relief may also be appropriate in the early days. It should also be clarified that the requirements for a SOC report and an ISR under the marketplace rules are the same. Having to do 2 separate reports makes little sense.
10. Pricing – Pricing will be market and liquidity driven. Pricing sources will also depend on the type of trading platform being operated and the business model. For example, we do not intend on using a third party pricing source. We intend to have subscribers who will have their own pricing sources and be able to establish quality prices in our systems. However, a platform going direct to retail may need to have a feed to determine appropriate levels of pricing. What is a reliable source? This is an open question in the markets. This area certainly requires more thought and consideration from market participants. We are hopeful that Omega's digital asset marketplace will become a source of quality pricing information.
11. We are supportive of leveraging IROC's market surveillance infrastructure, but market participants such as Omega and/or 4C may wish to also perform this role and, in furtherance thereof, establish requirements to seek to prevent manipulation.
12. Insurance – Platforms holding client crypto assets should have crime and theft insurance, especially if they are holding material amounts of crypto-assets in "hot" wallets. Verified "cold" wallet holdings should require lesser insurance amounts. Further, we think that if investment dealers are able to offer crypto trading in their clients' accounts, that CIPF insurance may well be available.
13. Clearing and settlement – We believe that a central counterparty clearing system with net settlement similar to that offered by CDS or CDCC should be encouraged, as we believe that it is much safer than the direct settlement methods used to date.

We thank you for the opportunity to comment.

Yours truly,

Laurence Rose

Laurence Rose
Chairman, Omega Securities Inc.
Co-founder, President & CEO, 4C Clearing Corporation



Email submission at comments@osc.gov.on.ca and Consultation-en-cours@lautorite.gc.ca

British Columbia Securities Commission

Alberta Securities Commission

Financial and Consumer Affairs Authority of Saskatchewan

Manitoba Securities Commission

Ontario Securities Commission

Autorité des marchés financiers

Financial and Consumer Services Commission (New Brunswick)

Superintendent of Securities, Department of Justice and Public Safety, Prince Edward Island Nova

Scotia Securities Commission

Securities Commission of Newfoundland and Labrador

Superintendent of Securities, Northwest Territories

Superintendent of Securities, Yukon

Superintendent of Securities, Nunavut

Re: Request for Input on Joint CSA/IIROC Consultation Paper 21-402 Proposed Framework for Crypto- Asset Trading Platforms

Dear Ms. Beaudoin and Ms. Pinnington:

The Wall Street Blockchain Alliance (the “WSBA,” “we,” “us” or “our”) welcomes the opportunity to submit to the Canada Securities Administrators (the “CSA,” “you” or “yours”) and the Investment Industry Regulatory Organization of Canada (the “IIROC,” “you” or “yours”) our comments in response to the Consultation Paper, with a goal of supporting and advancing the CSA/IIROC’s understanding of the risks and opportunities presented by platforms and relevant ecosystem participants that facilitate the buying and selling of crypto assets.

The WSBA is a 501c(6) non-profit trade association that is dedicated to the responsible advancement and adoption across global markets of cryptoassets and blockchain technology. Our goal is to stand as a neutral and unbiased steward of education and cooperation between and among our members and key market participants worldwide. We regularly engage with industry leaders, policymakers, technology innovators and others through direct communications, comment letters, best practice recommendations and more, with the aim of guiding blockchain and cryptoasset industry dialogue during this time of tremendous technological evolution.

We believe that the integration of cryptoassets and blockchain technology will result in improved consumer choices; safer and more efficient markets; cost-effective solutions for equity ownership,



investment and trading; lending and, ultimately, greater value and wealth. Given the infancy of the industry as a whole, and information asymmetries that exist between and among various participants, however, we believe that achieving such results will require thoughtful consideration, dedicated collaboration and coordinated effort by a variety of market participants, gatekeepers and others. For these and other reasons, we are pleased to provide our responses to the questions posed in the Consultation Paper.

Please do not hesitate to reach out to us by email at info@wsba.co if you would like to discuss any of our responses, or for any other reason. We hope that this will mark the beginning of a long and fruitful working relationship.

Disclaimer: Please note that nothing in this document is legal or investment advice, and that we are not admitted to practice law in Canada or in any other jurisdiction. The responses contained in this submission are intended for informational purposes only and should not be relied upon for any purposes. Such responses are based on our understanding of the plain meaning of the CSA Staff Notice 46-307 Cryptocurrency Offerings and CSA Staff Notice 46-308 Securities Law Implications for Offerings of Tokens Consultation Paper, NI 23-103, NI 31-103, and certain other documentation referred to in the Consultation Paper that we reviewed. We have not, however, completed an exhaustive review of all potentially relevant materials or applicable law.

General Comments

Our first takeaway is that it is clear you and your respective staffs took great care to educate yourselves about the industry. The breadth and depth of the questions posed throughout the document indicate substantial knowledge of the potential of these disruptive innovations, but also reflect an understanding of the risks that they present at this time. Although the WSBA believes in the technology, and strongly advocates on its behalf, we are well aware that it is not a finished product.

With that mindset, we recommend very carefully consideration before implementing a bespoke regulatory framework for crypto-asset trading platforms. As a general principle, we have found that it is more successful over the long term to regulate a particular function rather than a specific technology. Our belief is rooted in the fact that it is often difficult to predict how a given technology or industry is going to evolve over time, which could force legislators and regulators to frequently update and edit these proposed rules to account for new uses cases or to broaden/narrow their scope. This becomes even more challenging when we consider the transnational nature of blockchain technology. An additional complicating factor with these types of frameworks or proposals is that there is often a delay or information lag between the time that industry participants are aware of



material changes that require regulatory amendments, and when the relevant guidelines are updated. This level of uncertainty can create an unequal field between yourselves and other jurisdictions, such as the ones that you point out in Part 4 of the Consultation Paper that for the time being are relying on guidance explaining when certain assets and operators are subject to relevant legislation.

Additionally, having a separate or additional regulatory burden can be frustrating for key members of an industry that many feel is currently in a nascent stage and can often be singled out for criticism. On this note, we speak from experience. As a New York-based institution, we are intimately familiar with the BitLicense that was introduced in 2014 by the New York Department of Financial Services (NYDFS).¹ Like your respective organizations, we understood that the NYDFS was in a difficult position and tried to marry the opposing goals of fostering innovation without unduly risking consumer welfare. However, the impact of this legislation resulted in dozens of blockchain and crypto companies leaving New York state and the “blacklisting” of the state’s residents for purposes of crypto asset engagement.² To date, only 18 companies have received a BitLicense, many of which have been forced to delay their entry into the U.S. for several years.

Second, we would also recommend caution because it is important to keep in mind how frequently the ground is shifting beneath the blockchain and crypto industry, and how the lines and delineations between participants will move. Depending on the future trajectory of the industry, it could significantly impact the relevancy of an industry specific framework. For instance, many established broker-dealers in the financial services space are making strides to offer exposure to crypto assets to their clients in the near term. For instance, leading fintechs such as Square³ and Robinhood⁴ offer brokerage services to their retail customers. Furthermore, established industry players such as TD Ameritrade⁵ and Fidelity⁶ are doing the same for institutional investors. Moreover, while there are a number of exchanges being created that may offer direct access to their respective trading platforms, as noted in the Consultation Paper, it is still likely that broker dealers will be key points of ingress and egress from exchanges, ATs, and other industry participants. This assessment is rooted in some key assumptions.

1. As institutional investors increasingly enter this space, they will seek to facilitate these investments via procedures that they are already familiar and comfortable with. As evidence of

¹ https://www.dfs.ny.gov/legal/regulations/bitlicense_reg_framework.htm

² <http://fortune.com/2015/08/14/bitcoin-startups-leave-new-york-bitlicense/>

³ <https://cash.app/help/us/en-us/1016-bitcoin>

⁴ <https://techcrunch.com/2018/07/12/you-can-now-trade-litecoin-and-bitcoin-cash-on-robinhood-crypto/>

⁵ <https://www.tdameritrade.com/investment-products/cryptocurrency-trading.page>

⁶ <https://www.fidelitydigitalassets.com>



this trend already happening, new crypto-specific exchanges such as tZero have integrated with broker dealers such as Dinosaur Financial.⁷

2. Traditional exchanges and trading systems are going to increasingly offer access to tokenized securities. Nasdaq is leveraging its technology to facilitate this service for digitized securities, among others. Furthermore, legislative efforts in various states around the US such as Wyoming and Delaware are increasingly allowing for the issuance of digital shares and equities.
3. One of the larger trends taking place around the world is that exchanges and other key industry providers are increasingly looking to blockchain technology as a way to streamline the clearance and settlement of transactions. Two of the larger projects being undertaken, as you are likely already aware, include how the Australian Stock Exchange is utilizing a bespoke system built by Digital Asset Holdings to overhaul its incumbent CHES system⁸. Additionally, here in the U.S. the Depository Trust & Clearing Corporation (DTCC) is using blockchain technology to update its Trade Information Warehouse.⁹ As they get more comfortable and knowledgeable with operational aspects of the technology, it will transfer forward to the front-end user systems.

Third, the timing may not be ideal for such an endeavor because the industry is just now entering what we consider to be an adolescent stage of transition and maturation, which could limit the need for a bespoke framework. As you mention throughout the Consultation Paper, industry participants are designing and implementing solutions and best practices for challenges such as the secure issuance, clearance, and custody of assets. Furthermore, most of this important work is not only undertaken due to regulatory concerns, but also due to market/competition considerations and a general belief that key infrastructure providers such as custodians have a duty or responsibility to provide a safe and secure environment for participants.

Some examples of these initiatives include:

- Rapid advances in the field of cold storage to safeguard assets. While undoubtedly there are still security issues with certain crypto exchanges, this week's USD\$40.7 million hack of Binance's hot wallet being the most recent example, reputable exchanges and custodians are utilizing geographically-dispersed multi-signature HSMs and white-labeled addresses combined with deeply fortified and redundant physical locations, to protect customer assets. Companies leading the charge include Coinbase, BitGo, and Gemini, among others, which are certified as qualified custodians. Additionally, while details of these security arrangements are understandably kept

⁷ <https://www.prnewswire.com/news-releases/tzero-partners-with-dinosaur-for-launch-of-digital-securities-trading-300788223.html>

⁸ <https://www.asx.com.au/services/chess-replacement.htm>

⁹ <http://www.dtcc.com/news/2017/january/09/dtcc-selects-ibm-axoni-and-r3-to-develop-dtccs-distributed-ledger-solution>



secret, in the spirit of supporting the ecosystem as a whole Square open-sourced its crypto-native security solution, Subzero.¹⁰ We expect to see continued progress in this field and the dispersion of these technologies, policies, and procedures across the ecosystem.

- Crypto companies are becoming increasingly able to obtain insurance coverage for assets they custody, especially for those held offline in cold storage. The mere fact that industry participants are able to secure coverage for themselves is a reflection of the industry’s maturation because obtaining these policies requires a significant amount of due-diligence on behalf of the insurer. Some recently publicized policies include:
 - Bakkt obtaining \$100 million in coverage for assets held in cold storage through an undisclosed set of insurers¹¹
 - BitGo received a \$100 million policy from a Lloyd’s syndicate for assets held in cold storage¹²
 - Additionally, Coinbase recently revealed that it has a \$255 million policy from Lloyd’s registered broker Aon and sourced from a global group of US and UK insurance companies that covers assets held online in hot wallets.¹³

These policies are significant developments because the underwriters are putting their firms, and their own livelihoods at risk when they offer them. As more becomes known about the security threats associated with crypto assets and policies become more mature, we expect this trend to grow.

Finally, it is worth noting that significant progress is being made in the field of information sharing and market surveillance. Again, much of this work is being undertaken due to market opportunity and a feeling of responsibility to the community at large, as issues such as venue arbitrage threaten the industry’s reputation. Recent examples include:

- More than seven crypto exchanges are utilizing Nasdaq’s SMARTS Market Surveillance technology to monitor illicit trading on their platforms.¹⁴ Two mentioned by name in recent reporting include Gemini and SBI Virtual Currency. This is a noteworthy fact, because it is a significant endeavor for an exchange to become an authorized user of the software suite. Typically, the due-diligence involves a team of many individuals looking at three separate categories: Business Model, KYC/AML, and Exchange Governance &

¹⁰ <https://medium.com/square-corner-blog/open-sourcing-subzero-ee9e3e071827>

¹¹ <https://www.coindesk.com/bakkt-acquires-crypto-custodian-partners-with-bny-mellon-on-key-storage>

¹² <https://www.coindesk.com/bitgo-offering-100-million-in-crypto-insurance-through-lloyds-of-london>

¹³ <https://www.coindesk.com/coinbase-insurance-coverage>

¹⁴ <https://www.forbes.com/sites/michaeldelcastillo/2019/01/30/nasdaq-is-now-working-with-7-cryptocurrency-exchanges/>



Controls. It was also made clear from recent reporting in *Forbes* that Nasdaq also takes care to ask questions about the reputation of the founders and key personnel, the history and use cases for assets traded on the platform, as well as the listing criteria for future assets. These are all key points of discussion listed throughout the Consultation Paper.

- In addition, leading European crypto exchange Bitstamp recently implemented the Irisium Surveillance platform from Cinnober, a technology provider for mainstream financial markets, to monitor for suspicious activity.¹⁵ This is the same tool that entities such as Asia Pacific Exchange Pte Ltd (APEX) use to detect illicit behavior.

Conclusion

From our comments we hope to have demonstrated that significant progress is being made at the industry level around the world to address many of the key questions and risks identified throughout the Consultation Paper. **However, with all of that said, we do appreciate that much work still needs to be done, best practices must assimilate downstream to smaller players, and a significant gap remains between the best of breed venture-backed companies and other less-established companies.**

Furthermore, we also understand that even some of the biggest and most reputable companies are not above reproach. For instance, in recent weeks the NYDFS rejected Bittrex’s BitLicense application due to numerous shortcomings with their procedures and controls, which was best exemplified by their identification of numerous pseudonyms operating on the platform along with addresses allegedly from North Korea.¹⁶ Additionally, in recent months the New York Office for the Attorney General released the results of a survey of thirteen of the world’s most notable trading sites, including Coinbase, Kraken, Bitfinex, Bittrex, and Binance that demonstrated how many exchanges are still prone to market manipulation.¹⁷ Some of the key findings included:

- “Though some virtual currency platforms have taken steps to police the fairness of their platforms and safeguard the integrity of their exchange, others have not. Platforms lack robust real-time and historical market surveillance capabilities, like those found in traditional trading venues, to identify and stop suspicious trading patterns. There is no mechanism for analyzing suspicious trading strategies across multiple platforms. Few platforms seriously restrict or even monitor the operation of “bots” or automated algorithmic trading on their venues. Indeed, certain trading platforms deny any responsibility for stopping traders from artificially affecting prices.”

¹⁵ <https://www.coindesk.com/crypto-exchange-bitstamp-rolls-out-tech-to-spot-market-manipulation>

¹⁶ <https://www.coindesk.com/nydfs-why-we-rejected-bittrexs-application-for-a-bitlicense>

¹⁷ https://ag.ny.gov/sites/default/files/vmii_report.pdf



- “Protections for customer funds are often limited or illusory. Generally accepted methods for auditing virtual assets do not exist, and trading platforms lack a consistent and transparent approach to independently auditing the virtual currency purportedly in their possession; several do not claim to do any independent auditing of their virtual currency holdings at all. That makes it difficult or impossible to confirm whether platforms are responsibly holding their customers' virtual assets as claimed.”

Nevertheless, keeping all of this in mind, and as demonstrated throughout our comments, leading exchanges, ecosystem players, and members of the WSBA are actively working on solutions to these challenges. This is being done in large part irrespective of regulation because we feel a sense of ownership over the space and it is the best way to provide a competitive service and to aid in the development of the global crypto asset ecosystem.

Therefore, while we would not be so bold as to recommend that you avoid issuing a separate framework for crypto platforms, we suggest delaying or relying on existing legislation and regulatory statutes to give the industry more time to mature. Another option we would recommend is to evaluate the possibility of having the platforms that would be subject to the Framework Guidance create a Self-Regulatory Organization (SRO). As you are aware, SROs can be a valuable tool – especially in conjunction with companies that are graduating from sandboxes – to operate in a regulated manner with the speed and agility to react to changes in the technology or marketplace.

This is an approach that is being pursued here in the United States. For instance, a number of leading exchanges created the Virtual Commodity Association (VCA) with the goal of forming an SRO specifically for virtual commodity exchanges and custodians to work with the U.S.-based Commodity Futures Trading Commission (CFTC).¹⁸ More globally, a group of 50 traders named “CORA” is seeking to create a set of standards for OTC trading in cryptocurrency. Some of the leading members of this group include Galaxy Digital and Cumberland.¹⁹

Additionally, we would suggest you also consider certification programs that could facilitate the creation of a set of credentialed advisors that could serve as a second vetting layer for industry participants. This is a policy that Malta is currently implementing, and they are seeing significant

¹⁸ <https://medium.com/gemini/joining-the-virtual-commodity-association-8bdf3b2f803e>

¹⁹ <https://www.theblockcrypto.com/2019/05/13/jump-trading-galaxy-digital-and-many-other-traders-mull-instituting-crypto-market-white-list/>



interest from companies and individuals who seek to benefit financially from participating in the crypto economy while ensuring responsible stewardship of this developing industry.

Thank you for the opportunity to submit this response to the Consultation Paper. We look forward to speaking with you and welcome any questions or comments that you may have.

Respectfully Submitted,

Ron Quaranta

Chairman and Chief Executive Office
The Wall Street Blockchain Alliance
New York, New York



May 14, 2019

Investment Industry Regulatory Organization of Canada
British Columbia Securities Commission
Alberta Securities Commission
Financial and Consumer Affairs Authority of Saskatchewan
Manitoba Securities Commission
Ontario Securities Commission
Autorité des marchés financiers
Financial and Consumer Services Commission (New Brunswick)
Superintendent of Securities, Department of Justice and Public Safety, Prince Edward Island
Nova Scotia Securities Commission
Securities Commission of Newfoundland and Labrador
Superintendent of Securities, Northwest Territories
Superintendent of Securities, Yukon
Superintendent of Securities, Nunavut

**Raymond Chabot
Grant Thornton LLP**
Suite 2000
National Bank Tower
600 De La Gauchetière Street West
Montréal, Quebec
H3B 4L8

T 514-878-2691

Via email to: consultation-en-cours@lautorite.qc.ca, comments@osc.gov.on.ca and vpinnington@iroc.ca

Subject: Comments on Consultation Paper 21-402

We are pleased to have the opportunity to provide our input on the joint Canadian Securities Administrators (CSA)/Investment Industry Regulatory Organization of Canada (IIROC) Consultation Paper 21-402, *Proposed Framework for Crypto-Asset Trading Platforms* (hereafter “CP 21-402”).

We believe that CP 21-402 raises issues important to investor protection and public policies. It is an important step in informing the proposed platform framework, and we encourage the CSA and IIROC to move forward with this project and to clarify the rules applicable to participants in the crypto-asset market.

Based on Part 2 of CP 21-402, we understand that the CSA is evaluating how trading occurs on platforms to assess whether or not a security or derivative may be involved. To further refine the factors listed, the CSA may consider recent guidance¹ issued by the US Financial Crimes Enforcement Network (FinCEN) regarding the application of regulations to certain business models involving convertible virtual currencies.

As discussed in Part 4 of CP 21-402, different jurisdictions are taking different approaches to regulating platforms. We encourage the CSA and IIROC to work with

¹ FinCEN Application of FinCEN’s Regulations to Certain Business Models Involving Convertible Virtual Currencies (May 2019): <https://www.fincen.gov/resources/statutes-regulations/guidance/application-fincens-regulations-certain-business-models>

regulatory and self-regulatory bodies in other jurisdictions whenever possible to promote the consistency of requirements applicable to platforms. We believe that this consistency is key to minimize regulatory arbitrage, for Canadian-based platforms to be on a level playing field, and to allow Canadian investors appropriate access to this new asset class.

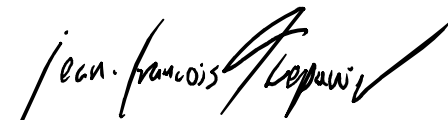
We believe that auditors have a key role to play in enhancing the trust in the crypto-asset market, including in response to the risks mentioned in Part 3 of CP 21-402. As auditors, we feel it is most appropriate for us to only provide input on questions 4 and 5 in section 5.2.1 of CP 21-402. Please find our detailed responses in the appendix to this letter.

Should you wish to discuss any of our comments, please contact the undersigned persons at roy.louis@rcgt.com or trepanier.jean-francois@rcgt.com.

Yours sincerely,



Louis Roy, CPA, CA



Jean-François Trépanier, CPA, CA

Appendix

- **Question 4: What standards should a Platform adopt to mitigate the risks related to safeguarding investors' assets? Please explain and provide examples both for Platforms that have their own custody systems and for Platforms that use third-party custodians to safeguard their participants' assets.**

We observe that instead of mandating the use of a specific set of standards to mitigate the risks related to safeguarding investors' assets, it may be preferable to provide platforms with flexibility regarding the standards they adopt. We note that a similar approach is currently used in securities regulation. For example, section 3.4 in NI 52-109 respecting certification of disclosure in issuers' annual and interim filings requires the use of a control framework to design the issuer's ICFR but without mandating a specific framework. Section 5.1 in Policy Statement to NI 52-109 provides examples of suitable frameworks.

It could be required that the standards adopted by platforms exhibit certain characteristics to ensure that they are of high quality. Characteristics could be based on those used in determining the suitability of criteria when conducting engagements in accordance with CSAE 3000² or CSAE 3416³ (i.e., characteristics of relevance, completeness, reliability, neutrality and understandability).

We believe that a flexible approach can result in a better outcome by allowing bodies of experts to suggest new standards that are more "fit for purpose" for custody of crypto-assets and by updating such standards as necessary. We observe that bodies of experts are already working on standards, including the "CryptoCurrency Security Standard (CCSS)" proposed by the CryptoCurrency Certification Consortium⁴ (C4) or the "ISO/NP TR 23576, *Blockchain and distributed ledger technologies – Security management of digital asset custodians*" currently under development by ISO/TC 307. We encourage the CSA and IIROC to monitor and, if appropriate, to participate in the activities of these and other bodies of experts. The CSA and IIROC may also consider forming or supporting a body of Canadian experts in developing standards codifying best practices for custody of crypto-assets.

- **Question 5: Other than the issuance of Type I and Type II SOC 2 Reports, are there alternative ways in which auditors or other parties can provide assurance to regulators that a Platform has controls in place to ensure that investors' crypto-assets exist and are appropriately segregated and protected, and that transactions with respect to those assets are verifiable?**

We strongly believe that assurance reports issued by independent auditors have an important role in the management of risks associated with custody of crypto-assets, including the risks mentioned in Part 3 of CP 21-402. We strongly support that the endgame is to require that platforms obtain an assurance report for their custody system and those of any third-party custodians.

We are however unsure whether the preconditions for an assurance engagement are present for all platforms that would be subject to the proposed platform framework, especially the precondition to expect to be able to obtain the evidence needed to support the practitioner's conclusion. The CSA and IIROC will have to

² CSAE 3000, *Attestation Engagements Other than Audits or Reviews of Historical Financial Information*.

³ CSAE 3416, *Reporting on Controls at a Service Organization*.

⁴ <https://cryptoconsortium.org/>

make a public policy decision about the acceptability of platforms that are not “audit-ready”.

CP 21-402 contemplates requiring the platforms to obtain a SOC 2 report. We have the following observations:

- The reason for requiring both a Type I and II is unclear. A Type I report is typically not produced if a Type II exists, because a Type II report contains an opinion on the operating effectiveness of controls (not only their design) and a detailed description of tests of controls performed.
- We encourage the CSA and IIROC to adopt an approach that is flexible regarding the criteria used. A SOC 2 report is based on using the Trust Services Criteria (TSC). The TSC relate to the following trust services principles: security, availability, processing integrity, confidentiality and privacy. While the “security” principle is common to all SOC 2 reports, the other principles are not. If the intent for requiring a SOC 2 report is to achieve comparability between platforms, we believe that it may not be achieved. The TSC can be used to evaluate controls relevant to a variety of different subject matters, and there may also be different interpretations of the applicability of each principle and how characteristics specific to platforms are to be included in the principles and criteria. These differences are more likely to exist when reporting on a new subject matter such as custody of crypto-assets.

To achieve more consistency, the TSC can be supplemented by other frameworks dealing with a specific subject matter and providing more detailed guidance about the risks and controls. For example, in our experience, it is frequent to refer to the National Institute of Standards and Technology (NIST) 800-53 *Cloud Controls Matrix (CCM)* when reporting on cloud solutions.

While the TSC are widely recognized and offer flexibility in application, they may not be the only suitable criteria for an assurance engagement. As mentioned in our response to question 4, other standards that are more “fit for purpose” for custody of crypto-assets may emerge.

- We believe that a SOC 1 report may also be needed. A SOC 1 report focuses on a service organization’s controls that are likely to be relevant to an audit of a user entity’s financial statements. When a platform has custody of an entity’s crypto-assets, it is likely that certain controls put in place by that platform are part of the entity’s information system and are relevant to financial reporting. Information about these controls relevant to financial reporting would be provided by a SOC 1 report, not a SOC 2 report. We note that traditional custodians often make a SOC 1 report available to user entities and their auditors.
- We caution against requiring auditors to report directly to regulators. We note that question 5 refers to “provide assurance to regulators that a Platform has controls in place”. We believe that platforms should be held accountable by regulators. SOC reports are typically addressed to management of the entity, and a requirement to address the report directly to a regulator may result in an unwillingness to accept such engagements.



#1740 240 4 Ave SW
Calgary, Alberta
T2P 4H4

BULL BITCOIN

RE: Bull Bitcoin/ Satoshi Portal's response to the **Joint Canadian Securities Administrators/Investment Industry Regulatory Organization of Canada**

Consultation Paper 21-402
Proposed Framework for Crypto-Asset Trading Platforms

The following letter is the collective response from the leadership of both Bull Bitcoin Inc. and Satoshi Portal Inc. to the Joint Canadian Securities Administrators/Investment Industry Regulatory Organization of Canada. It is of our objective observation and assessment that nearly every other "crypto asset" platform currently operating in Canada relies on the sale of what could be considered securities to the public as part of their current business model. We believe that digital asset platforms that offer any form of custodial solutions as storage for their clients represents a promise to hold and release their coins and qualifies them as a security. As well, we believe that platforms that issue financial instruments with a promise of delivery and are controlled by a subset of organizations or individuals are manipulable and are securities.

Background

Bull Bitcoin was formed in 2019 as the merger of two of the most established companies in the Canadian bitcoin/blockchain industry, Satoshi Portal, the operator of the Bylls platform and Bitcoin Brains. Founded by Francis Pouliot and Dave Bradley, Bull Bitcoin boasts over 60 years of combined experience in the bitcoin industry between our staff of 13. Bull Bitcoin is now Canada's largest and oldest continuously operating bitcoin brokerage as well as Canada's first and largest bitcoin payment processor.

Francis Pouliot, CEO and founder of Bull Bitcoin/ Satoshi Portal (@FrancisPouliot_)

In addition to being a notable Bitcoin/ DLT thought leader with over 47,000 Twitter followers, in his 6+ years of full-time bitcoin experience, Francis has served as an advisor to the Ontario Securities Commission as well as Fintrac on matters relating to Fintech and Digital Currency/Assets. With a background in public policy, Francis is uniquely positioned to understand the challenges at hand from the perspective of both regulators and first hand as an industry participant.

Dave Bradley, President and founder of Bull Bitcoin and Bitcoin Brains (@BitcoinBrains)

In the 8 years that Dave has been involved in bitcoin/blockchain, he has consulted for Fortune 500 Companies, extensively researched both public and private blockchains as well as helped the formation of numerous other industry players. Both Francis and Dave are highly regarded among the top bitcoin/blockchain experts in the world.

These combined and unique qualifications put Bull Bitcoin in a position to offer comments with a deeper level of insight and fewer conflicts of interest than other current market participants.

Crypto assets issued, sold and stored with the promise of disbursement should be regulated

The intention of this reply is to offer clear and specific guidance using our unique technical knowledge on how regulators should view certain assets in regards to securities regulations. In this letter, we will use Ethereum as an example because it has been the focus of most of the comments worldwide on the issue. The conclusions we draw about Ethereum should be extended to other “crypto assets” meeting the same criteria. We will also take the opportunity to share some of our expertise as it relates to the custody of “crypto assets” and the implications for regulators.

The first and potentially most important question that needs to be addressed is the question of decentralization. Some comments and direction from regulators internationally have indicated that they think some platforms like Ethereum might no longer be considered securities due to the fact that they may have become sufficiently decentralized to no longer meet the “Reliance on the Efforts of Others” prong of the Howey Test. Now that the SEC has released its first official guidance on the matter, we believe that contrary to previous verbal comments made by SEC officials, it’s very clear that the Ether asset, issued and sold by The Ethereum Foundation, does, in fact, meet the definition of a security within the framework of the Howey Test. Furthermore, we believe that the logic applied to US interpretations of the law is similar enough that the same conclusions should be drawn by Canadian regulators.

In order to answer the question of whether a platform is sufficiently decentralized, it will be very important to specifically define the term “decentralized”. Some platforms, like Ethereum, have a decentralized user base but the operation, control and ownership of the network are entirely centralized to a small coordinated group of foundation members. It is our opinion that the corporations who are by de facto, in charge of Ethereum development, such as Parity, Consensys and the Ethereum Foundation, act as fiduciaries and are providing the quasi-totality of efforts from which the market value of Ethereum is derived. All future decisions on the roadmap for the development of Ethereum will be made by this small group. These organizations are funded entirely from the sale of Ether tokens to the public with no risk disclosures whatsoever.

This is one example but any virtual currency or crypto asset which could reasonably be said to have a leader or leaders should not be considered decentralized and should in our view, be considered a security. This kind of structure is mirrored by many different crypto asset projects and offerings who have raised funds by selling their tokens to the public.

The only currently provably, truly decentralized virtual currency at scale/ digital asset is Bitcoin. In our opinion, to be considered decentralized, the following standards should be met and digital assets such as Ether do not meet this criteria:

- There should be no issuing body behind the asset or central governance process. Any project that has done an ICO with a single or small group of beneficiaries cannot be considered decentralized unless that issuer and its affiliates abandon the project entirely.

- There should be no leader or founder involved in the project. Even projects without an explicitly proclaimed leader often have a small number of people with near total control.
- The entire consensus layer should be open source and free of patents or other intellectual property claims to maintain the integrity and adoption at a wide scale and to protect the rules of engagement of those who use the network.
- The project should either maintain its own consensus layer or operate on another provably decentralized blockchain. Appcoins built on centralized networks like Ethereum should be considered under the ultimate control of the central entity behind the base network. It is technically, socially and functionally possible that The Ethereum Foundation could directly control transactions of any ERC20 token or other token based on their network. As such forks, derivations, applications built on securitized digital assets such as Ether should be regulated under the same conditions.
- Node and mining infrastructure should be separate so that the economic incentives driving each remain independent.
- A robust distributed network of non-mining, economic nodes should exist in a variety of jurisdictions. These include exchanges, brokerages, payment processors or merchants using the token directly. These economic nodes support the consensus of the network by providing independent input and verification on their version of the agreed upon rules of the network. Because these nodes represent a large portion of the real economic activity happening on the network, it would be impossible to meaningfully fork the network without first forming a near total consensus amongst these node operators. Because the interests of these node operators are varied and diverse, they may only converge as it relates to the overall health and security of the network and therefore can't be considered to be anything approaching a "Common Enterprise".
- A commoditized and competitive market for mining hardware should exist.

Custody: if a "Platform" holds value for a client, we believe that is an investment contract

When a user holds bitcoin or other digital assets in an account at a custodial exchange, we believe it's reasonable to consider this a contract for the future delivery of these coins/value. We believe this is a contract and a promise made between the client and the "platform". The ability for the exchange to deliver on this contract will be dependant upon their ability to hold the coins safe in the meantime. As in the case, most recently, with Quadriga CX the situation invites the question of where the Platform is holding that value and to what degrees of security should the "platform" adopt? Should these platforms be regulated as to how they hold this value as banks are? Is it lawful for these "platforms" to state that this value is no longer the clients when it is held as a custodial agent? Are these assets allowed to be used in other financial services/products and how much of collateral should these "platforms" hold to ensure proper delivery? A myriad of questions surrounding the complexities of being a custodian of digital assets drums up the same questions and begs for regulatory bodies to intervene much like the banking industry.

If a platform is determined to allow its users to hold coins on the platform, for the purposes of ongoing trading for example, then the best option available to limit the risk of losses is to strictly limit withdrawals to a specific, narrowly defined time frame.

Bitmex, the largest crypto asset exchange in the world by volume, allows for withdrawals only once per day. This allows users time to react if their account is hacked. It also allows the exchange to carefully control when and how they expose any of their stored coins to the live network. There is a very strong case to be

made that onramp and trading platforms should remain separate as onramp platforms require much quicker withdraws. Onramp platforms should remain non-custodial.

The best way to deal with the risk of loss of virtual currencies or crypto assets during the process of purchasing or selling these coins is to remove the option for custody entirely. Non-custodial services which immediately send coins to the user represent a much safer way for consumers to transact. Platforms which do not hold customer crypto assets cannot lose customer crypto assets. The inherent nature of truly decentralized digital assets is the ability to control, hold and use your own value. We believe that if a “platform” holds value on behalf of a client, it is an incredible amount of responsibility and should be regulated as such.

Considerations for a successful digital asset custodial solution

When a user holds bitcoin or other digital commodities in an account at a custodial exchange, we believe it’s reasonable to consider this a contract for the future delivery of these coins. The ability for the exchange to deliver on this contract will be dependant upon their ability to hold the coins safe in the meantime. When platforms store crypto assets the following best practices should also be applied:

- All crypto assets should be stored in segregated accounts. These need to be separate from both company operating funds as well as the funds of any other businesses served by third-party custody providers if they are used.

All crypto assets should be stored and controlled within Canada. Both the private keys, any physical backups thereof as well as the server infrastructure controlling any hot wallets should be within Canada. It would be impossible to define the jurisdictional risk posed by a third party custodian handling crypto assets from companies around the world and based in a country other than Canada. It’s not hard to imagine a scenario where a US-based custodian company holding crypto assets belonging to Canadians on behalf of a Canadian company has its entire pool of crypto assets frozen by a US government agency as a result of this custodian’s dealings in other parts of the world. The only way to control this risk is to keep the crypto assets in Canada.

- Custodial exchanges should also plan for the possibility of kidnappings or ransoms of key personnel or systems. Both physical and digital seizures of hardware or personnel should be considered. Platforms should also consider the risk of the destruction of private keys through acts-of-god or other disasters. Keys should be redundantly stored in a variety of geographic locations.
- Another consideration should be the ability to recover the private keys in the event of the death of one or more of the key parties managing the platform.

The specific technological risks associated with a particular project, token or blockchain should also be considered in the context of custody. Since each blockchain is potentially unique, the technology risks associated with it can be very hard to define. We don’t believe that these risks should be externalized to the holders of other assets on a single platform.

- A prime example of this happened in 2017 when QuadrigaCX burned around \$17M worth of customer Ether which they were holding as a result of the DAO fork when the Ethereum Foundation forked their version of the network away from their original codebase, creating Ethereum and Ethereum Classic. While this bug was caused by a technical error on the part of QuadrigaCX staff, the bug would not have been possible without the actions of The

Ethereum Foundation. A few important considerations arise from this situation. First, we don't believe that the lack of network solidity created by The Ethereum Foundation should be inflicted upon holders of other assets on the QuadrigaCX platform. Only holders of ETH on that platform should be subject to the losses. Second, we believe that The Ethereum Foundation has a fiduciary duty to those ETH holders who were victimized due to their actions.

Conclusion

Overall, we believe that the majority of "crypto assets" do fall under the jurisdiction of securities regulators. We also believe that existing action from these regulators has fallen significantly short of offering the investor protection they are mandated to provide.

At the same time, we believe that over-regulation of these assets is likely to simply push the industries tied to them to more favorable jurisdictions.

We believe in keeping Alberta and Canada a business-friendly environment. Part of how we can accomplish this is a very clear and concise regulatory regime with minimal requirements that would be easy for the public to understand.

To that end, we believe that "crypto assets" such as ICOs who wish to raise money like an IPO who are wishing to sell to Canadians should be required to make one simple but meaningful disclosure:

"How is the value of your token tied to the success or usefulness of your platform?"

Signed:



Francis Pouliot, Dave Bradley and the rest of the staff and management of Bull Bitcoin.

Montréal May 15, 2019

Me Anne-Marie Beaudoin
Corporate Secretary
Autorité des marchés financiers
800, square Victoria, 22e étage
C.P. 246, tour de la Bourse
Montréal (Québec) H4Z 1G3
Consultation-en-cours@lautorite.qc.ca

The Secretary of the Ontario Securities Commission
20 Queen Street West, 22nd floor
P.O. Box 55
Toronto (Ontario) M5H 3S8
Comments@osc.gov.on.ca

Ms. Victoria Pinnington
Senior Vice President, Market Regulation
Investment Industry Regulatory Organization of Canada
121 King Street West, suite 2000
Toronto (Ontario) M5H 3T9
Vpinnington@iiroc.ca

Re: Joint Canadian Securities Administrators/Investment Industry Regulatory Organization of Canada
- Consultation Paper 21-402 - Proposed Framework for Crypto-Asset Trading Platform (hereinafter
“**Joint Consultation**”)

Dear Madams and Sirs:

In June 2018, Messrs. David Durand¹ of Durand Morisseau LLP² and Mr. Drew Dorweiler³ of IJW & Co.⁴ were invited by the Canadian Standing Committee on Finance (“**FINA Committee**”) to testify before it on certain issues, including: (i) the characterization of a “virtual currency” (now commonly referred to as “digital assets”), (ii) indicators of fraud⁵, as well as (iii) the detection of potential fraud or money laundering activities at a point of conversion (or a convertibility mechanism)⁶. The FINA Committee invited us to submit our brief, entitled “*Don’t block the blockchain: How Canada can guard against money laundering while maintaining global competitiveness*” (“**FINA Brief**”), which we also invite you to take cognizance thereof, as it:

1. responds to a number of questions raised in the Joint Consultation⁸ with particular regard to the characterization of “crypto-assets”; and

¹ See: <https://ca.linkedin.com/in/daviddurandavocat>.

² See: <http://durandmorisseau.com>.

³ See: <https://ca.linkedin.com/in/drewdorweiler>.

⁴ See: <http://ijw.ca/en/>.

⁵ Reference can be made to FINTRAC Guidance, available at: <http://www.fintrac-canafe.gc.ca/guidance-directives/1-eng.asp>.

⁶ Reference can be made to Figure 2 of the FINA Brief.

⁷ See: <https://www.ourcommons.ca/Content/Committee/421/FINA/Brief/BR10007367/br-external/IJWAndCoLtd-2018-09-17-Updated-Final-e.pdf> (in English).

⁸ See: http://www.iiroc.ca/documents/2019/196069ad-9053-4d8b-8022-a8e11a6c4385_en.pdf.

2. raises jurisdictional concerns with respect to the oversight of crypto-assets (cf. Section 8 of the FINA Brief).

In connection with the foregoing matters, international regulators⁹ have been grappling since July 2018 with the appropriate categorization of virtual currencies (or types of crypto-assets or digital assets) and whether they fall within the definition of a 'security'. For example:

- On January 9, 2019, the **European Banking Authority** released its report on crypto-assets¹⁰, wherein it : (i) is stated: "market developments also point to the need for a further review of EU anti-money laundering legislation" and (ii) advises the European Commission: (a) "[...] regarding the need for a comprehensive cost/benefit analysis, taking account of issues inside and outside the financial sector to determine what, if any, action is required at the EU level at this stage", and (b) "[...] to take account of the October 2018 recommendations of the Financial Action Task Force (and any further standards or guidance)¹¹ regarding, in their terminology, 'virtual asset' activities, and to take steps, where possible, to promote consistency in the accounting treatment of crypto-assets";
- On January 9, 2019, the **European Securities Market Authority** released its Advice¹², wherein it states at paragraph 5: "[a] key consideration for regulators is the legal status of crypto-assets, as this determines whether financial services rules are likely to apply, and if so which, and hence the level of protection to investors. Because the range of crypto-assets are diverse and many have hybrid features, ESMA believes that there is not a 'one size fits all' solution when it comes to legal qualification. [...]";
- On January 23, 2019, the **UK's Financial Conduct Authority** published its draft guidance CP19/3¹³ for market participants in the developing crypto-asset sector, in which it illustrates different types of crypto-assets that could potentially be impacted by financial regulation. It is worth noting that the Her Majesty's Treasury will consult later this year on the extension of a "regulatory perimeter" to address crypto-assets¹⁴;
- On March 20, 2019, the **Swiss Parliament** approved a motion directing the Federal Council to regulate cryptocurrencies¹⁵; such in furtherance to the existing issuance of FinTech licences, which allows institutions to accept public deposits of up to CHF 100 million, provided that these are not invested and no interest is paid on them¹⁶;

⁹ See: <https://www.loc.gov/law/help/cryptocurrency/world-survey.php>.

¹⁰ See: <https://eba.europa.eu/-/eba-reports-on-crypto-assets>, and <https://eba.europa.eu/documents/10180/2545547/EBA+Report+on+crypto+assets.pdf>.

¹¹ See: <https://www.fatf-gafi.org/publications/fatfrecommendations/documents/regulation-virtual-assets.html>, released on October 19, 2018.

¹² See https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf, released on January 9, 2019.

¹³ See: <https://www.fca.org.uk/publications/consultation-papers/cp19-3-guidance-cryptoassets>.

¹⁴ See: <http://blockchain.bakermckenzie.com/2019/02/20/fca-finally-speaks-on-crypto-uk-regulator-clarifies-regulatory-perimeter-for-cryptoassets/>, accessed on May 9, 2019.

¹⁵ See: <https://www.ccn.com/swiss-parliament-introduce-cryptocurrency-regulations>; and https://www.parlament.ch/de/services/news/Seiten/2019/20190320125259514194158159041_bsd093.aspx. A PWC Swiss primer is also available at: <https://cryptovalley.swiss/?mdocs-file=54694>.

¹⁶ See: <https://www.finma.ch/en/news/2018/12/20181203-aktuell-fintech-bewilligung/>

- On April 3, 2019, the **U.S. SEC** released a public statement on the “*Framework for ‘Investment Contract’ Analysis of Digital Assets*”¹⁷, in which it referred to a threshold issue of “[...] whether the digital asset is “security” under those laws”.¹⁸ The said laws consist of section 2(a)(1) of the *Securities Act of 1933*, section 3(1)(1) of the *Securities Exchange Act of 1934*, section 2(a)(36) of the *Investment Company Act of 1940*, and section 202(a)(18) of the *Investment Advisers Act of 1940*. The authors of this statement identify a series of non-exhaustive factors market participants should consider in assessing whether a digital asset is offered or sold as an investment contract and, therefore, is a security or not, on a case-by-case basis; and
- On April 26, 2019, the **FIN-FSA** released a Supervision¹⁹ entitled “Virtual currency providers to be supervised by the FIN-FSA – briefing for virtual currency providers on 15 May”, wherein it indicated that the *Act on virtual currency providers (572/2019)*, coming into force on May 1, 2019, will not introduce investor protection to virtual currency services and that the foregoing Act is based on Europe’s anti-money laundering legislation.

The Current Situation in Canada

Subsequent to the presentation of the FINA Brief, the FINA Committee submitted its Report to the Government in November 2018, which, in turn, provided its Government Response²⁰, in which Chapter 4 concludes “[b]usinesses that provide [virtual currency]-related financial services, such as exchange and value transfer services, will be deemed financial entities or money services businesses (MSBs)”. Consequently, on April 8, 2019, Bill C-97, entitled *An Act to implement certain provisions of the budget tabled in Parliament on March 19, 2019 and other measures* underwent a first reading²¹, wherein the following mentions of “virtual currencies” are made:

“Subdivision C of Division 2 of Part 4 amends the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* to, among other things,

- (a) allow the Governor in Council to make regulations defining “virtual currency” and “dealing in virtual currencies”;
- (b) require the Financial Transactions and Reports Analysis Centre of Canada (“the Centre”) to disclose information to the Agence du Revenu du Québec and the Competition Bureau in certain circumstances;
- (c) allow the Centre to disclose additional designated information that is associated with the import and export of currency and monetary instruments;
- (d) provide that certain information must not be the subject of a confidentiality order made in the course of an appeal to the Federal Court; and
- (e) require the Centre to make public certain information if a person or entity is deemed to have committed a violation or is served a notice of a decision of the Director indicating that a person or entity has committed a violation.”

¹⁷ See: <https://www.sec.gov/news/public-statement/statement-framework-investment-contract-analysis-digital-assets>.

¹⁸ See note 17.

¹⁹ See: <https://www.finanssivalvonta.fi/en/publications-and-press-releases/supervision-releases/2019/virtual-currency-providers-to-be-supervised-by-the-fin-fsa--briefing-for-virtual-currency-providers-on-15-may/>.

²⁰ See: <https://www.ourcommons.ca/DocumentViewer/en/42-1/FINA/report-24/>.

²¹ See: <https://www.parl.ca/DocumentViewer/en/42-1/bill/C-97/first-reading>.

PROPOSED RECOMMENDATIONS

In light of the foregoing, we propose the following recommendations:

1. Characterize and define what a “digital asset” is and the role it is intended to serve (i.e., method of payment, payment processing, open banking, investment contract, etc.) to (a) avoid ambiguity between asset classes and (b) clarify the objectives of provincial and federal legislation;
2. Determine in which circumstances digital assets might satisfy the “investment contract” test set forth in the Supreme Court of Canada’s decision in *Pacific Coast* (relying on the U.S. Supreme Court decision in *Howey*)²²;
3. Provide guidance or instruction with respect to know-your-client (“KYC”) and “suspicious transaction”²³ thresholds so as to mitigate risk, within a securities context, as applicable; and
4. Create dialogue with relevant stakeholders (e.g., provincial and federal governments, technology-driven entities, independents, etc.) so to ensure that provincial and federal legislative objectives are met, as well as those of legislation under international auspices (i.e., FATF²⁴, OECD²⁵ and other regulatory bodies).

In support of the foregoing recommendations, we respectfully submit that we have addressed such topics, including the reasoning and support therefore, in the FINA Brief. We encourage the addressees to review the discussion contained in the FINA Brief and, should you require further information, please do not hesitate to contact the undersigned. We look forward to having a fruitful ongoing dialogue with the AMF, OSC, IIROC and CSA.

Yours truly,



Me David Durand, B.Sc. (chem.), LL.L



Drew S. Dorweiler, FCBV, FRICS, CPA•ABV, CFE

²² In this regard, the undersigned refer the authorities to page 14 of the FINA Brief of July 2018, wherein it is written: “[...]. While the SEC has remained silent recently on the status of cryptoassets other than Bitcoin and Ethereum, it is reasonable that the CSA should re-evaluate its identification of various coins as investment contracts, and thus as a security.”

²³ See: <http://www.fintrac-canafe.gc.ca/guidance-directives/transaction-operation/Guide2/2-eng.asp> and http://www.fintrac-canafe.gc.ca/guidance-directives/transaction-operation/indicators-indicateurs/msb_mltf-eng.asp.

²⁴ Reference can be made to <https://cointelegraph.com/news/fatf-issues-preliminary-guidelines-on-digital-assets-to-combat-money-laundering>, as well as the recent guidelines it publishes with respect to <http://www.fatf-gafi.org/publications/fatfrecommendations/documents/regulation-virtual-assets-interpretive-note.html>.

²⁵ See: [http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=COM/SDD/DAF\(2018\)1&docLanguage=En](http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=COM/SDD/DAF(2018)1&docLanguage=En).

DON'T BLOCK THE BLOCKCHAIN: HOW CANADA CAN GUARD AGAINST MONEY LAUNDERING WHILE MAINTAINING GLOBAL COMPETITIVENESS

EXECUTIVE SUMMARY

Our study examines the current environment in Canada surrounding cryptoassets with a dual objective: how might the Government of Canada contribute to enhancing public trust in the financial system by securing it against money laundering and terrorism financing while fostering a domestic climate enabling participants in the cryptoasset/blockchain sector to thrive and compete favourably on an international basis?

1. INTRODUCTION

In today's digital world and economy, in which transactions know few borders, vigilance against money laundering and terrorism financing activities requires heightened international cooperation, including interoperability¹ and data exchanges amongst various domestic stakeholders. Such interoperability is required to involve Canada both domestically and as a founding member of the Financial Action Task Force ("FATF")² within the international community. To combat these threats, the Government of Canada enacted an anti-money laundering ("AML") and anti-terrorism financing ("ATF") legislative framework, including the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA)*,³ which is currently under statutory review.⁴ In this connection, the Government of Canada concurrently released a series of proposed amendments to the regulations made under the *PCMLTFA*, 2018⁵ on June 9, 2018 to "strengthen Canada's AML/ATF Regime, and ensure its measures are aligned with the FATF standards,"⁶ therefore meeting its international commitments (hereinafter the "Proposed Amendments"). According to the June 9, 2018 Regulatory Impact Assessment Statement of the Proposed Amendments [emphasis added]:

¹ "Interoperability" is defined as "the ability of the federal government's numerous security information systems to work together technically, legally, semantically (through standard terminology), and culturally (through the willingness of organizations to share information)," as set forth in chapter 1 of the 2009 March Status Report of the Auditor General of Canada, <http://www.oag-bvg.gc.ca/internet/English/parl_oag_200903_e_32304.html>.

² Canada, Government of Canada, *Money Laundering* (Ottawa: 2017) <http://international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_seculte/money_laundering-blanchiment_dargent.aspx?lang=eng> accessed 02 July 2018.

³ SC 2000, c 17 [*PCMLTFA*].

⁴ Canada, Department of Finance, *Reviewing Canada's Anti-Money Laundering and Anti-Terrorist Financing Regime*, (Ottawa: Department of Finance, 2018) <<https://www.fin.gc.ca/activity/consult/amlatfr-rpcfat-eng.asp>> accessed 01 July 2018.

⁵ Gazette, Part I, Volume 152, Number 23: Regulations Amending Certain Regulations Made Under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act, 2018, <<http://www.gazette.gc.ca/rp-pr/p1/2018/2018-06-09/html/reg1-eng.html>> accessed 04 July 2018 [Canada Gazette].

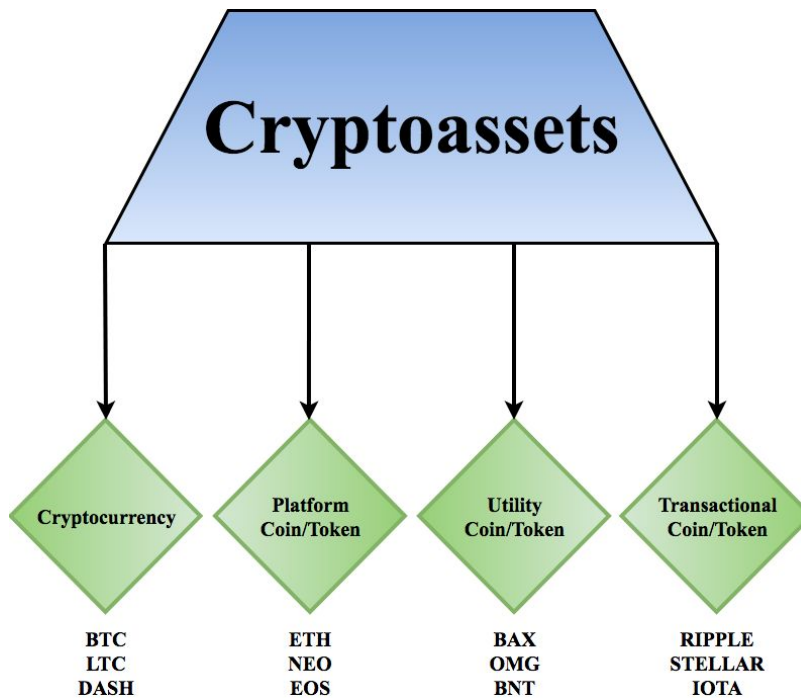
⁶ *Ibid.*

The proposed amendments to the regulations would strengthen Canada’s AML/ATF Regime by updating customer due diligence requirements and beneficial ownership reporting requirements; regulating businesses dealing in virtual currency; updating the schedules to the regulations; including foreign money service businesses (MSB) in Canada’s AML/ATF Regime; clarifying a number of existing requirements; and making minor technical amendments.⁷

2. WHAT ARE CRYPTOASSETS?

Bitcoin, Ether and Ripple have often been referred to as virtual currencies, which can be somewhat of a misnomer, as these “units” do not comprise currency. We shall define these units as “cryptoassets.” Within the Proposed Amendments⁸ put forth by the Department of Finance, as the term “virtual currency” is utilized, it creates judicial gaps, being that neither the said term, nor the often-used synonyms “digital currency” and “electronic money” are defined in Canadian legislation. Furthermore, the words “money” and “currency” do not accurately describe the inherent characteristics of a cryptoasset; *viz.*, a cryptoasset is not a store of value. Moreover, such units should not be considered to be commodities or securities, as will be outlined hereinbelow. For the purpose of harmonization and ease of use, the term cryptoassets has been used hereinafter. A visual representation of cryptoassets appears in Figure 1.

Figure 1: Cryptoasset Categories⁹



⁷ *Ibid.*

⁸ Canada Gazette, *supra* note 5.

⁹ Adam Haeems, “What is a crypto-asset” (27 April 2018), *Medium* (blog), online: <<https://medium.com/babb/what-is-a-crypto-asset-1f0fcc517887>>.

The term cryptoasset is a relatively new term describing digital assets that are recorded on a distributed public ledger. “Cryptoassets facilitate the decentralization of industries, removing the middlemen through the use of and peer-to-peer networking, reducing costs”¹⁰ and improving efficiency and accuracy. While various terms such as cryptocurrency, virtual currency, utility token, transactional token and platform token are often used synonymously, these all fall under the umbrella of cryptoassets.

In the Canadian regulatory sphere, various Canadian regulatory bodies have been struggling with the definition of “virtual currencies,” including cryptoassets, under the headers of currencies, securities and commodities. Under the regulatory regime of the United States, Americans have been facing similar problems. In July 2017, the U.S. Securities and Exchange Commission (“SEC”) stated that cryptoassets or, in the SEC’s terminology, “digital assets,” would be subject to securities law under this regulatory body.¹¹ Less than one year later, in June 2018, during the *Yahoo! All Markets Summit: Crypto* event, the SEC’s Director for Corporate Finance stated in a presentation that the SEC no longer considered Bitcoin and Ether to constitute securities.¹²

Moreover, the U.S. Financial Crimes Enforcement Network (“FinCEN”) settled with Ripple Labs Inc., and its subsidiary XRP II, LLC in a \$700,000 civil suit, where it was made clear the FinCEN had considered XRP to constitute the “currency of the Ripple network” based on the statement of facts in the settlement agreement.¹³ Furthermore, since September 17, 2015, the Commodity Futures Trading Commission (“CFTC”) has considered Bitcoin and other virtual currencies to be commodities, as determined in the matter of *Coinflip, Inc., d/b/a Derivabit, and Francisco Riordan*.¹⁴ This decision was re-affirmed during the granting of CFTC’s preliminary injunction against Patrick K. McDonnell and CabbageTech, Corp. d/b/a Coin Drop Markets in March 2018 when a federal judge ruled that virtual currencies like Bitcoin will be regulated as commodities by the CFTC.¹⁵

¹⁰ *Ibid.*

¹¹ Securities and Exchange Commission, Release No 81207, *Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO* (25 July 2017), online: Securities and Exchange Commission <<https://www.sec.gov/litigation/investreport/34-81207.pdf>>.

¹² William Hinman, “Digital Asset Transactions: When Howey Met Gary (Plastic)” (June 14 2018), online: SEC <<https://www.sec.gov/news/speech/speech-hinman-061418>>.

¹³ U.S. Department of Justice, United States Attorney Northern District of California, *Settlement Agreement*, (between United States Attorney’s Office in the Northern District of California v Ripple Labs Inc.) online: DOJ <https://www.justice.gov/sites/default/files/opa/press-releases/attachments/2015/05/05/settlement_agreement.pdf>.

¹⁴ *Commodity Futures Trading Commission v Coinflip, Inc., Derivabit, and Francisco Riordan* (17 September 2015), CFTC Docket No 15-29, online: Commodity Futures Trading Commission <<https://www.cftc.gov/sites/default/files/idc/groups/public/@lrenforcementactions/documents/legalpleading/enfcoi nfliprorder09172015.pdf>>.

¹⁵ *Commodity Futures Trading Commission v Patrick K. McDonnell, and CabbageTech Corp. d/b/a Coin Drop Markets* (6 March 2018), 18-CV-361, online: Commodity Futures Trading Commission <<https://www.cftc.gov/sites/default/files/idc/groups/public/@lrenforcementactions/documents/legalpleading/enfcoi ndroporder030618.pdf>> [*CabbageTech*].

3. WHAT IS BLOCKCHAIN?

In order to understand cryptoassets, we must begin with an introduction of the underlying technology through which cryptoassets are created. One of the features of cryptoassets is the use of blockchain technology, which provides users anonymity, and a payment system structure.¹⁶ Blockchain is a “distributed ledger that is usually managed by a peer-to-peer network.”¹⁷ In a blockchain, each transaction is separated into various blocks that are attached to one another using the “hash value of the previous block” which is referred to as that block’s “parent.”¹⁸ Each block contains several transactions. As blocks are hashed together, the ensuing structure creates a blockchain. New blocks are added to the chain through a process known as mining, wherein miners are rewarded with an amount of a cryptoasset for solving mathematical equations through computation.¹⁹ A timestamp, and a nonce, which is a pseudo-random number for verifying the hash, are also included on each block.

Blockchain is a unique means which can be used to prevent fraud, since any change in a block would alter the hash value of the block. In order for a block to be added to the blockchain it must first be validated. “A majority of nodes [a computer which is connected to the cryptoasset network] in the network agree by a consensus mechanism on the validity of transactions in a block and on the validity of the block itself”²⁰ before a particular block will be added to the blockchain. Once the information has been entered onto the blockchain, it can never be erased, creating a public and verifiable ledger through which every single transaction ever made on this blockchain can be observed.²¹ A copy of the blockchain is automatically downloaded to every computer that is connected to the cryptoasset network.²²

4. WHAT IS CURRENCY?

In Canada, “currency” is defined and regulated by statute under the *Currency Act*.²³ The *Currency Act* established that the monetary unit in Canada shall be measured in Canadian dollars (“CAD”), and the denominations of money will be in dollars and cents.²⁴ Under section 13 of the *Currency Act*, it is stipulated that [emphasis added]:

Every contract, sale, payment, bill, note, instrument and security for money and every transaction, dealing, matter and thing relating to money or involving the payment of or the liability to pay money shall be made, executed, entered into, done or carried out in the currency of Canada, unless it is made, executed, entered into, done or carried out in

¹⁶ United States, Press Release, “IBM Announces Major Blockchain Solution to Speed Global Payments” (16 October 2017), online IBM: < <https://www-03.ibm.com/press/us/en/pressrelease/53290.wss>>.

¹⁷ Yan Chen, “Blockchain Tokens and the Potential Democratization of Entrepreneurship and Innovation” (2017) 61:4 Business Horizons 567.

¹⁸ M. Nofer et al., “Blockchain” (2017) 59:3 Bus Inf Syst Eng 183.

¹⁹ Oleg Straitev, “Crypto-currency and Blockchain: How to Regulate Something We Do Not Understand” (2018) 33:2 BFLR 90.

²⁰ Nofer, *supra* note 18 at 184.

²¹ Steve Mitch, “Crypto Currency & Block Chain Technology: A Decentralized Future, RBC Capital Markets” (January 3 2018) at 1. online: RBC Capital Markets <<https://ca.rbcwealthmanagement.com/documents/616937/616953/Crypto+Currency+%2B%20Blockchain++RBC++2018+01+03.pdf/61959d80-b77b-43c4-80cb-38e1187793a1>>.

²² Investopedia, Blockchain, *Investopedia* (blog), online: <<https://www.investopedia.com/terms/b/blockchain.asp>>.

²³ RSC, 1985, c C-52.

²⁴ *Ibid* at s 3 and s 7.

- (a) the currency of a country other than Canada; or
- (b) a unit of account that is defined in terms of the currencies of two or more countries.

The *Currency Act* also states that the only coins which may be used as currency of Canada must be minted by the Royal Canadian Mint or have been issued by the “Crown in any province of Canada before it became part of Canada and if the coin was, immediately before October 15, 1952, current and legal tender in Canada.”²⁵ The value of currency as a payment of money “derives solely from the quality of being legal tender which is conferred to them by section [8](1) of the *Currency Act*.”²⁶

5. ARE CRYPTOASSETS CURRENCIES?

If cryptoassets are to be defined as a currency, it would mean that they could be used to purchase goods and services. It could also be argued that cryptoassets are not currencies *per se*, as a currency by general definition consists of “notes and coins that are of fixed nominal values and are issued or authorized by the central bank or government.”²⁷ By way of example, it has been mentioned that Bitcoin “operates without a centralized steering-mechanism and without direct intervention of central private regulator.”²⁸

As the *Currency Act* is the statutory basis for currency regulation in Canada, it requires that money²⁹ or currency must serve three primary functions:³⁰

- (i) It is a generally accepted medium of exchange;
- (ii) It serves as a unit of account; and
- (iii) It can be used as a store of value.

For cryptoassets to be considered money under the Bank of Canada’s guidelines, they would need to satisfy all three of these criteria. We do not contend that cryptoassets cannot serve as a unit of account; however, they currently appear to fall short in terms of being viewed as a generally-accepted medium of exchange or as a store of value. Nevertheless, potential exists for success in this area as there are vendors throughout Canada that allow for transactions to be conducted in Bitcoin and/or other cryptoassets. One of the issues in the legitimization of cryptoassets as a currency is that a large number of the vendors that accept cryptoassets continue to base the “underlying value of transactions... in terms of national currencies such as the U.S. or Canadian dollar”³¹ instead of denominating such transactions in cryptoasset units.

²⁵ *Ibid* at s 7(1)(b).

²⁶ Guy David, “Money in Canadian Law” (1986) 65 Can Bar Rev 192 at 200.

²⁷ Public Sector Debt, p. 1-6, online: OECD statistics <https://www.oecd.org/statistics/data-collection/Public%20sector%20Debt_guidelines.pdf>.

²⁸ Rainer Kulms, “Bitcoin – a Technology and a Currency” Central Bank Journal of Law and Finance, No. 1/2016.

²⁹ Straitev, *supra* note 19 at 199.

³⁰ Johnson Grahame, Pomorski Lukasz, *Briefing on Digital Currencies*, Senate of Canada, Ottawa Ontario, (2, April 2014), online: Bank of Canada <https://www.bankofcanada.ca/wp-content/uploads/2014/04/Senate_statement.pdf> at 8.

³¹ *Ibid*.

Many major Canadian financial institutions currently ban “credit and debit card customers from participating in [cryptoasset] purchases with their cards,”³² including BMO Financial Group and TD Bank, while Royal Bank of Canada accepts cryptoasset transactions in only very limited circumstances. In a leaked memo, BMO apparently restated its decision to ban these transactions was “due to the volatile nature of cryptocurrencies and to better protect the security of our clients and the bank.”³³

The current prevailing climate indicates that the majority of the financial institutions in Canada are hesitant to deal with any business related to cryptoassets, including cryptoasset exchanges. Such reluctance is not strictly a Canadian initiative. The Commonwealth Bank of Australia stated that it will no longer allow its customers to acquire cryptoassets with credit cards, stating, “we have made this decision because we believe virtual currencies do not meet a minimum standard of regulation, reliability, and reputation when compared to currencies that we offer to our customers. Given the dynamic, volatile nature of virtual currency markets, this position is regularly reviewed.”³⁴

It is difficult to argue that cryptoassets should be characterized as a currency when the institutions that are most closely connected to the exchange of currency are hesitant in allowing their customers to purchase cryptoassets with their credit and debit card payment systems. As in the case of the newly-regulated cannabis regime in Canada, it appears that financial institutions may be less reluctant to facilitate cryptoasset transactions once proper regulatory practices and procedures are established, as illustrated by the recent \$250 million loan facility granted by BMO Financial Group, one of the “big-six” Canadian banks, to Aurora Cannabis Inc.³⁵

³² Nathan Reiff, “Canada Banks Ban Users from Buying Cryptocurrency” (11 April 2018), *Investopedia* (blog), online < <https://www.investopedia.com/news/canada-banks-ban-users-buying-cryptocurrency/>>.

³³ Aziz Abdel-Qader, “Cryptocurrency Ban Expands Across Canadian Banks as BMO Joins Crackdown”, *Finance Magnates* (30 March 2018), online: Finance Magnates <<https://www.financemagnates.com/cryptocurrency/news/cryptocurrency-ban-expands-across-canadian-banks-bmo-joins-%E2%80%8Ecrackdown/>>.

³⁴ Commonwealth Bank of Australia, “Commonwealth Bank Blocks Credit Card Purchases of Virtual Currencies” (14 February 2018), online: On the Record < <https://www.commbank.com.au/cs/newsroom/virtual-currency-credit-card-block-201802.html?ei=card-view>>.

³⁵ The Canadian Press, “Aurora Cannabis signs loan deal for up to \$250-million with Bank of Montreal”, *The Globe and Mail* (26 June 2018), online: The Canadian Press < <https://www.theglobeandmail.com/business/article-aurora-cannabis-signs-loan-deal-for-up-to-250-million-with-bank-of/>>.

While it has been argued that cryptoassets may be utilized as a store of value, the observed high levels of volatility make them a less-than-ideal medium to be used as a currency. Examples of cryptoasset volatility include Bitcoin growing by 1,318% in 2017 while ranking 14th among the fastest-growing cryptoassets of the year. Ripple was the top performer in 2017 due to its value rising 36,018%, followed by NEM and Ardor which grew 29,842% and 16,808%, respectively.³⁶ Ethereum also rose 9,162% in 2017.³⁷ According to Gangwal *et al*, the daily volatility of Bitcoin is calculated at 7.18%, which is approximately ten times higher than the volatility of fiat currencies backed by central banks or governments.³⁸ In order to be a legitimate store of value, “economic agent[s] should be able to transfer his/her purchasing power over time, especially on the short term.”³⁹ This extreme price volatility experienced significantly contributes to the rejection of the argument that cryptoassets should be considered as a store of value and, hence, regulated as a currency.

Thus, for cryptoassets to fall within the category of currency, the *Currency Act* would have to be amended by the Canadian legislature. Based on the foregoing, it would be incorrect to equate cryptoassets to currency *stricto sensu*.

³⁶ Wong, Ian Joon, “2017’s biggest cryptoassets ranked by performance”, online: The Atlas <<https://www.theatlas.com/charts/B1pWqcDQM>>.

³⁷ *Ibid*.

³⁸ Sashwat Gangwal and François Longin, “Extreme Movements in Bitcoin prices: A study based on extreme value theory” (2017) at 5 online: Longin Inside <https://www.longin.fr/Recherche_Publications/Resume_pdf/Gangwal_Longin_Extreme_movements_Bitcoin_prices.pdf>.

³⁹ *Ibid* at page 6.

6. WHAT IS A SECURITY?

In order to determine whether a cryptoasset should fall under the purview of provincial and territorial securities legislation, it is vital to understand what a security is, pursuant to the applicable legislative enactment. Generally, securities are financial instruments or claims issued by businesses or financial organizations to investors with the objective of raising capital for enterprises. Though not defined in each provincial and territorial securities legislation, the Ontario *Securities Act*, by way of example, defines a security.⁴⁰

Securities in Canada are regulated by provincial or territorial regulators, who are “organized and coordinated”⁴¹ by the Canadian Securities Administrators (“CSA”). Their aim is to create some sense of conformity and uniformity across the thirteen (13) Canadian jurisdictions. From time-to-time, the provincial and territorial regulators release policies that provide some insight into the interpretation of existing securities legislation.⁴² Staff Notices, which are released by the CSA, also provide insight on potential future policies created by provincial and territorial regulators. The objectives of the securities regulators are fairly consistent, as they are focused on the idea that “investors pay enormous amounts of money to strangers for completely intangible rights, whose value depends entirely on the quality of the information that the investor receives and on the seller’s honesty.”⁴³

The purpose of provincial and territorial securities legislation is fairly standardized. For example, under the Ontario *Securities Act*, it is stated at section 1.1 thereof that:

⁴⁰ RSO 1990, c S.5, at s 1(1) [*Securities Act*], wherein security is defined as:

- (a) any document, instrument or writing commonly known as a security,
- (b) any document constituting evidence of title to or interest in the capital, assets, property, profits, earnings or royalties of any person or company,
- (c) any document constituting evidence of an interest in an association of legatees or heirs,
- (d) any document constituting evidence of an option, subscription or other interest in or to a security,
- (e) a bond, debenture, note or other evidence of indebtedness or a share, stock, unit, unit certificate, participation certificate, certificate of share or interest, preorganization certificate or subscription other than,
- (i) a contract of insurance issued by an insurance company licensed under the *Insurance Act*, and
- (ii) evidence of a deposit issued by a bank listed in Schedule I, II or III to the *Bank Act* (Canada), by a credit union or league to which the *Credit Unions and Caisses Populaires Act, 1994* applies, by a loan corporation or trust corporation registered under the *Loan and Trust Corporations Act* or by an association to which the *Cooperative Credit Associations Act* (Canada) applies,
- (f) any agreement under which the interest of the purchaser is valued for purposes of conversion or surrender by reference to the value of a proportionate interest in a specified portfolio of assets, except a contract issued by an insurance company licensed under the *Insurance Act* which provides for payment at maturity of an amount not less than three quarters of the premiums paid by the purchaser for a benefit payable at maturity,
- (g) any agreement providing that money received will be repaid or treated as a subscription to shares, stock, units or interests at the option of the recipient or of any person or company,
- (h) any certificate of share or interest in a trust, estate or association,
- (i) any profit-sharing agreement or certificate,
- (j) any certificate of interest in an oil, natural gas or mining lease, claim or royalty voting trust certificate,
- (k) any oil or natural gas royalties or leases or fractional or other interest therein,
- (l) any collateral trust certificate,
- (m) any income or annuity contract not issued by an insurance company,
- (n) any investment contract,
- (o) any document constituting evidence of an interest in a scholarship or educational plan or trust, and
- (p) any commodity futures contract or any commodity futures option that is not traded on a commodity futures exchange registered with or recognized by the Commission under the *Commodity Futures Act* or the form of which is not accepted by the Director under that Act,

⁴¹ Canadian Securities Administrators, *About CSA: Overview* (Montreal: Canadian Securities Administrators, 2009) <<https://www.securities-administrators.ca/aboutcsa.aspx?id=45>>.

⁴² *Securities Act*, *supra* note 40 at s 143.8.

⁴³ Bernard Black, “The Legal and Institutional Preconditions for Strong Securities Markets”, (2001) 48:4, *UCLA Law Review*, online: Northwestern Scholars <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=182169>.

The purposes of this Act are:

- (a) to provide protection to investors from unfair, improper or fraudulent practices;
- (b) to foster fair and efficient capital markets and confidence in capital markets; and
- (c) to contribute to the stability of the financial system and the reduction of systemic risk.⁴⁴

The issue of regulating of cryptoassets as securities arose following a 2016 U.S. incident in which there was an attempt at a cryptocurrency heist after an Initial Coin Offering (“ICO”), which had raised \$150 million USD, became the largest crowdfunding project in history.⁴⁵ Through an anomaly in the system, a hacker was able to divert approximately \$50 million USD worth of assets from the ICO into another account.⁴⁶ While the hacker was unable to receive the assets and the transaction was cancelled, this attack led critics to question under which particular regime such ICOs should be regulated.⁴⁷ In response to this attack, the SEC released a report to determine whether the ICO in the aforementioned attack, as well as other cryptoassets, should fall under the auspices of U.S. federal securities laws.⁴⁸ The SEC was of the opinion that various cryptoassets fall within the scope of the *Securities Act*.⁴⁹ More specifically, the SEC concluded that many cryptoassets may be considered *prima facie* to constitute an “investment contract” pursuant to section 2(a)(1) of the U.S. *Securities Act*.⁵⁰

⁴⁴ *Securities Act*, *supra* note 40.

⁴⁵ David Siegel, “Understanding the DAO Attack” Coindesk (blog) (25 June 2016), online: <www.coindesk.com/understanding-dao-hack-journalists/>.

⁴⁶ *Ibid.*

⁴⁷ *Ibid.*

⁴⁸ United States, Securities and Exchange Commission, Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO (Release No 81207) (Washington, DC: US Government Printing Office, 2017).

⁴⁹ 15 U.S.C. § 77a.

⁵⁰ *Ibid.*

In response to the SEC finding above, the CSA released Staff Notice 46-307⁵¹ (“Staff Notice 46-307”) on August 24, 2017, in which the CSA warned that many “cryptocurrency offerings, such as initial coin offerings (ICO), initial token offerings (ITO) and sales of securities of cryptocurrency investment funds” would fall under the securities laws of Canada, as they would be considered investment contracts (similar to the status thereof in the United States). To support its position, the CSA refers to the four-prong test set forth in *Pacific Coast Coin Exchange v. Ontario (Securities Commission)*⁵² (“*Pacific Coast*”) to determine whether a coin or token would be considered to be an investment contract. The *Pacific Coast* four-prong test reads:⁵³

- (1) Does the scheme involve an investment of money?
- (2) Is the scheme in a common enterprise?
- (3) Has an investment of money been made with the intention of profit?
- (4) Are the profits to come solely from the efforts of others?

In order for a cryptoasset to be considered an investment contract under the current judicial precedent, each component of this test must be answered in the affirmative. Only then would a cryptoasset be considered a security and therefore subject to Canadian securities laws.

Interestingly, on June 11, 2018, the CSA released Staff Notice 46-308,⁵⁴ in which it outlined fourteen (14) situations that impact the presence of one or more of the elements of an investment contract. In Staff Notice 46-308, the CSA referred to its own publication, Staff Notice 46-307, writing [emphasis added]:

⁵¹ Canadian Securities Administrators, “CSA Staff Notice 46-307: Cryptocurrency Offerings”, 40 OSCB 7233 at 7321 (Toronto: OSCB, 24 August 2017), online: Canadian Securities Administrators <http://www.osc.gov.on.ca/en/SecuritiesLaw_csa_20170824_cryptocurrency-offerings.htm>.

⁵² [1978] 2 SCR 112, 1977 CarswellOnt 50, 2 BLR 212 [*Pacific Coast*]. The majority held at page 113-114:

Per Martland, Judson, Ritchie, Spence, Pigeon, Dickson, Beetz and de Grandpré JJ.: Section 35 of the Act prohibits anyone trading in a security in the absence of a prospectus and section 1(1) (22) xiii defines security as including “any investment contract, other than an investment contract within the meaning of *The Investment Contracts Act*”. [The contract in question was not one covered by *The Investment Contracts Act*]. While the term investment contract is not defined, the policy of the legislation is clearly the protection of the public through full, true and plain disclosure of all material facts relating to securities being issued. The fourteen subdivisions of the definition encompass practically all types of transactions and indeed the definition had to be narrowed down by the long list of exceptions in s. 19. The categories in the definition are not mutually exclusive and are in the nature of ‘catchalls’. Such remedial legislation should be construed broadly. Substance, not form, is the governing factor. The legislation is not aimed solely at schemes that are actually fraudulent but rather relates to arrangements that do not permit the customers to know exactly the kind of investment they are making.

The Supreme Court of the United States in *SEC v. W.J. Howey Co.*, 328 U.S. 293 (1946), with the foregoing in mind laid down the test “Does the scheme involve ‘an investment of money in a common enterprise, with profits to come solely from the efforts of others?’” In the case at bar all aspects of this test can be answered in the affirmative. Clearly an investment of money was involved; as to the common enterprise aspect the only commonality necessary for an investment contract is that between the investor and promoter; and as to the dependence of the customer for the success of the enterprise the end result of the investment by each customer was dependent upon the quality of the expertise brought to the administration of the funds obtained by appellant from its customers. The test to determine the economic realities of a securities transaction based on “the risk capital approach” adopted by the Supreme Court of Hawaii in *State of Hawaii v. Hawaii Marker Center, Inc.*, 485 P. 2d 105, results in the same conclusion that the agreement in question is an investment contract.

The facts were examined in the sole light of the *Howey* and *Hawaii* tests at the invitation of the parties. A broader approach could however have been taken. The clear legislative policy was to replace the harshness of *caveat emptor* in security related transactions and the courts should seek to attain that goal even if tests formulated in prior cases prove ineffective and have to be broadened in scope.

⁵³ *Ibid* at pg 128.

⁵⁴ Canadian Securities Administrators, “CSA Staff Notice 46-308 Securities Law Implications for Offerings of Tokens”, (Toronto: OSCB, 11 June 2018), online: Canadian Securities Administrators <http://www.osc.gov.on.ca/documents/en/Securities-Category4/csa_20180611_46-308_implications-for-offerings-of-tokens.pdf>.

[...] As indicated in SN 46-307 every offering is unique and must be assessed on its own characteristics. An offering of tokens may involve the distribution of securities because:

- the offering involves the distribution of an investment contract; and/or
- the offering and/or the tokens issued are securities under one or more of the other enumerated branches of the definition of security or may be a security that is not covered by the non-exclusive list of enumerated categories of securities.

In determining whether or not an investment contract exists, the case law endorses an interpretation that includes considering the objective of investor protection. This is especially important for businesses to consider in the context of offerings of tokens where the risk of loss to investors can be high. Businesses and their professional advisors should consider and apply the case law interpreting the term “investment contract” [FN1], including considering whether the offering involves:

1. An investment of money
2. In a common enterprise
3. With the expectation of profit
4. Derived significantly from the efforts of others

In analyzing whether an offering of tokens involves an investment contract, businesses and their professional advisors should assess not only the technical characteristics of the token itself, but the economic realities of the offering as a whole, with a focus on substance over form.

We have received submissions from businesses and their professional advisors that a proposed offering of tokens does not involve securities because the tokens will be used in software, on an online platform or application, or to purchase goods and services. However, we have found that most of the offerings of tokens purporting to be utility tokens that we have reviewed to date have involved the distribution of a security, namely an investment contract. The fact that a token has a utility is not, on its own, determinative as to whether an offering involves the distribution of a security.

Examples of situations and their possible implication on one or more of the elements of an investment contract

We have identified in the table below situations that have an implication on the presence of one or more of the elements of an investment contract. [...] ⁵⁵

⁵⁵ *Ibid.*

[FN1]: See, for example: the Supreme Court of Canada's decision in *Pacific Coast Coin Exchange v. Ontario (Securities Commission)*, [1978] 2 SCR 112, the Ontario Securities Commission's decision in *Universal Settlements International Inc.* (2006), 29 OSCB 7880, and the Alberta Securities Commission's decisions in *The Land Development Company Inc. et al* (2002), ABSECCOM REA #1248840 v1 and *Kustom Design Financial Services Inc. (Re)*, 2010 ABASC 179.

In Staff Notice 46-308, the CSA also refers to its Regulatory Sandbox,⁵⁶ the purpose of which is to allow:

[...] firms to register and/or obtain exemptive relief from securities laws requirements, under a faster and more flexible process than through a standard application, in order to test their products, services and applications throughout the Canadian market on a time-limited basis.

The CSA Regulatory Sandbox is part of the CSA's 2016-2019 Business Plan to gain a better understanding of how technology innovations are impacting capital markets, assess the scope and nature of regulatory implications and what may be required to modernize the securities regulatory framework for fintechs.⁵⁷

Moreover, the CSA has published a list of decisions⁵⁸ granted through the CSA Regulatory Sandbox, as well as the terms and conditions of registration of the firms authorized to participate in the CSA Sandbox.

7. ARE CRYPTOASSETS SECURITIES?

In Staff Notice 46-307, the CSA made it clear that “in many instances [the CSA] found that the coins/tokens in question constitute securities for the purposes of securities laws.”⁵⁹ If cryptoassets are to be considered investment contracts, many extraneous securities law obligations would arise that are not present in the current regulatory sphere. Included in these obligations would be the prospectus requirement (or corresponding exemption) and the registration requirement (and/or its corresponding exemption).⁶⁰ These obligations would be much more onerous than the current requirements put forth by the various regulatory bodies that are trying to regulate this space. When considering whether or not securities law is going to apply to a cryptoasset, the CSA has mentioned it will “consider substance over form” when determining whether or not that particular asset should be considered a security. For example, the SEC is under the impression that neither Bitcoin nor Ether should be considered a security under the current securities regulations.⁶¹

⁵⁶ *Ibid.*

⁵⁷ *Ibid.*

⁵⁸ Canadian Securities Administrators, *CSA Regulatory Sandbox* (Montreal: Canadian Securities Administrators, 2009) <https://www.securities-administrators.ca/industry_resources.aspx?id=1626>.

⁵⁹ Canadian Securities Administrators, *supra* note 51.

⁶⁰ *Ibid.*

⁶¹ Hinman, *supra* note 12.

Currently, the CSA appears to be of the view that many cryptoassets should be treated as securities and consequently become subject to stringent regulatory obligations, despite the SEC's reversal on its classification of cryptoassets as securities. Indeed, the SEC recently announced in a June 14, 2018 statement⁶² that it no longer considered *Ether* or *Bitcoin* to be securities. In this statement, the SEC reviewed whether cryptoassets would be deemed securities according to *SEC v Howey*,⁶³ one of the U.S. Supreme Court decisions that the Supreme Court of Canada ("SCC") refers to in *Pacific Coast* regarding the above four-prong test for investment contracts.⁶⁴ Through its application of the four-prong test, the SEC expressed concern that purchasers of a cryptoasset would "no longer reasonably expect a person or group to carry out essential managerial or entrepreneurial efforts."⁶⁵

In these cases, when a cryptoasset reaches the level where it is so decentralized that any third-party activity no longer influences its success, the identification of such third parties no longer plays a vital role in protecting the rights and interests of the users of the cryptoassets. When these third parties lose their influence to exert any influence on these decentralized networks, specific information regarding their "background, financing, plans, financial stake and so forth"⁶⁶ become minimally relevant to the efficient functioning of the market for the cryptoasset.

Bitcoin was supposedly created by someone under the pseudonym Satoshi Nakamoto, who released a paper entitled "Bitcoin: A Peer-to-Peer Electronic Cash System"⁶⁷ on October 31, 2008, which detailed a system of decentralized peer-to-peer electronic transactions. The Bitcoin network was established on January 3, 2009, when Mr. Nakamoto mined the first Bitcoin block and was rewarded with 50 bitcoins.⁶⁸ As the Bitcoin network has been decentralized since its creation,⁶⁹ attempting to regulate Bitcoin as a security in Canada would be highly ineffective from an enforcement perspective.

⁶² *Ibid.*

⁶³ *SEC v W.J. Howey Co.*, 328 U.S. 293 (1946).

⁶⁴ *Pacific Coast*, *supra* note 52 at 128.

⁶⁵ Hinman, *supra* note 12.

⁶⁶ *Ibid.*

⁶⁷ Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", (31 October 2008), online: <<https://bitcoin.org/bitcoin.pdf>>.

⁶⁸ Benjamin Wallace, "The Rise and Fall of Bitcoin", *Wired* (blog) (23 November 2011), online: <https://www.wired.com/2011/11/mf_bitcoin/>.

⁶⁹ Hinman, *supra* note 12.

In late 2013, a Canadian by the name of Vitalik Buterin proposed the development of the Ethereum network; the pre-sale of Ether tokens began on July 22, 2014 and raised over \$14 million USD by August 6, 2014.⁷⁰ Subsequently, the network has grown exponentially, with Ether currently ranking second behind Bitcoin in market capitalization.⁷¹ The SEC has proposed a similar treatment for Ether and Bitcoin: based on the decentralization of the current Ethereum network, Ether transactions should not be subject to disclosure requirements under U.S. securities laws.⁷² Requiring securities disclosure for such cryptoassets, where the distributed network is functional and efficient without any significant influence exerted by a third-party, provides little benefit. While securities regulations are intended to protect investor rights, as well as those of other stakeholders, in decentralized systems such as those underpinning cryptoassets, there is very little that securities regulatory bodies need do to protect its users, as no single participant is able to manipulate the network.

While the SEC has remained silent recently on the status of cryptoassets other than Bitcoin and Ethereum, it is reasonable that the CSA should re-evaluate its identification of various coins as investment contracts, and thus as a security. Proposing overreaching securities regulation on the cryptoasset regime would likely create a system where onerous requirements are placed on users of such assets, with an end result of suppressing innovation in financial technology and motivating human and financial capital to leave Canada seeking more favourable environments.

Given the nature of cryptoassets, they do not fit the definition of a security. The fact that securities regulations would have scant effect in protecting users on decentralized networks makes it evident that defining cryptoassets as a security would provide ineffective regulatory enforcement in this respect.

Thus, it could be postulated that a divergence of position and legislative interpretation has formed between various jurisdictions with respect to the characterization of cryptoassets as a security.

8. DIVISION OF POWERS - A LOOMING CONFLICT FOR REGULATORY OVERSIGHT OF CRYPTOASSETS

During June 2018, both the provincial and federal levels of government were active in releasing numerous documents regarding cryptoassets, including Proposed Amendments, Staff Notices, studies and other documents; the latest of which was published by the Ontario Securities Commission (“OSC”) on June 28, 2018.⁷³

⁷⁰ Investoo Group, “History of Ethereum: How it’s set to overtake Bitcoin by 2018”, (June 26 2017), online: Investoo Group (blog), online: Mining < <http://www.mining.com/web/history-ethereum-set-overtake-bitcoin-2018/>>.

⁷¹ “Top 100 Cryptocurrencies By Market Capitalization”, online: CoinMarketCap: <<https://coinmarketcap.com/coins/>> [Top 100].

⁷² Hinman, *supra* note 12.

⁷³ Ontario, Ontario Securities Commission, *Taking Caution: Financial Consumers and the Cryptoasset Sector* (Toronto: Ontario Securities Commission, 2018) <https://www.osc.gov.on.ca/documents/en/Investors/inv_research_20180628_taking-caution-report.pdf>.

In this publication entitled *Taking Caution: Financial Consumers and the Cryptoasset Sector*, the OSC claims that “most ICOs are subject to securities regulations,”⁷⁴ referring to their own studies, without disclosing the methodology or the sample set, as well as to other reports. Throughout this publication, the OSC provides various statistics from a survey of Ontarians who own or have owned cryptoassets relating to motives and methods of purchase, as well as various other pieces of information. At one point, the OSC comments that many users of cryptoassets are unsure of whether cryptoassets are subject to regulation and, if so, who the regulatory authority might be. In response to their finding, the OSC asserts “this belief is incorrect. The OSC regulates ICOs that constitute securities offerings.”⁷⁵ CSA Staff Notice 46-308 is mentioned as the authority from where this regulatory power is derived.

However, as stated in section 143.8 of the *Securities Act* of Ontario, even when a Staff Notice becomes a policy, it “is not of a legislative nature.”⁷⁶ Furthermore, the *Securities Act* is clear that before a Staff Notice becomes a policy, the public must be provided “reasonable opportunity to interested persons and companies to make written representations with respect to the proposed policy within a period of at least 60 days after the publication.”⁷⁷ Thus, review of a Staff Notice is necessary before it becomes policy; while the OSC may be able to provide “guidance on the potential application of, and possible approaches required to comply with, securities legislation,” its current role in regulating ICOs has not been defined by either Canadian or Provincial regulators or legislation.

Interestingly, CSA Staff Notice 46-308 further refers the reader to *Reference Re Securities Act (Canada)*⁷⁸ (“*Re Securities Act*”), consisting of an opinion rendered by the SCC in which it analyzed the extent of the ability of the Parliament of Canada to use its trade and commerce power under the section 91 of the *Constitution Act, 1867*.⁷⁹ At paragraph 45 of *Re Security Act*, the Supreme Court of Canada wrote:

[45] The provincial power over securities extends to impacts on market intermediaries or investors outside a particular province (*Global Securities*, at para. 41; *R. v. W. McKenzie Securities Ltd.* (1966), 56 D.L.R. (2d) 56 (Man. C.A.), leave to appeal refused, [1966] S.C.R. ix (*sub nom. West & Dubros v. The Queen*); *Gregory & Co. v. Quebec Securities Commission*, [1961] S.C.R. 584). The case law also recognizes provincial jurisdiction where the province’s capital markets are engaged (*Québec (Sa Majesté du Chef) v. Ontario Securities Commission* (1992), 10 O.R. (3d) 577 (C.A.), leave to appeal refused, [1993] 2 S.C.R. x (*sub nom. R. du chef du Québec v. Ontario Securities Commission*); *Bennett v. British Columbia (Securities Commission)* (1992), 94 D.L.R. (4th) 339 (B.C.C.A.)).

In other words, the SCC “[...] sank the federal government’s attempt to create a national securities regulator. The Court ruled that the proposed Canadian *Securities Act* (Act), as presently drafted, is *ultra vires* the federal government.”⁸⁰ The SCC further noted:

⁷⁴ *Ibid* at 1.

⁷⁵ *Ibid* at 5.

⁷⁶ *Securities Act*, *supra* note 40 at s 143.8(1).

⁷⁷ *Securities Act*, *supra* note 40 at s 143.8(5).

⁷⁸ 2011 SCC 66, [2011] 3 SCR 837 [*Re Securities Act*].

⁷⁹ (UK), 30 & 31 Vict, c 3, reprinted in RSC 1985, App II, No 5 [*Constitution Act*].

⁸⁰ Wayne Gray and Stephen Ganttner, “Supreme Court’s Unanimous Ruling Sinks Canadian *Securities Act* (But Leave Much to be Salvaged)” (23 December 2011), *McMillan LLP* (blog), online: <<https://mcmillan.ca/Supreme-Courts-Unanimous-Ruling-Sinks-Canadian-Securities-Act-But-Leaves-Much-to-be-Salvaged>>.

To determine the constitutional validity of legislation from a division of powers perspective, the pith and substance analysis requires the courts to look at the purpose and effects of the law. The inquiry then turns to whether the legislation falls under the head of power said to support it. If the pith and substance of the legislation is classified as falling under a head of power assigned to the adopting level of government, the legislation is valid. When a matter possesses both federal and provincial aspects, the double aspect doctrine may allow for the concurrent application of both federal and provincial legislation.

Though Parliament's power over the regulation of trade and commerce under s. 91(2) of the *Constitution Act, 1867* has two branches – the power over interprovincial commerce and the general trade and power – “[...] it cannot be used in a way that denies the provincial legislatures the power to regulate local matters and industries within their boundaries. Nor can the power of the provinces deprive the federal Parliament of its powers under s. 91(2) to legislate on matters of genuine national importance and scope – matters that transcend the local and concern Canada as a whole.” As the Supreme Court of Canada further stated in the summary of in *Re Securities Act* [emphasis added]:

As held in *General Motors of Canada Ltd. v. City National Leasing*, [1989] 1 S.C.R. 641, to fall under the general branch of s. 91(2), legislation must engage the national interest in a manner that is qualitatively different from provincial concerns. Whether a law is validly adopted under the general trade and commerce power may be ascertained by asking (1) whether the law is part of a general regulatory scheme; (2) whether the scheme is under the oversight of a regulatory agency; (3) whether the legislation is concerned with trade as a whole rather than with a particular industry; (4) whether it is of such a nature that provinces, acting alone or in concert, would be constitutionally incapable of enacting it; and (5) whether the legislative scheme is such that the failure to include one or more provinces or localities in the scheme would jeopardize its successful operation in other parts of the country. These indicia of validity are not exhaustive, nor is it necessary that they be present in every case.⁸¹

The inherent conflict between federal and provincial powers to regulate various aspects of (i) trade and commerce under s. 91(2) [federal jurisdiction], (ii) civil rights under s. 92(13) [provincial jurisdiction] and matters of merely local or private nature under s. 92(16) [provincial jurisdiction] of the *Constitution Act, 1867*⁸² is well known, and is indicative of a brewing conflict that may occur between the federal and provincial levels of government with respect to the regulation of cryptoassets, especially considering provincial securities regulators, such as the OSC⁸³ have characterized them as securities, whilst others (such as Quebec's Autorité des Marchés Financiers) have not,⁸⁴ and the Canadian Parliament has released its Proposed Amendments.

⁸¹ *Re Securities Act*, *supra* note 78 at page 839.

⁸² *Constitution Act*, *supra* note 79.

⁸³ Ontario Securities Commission, *supra* note 73.

⁸⁴ Jacob Serebrin, “Virtual currencies like Bitcoin fall into a cryptic regulatory gap in Quebec”, *Montreal Gazette* (11 January 2018), online < <https://montrealgazette.com/business/amf-on-bitcoin>>.

As applied to the regulation of cryptoassets, it could be argued that the federal government has the authority to regulate cryptoassets; such through the application of section 91 of the *Constitution Act, 1867*⁸⁵ and application of the national concern doctrine.

The first mention of the national concern doctrine was asserted in *Attorney-General for Ontario vs. Attorney-General for the Dominion and The Distillers and Brewers' Association of Ontario*:

[13] [...] Their Lordships do not doubt that some matters, in their origin local and provincial, might attain such dimensions as to affect the body politic of the Dominion, and to justify the Canadian Parliament in passing laws for their regulation or abolition in the interest of the Dominion. But great caution must be observed in distinguishing between that which is local and provincial, and therefore within the jurisdiction of the provincial legislatures, and that which has ceased to be merely local or provincial, and has become matter of national concern, in such sense as to bring it within the jurisdiction of the Parliament of Canada. [...] ⁸⁶

Fifty years after this decision, the doctrine was given its modern interpretation through the *Reference re Canada Temperance Act* decision, wherein it was acknowledged that:

[...] if [the subject matter of the legislation] is such that it goes beyond local or provincial concern or interests and must from its inherent nature be the concern of the Dominion as a whole [...] then it will fall within the competence of the Dominion Parliament as a matter affecting the peace, order and good government of Canada. [...] ⁸⁷

The modern-day interpretation was affirmed through *Johannesson v. West St. Paul*, wherein it was held:

[19] [...] the true test must be found in the real subject matter of the legislation: if it is such that it goes beyond local or provincial concern or interests and must from its inherent nature be the concern of the Dominion as a whole . . . then it will fall within the competence of the Dominion Parliament as a matter affecting the peace, order and good government of Canada, though it may in another aspect touch on matters specially reserved to the provincial legislature. [...] ⁸⁸

This was re-affirmed in *Munro v. National Capital Commission*, wherein it was held:

⁸⁵ *Supra* note 79.

⁸⁶ 1896 CarswellNat 45, [1896] AC 348, 5 Cart BNA 295.

⁸⁷ 1946 CarswellOnt 100 at 205-206, [1946] 2 WWR, 1, [1946] 2 DLR 1.

⁸⁸ [1952] 1 SCR 292, [1951] 4 DLR 609.

[...] [24] I find it difficult to suggest a subject matter of legislation which more clearly goes beyond local or provincial interests and is the concern of Canada as a whole than the development, conservation and improvement of the National Capital Region in accordance with a coherent plan in order that the nature and character of the seat of the Government of Canada may be in accordance with its national significance. Adopting the words of the learned trial judge, it is my view that the Act “deals with a single matter of national concern. [...]”⁸⁹

For the point of this discussion, reference can be made to paragraph 33 of *R v. Crown Zellerbach Canada Ltd.*⁹⁰ (“*Zellerbach*”), wherein it was established that [emphasis added]:

[...]

1. The national concern doctrine is separate and distinct from the national emergency doctrine of the peace, order and good government power, which is chiefly distinguishable by the fact that it provides a constitutional basis for what is necessarily legislation of a temporary nature;
2. The national concern doctrine applies to both new matters which did not exist at Confederation and to matters which, although originally matters of a local or private nature in a province, have since, in the absence of national emergency, become matters of national concern;
3. For a matter to qualify as a matter of national concern in either sense it must have a singleness, distinctiveness and indivisibility that clearly distinguishes it from matters of provincial concern and a scale of impact on provincial jurisdiction that is reconcilable with the fundamental distribution of legislative power under the Constitution;
4. In determining whether a matter has attained the required degree of singleness, distinctiveness and indivisibility that clearly distinguishes it from matters of provincial concern it is relevant to consider what would be the effect on extra-provincial interests of a provincial failure to deal effectively with the control or regulation of the intra-provincial aspects of the matter.

⁸⁹ [1966] SCR 663.

⁹⁰ [1988] 1 SCR 401 at para 33, 1988 CarswellBC 137, [1988] SCJ No [Zellerbach].

The *Zellerbach* decision presented the modern-day interpretation of the national concern doctrine, which will show how the cryptoasset regime would be best regulated through federalism. The national concern doctrine is concerned with matters that did, (a) not exist before Confederation, and (b) which have become a matter of national concern. It is clear that the first requirement of the test has been passed. The analysis will focus on whether or not the cryptoasset regime has become a matter of national concern. *Zellerbach* makes it clear that in order for the cryptoasset regulatory regime to have reached the level of a matter of national concern it must attain the levels of “singleness, distinctiveness and indivisibility that clearly distinguishes it from a matter of provincial jurisdiction.”⁹¹ The *A.G. Canada v Hydro Quebec et al* (“*AG Canada*”) decision made distinctive that “the test for singleness, distinctiveness and indivisibility is a demanding one. Because of the high potential risk to the Constitution's division of powers presented by the broad notion of national concern, it is crucial that one be able to specify precisely what it is over which the law purports to claim jurisdiction.”⁹² *Zellerbach* extends the definition of a national concern where it states that what classifies singleness, distinctiveness and indivisibility is to “consider what would be the effect on extra-provincial interests of a provincial failure to deal effectively with the regulation or control or regulation of the intra-provincial aspects of this matter.”⁹³

On January 7, 2018, the twenty-four (24) hour volume of cryptoasset trading reached a high of over \$80 billion USD a day.⁹⁴ Millions of dollars are being converted into and out of Canadian fiat currency and cryptoassets while hundreds of millions of dollars are being converted into USD daily on cryptocurrency exchanges.⁹⁵ Fortunes have been made and cryptoassets have become a global phenomenon. While different regulatory bodies in Canada struggle to determine who should be in charge of regulating this growing marketplace, it should be recognized that cryptoassets are potentially much “too important and impactful”⁹⁶ and the social benefits far too large for Canada to stifle the potential to become a global leader in this market.

⁹¹ *Ibid.*

⁹² [1997] 3 SCR 213 at para 673.

⁹³ *Zellerbach*, *supra* note 90 at para 3.

⁹⁴ Coinmarketcap, “Total Market Capitalization”, online: Coinmarketcap <www.coinmarketcap.com/charts> [Total Market].

⁹⁵ “CryptoCompare Index: BTC”, online: Cryptocompare <<https://www.cryptocompare.com/coins/btc/analysis/CAD>>.

⁹⁶ William Michael Cunningham, “Cryptocurrency Regulation is a job for treasury” *American Banker* 183:37 (23 February 2018), online: <<https://www.americanbanker.com/opinion/cryptocurrency-regulation-is-a-job-for-treasury>>.

Considering the objectives⁹⁷ of the *PCMLTFA*, the most effective and the most important areas of regulation are to prevent money laundering, terrorist financing and tax evasion. These new technologies “threaten existing approaches to regulation, and empower groups and individuals – including criminals and terrorists – seeking to skirt regulations for nefarious purposes.”⁹⁸

Under section 91(27) of the *Constitution Act, 1867*,⁹⁹ criminal law will be regulated by the Parliament of Canada. Currently the AML and ATF regime are federally regulated under *Proceeds of Crime (Money Laundering and Terrorist Financing Act*,¹⁰⁰ (“*PCMLTFA*”). Money laundering has and will continue to be a threat to Canada’s financial institutions.¹⁰¹ Without the proper resources and appropriate authority that stems from federal legislation, this problem will continue to grow.

In addition to this consideration, the *PCMLTFA* also relates to section 91(7) of the *Constitution Act, 1867*,¹⁰² which focuses on the defense and military of Canada, including preventing any threats of terrorism. It is extremely important to have effective measures to prevent terrorism; this effort begins with the obstruction of terrorist financing which can lower the risk of terrorist attacks on Canadian citizens both at home and abroad. We see no reason why such endeavours should be regulated provincially. The resources and the current legislation that would be provided by federal regulation will be the most effective process in preventing money laundering and terrorist financing.

The regulation of the convertibility mechanism where cryptoassets are transferred into fiat currency (and vice versa) through a cryptoasset exchange is the stage of the cryptoasset transaction that will be able to most effectively protect Canada against these threats.

⁹⁷ The objective of the *PCMLTFA* is to:

- implement specific measures to detect and deter money laundering and the financing of terrorist activities to facilitate the investigation or prosecution of money laundering and terrorist financing offences, including:
 - establishing record keeping and client identification requirements for financial services providers and other persons that engage in businesses, professions or activities that are susceptible to being used for money laundering, and the financing of terrorist activities, [...];
 - requiring the reporting of suspicious financial transactions and of cross-border movements of currency and monetary instruments, and
 - establishing an agency that is responsible for dealing with reported and other information;
- respond to the threat posed by organized crime by providing law enforcement officials with the information they need to investigate and prosecute money laundering or terrorist financing offences, while ensuring that appropriate safeguards are put in place to protect the privacy of persons with respect to personal information about themselves; and
- assist in fulfilling Canada’s international commitments to participate in the fight transnational crime, particularly money laundering and the fight against terrorist activities [...].

⁹⁸ Alex Wilner & Evangeline Ducas, “The security and financial implications of blockchain technologies: Regulating emerging technologies in Canada” (2017) 72:4 Intl J 539.

⁹⁹ *Constitution Act*, supra note 79.

¹⁰⁰ *PCMLTFA*, supra note 3.

¹⁰¹ Nicolas W. R. Burbidge, “International anti-money laundering and anti-terrorist financing: the work of the Office of the Superintendent of Financial Institutions in Canada” (2004) 7:4 Journal of Money Laundering Control 320.

¹⁰² *Constitution Act*, supra note 79.

Blockchain and related technologies also provide opportunities for innovation and profit on a large scale. On January 7, 2018 the global market capitalization for cryptoassets reached a value of over \$810 billion USD.¹⁰³ This market is much too large to be regulated by individual provinces. Under section 91(2) of the *Constitution Act, 1867*¹⁰⁴ it shall be within the power of the Parliament of Canada to regulate Trade and Commerce throughout the country. It is therefore important for the Federal Parliament to create legislation that finds the balance between a prohibitive regulatory environment and a lax AML and ATF regime without stifling innovation and favouring a competitive Canadian cryptoasset industry within a global economy; such being within its powers.

Currently, Canada has assumed a “watchful approach.”¹⁰⁵ They are watching the global regulation and weigh the risks and commensurate opportunities in the cryptoasset environment. Other jurisdictions (such as Singapore and Switzerland) have adopted a more “facilitative approach,”¹⁰⁶ electing to become attractive destinations in the growing cryptoasset market. They have chosen to “regulate blockchain technologies in order to both capitalize on potential opportunities that emerge, while minimizing identified risks.”¹⁰⁷ These foreign jurisdictions are slowly becoming the global FinTech leaders; Canada needs to ensure that it does not fall behind in this respect. “Canada risks losing its competitive advantage in developing and profiting from blockchain technologies.”¹⁰⁸ In the future, jurisdictions that have benefited from facilitative cryptoasset regulation shall benefit from the lessons they learned during the progression of this technology.¹⁰⁹ It is therefore imperative for Canada to become one of the jurisdictions that is a global leader in this space.

A failure of the provinces to implement proper regulation for cryptoassets intra-provincially would likely have extra-provincial effects that would be felt on a national and potentially global level. The level of impact that improper regulation of this technology could have regarding money laundering and terrorist financing is a matter that falls directly within the “pith and substance” of the federal legislation. Additionally, the necessity to promote Canada as an emerging global leader in this space falls within the areas of trade and commerce as regulated by section 91(2) of the *Constitution Act, 1867*.¹¹⁰

In addition to the desirability of the creation of a viable national cryptoasset regulatory framework, such a framework, under the federal regime, would:

¹⁰³ Coinmarketcap, *supra* note 94.

¹⁰⁴ *Constitution Act*, *supra* note 79.

¹⁰⁵ Wilner et al., *supra* note 98.

¹⁰⁶ *Ibid.*

¹⁰⁷ *Ibid.*

¹⁰⁸ *Ibid.*

¹⁰⁹ United States, *Foundation for Defense of Democracies, An Analysis of Illicit Flows into Digital Currency Services*, Yaya J Fanusie & Tom Robinson, (Washington D.C, January 2018) at 11.

¹¹⁰ *Constitution Act*, *supra* note 79.

- allow FINTRAC¹¹¹ to fulfil its mandate, which is “to facilitate detection, prevention and deterrence of money laundering and the financing of terrorist activities, while ensuring the protection of personal information under its control,” as well as respect Canada’s international commitments to its partners;¹¹²
- Enable the use of an existing and highly functional AML/ATF federal framework to regulate cryptoassets, with known requirements (i.e., reporting requirements, money services business (“MSB”) reporting requirements, etc.), under an existent set of laws and rules designed to permit uniform regulation and enforcement on a national basis, thus fostering the integrity and stability of Canada’s financial system, among other considerations;

Moreover, given the nature of cryptoassets described in this paper, they are impacted by other forms of federal legislation, including, but not limited to (i) the *Clearing and Settlement Act*, (ii) the *Bank Act*, and (iii) the *Payment Act*;¹¹³ especially if cryptoassets are used in financial institutions on a day-to-day, as well as mainstream basis. Furthermore, technological innovation is federally regulated under the *Patent Act* and Constitution. In light of the foregoing, it could be argued that the cryptoasset regulatory regime is *intra vires* of the Parliament of Canada to regulate.

¹¹¹ Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) is Canada’s financial intelligence unit (FIU). According to its website, “the Centre assists in the detection, prevention and deterrence of money laundering and the financing of terrorist activities. FINTRAC’s financial intelligence and compliance functions are a unique contribution to the safety of Canadians and the protection of the integrity of Canada’s financial system. FINTRAC acts at arm’s length and is independent from the police services, law enforcement agencies and other entities to which it is authorized to disclose financial intelligence. It reports to the Minister of Finance, who is in turn accountable to Parliament for the activities of the Centre”, available at: <http://www.fintrac-canafe.gc.ca/fintrac-canafe/1-eng.asp>.

¹¹² Canada, Financial Transactions and Reports Analysis Centre of Canada, *Who we are* (Ottawa: 2017) <<http://www.fintrac-canafe.gc.ca/fintrac-canafe/1-eng.asp>>.

¹¹³ *Re Securities Act*, *supra* note 78 at para 46. The Constitution gives Parliament powers that enable it to pass laws that affect aspects of securities regulation and, more broadly, to promote the integrity and stability of the Canadian financial system. These include Parliament’s power to enact laws relating to criminal law (s. 91(27)), banks (s. 91(15)), bankruptcy (s. 91(21)), telecommunications (ss. 91 and 92(10) (a)), and peace, order and good government (s. 91) (*Multiple Access*; *Bell Canada v. Quebec (Commission de la santé et de la sécurité du travail)*, [1988] 1 S.C.R. 749, at pp. 765-66; *Smith v. The Queen*, [1960] S.C.R. 776, at p. 781). Parliament has exercised its powers by enacting, for example, the following statutes and provisions: the *Canada Business Corporations Act*, R.S.C. 1985, c. C-44; the *Criminal Code*, R.S.C. 1985, c. C-46, ss. 380(2), 382, 382.1, 383, 384 and 400; the *Bank Act*, S.C. 1991, c. 46; the *Investment Canada Act*, R.S.C. 1985, c. 28 (1st Supp.); the *Payment Clearing and Settlement Act*, S.C. 1996, c. 6, Sch.; the *Telecommunications Act*, S.C. 1993, c. 38; the *Bankruptcy and Insolvency Act*, R.S.C. 1985, c. B-3, Part XII. Finally, s. 91(2) of the *Constitution Act, 1867* gives Parliament power over the regulation of trade and commerce. This power has two branches: the power over interprovincial and international commerce (*Citizens Insurance Co. of Canada v. Parsons* (1881), 7 App. Cas. 96 (P.C.) (“*Parsons*”)) and the general trade and commerce power that authorizes laws where the national interest is engaged in a manner that is qualitatively different from provincial concerns, as discussed more fully later in these reasons.

9. WHAT IS A COMMODITY?

It has been argued that the currency and securities regulatory bodies may not be the most effective authorities to regulate cryptoassets. It has also been suggested by both the United States Federal Court¹¹⁴ and by the Canadian Revenue Agency¹¹⁵ that cryptocurrencies should be treated as commodities.

The Law Library defines a commodity as “a good that is sold freely to the public. It can be agriculture, fuel or metals. It is traded in bulk in the commodity or spot market.”¹¹⁶ Canadian jurisprudence defines a commodity as “anything produced for use or sale, article of commerce or object of trade,”¹¹⁷ or “in its ordinary business and derivative sense, it means anything moveable that is a subject of trade of acquisition, a kind of thing produced from a sale, an article of commerce, an object of trade.”¹¹⁸ Statutes define commodities in several places, most prevalently in the Alberta *Securities Act* under section 1(h), which defines a commodity too as: “(i) any good, article, service, right or interest of which any unit is, from its nature or by mercantile custom, treated as the equivalent of any other unit, (ii) the currency of any jurisdiction, (iii) any gem, gemstone or other precious stone.”¹¹⁹ The *Commodity Futures Act* defines commodity in section 1(1) as: “whether in the original or a processed state, any agricultural product, forest product, product of the sea, mineral, metal, hydrocarbon fuel, currency or precious stone or other gem, and any goods, article, service, right or interest or class thereof, designated as a commodity under the regulations.”¹²⁰

While the definitions are not entirely consistent in their interpretations of a “commodity” in the Canadian regulatory sphere, they do provide guidelines to assist in helping us determine whether cryptoassets would fall under this definition, and therefore be regulated as such.

¹¹⁴ *CabbageTech*, *supra* note 16 at 27.

¹¹⁵ Canada, Canadian Revenue Agency, *What you should know about digital currency*, (Ottawa: Canadian Revenue Agency, 2013) <<https://www.canada.ca/en/revenue-agency/news/newsroom/fact-sheets/fact-sheets-2015/what-you-should-know-about-digital-currency.html>>. Further reference can be made to Schedule 1.

¹¹⁶ *Black's Law Dictionary*, 10th ed, *sub verbo* “commodity”.

¹¹⁷ *Enron Capital & Trade Resources Canada Corp. v Blue Range Resource Corp.*, 2000 ABCA 239 at para 39, 192 DLR (4th) 281, [2001] 2 WWR 454 [*Enron*].

¹¹⁸ *Canadian Pacific Railway v Ottawa Fire Insurance Company*, 1906 CarswellOnt 143, 7 OWR 353, aff'd 1905 CarswellOnt 143.

¹¹⁹ *Securities Act*, RSA 2000, c S-4 at s 1 [ASA].

¹²⁰ RSO 1990, c C.20 at s 1(1) [CFA].

10. ARE CRYPTOASSETS COMMODITIES?

Perhaps the most relevant argument to cryptoassets being defined as a commodity in Canada comes from the U.S. decision in *Commodity Futures Trading Commission v. Patrick K. McDonnell and CabbageTech, Corp. d/b/a Coin Drop Markets*¹²¹ (“CabbageTech”) where Federal Judge Jack B. Weinstein ruled that he agreed with the CFTC and the Chicago Mercantile Exchange Inc. that cryptoassets (or, as they defined therein, “virtual currencies”) should be considered commodities pursuant to the *Commodity Exchange Act* (“CEA”). In CabbageTech, the plaintiffs were granted a preliminary injunction due to Justice Weinstein’s ruling that without it, there was a “reasonable likelihood that defendants will continue to violate the CEA”¹²² without the injunction. The U.S. courts agreed with the plaintiffs that virtual currency should be regulated as a commodity and therefore the CFTC would have proper standing in this decision.¹²³

CabbageTech cited various sources why they believed that it was likely that a virtual currency would be best regulated as a commodity under the CFTC, as defined in American legislation and jurisprudence. Prentis wrote in his 2015 article that:

“It would make sense for regulators to treat Bitcoin as a commodity. Commodities are generally defined as ‘goods sold in the market with a quality and value uniform throughout the world.’ This categorization would be appropriate because it realistically reflects the economic behavior of Bitcoin users and squares with traditional economic concepts of exchange.”¹²⁴

Prentis elaborates, discussing how participants in the Bitcoin community use the asset in exchange for property or currency, and how Bitcoin actually behaves very similarly to traditional commodities when considered in a supply and demand framework. As more Bitcoin are released into the market, and the difficulty in mining the Bitcoin is heightened, the value rises; in a manner similar to gold or other precious metals, a Bitcoin “is worth whatever someone is willing to pay for it.”¹²⁵

Critics of this analysis have argued that where Bitcoin may fail to conform to the commodity analysis is the “lack of inherent use value that is often included in the definition of a Bitcoin.”¹²⁶ It is through this argument that Bitcoin may face its strongest resistance as to whether it should be defined as a commodity. It is evident on the surface that Bitcoin does not comprise the traditional functions of a commodity that grain, energy or livestock may have when viewed from a high-level perspective.

¹²¹ *Commodity Futures Trading Commission v. Patrick K. McDonnell, and CabbageTech Corp. d/b/a Coin Drop Markets* (18 January 2018), 18-CV-361, online: Commodity Futures Trading Commission <<https://www.cftc.gov/sites/default/files/idc/groups/public/@lrenforcementactions/documents/legalpleading/enfcdmcomplaint011818.pdf>> [CabbageTech Complaint].

¹²² *CabbageTech*, *supra* note 15 at 27.

¹²³ *CabbageTech* Complaint, *supra* note 121.

¹²⁴ Mitchell Prentis, “Digital Metal: Regulating Bitcoin As A Commodity” (2015) 66:2 Case W Res L Rev 609. s

¹²⁵ *Ibid* and from Brad Jacobsen & Fred Pena, “What Every Lawyer Should Know About Bitcoins” (2014), Utah B.J., 40.

¹²⁶ Nicholas Godlove, “Regulatory Overview of Virtual Currency” (2014) 10:1 Okla J. L. & Technology 70 1.

While Bitcoin cannot be used for consumption and its intrinsic value may be difficult to quantify or value, Prentis states that its intrinsic value would benefit from its ability to decrease transaction fees online.¹²⁷ In a comparison between PayPal and other electronic transaction operators or payment services (i.e. payment processing), Bitcoin transaction fees are much lower. It may be evident that this is where Bitcoin's intrinsic value lies; however, this argument only takes into account direct peer-to-peer transactions of Bitcoin, which are declining in popularity as various cryptocurrency exchanges are increasingly facilitating these transactions and charging similar, if not higher transaction fees than PayPal or other intermediaries had previously been demanding.¹²⁸

Based on this analysis, it could be argued that Bitcoin's intrinsic value would be minimal unless a majority of transactions were performed without the use of an exchange or intermediary to facilitate the transaction.

Jeff Currie, who was also cited in CabbageTech, commented as follows regarding the "store of value" function that commodities may contain:

A commodity is any item that "accommodates" our physical wants and needs. And one of these physical wants is the need for a store of value. Throughout history humans have used different commodities as a store of value – even cocoa beans – but, more persistently, gold. In contrast, a security is any instrument that is "secured" against something else. As a currency is usually secured by a commodity or a government's ability to tax and defend, it is considered to be a security. By these definitions, bitcoin with a lower case "b," is a commodity, and not a currency, while Bitcoin with a capital "B" is the technology, or network, that bitcoin moves across. The analogy would be Shale technology versus shale oil.¹²⁹

While Currie is correct in his argument that Bitcoin and other cryptoassets may comprise some store of value, it is also consistent with our above discussion of whether cryptoassets should be defined as a currency. Though cryptoassets do, inherently, contain a "store of value" element, it would be inaccurate to argue that such element is a defining factor of a Bitcoin. With its extremely high rate of volatility that is approximately ten (10) times higher than a traditional currency,¹³⁰ the argument that Bitcoin facilitates market demand for a commodity that stores value appears to be inherently flawed, as such "want and need" is already served by traditional currencies, as well as other commodities (such as precious metals), both of which feature far lower volatility.

While the CFTC has made it clear that cryptoassets fit into the definition of a commodity under Title 7 U.S.C. § 1(a)(9) as, "all other goods and articles... and all services, rights, and interests... in which contracts for future delivery are presently or in the future dealt in,"¹³¹ the definitions are not consistent under Canadian jurisprudence and legislation. For example, under section 1(h)(a) of the Alberta *Securities Act*, a commodity is defined as "any good, article, service, right or interest of which any unit is, from its nature or by mercantile custom, treated as the equivalent of any other unit."¹³²

¹²⁷ Prentis, *supra* note 124.

¹²⁸ Finder "Bitcoin vs. PayPal" (27 April 2018), online : Finder <<https://www.finder.com/bitcoin-vs-paypal>>.

¹²⁹ Jeff Currie, "Bullion Beats bitcoin, Not Bitcoin" *Goldman Sachs Global Macro Research* 21 (11 March 2014) <<https://www.paymentlawadvisor.com/files/2014/01/GoldmanSachs-Bit-Coin.pdf>>.

¹³⁰ Gangwal *et al*, *supra* note 38.

¹³¹ *CabbageTech* Complaint, *supra* note 121.

¹³² ASA, *supra* note 119.

While the value of a cryptoasset might measure its value in U.S. dollar terms, similar to other commodities, the value of each of these assets will be uniform. Based on this definition, a cryptoasset may be considered a commodity. Section 1(1) of the *Commodity Futures Act* provides itself with a proverbial catch-all clause, wherein a commodity is defined as "... any goods, article, service, right or interest or class thereof, designated as a commodity under the regulations."¹³³ In this sense, amendments to this Act or relevant jurisprudence to designate a cryptoasset as a commodity under this act may be necessary.

A commodity may also fit into the definition provided in *Enron Capital & Trade Resources Canada Corp v. Blue Range Resource Corporation* wherein it was held that a commodity should be defined as "anything produced for use or sale, article of commerce or object of trade."¹³⁴ The majority of cryptoasset users are deploying their assets strictly as an "object of trade," either in exchange for other cryptoassets or for fiat currency.¹³⁵ Per *CPR v. Ottawa Fire Insurance Company* decision, a cryptoasset could also fit under the definition of a commodity as "... anything moveable that is a subject of trade or acquisition, a kind of thing produced from a sale, an article of commerce, an object of trade."¹³⁶ Thus, a cryptoasset generally seems to fit under this broad and traditional definition of a commodity, as its technological sophistication is much greater than any other commodity defined as such under Canadian legislation. In that sense, we contend that labelling and regulating cryptoassets as commodities would be both ineffective and inconsistent with the goals of the Canadian government and associated various regulatory bodies.

The potential multiple characterizations of cryptoassets under different heads of currencies, securities, commodities, etc. could create regulatory chaos, as competing authorities could lay claim to governing power, creating conflicting jurisdictional approaches, ineffective regulation and enforcement and divergent regulation. It appears that regulators of cryptoassets would best be served by a single federal authority in Canada under the AML/ATF framework.

¹³³ *CabbageTech* Complaint, *Supra* note 120.

¹³⁴ *Enron*, *supra* note 117 at para 39.

¹³⁵ Christine Lagarde, "Addressing the Dark Side of the Crypto World" (13 March 2018), online: IMFBlog (blog) <<https://blogs.imf.org/2018/03/13/addressing-the-dark-side-of-the-crypto-world/>>.

Spencer Applebaum, "Analysis of the Cryptocurrency Landscape" (31 December 2017), online: Medium (blog) <<https://medium.com/@MUBC/analysis-of-the-cryptocurrency-exchange-landscape-948752318fae>>.

¹³⁶ *ASA*, *supra* note 119.

11. RECOMMENDATION

Indeed, rather than instructing regulatory bodies to implement resource-heavy policies restricting decentralized cryptoasset networks that would ultimately offer little protection for the users of these networks, it would be most prudent for Canada to concentrate its regulatory efforts on the area where the government could provide greater public benefit: cryptoasset exchanges. This approach to concentrate regulatory efforts at the locus of cryptoasset transactions – the convertibility mechanism - is imperative as cryptoasset exchange users are theoretically able to transact in almost complete anonymity in terms of identity, location or source of income. In the absence of some degree of regulatory oversight, cryptoasset transactions may be used by innominate parties to swiftly move large amounts of wealth across borders.

The implications of this structure from an AML perspective are of obvious concern. Essentially, the only effective method to ascertain the identity of parties to a cryptoasset transaction would be to ensure that sufficient “know-your-client” (“KYC”) information is collected with respect to the parties opening accounts (known as “wallets”) at cryptoasset exchanges, as well as their sources of funds (e.g., fiat currency that is exchanged into cryptoassets) that are deposited into the wallets to be used in transactions.¹³⁷ *Details supporting our foregoing recommendations appear in the remainder of our brief.*

12. WHAT IS AML/ATF AND HOW ARE CRYPTOASSETS RELEVANT TO THE DISCUSSION?

Though Canadian law does not define “money laundering” *per se*,¹³⁸ it can be described in different ways, such as, *inter alia*:

- (i) “a form of financial crime in which the proceeds from criminal activity are made to appear legitimate. The goal of many criminal acts is to make a profit for the individual or group that commits the crime. A strategy to fight money laundering seeks to reduce crime by making it harder for criminals to keep and use their profits”;¹³⁹
- (ii) “the process of concealing illicit gains that were generated from criminal activity”;¹⁴⁰
- (iii) “the processing of these criminal proceeds to disguise their illegal origin.”¹⁴¹

In addition, money laundering is often referred to as a three-stage process involving:

- (1) placement of proceeds of crime into the financial system;

¹³⁷ Perri Reynolds & Angela S.M. Irwin, “Tracking digital footprints: anonymity within the bitcoin system” (2017) 20: 2 J Money Laundering Control 172.

¹³⁸ Canada, Office of the Auditor General of Canada, *2003 April Report of the Auditor General of Canada*, (Ottawa: Office of the Auditor General of Canada) at s 3.20.

¹³⁹ *Ibid* at s 3.6.

¹⁴⁰ Organization for Economic Co-operation and Development, “Money Laundering”, online: OECD <<https://www.oecd.org/cleangovbiz/toolkit/moneylaundering.htm>>.

¹⁴¹ Financial Action Task Force on Money Laundering, “What is Money Laundering”, online: FATF <<http://www.fatf-gafi.org/faq/moneylaundering/#d.en.11223>>.

(2) creation of layers (i.e., *layering*) of financial transactions to disguise their origins, and

(3) moving the laundered funds back into the legitimate economy (i.e., *integration*).¹⁴²

On the other hand, “terrorist financing” consists of the provision of funds for terrorist activity¹⁴³ and/or as “[...] the financing of terrorist acts, and of terrorists and terrorist organisations.”¹⁴⁴ Chapter 3 of the 2003 *Report of the Auditor General of Canada to the House of Commons*¹⁴⁵ describes the relationship between money laundering and terrorist financing as follows:

[3.25] Money laundering involves the processing of the profits of crimes that were committed in the past so as to disguise their illegal origin. The financing of terrorism, however, involves the processing of funds—whether obtained legally or illegally—to be used in future crimes.

[3.26] Following the terrorist attacks of 11 September 2001, Canada has taken a number of steps to combat terrorist financing. They are aimed at assisting the police to detect and deter the financing of terrorist activities and to investigate and prosecute offences that are related to terrorist financing.

[3.27] Terrorist groups differ from large criminal organizations in several important ways.

- **Motivation.** While drug traffickers and organized crime groups seek primarily monetary gain, terrorist groups usually have non-financial goals that motivate them. According to one definition, the primary goal of terrorism is “to intimidate a population or to compel a government to do something, or abstain from doing any act.”
- **Source of funds.** The financial dealings of a terrorist organization are difficult to investigate since its funds may come from legitimate businesses that the terrorists may own and donations they have received from sympathizers. The apparently legal sources of funds may mean there are few, if any, indicators that would make one or a series of transactions stand out.
- **The size and nature of financial transactions.** Individual financial transactions tied to terrorist operations may involve amounts that are not large enough to trigger existing reporting thresholds. An FBI analysis of the events surrounding 11 September 2001, for example, indicates that the hijackers each opened accounts with a single cash or wire transfer deposit in the average amount of US \$3,000 to \$5,000. The analysis also showed that they made numerous withdrawals in small amounts using mostly debit cards.

¹⁴² Canada, *supra* note 138 at s 3.34.

¹⁴³ Canada, Financial Transactions and Reports Analysis Centre of Canada, *What is terrorist financing?* (Ottawa: 2015) < <http://www.fintrac-canafe.gc.ca/fintrac-canafe/definitions/terrorist-terroriste-eng.asp>>.

¹⁴⁴ Financial Action Task Force on Money Laundering, “International Standard on Combatting Money Laundering and the Financing of Terrorism and Proliferation” (February 2018) at 123, online: FATF < <http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf>>.

¹⁴⁵ Canada, *supra* note 138.

- **Transfers of money outside the traditional financial system.** There are ways to transfer money from one person or country to another other than using banks or financial institutions. *Hawala* and similar methods of transferring money such as the *Fei ch'ien* and *Hundi* systems have also played a role in moving terrorist funds. In the *Hawala* system, a person gives money to an agent in one country, who tells an agent in another country to give money to a specific person. The transfer is all handled through word of mouth. Funds moved this way do not leave a paper trail similar to one that would be left if the person used a traditional financial setting like a bank.

3.28 As a result, it is difficult to follow terrorist money trails. For the three-year period ending 2003-04, the government has allocated a total of \$34 million to the Financial Transactions and Reports Analysis Centre to detect and deter terrorist financing. Regulations have been developed for reporting transactions that appear to be related to terrorist financing.

One of the rationales or concerns as to why cryptoassets may pose a specific risk in the area of money laundering and terrorist financing,¹⁴⁶ or as a vehicle thereof,¹⁴⁷ may be related to the anonymous nature of cryptoassets and the source of funds thereof. Other concerns (amongst others) relate to:

- (i) “[...] degree of anonymity that can potentially be exploited by money launderers or terrorist activity financiers,”¹⁴⁸ especially in transactions conducted through the Internet;
- (ii) the “origins of funds are difficult to trace and it is difficult to ascertain whether or not the money is from a legitimate source (e.g. some cards can be anonymously loaded with cash at a third party reseller location, such as a Canada Post office)”;
- (iii) “convertible virtual currencies are vulnerable to abuse for money laundering and terrorist activity financing purposes because they allow greater levels of anonymity, or in some cases complete anonymity, when compared to traditional non-cash payment methods.”

¹⁴⁶ Banque de France, “The emergence of bitcoin and other crypto-assets: challenges, risks and outlook” (5 March 2018) 16, online: Focus <https://publications.banque-france.fr/sites/default/files/medias/documents/focus-16_2018_03_05_en.pdf>.

¹⁴⁷ Christine Lagarde, “Addressing the Dark Side of the Crypto World” (13 March 2018), online: IMFBlog (blog) <<https://blogs.imf.org/2018/03/13/addressing-the-dark-side-of-the-crypto-world/>>.

¹⁴⁸ Canada Gazette, *supra* note 5.

Figure 2: At Which Point Should Cryptoassets Be Regulated?

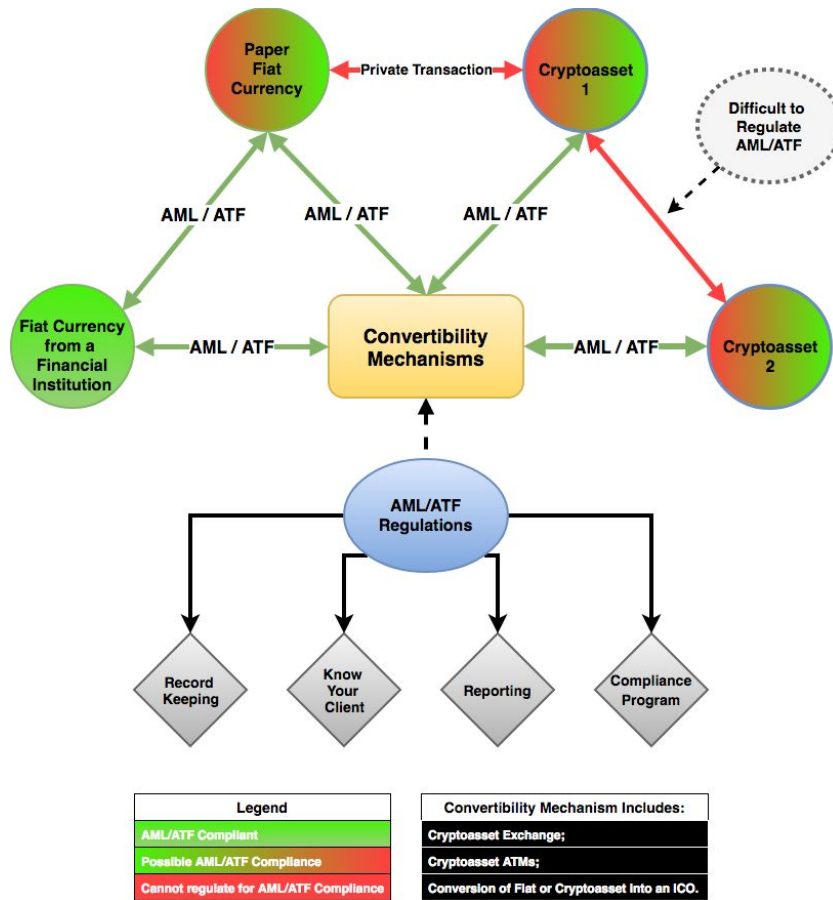


Figure 2 highlights the proposed method we recommend as the most effective way to regulate cryptoassets under a Canadian regulatory framework.

The three main methods of entry into the cryptoasset network are through (i) physical fiat currency, (ii) fiat from a financial institution, and (iii) by exchanging a currently-owned cryptoasset for another cryptoasset. In addition to these methods of entry, there exist convertibility mechanisms that are operated as a method for conversion from currency into cryptoassets and *vice versa*. Our proposal theorizes that the best area wherein the Federal government will be able to effectively and efficiently monitor this space is at the **convertibility mechanism** point. The convertibility mechanisms have been divided into three categories:

- 1) cryptoasset exchanges, which are operations that allow their users to exchange cryptoassets for fiat currency or for other types of cryptoassets and *vice versa*;
- 2) cryptoasset ATMs, which are machines that allow users to exchange cryptoassets for fiat currency and *vice versa*; and
- 3) conversion of fiat or cryptoasset into an ICO, which is the method by which a user would exchange fiat currency or another cryptoasset for ICO tokens or coins issued by a start-up business.

We recommend that these three entry points comprise the space where the Canadian regulators are going to be able to most effectively regulate cryptoassets. As illustrated in Figure 2, there are two methods of convertibility where it will be difficult or impossible to regulate the transfer of cryptoassets and fiat currency. The first of these methods constitute private transactions made between cryptoassets and paper fiat currency. If users wish to purchase cryptoassets with physical fiat currency or if they wish to exchange their cryptoassets for physical fiat currency in a private transaction without the use of a convertibility mechanism, it is going to be extremely difficult to monitor whether this transaction was completed without a criminal element involved. In the same manner in which a person may sell any type of physical asset with paper fiat currency, this type of transaction will be very difficult to monitor in terms of its legality.

The second convertibility situation occurs when users trade cryptoassets among each other without the use of a convertibility mechanism. Similar to the previous transaction category, the legality of these transactions will also be difficult to regulate, given the degree of anonymity involved in this exchange. Fortunately, the large majority of transactions are conducted in the cryptoasset network using convertibility mechanisms. Hence, just as it is impossible for authorities to monitor every transaction occurring in fiat currency, the government's regulatory framework should focus on the preponderance of transactions that can be monitored, being those transactions completed at the point in which convertibility mechanisms exist.

In Figure 2, the green arrows represent the areas through which AML/ATF compliance can be effectively monitored. The green circle, "Fiat Currency from a Financial Institution", represents any fiat currency that is being stored in a financial institution. This green circle indicates that this currency should already have undergone the proper practices and procedures imposed by the financial institution to ensure that the currency is compliant with AML/ATF requirements promulgated by Canadian legislation. Thus, it can be securely concluded that the financial institution has already performed its KYC obligations to ensure that this currency is "clean" and does not originate from proceeds of crime or terrorist financing.

The other three circles in Figure 2, Paper Fiat Currency, Cryptoasset 1 and Cryptoasset 2, all have a possibility of not being "clean" from an AML/ATF standpoint. It is often difficult to accurately identify the source through which paper fiat currency and cryptoassets originated from. It is therefore vital to ensure that these methods of entry into the cryptoasset regime have gone through the proper AML/ATF scrutiny, including record keeping, KYC, reporting of suspicious transactions and compliance program requirements. When physical fiat currency is used in a transaction at a financial institution, the said transaction must already undergo proper AML/ATF regulatory compliance in order to be accepted at the institution. It is vital for the protection of Canada's AML/ATF regime that we also ensure that proper AML/ATF compliance occurs at the convertibility mechanism stage for cryptoassets.

Furthermore, if Canada can properly regulate the convertibility mechanisms, which is the point of entry for a large majority of these transactions, then the Federal government will be able to effectively monitor the only point in cryptoasset transactions where the identity of users and source of funds can be accurately determined.

It is important to bear in mind that regardless of the regulations implemented into this space by the Canadian legislators, there are always going to be areas where proper enforcement of these regulations is going to be difficult, such as the exchange of one cryptoasset to another without the use of a convertibility mechanism. However, by focusing regulatory efforts on the convertibility mechanisms using an AML/ATF framework, Canada will be able to minimize the risk of money laundering and terrorist financing in this space.

13. AT WHAT POINT SHOULD CRYPTOASSETS BE REGULATED?

As set forth above, we suggest that the key point of regulation should occur at the coverability mechanism. Governments and international organizations have struggled with the details of how cryptoassets should be regulated in this rapidly-growing space. An important aspect of this debate focuses on the Canadian government balancing protection of cryptoassets users with ensuring Canadian competitiveness of its financial technology. Other points of this debate include seeking regulatory equilibrium among innovation, privacy and protection of stakeholders. Ms. Christine Lagarde, Director of the International Monetary Fund, has stated that regulators need to respond to these cryptoasset-driven issues in order to “combat tax evasion, money laundering, and the financing of terrorism, ensuring that risks are thoroughly understood and managed.”¹⁴⁹

In this regard, the initial popularity of decentralized cryptoassets was due to their high degree of anonymity and lack of government regulation.¹⁵⁰ These cryptoasset attributes created an environment that could be used by criminals to facilitate money laundering and terrorist financing with a high degree of anonymity. Brown discusses the benefits of anonymity in the cryptoasset space as follows:

In money laundering investigations, a main strategy has always been ‘to follow the money’. Given that the details of all Bitcoin transactions are distributed to all account holders in the ledger, analysis of transaction flows and values against the timing of criminal activities should make it possible to spot the Bitcoin pseudonyms involved and to follow their transaction history. The challenge then would be to link the pseudonym to a real person and, as mentioned already, the decentralised nature of Bitcoin makes this particularly difficult.¹⁵¹

¹⁴⁹ Christine Lagarde, “A Regulatory Approach to Fintech”, (March 2018) online: *Finance & Development* 55:2 <<http://www.imf.org/external/pubs/ft/fandd/2018/06/how-policymakers-should-regulate-cryptoassets-and-fintech/straight.pdf>>.

¹⁵⁰ Steven David Brown, “Cryptocurrency and criminality: the Bitcoin opportunity” (2016) 89:4 *The Police Journal: Theory, Practice and Principals* 327.

¹⁵¹ *Ibid.*

Such anonymity makes it highly improbable that any modern tool or mechanism would be able to track any direct exchange of cryptoassets when they are strictly peer-to-peer transactions from one user to another (e.g., over-the-counter transactions). Attempting to regulate this segment of cryptoasset transactions will ultimately generate little value for the regulators, as this activity will expend significant resources on the incorrect aspect transaction. This concept is similar to two criminals exchanging large amounts of physical fiat currency (cash) between one another without the use of a financial institution intermediary. In both examples, effective monitoring will be both costly and highly ineffective, as attempting to regulate every aspect of a cash or a cryptoasset transaction will largely be futile. Sharma effectively explains this concept:

It is important to note that all of the money laundering and illegal activities that Bitcoins can be used for, can also be done cash. That is, cash has been the primary mode of payment for drug dealers, money launderers, and other violent criminals. But since so many ordinary citizens also rely on cash for everyday payments, governments cannot ban cash. Similarly, even though a small fraction of Bitcoin transactions may be used for illegal activities, it is counterproductive to ban all of cryptocurrencies as that they have potential to improve the current banking system by a lot. Instead, governments should focus their energies on using this revolutionary technology to bring more transparency into their function.¹⁵²

One option for regulation would be a complete and outright ban on cryptoassets, which has been the method pursued by the People's Bank of China¹⁵³ and the State Bank of Vietnam,¹⁵⁴ both of which have enacted laws banning any financial institution from handling or conducting any cryptoasset transaction. We concur with Sharma's comments above that such prohibition seems counter-intuitive, as an intrusive degree of regulation or an outright ban may even result in negative externalities through the creation of an underground network, eventually leading these states to reverse their bans and focus instead on how to best regulate cryptoassets.¹⁵⁵ Such extensive regulation would hence be counter-productive to protecting the AML/ATF regimes of Canada.

¹⁵² Toshendra Kumar Sharma, "How does Bitcoin Money Laundering Work" (27 January, 2018), Blockchain Council (blog), online: <www.blockchaincouncil.org>.

¹⁵³ Xie Yu, "China orders banks to stop financing cryptocurrencies as noose tightens around disrupter", *South China Morning Post* (19 January 2018), online: <<https://www.scmp.com/business/banking-finance/article/2129645/pboc-orders-banks-halt-banking-services-cryptocurrency>>.

¹⁵⁴ Bank Indonesia Communication Department, Press Release, 20/50/DK0m, "Trade Balance Deficit Decreases" (25 June 2018), online: <https://www.bi.go.id/en/ruang-media/siaran-pers/Pages/sp_205018.aspx>.

¹⁵⁵ Gilly Wright, "Cryptocurrencies Face Bans, More Regulation", *Global Finance magazine* 32:2 (2 February 2018) 10, online: <<https://www.gfmag.com/magazine/february-2018/cryptocurrencies-face-bans-more-regulations>>.

Again, these considerations favour a regulatory focus on convertibility mechanisms. A convertibility mechanism constitutes the exchange mechanism or processor through which users are able to convert their cryptoasset into fiat money (or *vice versa*). The French Ministry of Finance stated that “assessing the risks associated with virtual currencies must factor in how these currencies are issued, how they are used and in particular transparency of flows, issues of liquidity and their convertibility to legal tender.”¹⁵⁶ Initial concerns expressed by the French Ministry of Finance related to the potential lack of transparency required when setting up a cryptoasset wallet and the total anonymity underlying cryptoasset transactions, rendering critical the necessity to “address the issues of the identities of the principal and effective beneficiary.”¹⁵⁷ The French Ministry of Finance was also concerned with the extraterritoriality aspect of cryptoassets, given the ability of the cryptoasset transactions to be rapidly and discreetly conducted across international borders.

While attempting to regulate peer-to-peer cryptoasset transactions is largely futile, it would be far more effective to instead place the regulatory burden on cryptoasset exchanges that are the primary convertibility mechanism used in order to convert the value of fiat currency into cryptoassets. While this structure would still permit certain cryptoasset transactions to be executed through trades between cryptoassets and physical cash in an “underground” market, while the preponderance of transactions are completed on cryptoasset exchanges, these exchanges constitute the area where regulatory bodies should concentrate their AML/ATF efforts. For this reason, certain exchanges have voluntarily registered themselves in Canada to be MSBs to be compliant with the current AML/ATF framework, prior to the Proposed Amendments, with the intent to gain the public trust.

14. KYC

The term KYC describes the process of a business verifying the identity of its potential clients and assessing potential risks of illegal activities underlying the business relationship. KYC is one of the key measures which can be implemented to reduce the risk of money laundering and terrorist financing. Indeed, as noted in the summary of the Supreme Court of Canada’s decision in *Canada (A.G.) v. Federation of Law Societies*:¹⁵⁸

There is a risk that financial intermediaries — those who handle funds on behalf of others — may facilitate money laundering or terrorist financing. To reduce that risk, Canada’s anti-money laundering and anti-terrorist financing legislation imposes duties on financial intermediaries, including lawyers, accountants, life insurance brokers, securities dealers and others. They must collect information in order to verify the identity of those on whose behalf they pay or receive money, keep records of the transactions, and establish internal programs to ensure compliance. The legislation also subjects financial intermediaries, including lawyers, to searches and seizures of the material that they are required to collect, record and retain.

¹⁵⁶ Virtual Currencies Working Group, “Regulating Virtual Currencies – Recommendations to prevent virtual currencies from being used for fraudulent purposes and money laundering” (June 2014), online: Docplayer <<https://www.economie.gouv.fr/files/regulatingvirtualcurrencies.pdf>>.

¹⁵⁷ *Ibid* at 4.

¹⁵⁸ 2015 SCC 7, [2015] 1 SCR 401.

The Auditor General of Canada identified the best point to combat money laundering and terrorist financing as occurring with the “front-line employees – who deal with customers on a day to day basis.”¹⁵⁹ These employees are in the ideal position to be able to identify transactions that may be categorized as unusual or suspicious. It is important for employees who are positioned on the “front-line” to be able to recognize what constitutes an unusual or suspicious transaction, which define the triggering events leading to suspicious transactions, as they are the gatekeepers for preventing money from being laundered through the organization by which they are employed.

KYC is guided in Canada by FINTRAC, which updated its guidelines in June 2017, expanding and further defining the accepted methods for identifying a client in order to ensure compliance with AML/ATF objectives. FINTRAC has outlined various types of transactions or activities required to identify individuals and confirm the existence of entities. Included in this list of transactions and activities are casinos, financial entities, real estate, securities dealers and money services businesses (“MSBs”). The various KYC requirements for these occupations are detailed under the *PCMLTFA*, including those relating to business relationships, ongoing monitoring processes, beneficial ownership guidelines, third-party determination and regulations relating to politically-exposed persons and heads of international organizations.

In relation to cryptoasset transactions, KYC requirements will most easily and efficiently be completed at the point of a cryptoasset convertibility mechanism. **We recommend that entities operating as convertibility mechanisms would ideally be required to register as MSBs for purposes of AML/ATF enforcement.** As discussed hereinabove, it is at the convertibility mechanism level where government regulation would be most effectively able to implement a KYC-based strategy.

15. CRYPTOASSET EXCHANGES UNDER MSB

In Canada, the law that establishes the AML/ATF framework, Bill-31, *An Act to Implement Certain Provisions of the Budget Tabled in Parliament on February 11, 2014 and Other Measures*¹⁶⁰ (“Bill C-31”) was given Royal Assent on June 19, 2014. Despite the fact that the Governor in Council was conferred the right in subsection 73.1(a) of the *PCMLTFA*¹⁶¹ to make any regulations with respect to “*dealing in virtual currencies*,” the *PCMLTFA* was never amended to include a definition of “*dealing in virtual currencies*,” therefore creating a legislative gap. If “*virtual currencies*” are not to be clearly defined, this situation has the potential to create an over-reaching regime wherein every person who is involved in the cryptoasset sphere be required to register as an MSB.

¹⁵⁹ Canada, *supra* note 138.

¹⁶⁰ Bill C-31, *An Act to implement certain provisions of the budget tabled in Parliament on February 11, 2014 and other measures*, 2nd Sess, 41st Parl, 2014, c 256(2) (assented to 19 June 2014), SC 2014, c 20.

¹⁶¹ *PCMLTFA*, *supra* note 3. Indeed, under the Section entitled “AMENDMENTS NOT IN FORCE” of the *PCMLTFA*, it is expressly written:

AMENDMENTS NOT IN FORCE

— 2014, c. 20, s. 256(2), as amended by 2017, c. 20, s. 436

2006, c. 12, s. 3(1)

256 (2) Paragraph 5(h) of the Act is replaced by the following:

(h) persons// and entities that have a place of business in Canada and that are engaged in the business of providing at least one of the following services:

[...]

(iv) *dealing in virtual currencies*, or

(v) any prescribed service;

[...]

In addition to this problem, the legislators, for reasons unknown to us, did not replace paragraph 5(h) of the *PCMLTFA* to include those persons “dealing in virtual currencies.” Accordingly, there is no regulatory requirement for such persons to fall under the auspices of “money services businesses,” obligating them to comply with the various requirements of the *PCMLTFA*, including: (a) record keeping, (b) verifying identity, (c) reporting of suspicious transactions, and (d) registration, as set forth in the FINTRAC Advisory regarding Money Services Businesses dealing in virtual currency.¹⁶² The legislation also does not appear to explore any of the mechanisms relating to the convertibility of cryptoassets into fiat currency (and *vice versa*), which should trigger the application of the *PCMLTFA*. FINTRAC also appears to have given conflicting policy interpretations¹⁶³ as to how cryptoasset businesses must be treated under the *PCMLTFA* and whether they would be defined as an MSB, which can be observed in Schedule A thereof (Schedule A is appended to our report).

When Bill C-31 was given Royal Assent in 2014, it is curious that the legislators never defined “dealing in virtual currencies” in the *PCMLTFA*. It is also perplexing why this phrase was never amended into paragraph 5(h) of the Act in order to regulate certain cryptoasset businesses as MSBs. In this connection, it is important for the legislators to enact legislation that strikes a balance between an effective AML/ATF regime and one that does not stifle innovation in Canadian financial technology, preventing it from becoming a global leader in this space.

(h.1) persons and entities that do not have a place of business in Canada, that are engaged in the business of providing at least one of the following services that is directed at persons or entities in Canada, and that provide those services to their clients in Canada:

[...]

(iv) dealing in virtual currencies, or
(v) any prescribed service;

[...]

¹⁶² Canada, Financial Transactions and Reports Analysis Centre of Canada, *Register your money services business (MSB)* (Ottawa: 2017) <<http://www.fintrac-canafe.gc.ca/msb-esm/register-inscrire/reg-ins-eng.asp>>.

¹⁶³ Canada, Financial Transactions and Reports Analysis Centre of Canada, *FINTRAC Policy Interpretations* (Ottawa: 2017) <<http://www.fintrac-canafe.gc.ca/guidance-directives/overview-apercu/FINS/2-eng.asp?s=12>>.

16. AN EXAMINATION OF REGULATORY MODELS FROM SWITZERLAND AND SINGAPORE

16.1. SINGAPORE¹⁶⁴

I. Introduction

Singapore has comfortably settled into its position as one of the world's cryptohavens, as it continues to be a magnet for blockchain ecosystem operations and capital raises, amidst the ups and downs of some of the most popular virtual currencies, such as Ethereum. We examine and analyse below some of the key components of Singaporean legal and regulatory aspects, including legal documentation, data protection, KYC and AML considerations, as well as intellectual property.

II. The Bedrock is the "Solution"

In a typical blockchain cryptocurrency ecosystem, a community exists whose members all have roles to play in the implementation of a solution to an identified problem. Alternatively referred to as a protocol or platform, the solution is the crucial bedrock, as without a viable, practical solution, irrespective of capital raised or number of supporters, the ecosystem is unlikely to succeed. In addition to the technology, thought processes and sophistication behind some of the solutions, the same simplistic market feasibility exercises of the past could work in determining the predicted success or not of a solution, in terms of its usefulness, practicality and sustainability. So, before even starting, the critical question to be considered is "is our solution useful, practical and desirable, and does it make business sense?"

There are, however, some founders who create a new virtual currency on the pretense of a solution, but whose main goal is to see it trade on an exchange, hopefully increase in its value, and gain quick wealth. These participants are not concerned at all about the development or use of the ecosystem and building a community, but only in creating an asset that is driven by speculation. Further to this extent, some participants do not mind that they are engaging in a speculative activity, as long as they ultimately profit, as they never intended on being a long-term part of a cryptoasset ecosystem.

III. Why is Singapore an Attractive Option?

Singapore has been described by many as a conducive landscape for cryptocurrencies and blockchain technology to flourish due to its superb communications network, its global reputation as a financial hub, characterized by non-interference and a balanced approach by regulators, and growing interest in FinTech.

¹⁶⁴ Franca Ciambella *et al.*, *Blockchain Cryptocurrency & the Legal Environment in Singapore* (Singapore: Consilium Law Corporation, 2017).

Unlike some other countries, Singapore has taken a liberal approach and opted for a more balanced view – it has embraced cryptoasset start-ups - and the government has set into motion large-scale initiatives to drive FinTech growth and innovation. The challenge faced by the Singaporean regulator, the Monetary Authority of Singapore (“MAS”) is in ensuring the retail investor and the greater public are adequately protected from “scam” offerings and to instill proper safeguards. Importantly, a key objective of the MAS is to not adopt too many restrictions so as to stifle the crypto environment.

The great interest in the cryptocurrency space in Singapore is from investors and corporations (both local and foreign) alike. The individual investors or token purchasers want to invest in the various cryptocurrencies being issued, while corporations are interested in conducting a token-generation event (“TGE”) related to the issue of digital tokens in Singapore and raising capital (the terms ICO and TGE are used herein interchangeably).

Singapore is viewed as an attractive jurisdiction to conduct a TGE because, among other things; (1) it is easy to incorporate an entity in Singapore; and (2) the MAS has taken the position (as of August 1, 2017) that it will not regulate the offer or issue of digital tokens provided the digital tokens do not constitute products that are regulated under the *Securities and Futures Act* (Cap. 289) (“SFA”) in Singapore. The lack of express prohibition on the issuance of digital tokens and the perception that decentralised cryptocurrencies are considered unregulated assets is therefore the reason Singapore, along with Switzerland, has been identified by many as a “crypto-haven.”

Having said that, it must be noted that more recently, after the publication of “The DAO Report” in July 2017 by the SEC, MAS issued “A Guide to Digital Token Offerings” on November 15, 2017. The guide elaborated that the offering of digital tokens must comply with the SFA only if the digital token constitutes a product regulated under the SFA.

In its guide, MAS also provides several hypothetical case studies of digital tokens that would be regulated in Singapore and others that would fall outside the ambit of its regulatory framework. There is now a clearer picture for potential offerors on which of their offerings may be caught by MAS’ regulatory framework.

MAS has said that it will carefully assess the nature, composition and specifications of the digital token, and has created a “Sandbox” approach in doing so, in an effort to provide speedy replies.

Notwithstanding regulation, an investor must take into account that there will always be inherent commercial risks in the investment, largely due to the success of the solution as discussed above, which could result in an investor losing all or a substantial portion of its investment. This brings us to the second step in the regulatory analysis: It could very well be that the token itself is not regulated, but that the solution or activity of the platform is regulated. For example, if tokens are used for a protocol whose activity is regulated in Singapore, such as insurance or moneylending, then the licenses required by these activities would need to be procured.

IV. Typical Legal Documentation Used for TGE/ICO

The practical reality then is that the only recourse available to a supporter or investor investing or buying into an unregulated digital token or coin offering may be the legal provisions found in the commercial agreements entered into between an investor or supporter and the Token/Coin Generator.

In terms of structuring a TGE or ICO, one way might be for the actual Generator to be set up as a foundation, which is usually in the form of a company limited by a guarantee, as this company is meant to carry out non-profit making activities that have some basis of national or public interest. The actual platform may be operated by a separate operating company. This can be a private limited company which should ideally be responsible for the on-boarding of the users and platform development. The agreements typically involved in such a structure are both a development and service contract.

We set out below some of the other documentation and agreements typically used in digital token or coin offerings in Singapore:

(1) *White Paper*

The “White Paper” is a document that provides an investor with a preliminary understanding of the intent of the Token or Coin Generator, objectives of the offering, technology behind the project (for example if it is underpinned by blockchain technology), type of corporate structure used in a potential offering and also the financial modelling of the token generation.

The White Paper is often the first document published on the website of the Token Generator and serves as an “expression of interest” to the potential investor. It is imperative for a potential investor to review the information in the White Paper carefully and ask the right questions so that he or she understands the technology behind the digital tokens issuance for example, prior to making an investment.

(2) *Legal Opinion*

The “Legal Opinion” is an essential first step in Singapore, as its purpose is to analyse the characteristics of the token and determine whether its “behaviour” falls within the scope of the SFA, and any other legislation pertaining to securities law. It would provide advice on any licenses or disclosure requirements required for an ICO. The Legal Opinion would also typically include advice on any other laws that would apply to the operation of the platform.

(3) *Pre-Sale Agreement*

The Pre-Sale Agreement (“PSA”), as its name implies, is an agreement that is entered into between selected investors and the Generator ahead of the “crowd-sale.”

The pre-sale is usually convened prior to the main TGE or ICO process in order for the Generator to pre-sell the digital tokens or coins to a select group of potential supporters or investors (such as family, friends and selected investors) at discounted prices and for a limited period of time as determined by the Generator. The pre-sale is also a useful way for the Generator to gauge interests in the digital token offering ahead of the crowd-sale with the TGE/ICO. It must also be emphasized that selling too many tokens at a pre-sale may not in fact be a good thing because for an ecosystem or a community to be successful, it often needs a large number of supporters. Selling tokens quickly to a small group may limit the number and scope of supporters, and ultimately the success of a community.

In certain cases, Generators offer a localized version of the Sale of Future Tokens Agreement (“SAFT”) that is compliant with Singapore law, as a means of a pre-sale document.

In certain transactions, parties may decide to enter into an escrow arrangement ahead of the TGE whereby an escrow agent will hold relevant cryptocurrency in trust for the investor, which will be released to the Token Generator upon certain trigger events occurring.

(4) *TGE Terms & Conditions*

The TGE or ICO Terms & Conditions (the “TGE Documentation”) comprise the main documentation used in the “crowd-sale.”

The TGE Documentation usually contains, among other things, information about the Token Generator, restrictions on distribution of the tokens, disclaimer, indemnification and self-regulation, features of the tokens, procedures for acquiring and receiving tokens and representations and warranties by investors.

In other words, the TGE Documentation is the main legally-binding agreement between the investor and Token Generator and will clearly set out the liability of the Token Generator to the investor in the event that any risks in the issuance materialize. It is therefore essential for the investor to carefully review the TGE Documentation and understand its implications ahead of the investment.

The TGE Documentation will also contain certain commercial terms which will be specific to each offering and differ, depending on the factual matrix and technological details of the offering.

(5) *Compliance Manual*

The Token Generator would generally have in place a robust compliance manual that will contain information on general compliance of the operating entity (that issues the tokens), relationship with regulators (if applicable), corruption and anti-bribery provisions, record keeping and personal data protection policy and more importantly, anti-money laundering and fraud provisions.

MAS has emphasized that the relevant MAS Notices on Prevention of Money Laundering and Countering the Financing of Terrorism may still apply to digital tokens that fall outside the MAS regulatory framework (especially the obligations to report suspicious transactions with the Suspicious Transaction Reporting Office of the Commercial Affairs Department and prohibitions against dealing with or providing financial services to designated individuals and corporates pursuant to the *Terrorism (Suppression of Financing) Act* (Cap. 325)), as well as any related subsidiary legislation.

It would be prudent for an investor to ask the Token Generator if it has in place a robust compliance manual containing all of the provisions mentioned above and whether the Token Generator is willing to share such compliance manual with the investor at the opportune time.

The MAS has also announced that it will, in due course, establish a new payment services framework to include rules to address money laundering and terrorism financing risks related to the dealing or exchange of virtual currencies for fiat or other virtual currencies. It is advisable that the investors seek clarification from the Token Generator intermediaries on whether MAS has issued those guidelines already and, if so, whether they have put in place the required framework before investing.

V. Personal Data Protection

Section 2(1) of the Personal Data Protection Act (“**PDPA**”) states that:

“‘personal data’ means data, whether true or not, about an individual who can be identified —
(a) from that data; or
(b) from that data and other information to which the organisation has or is likely to have access;”

The personal details of the participants collected online at the time of the ICO will constitute personal data under the PDPA. According to the PDPA, a Generator will have to obtain the consent of the participants in order to collect, use and disclose the personal data, and the collection has to be reasonable to provide the product services. The Generator also has to ensure it has made reasonable efforts to prevent unauthorised access to the data. Once the purpose for having the data is over, then the Generator has to cease retaining the personal data.

Section 26 of the PDPA requires that a Generator refrain from transferring any personal data to a country or territory outside Singapore except to organisations that provide a standard of protection to personal data that is comparable to the protection under the PDPA. This is relevant when an ICO is undertaken over a number of countries.

The recent passage of the General Data Protection Regulation and its extra territorial application also presents certain obligations in Singapore if any of the Participants are from the European Union.

VI. KYC/AML

The KYC and AML considerations, as stated above and as included in the compliance manuals, would also be included in the questionnaires for information on supporters or buyers of tokens. While it is unclear whether the *Corruption, Drug Trafficking and other Serious Crimes (Confiscation of Benefits) Act* (Cap.65A) (“CDSA”) may apply to cryptocurrencies, it would be prudent for the Generator to have in place comprehensive questionnaires collecting the identifying information under the CDSA from potential investors, or supporters either at the pre-TGE or TGE stage.

VII. Intellectual Property

In Singapore, copyright is not registrable. Therefore, in order to protect the copyright of the software source codes, the Generator should keep concise records, including dates of creation, of the software source codes for the blockchain protocol.

The Generator should also look into the possibility of registering its patent (if any) for any new processes for its blockchain technology and consider registering any trademarks it has with the Intellectual Property Office of Singapore.

VIII. Conclusion

The decentralised monetary system of cryptocurrencies is likely to be the future of financial transactions in Singapore and will also revolutionise the global financial landscape. It will be interesting to see how MAS attempts to strike a balance between permitting this virtual currency platform to grow and prosper in Singapore and enhancing an already complex regulatory regime with safeguards, with its attempts to protect not only investors, but the public at large. It will also be interesting to see what methods Token or Coin Generators take to ensure their “Solutions” make good commercial sense so that their communities or ecosystems succeed.

16.2 SWITZERLAND¹⁶⁵

On November 16, 2016, the Swiss Financial Market Supervisory Authority (FINMA) issued its strategic goals for 2017 to 2020. Goal No. 5 is to “push for the removal of unnecessary regulatory obstacles for innovative business models,”¹⁶⁶ for crowdfunding in particular and FinTech in general.

On August 1, 2017, the first new FinTech rules entered into force.¹⁶⁷ Moreover, a new banking license (banking license light) is currently being discussed in Switzerland based on a draft of regulations published on June 21, 2018. The objective of this new license is for entities (other than banks) to be able to accept deposits up to CHF 100 million.¹⁶⁸

Given, in particular, the Swiss political decision to open its regulations to FinTech (as a strategic objective), events are currently moving quite fast in Switzerland.

On February 16, 2018, FINMA has published guidelines on ICOs¹⁶⁹ (the FINMA Guidelines).

This article is based principally on these FINMA Guidelines (as well as on the first FINMA decisions received), given that they provide for a relatively clear definition of the different categories of tokens and of the applicable Swiss regulation.

I. FINMA Guidelines / Categories of Tokens

FINMA bases its approach on the underlying economic function of the token.¹⁷⁰ It distinguishes three types of tokens:

(1) *Payment Tokens*

Payment tokens (synonymous with cryptocurrencies) are tokens which are intended to be used as a mean of payment for acquiring goods or services or as a means of money or value transfer.¹⁷¹

According to Article 3 Para. 2 Let. b, the issuance of means of payment (which includes payments tokens/cryptocurrencies) by a Swiss entity (i.e. one having a physical presence in Switzerland) is subject to the *Swiss Anti-Money Laundering Act* of October 10, 1997.

One of the consequences of this regulation is that the Swiss issuing entity should be affiliated to a self-regulatory organization (SRO) for AML purposes. This being said, the issuer may choose the option to delegate the acceptance of the funds/amounts to be received to a third-party Swiss financial intermediary (itself being subject to AML).

¹⁶⁵ Alexandre de Bocard, *Swiss regulatory framework applicable to Token Generating Event (TGE / Initial)*, (Switzerland, Ochsner & Associates, 2018).

¹⁶⁶ Swiss Financial Market Supervisory Authority, “FINMA’s strategic goals” <<https://www.finma.ch/en/finma/supervisory-objectives/strategy/>>.

¹⁶⁷ Switzerland Government, The Federal Council, *Federal Council puts new fintech rules into force* (Bern: 05 July 2017) <<https://www.admin.ch/gov/en/start/documentation/media-releases.msg-id-67436.html>>.

¹⁶⁸ Government of Switzerland, Le Chef du Département fédéral des finances DFF, *Modification de l'ordonnance sur les banques (autorisation FinTech) : ouverture de la procédure de consultation* (Switzerland : 21 June 2018) <https://www.admin.ch/ch/f/gg/pc/documents/2967/OB-autorisation-FinTech_Lettre_fr.pdf>.

¹⁶⁹ Swiss Financial Market Supervisory Authority, “FINMA publishes ICO guidelines” (16 February 2018) <<https://www.finma.ch/en/news/2018/02/20180216-mm-ico-wegleitung>>.

¹⁷⁰ FINMA Guidance 04/2017, 29 September 2017 (Switzerland), § 3.1, page 3 [FINMA].

¹⁷¹ *Ibid.*

In case of such delegation, the issuer should not be subject to AML (as this may be confirmed by FINMA in the context of a non-action letter). Several third-party financial intermediaries currently provide for such KYC/AML tasks. In addition, several Swiss banks have agreed to open commercial accounts (denominated in fiat) for companies that have performed an ICO.

(2) *Utility Tokens*

Utility tokens are tokens which are intended to provide access digitally to an application or service by means of a blockchain-based infrastructure.¹⁷²

For example, the utility token “has additionally an investment purpose at the time of its issuance,”¹⁷³ in other words, if the proceeds (even part of them) of the ICO are used to develop the main function of the token/platform (blockchain technology), FINMA treats such a token as a security.¹⁷⁴

However, in the case where the security does not provide for (i) voting rights (such as equity/stocks/shares), and/or (ii) economic rights of the issuer (such as equity, stock, shares or participation rights) and/or (iii) a claim (debt issued by the issuer, such as bonds), the token may qualify as “uncertificated security.” The main requirement to issue such uncertificated securities (on the primary market) is to maintain a token and tokenholders’ register (which can be accomplished digitally using a blockchain, as this has been confirmed by FINMA).¹⁷⁵ However, based on the same assumption (i.e., no voting or ownership rights granted by the issuer, and/or no outstanding debt of the issuer), no prospectus is required under current Swiss laws (more specifically the *Swiss Code of Obligations*).

(3) *Asset Tokens (Securities Tokens)*

FINMA uses the term “asset token” instead of “security token.” This being said, materially and from a Swiss legal perspective, these concepts are essentially similar.

According to the FINMA Guide, asset tokens represent assets such as a debt or equity of the issuer. In terms of their economic function, these tokens are analogous to equities, bonds or derivatives.¹⁷⁶ To complete the picture, we could add the structured products and the mutual funds.

In case the tokens qualify as equities (including participation rights; i.e., shares without voting rights) or bonds, an issuing prospectus according to Swiss law is required in case the tokens are offered or sold to the public (i.e., not being exclusively offered to a limited circle of investors). However, under the current laws (more specifically the *Swiss Code of Obligations*), no filing or review of the prospectus by the regulator or another official or self-regulated body is required.

In addition, in case the issuance is performed “for own account,” no license (as securities trader) is required under Swiss law. In other words, the issuance of share tokens, participation-right tokens or debt tokens for own account is, in principle, not subject to Swiss financial laws, authorization requirements, or prospectus content requirements.

¹⁷² *Ibid.*

¹⁷³ *Ibid* at § 3.2.2, page 5.

¹⁷⁴ *Ibid.*

¹⁷⁵ *Ibid* at § 3.2, page 4.

¹⁷⁶ *Ibid* at § 3.1, page 3.

Finally, tokens enabling physical assets to be traded on the blockchain also fall within the category of asset tokens. Such tokens may qualify as “uncertificated securities.”

II. Cantons: Zoug, Neuchâtel & Geneva

As in Canada, Switzerland is a federal jurisdiction. The "provinces" are called "Cantons." Several Cantons are very welcoming to blockchain and issuers of tokens, such as Zoug, Neuchâtel & Geneva.

On May 28, 2018, the Canton of Geneva published an ICO guide to provide specific information (including taxation-related matters) and to assist token issuers (whether Swiss or foreign promoters) on all aspects and different steps of an ICO,¹⁷⁷ including post-ICO events.

Thanks to the sophisticated blockchain, crowdfunding and smart contract ecosystem developed promptly and efficiently by the Canton of Geneva, token projects can be presented to the Canton within a short time frame, as well as simultaneously to various experts, such as Swiss banks, Geneva tax authorities, KYC/AML providers, FinTech specialists, as well as tax advisors and lawyers specialized in FinTech (all subject to a non-disclosure agreement and other internal rules).

17. CONCLUSIONS — TOWARDS A NEW CRYPTOASSET REGULATORY REGIME

Through our above comparative examination of the current global regulatory regimes addressing cryptoassets and the complexity of the cryptoasset space, we propose that establishing a new regulatory regime in Canada would constitute the most prudent approach “on the grounds that these offerings are so new and multi-faceted that they cannot be captured satisfactorily by existing regulations.”¹⁷⁸ To this extent, “creating a new regulatory regime... is an extremely difficult and resource-consuming task”; realistically, the requisite time required to implement such a framework would necessitate a long-term planning horizon.¹⁷⁹

¹⁷⁷ Republic and State of Geneva, Department of Security and Economy, *Initial Coin Offerings (ICOs) in the Canon of Geneva* (Geneva: 28 May 2018) <<https://www.ge.ch/document/guide-initial-coin-offerings-icos-canton-geneva>>.

¹⁷⁸ France, Autorité Des Marchés Financiers, *Discussion Paper on Initial Coin Offerings* (Discussion Paper) (2017).

¹⁷⁹ *Ibid.*

As an initial measure, there exists notable support¹⁸⁰ that those “dealing in virtual currencies” should be regulated under Canada’s AML/ATF legislative framework, and, more particularly, as domestic and/or foreign MSBs (i.e., reporting entities) that are subject to obligations of: (i) record keeping, (ii) KYC, and (iii) reporting.¹⁸¹ Furthermore, the Federal Government has appropriately taken the initiative in releasing its Proposed Amendments (on June 9, 2018), containing the *caveat* that cryptoassets might actually be harder to launder than traditional fiat.¹⁸²

Based on the conclusions gleaned from our examination of the current Canadian regulatory landscape, review of the inherent attributes of cryptoassets and analysis of certain international models of cryptocurrency from the United States, Switzerland and Singapore, we offer the following recommendations:

1. The definition of “virtual currency” (or cryptoasset) should be replaced by “cryptoasset” so as to avoid ambiguity and indefiniteness

Under the heading “Virtual Currencies” of the Federal Regulatory Impact Assessment Statement, virtual currencies are described therein as:

The evolving financial services landscape is further influenced by virtual currencies, especially decentralized digital payment systems, like Bitcoin, that operate outside the traditional financial system. A virtual currency is a medium of exchange that allows for value to be held and exchanged in an electronic, non-physical manner, is not a fiat currency (i.e. the official currency of a country), has the intended purpose of being exchanged for real and virtual goods and services, and allows peer-to-peer transfers.

Virtual currencies can be “centralized,” in that they are issued and controlled by a single company or entity, or “decentralized,” in that there is no central authority that creates or manages it (e.g. Bitcoin). Rather, these tasks are managed collectively by the network of some virtual currency users.

¹⁸⁰ See the evidence submitted by:

- **Dominion Bitcoin Mining Company** (available at: <http://www.ourcommons.ca/Content/Committee/421/FINA/Brief/BR9977217/br-external/DominionBitcoinMiningCompany-e.pdf>);
- **Ms. Annette Ryan (Associate Assistant Deputy Minister, Financial Sector Policy Branch, Department of Finance)** (available at: <http://www.ourcommons.ca/DocumentViewer/en/42-1/FINA/meeting-163/evidence#Int-10230587>);
- **Mr. Luc Beaudry (Assistant Director, Collaboration, Development and Research Sector, Financial Transactions and Reports Analysis Centre of Canada)** (available at: <http://www.ourcommons.ca/DocumentViewer/en/42-1/FINA/meeting-133/evidence#Int-9976970>);
- **Mr. Kyle Kemper (Executive Director, Blockchain Association of Canada)** (available at: <http://www.ourcommons.ca/DocumentViewer/en/42-1/FINA/meeting-140/evidence#Int-10039264>);
- **Stuart Davis, Chief Anti-Money Laundering Officer, AML Enterprise, BMO Financial Group** (available at: <http://www.ourcommons.ca/DocumentViewer/en/42-1/FINA/meeting-140/evidence#Int-10039264>).

¹⁸¹ It is worth mentioning that FINTRAC’s guidance document, entitled “Guideline 2: Suspicious Transactions” (June 2017), available at: <http://www.fintrac.gc.ca/guidance-directives/transaction-operation/Guide2/2-eng.asp>, provides, at sections 7 and 8 thereof, good indicators and KYC measures with respect to triggering events of suspicious transactions.

¹⁸² Kai Sedgwick, “Cryptocurrency is Harder to Launder Than Fiat Currency” (2 February 2018) online: Bitcoin.com <<https://news.bitcoin.com/cryptocurrency-harder-launder-fiat-currency/>> as shown through the quote (“[d]ue to the nature of public blockchains and the need to cash out into fiat, cryptocurrency is easier to monitor”).

In addition, virtual currencies can be “convertible” or “non-convertible,” depending on whether they can be exchanged for funds. Convertible virtual currencies are vulnerable to abuse for money laundering and terrorist activity financing purposes because they allow greater levels of anonymity, or in some cases complete anonymity, when compared to traditional non-cash payment methods. Virtual currencies can be accessed globally via online or mobile systems. They allow for the rapid transfer of funds within or across borders, oftentimes without any intermediary, are generally characterized by non-face-to-face customer relationships and can circumvent the physical “brick and mortar” financial system entirely. Due to these characteristics, virtual currencies are increasingly being used to facilitate fraud and cybercrime, and to purchase illicit goods and services on the Dark Web.

The Proposed Amendments currently define the term “virtual currency” as:

- (a) a digital currency that is not a fiat currency and that can be readily exchanged for funds or for another virtual currency that can be readily exchanged for funds; or
- (b) information that enables a person or entity to have access to a digital currency referred to in paragraph (a).¹⁸³

This proposed definition of “virtual currency” is insufficient, as it promotes the perception that it is: (i) a “currency,” which it is not (discussed in Section 5 above), (ii) a “digital currency,”¹⁸⁴ which it cannot be considered, as there is no definition thereof under current Canadian legislation for such expression,¹⁸⁵ (iii) a form of “electronic money,” similarly for which no definition thereof exists under current Canadian legislation, (iv) or money.¹⁸⁶

Moreover, it is not possible to ascertain whether the current definition of “virtual currency” would capture ICOs, ITOs and their corresponding tokens, such as transactional, utility and platform tokens. Tokens may not share similar characteristics (or attributes) with traditional currency or cryptocurrencies, such as Bitcoin and/or Ether.¹⁸⁷ Among the unintended negative consequences of using the phrase “dealing in virtual currency” is that it is not possible to determine whether users of the cryptoassets, exchange services, value transfer services, mining services or such other exchanges, all of which may act as convertibility mechanisms, are encompassed by said terminology.

¹⁸³ Canada Gazette, *supra* note 5 at 1(7), 14, 15, 25, 26, 27, 29, 31, 32, 33, 35, 36, 40, 42, 49, 51, 55, 57, 61, 63, 67, 69, 70, 73, 79, 81, 82, 84, 86, 95, 116, 120, 121, 122, 123, 125, 129, 133, 135, 136, 137, 144, 146, 154, 155, the section as it pertains to Schedule 4 and 5 of the Proposed Amendments.

¹⁸⁴ Government of Canada, Financial Consumer Agency of Canada, *Digital Currency* (Ottawa: 19 January 2018) <<https://www.canada.ca/en/financial-consumer-agency/services/payment/digital-currency.html>>. According to the Government of Canada’s website “digital currency” can be considered “electronic money”.

¹⁸⁵ As of July 9th, 2018, there is no mention of “digital currency” on the legislation (using ‘<http://laws-lois.justice.gc.ca/Search/Search.aspx>’ to search).

¹⁸⁶ Straitev, *supra* note 19.

¹⁸⁷ Haeems, *supra* note 9.

One possible course of action could be to amend the *PCMLTFA* to include the definition of “virtual currencies” or, ideally utilize the term “cryptoasset” in the legislation, which would fall in line with European Union banking authorities and/or FINCEN’s definition of same, as there does not currently exist any consensus in Canada¹⁸⁸ as to how a “virtual currency” (or “cryptoasset”) should be defined. Specifically, “cryptoasset” could be defined (as per the EU banking authorities) as: “a digital representation of value that is neither issued by a central bank or a public authority, nor necessarily attached to a [fiat currency], but is accepted by natural or legal persons as a means of payment and can be transferred, stored or traded electronically.”¹⁸⁹

2. AML/KYC enforcement pertaining to cryptoassets should occur at the convertibility mechanism nexus

In our view, the existing KYC framework in Canada is sufficient, indeed exemplary, in enforcing AML/ATF provisions relating to cryptoassets. To this extent, FINTRAC released “Guideline 2: Suspicious Transactions” in June 2017, which detail KYC procedures to be followed, as well as “red flags” that are potential indicators of money laundering and/or terrorist financing activities.

Moreover, KYC procedures are highly effective, as they may utilize sophisticated technological advancements to ascertain an individual’s identity (e.g., facial recognition, document scanning and authentication). Such procedures may be easily implemented to ensure documents required to verify customer identity constitute those that are “authentic, valid and current”¹⁹⁰ and verifiable by an independent third party.

Such enforcement could occur by obligating those persons “*dealing in virtual currencies*” (or “*dealing in cryptoassets*”), for example, cryptoasset exchanges that would fall into the MSB regime, to adhere to the current *PCMLTFA*-MSB regime. These obligations would have the benefit of compelling compliance with the *PCMLTFA* requirements, including KYC processes to be implemented for the convertibility mechanisms. Moreover, “FINTRAC Guideline 2: Suspicious Transactions,” should be continued to be used as a paradigm for KYC compliance.

¹⁸⁸ The Financial Consumer Agency of Canada loosely defines “digital currency” as electronic money that is not available as bills or coins, and are not legal tender in Canada. See: <https://www.canada.ca/en/financial-consumer-agency/services/payment/digital-currency.html>.

¹⁸⁹ European Banking Authority, “EBA Opinion on ‘virtual currencies’” (4 July 2014), online: EBA <<https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf>>.

¹⁹⁰ Canada Gazette, *supra* note 5.

18. AUTHORS AND ACKNOWLEDGEMENTS

AUTHORS

David Durand LL.L., B.Sc. (chem.) is a Founding Partner at Durand Morisseau LLP and is a member of the Québec Bar since 2011. Prior to founding Durand Morisseau LLP, David worked for various intellectual property boutique firms where he focused on technology and IP. David has recently been expanding his international network during his collaboration with firms from Switzerland and Singapore during the writing of this publication, as well as his practice in FinTech and regulatory issues.

Drew Dorweiler FRICS, FCBV, MBA, CPA•ABV, CPA (IL), ASA, CVA, CBA, CFE is a Managing Director of IJW & Co., Ltd. He possesses over 33 years of experience in valuation of hundreds of privately and publicly-held companies in business valuation, corporate finance and litigation support mandates on a global basis. Drew has frequently participated as a financial advisor in corporate mergers and acquisitions, divestitures and start-up businesses and in sourcing financing in North America and internationally. He has testified as expert witness in more than 27 cases before Québec Superior Court, Ontario Superior Court of Justice, U.S. District Court, Tax Court of Canada, Court of Queen's Bench of Alberta and arbitration panels in high-profile, complex financial litigation and valuation matters.

Drew has given numerous interviews featured in international TV, radio and print media on business valuation, financial and sports business matters. He has spoken at myriad conferences and authored many articles in professional publications on business valuation, litigation support and fraud-related topics during the past 28 years. Drew was elected to Board of Trustees of The Appraisal Foundation for 2013-2018 and to Board of Directors of The Canadian Institute of Chartered Business Valuators from 2006-2009 (he was named a Fellow in 2018). He was named a Fellow of Royal Institution of Chartered Surveyors in 2013 and elected President of the Board of Directors of the Montreal Chapter of the Association of Certified Fraud Examiners for 2005-2007. Drew graduated with a Bachelor of Arts, Economics, Dartmouth College. He obtained a dual MBA, Corporate Finance and Accounting, Lubin Graduate School of Business, Pace University.

Franca Ciambella is Managing Director of Consilium Law Corporation. Trained in law and business in Canada, New York and Singapore, Franca has been a member of the Québec Bar since 1990, and in 2010, was one of the first foreign lawyers to gain full admission to the Singapore Bar. Her legal career of over 25 years encompasses 16 years of private practice including being the Managing Partner of the Singapore office of Stikeman Elliott and a Legal Associate at Norton Rose, seven years as General Counsel for Asia Pacific for Tyco International Ltd. (a US based Fortune 500 corporation), acting as a technical advisor on regional economic integration to high levels of government in ASEAN, carrying on a mediation practice and since 2010, being the Managing Director of the Singapore-based international law firm of Consilium Law Corporation ("CLC"). CLC represents clients doing business in emerging economies, including in south-east Asia and Africa, as well as in Canada, in diverse sectors.

Franca's subject areas of legal expertise are in corporate and commercial law, contracts, technology law and FinTech, cross border M&A, foreign investment law and international trade with a focus on Canada, ASEAN and West Africa. Currently she is focusing on a number of technology projects and cutting-edge, multi-jurisdictional legal practice in the area of cryptocurrency and ICOs. She also assists clients in creating compliance programs, including anti-bribery, and trade compliance. Franca is accredited as a mediator with the Singapore Mediation Centre and with the ADR Group in London, UK, and acts as a mediator in various areas including cross-border family law disputes. Having an undergraduate commerce degree and a certificate in business (from the US and Canada), she also serves as an advisor to multinational businesses and as a director on several boards of corporations and non-profit organizations. She has authored numerous legal and business publications including a book entitled "Investments in South-east Asia: Policies and Laws," contributes regularly to various chambers of commerce publications and websites, and guest lectures to MBA students at McGill University and other educational institutions.

Alexandre de Boccard is a Swiss- and US-trained lawyer specialized in financial regulation. He is a partner of the Swiss law firm Ochsner & Associés. Alexandre de Boccard advises financial institutions such as banks, securities dealers, and asset managers on regulatory matters, contract law, corporate law, FinTech regulation, as well as stock exchange law. He also advises companies that are active in FinTech and has been the official legal partner of the Swiss Crowdfunding Association since its incorporation in 2015. Alexandre de Boccard assists clients in obtaining licenses from the Swiss Financial Market Supervisory Authority (FINMA), as well as negative rulings for activities such as crowdfunding, issuance of means of payment, Token Generating Events (TGE) and Initial Coin Offerings (ICOs). Ochsner & Associés is referenced by the Canton of the Geneva as an expert in ICOs.

Alexander Schaefer is entering his third year of law at the University of Windsor and has been working as a Student at Law for Durand Morisseau LLP at its Montréal office since May 2018. He has worked primarily on Regulatory and FinTech law during his time at the firm. Previous to this, Alexander worked as financial analyst at BMO Financial Group at the London, Ontario branch. Alexander graduated from the University of Western Ontario with a bachelor's degree in Political Science with Distinction.

SIGNATORY FIRMS

Durand Morisseau LLP provides various legal services to clients, including litigation, representation in IP prosecution, and business and commercial transactions, both in Canada and abroad. For more information about Durand Morisseau LLP's practice, please visit durandmorisseau.com.

Because of its generality, the information provided herein may not be applicable in all situations and should not be acted upon without specific legal advice based on particular situations. If you wish to make a comment on this publication, please write to: David Durand at Durand Morisseau LLP, 3 Place Ville Marie, Suite 400, Montréal (Québec) Canada, H3B-2E3 or email info@durandmorisseau.com.

IJW & Co., Ltd. is an investment bank providing mergers and acquisitions advisory, business valuation, litigation support (expert witness) and corporate finance services to clients globally. Headquartered in Canada, the firm has offices in the United States, Hong Kong, Singapore and Antigua. For more information on IJW & Co., Ltd.'s practice, please visit www.ijw.ca.

SCHEDULE A

Summary of FINTRAC Policy Interpretations Regarding MSBs (Virtual Currency)

Policy Interpretation	Rendered on	Description	Decision rendered by FINTRAC
PI-5404	2012-05-02	Securities dealer v. MSB - “There is additional clarification in the interpretations notice that states that a business would be exempt from MSB registration if the activity was carried out as part of another regulated activity (purchasing securities is provided as an example here). The question in this regard is whether the MSB definition would apply to a securities dealer that is also conducting foreign exchange transactions outside of the scope of securities related purchases - are they also required to be registered as an MSB?”	“Should a securities dealer provide money services business (MSB) activities, such as foreign exchange, outside of their securities dealer activities, the securities dealer would be required to register as an MSB. Upon registration as an MSB, the registrant would indicate that their business is also another type of reporting entity (i.e., a securities dealer). As an MSB and a securities dealer, the entity would be subject to all applicable sections of the [PCMLTFA] and its associated regulations.”
PI-5549	2013-05-09	Business engaged in the trade of digital tokens, particularly Bitcoin and Litecoin.	“Based on the information you provided, namely that your ‘business is engaged in the trade of digital tokens, particularly Bitcoin and Litecoin’, it appears that your entity is not, at this time, engaged as an MSB in Canada as per the Proceeds of Crime (Money Laundering) and Terrorist Financing Act and its associated Regulations. In fact, your business doesn’t provide the services of remitting and/or transferring funds for the sake of the service. The transfer of funds is simply a corollary of your actual service of trading virtual currency. Therefore, you do not have to register your entity with us.”

PI-5550	2013-05-09	Buying and selling Bitcoins directly from customers; bitcoin payment provider; start an exchange.	“Based on the information you provided, namely that your entity ‘Buy and Sell Bitcoins directly from customers’, it appears that your entity is not, at this time, engaged as an MSB in Canada as per the [PCMLTFA] and its associated Regulations. In fact, your entity doesn’t provide the services of remitting and/or transferring funds for the sake of the service. The transfer of funds is simply a corollary of your actual service of buying and selling virtual currency. Also, the creation of a ‘software for business to accept Bitcoin payments and either keep Bitcoins or automatically convert to CAD’ and an ‘order book where people can put in an order at x price and hope it gets filled’ does not make your entity, at this time, engaged as an MSB in Canada since your entity provides a platform allowing businesses to accept or trade virtual currency.”
PI-5551	2013-05-09	Virtual currency – “Company ABC purchases virtual currency such as bitcoins, litecoins, Facebook credits, world of Warcraft coins at bulk discount rates and sells it at physical locations across the country as well as online through cash deposits in banks. In our physical stores we will collect the money from buyers first before sending them the virtual currencies.”	Based on the fact pattern, “[...] it appears that your entity is not, at this time, engaged as a [MSB] in Canada as per the [PCMLTFA] and its associated Regulations. In fact, your entity doesn’t provide the services of remitting and/or transferring funds for the sake of the service. The transfer of funds is simply a corollary of your actual service of buying and selling virtual currency. Therefore, you do not have to register your entity with us.”
PI-5554	2013-05-16	Bitcoin exchanges.	“At this time, if the entity buys and sells Bitcoins directly from customers, it appears that this entity is not engaged as an MSB in Canada as per the [PCMLTFA] and its associated Regulations. In fact, this kind of entity doesn’t provide the services of remitting and/or transferring funds for the sake of the service. The transfer of funds is simply a corollary of their actual service of buying and selling virtual currency.”

<p>PI-5561</p>	<p>2013-06-04</p>	<p>Bitcoin exchange – trade of digital tokens</p>	<p>Trade of digital coins is not recognized under the <i>PCMLTFA</i> as one of the three MSB activities. “While the remitting or transmitting of funds is an MSB activity, in this specific scenario, the remitting or transmitting of funds that occurs is incidental and only happens as the business carries out its core activity of trading digital token. The remitting and transmitting of funds is the method used by this business to provide its service of trading digital token. In addition, handling Bitcoins, or defining a business as a Bitcoin Exchange, does not automatically make the business exempt from registering as a MSB. The business may perform other activities, which may or may not involve Bitcoins, which would make it subject to the <i>PCMLTFA</i>. While the <i>PCMLTFA</i> applies to business engaged in ‘foreign exchange dealing,’ this does not apply to Bitcoin as it is not a national currency of any country.”</p>
<p>PI-5573</p>	<p>2013-07-16</p>	<p>Digital cash platform which mints high-encrypted single use digital coins that can be validated and settled in real-time.</p>	<p>If the entity is remitting and/or transmitting funds of merchants and/or consumers for the purpose of carrying out “electronic payments,” or more specifically, “P2P payments” or person to business payments, the entity, at this time, is engaged as a MSB.</p>
<p>PI-5598</p>	<p>2013-08-19</p>	<p>Bitcoin/fiat currency transactions in Canada, wherein the transaction occurs as follows: (1) log into Exchange account and selects add CAD100 credit, (2) transfers CAD100 from personal account into Exchange’s bank account, quoting on-off payment reference, (3) buys CAD100 of BTC from the Exchange at a quoted rate based on the Exchange’s bid/ask spread, (4) uses BTC balance to buy GBP from the Exchange at a quoted rate based on the Exchange’s bid/ask spread, (5) withdraws GBP from the Exchange to personal GBP bank account. - “Even where users think they are making a straight conversion from, for instance, CAD to GBP, the actual Back-office transaction will include Bitcoin as a mid-way currency [...]” and that “[t]he Exchange will hold bank accounts with a major bank in each jurisdiction in whose currency we trade – e.g. CAD bank account in Canada & GBP bank in the UK.”</p>	<p>The entity will be engaged in foreign exchange dealing and as such, will be a MSB per the Act and its associated Regulations.</p>

PI-5601	2013-08-22	Company ABC provides real time purchasing of small amounts of crypto-currency using an INTERAC debit card. It also facilitates online checkouts where merchants accept Bitcoin while consumers hold debit card balances.	The business is not engaged as a MSB.
PI-5603	2013-08-27	Consumer will scan a digital wallet and specify the amount being sold to the ATM. The ATM will then calculate the market price of Bitcoin and subtract the transaction fee (a pre-set percentage) from the total amount to be received in fiat. The Bitcoins purchased from the consumer will then be transferred to Company ABC's online exchange account and an amount in Canadian dollars will be dispensed to the consumer.	Based on the summary of Company ABC, it appears that your entity is not, at this time, engaged as an MSB.
PI-5685	2014-01-21	Selling a pre-paid bitcoin card at retail locations and that "those cards have activation codes on them. The activation codes can be redeemed only on our website for credit."	The entity is not, at this time, engaged as an MSB in Canada.
PI-6095	2014-02-17	Virtual currency exchange not covered – clarifications	<i>PCMLTFA</i> does not apply to virtual currencies because they do not fall within the definition of "funds" under the <i>PCMLTFA</i> . The <i>PCMLTFA</i> also covers businesses engaged in "foreign exchange dealing," however; this also does not apply to virtual currencies as they are not a national currency of any country. With this in mind, it is important to note that handling virtual currency, or defining a business as a virtual currency exchange, does not automatically make the business exempt from registering as a MSB. The business may perform other activities, which may or may not involve virtual currency, which would make it subject to the <i>PCMLTFA</i> .

PI-6110	2014-03-04	Bitcoin – payment for invoices through EFT as an online bill payee – “Company ABC is a convenient and easy option for the small business, entrepreneur or professional to collect and receive payments directly to their bank accounts from their customers through [EFT] as online bill payee” - ABC’s clients will have to provide the following during the sign-up process: (1) full legal name of the company; (2) business number incorporation number; (3) existing banking information including a banking reference; (4) type of industry and expected monthly volumes; (5) contact details of at least one director; and (6) all companies using NoCheque need to have been in business for at least 3 years.	The entity is a MSB.
PI-6244	2014-09-30	Using crypto-currency for exchanges – “the client could be depositing \$CAD in his account, convert the funds into a crypto-currency and then sell back that currency in exchange of \$USD”	The company will be providing a foreign exchange dealing service, and will, therefore, be engaged as an MSB in Canada.
PI-6246	2014-10-01	“Bitcoin as the underlying internal transfer technology that allows users to send remittances online” and “User accounts that hold Canadian dollars send funds through Bitcoin’s payment protocol only as a method of simplified monetary movement”	If a user can request the remittance of fiat currency to another individual or entity, then ABC INC. will be considered as engaged as a MSB in Canada, with all of the associated obligations.

PI-6268	2014-12-10	Bitcoin business – “funds will be exchanged at a local Bitcoin exchange and sent to a foreign Bitcoin exchange to be converted back to fiat currency.”	<p>“[...] The Government of Canada has made changes to what services make an individual or an entity an MSB in Canada to include virtual currency services; however, these changes are not yet in force. Individuals and entities engaged in the business of dealing solely in virtual currencies will be MSBs, but cannot yet register with FINTRAC. Before these individuals and entities will be subject to [PCMLTFA], regulations need to be written to define what it means to be engaged in the business of providing services such as dealing in virtual currency.</p> <p>Based on the information you provided in your business model, namely that ‘funds will be exchanged at a local Bitcoin exchange and sent to a foreign Bitcoin exchange to be converted back to fiat currency,’ it appears that your entity is providing fiat to fiat currency remittance services and therefore appears to be, at this time, engaged as an MSB, as per the <i>PCMLTFA</i> and its associated Regulations.</p> <p>As a MSB in Canada, you have legal obligations under Canada’s <i>PCLMTFA</i> [...]”</p>
PI-6367	2015-10-16	Purchase and/or sale of virtual currency from an online virtual currency exchange; matching of buyers and sellers and receipt of funds directly from the individual.	<p>Not a MSB, as “changes are not yet in force. Individuals and entities engaged in the business of dealing in virtual currency services will be MSBs, but cannot yet register with FINTRAC. [...]”</p> <p>Based on the information you provided, it appears you are not providing any of the MSB services identified above, therefore, at this time, you are not engaged as an MSB in Canada as per the [PCMLTFA] and its associated Regulations and cannot register with us.”</p>
PI-6369	2015-11-09	Transfer of funds from one individual to another using an electronic funds transfer network	<p>You are a MSB as a result of the following summarized scenarios:</p> <ol style="list-style-type: none"> 1. Pay-out service provided to merchants outside of Canada to pay end recipients in Canada; 2. Pay-out service provided to merchants in Canada with end recipients outside of Canada; <p>Pay-out service provided to merchants in Canada with end recipients in Canada; [...]</p>

To :

Joint Canadian Securities Administrators / Investment Industry Regulatory Organization of Canada

Subject :

Comments on consultation Paper 21-402 "Proposed Framework for Crypto-Asset Trading Platforms"

Bitcoin is not a security. It was never a security. It will never be a security based on the current generally accepted definition of what is and what is not a security.

"A pure medium of exchange, the one that's most often cited, is Bitcoin. As a replacement for currency, that has been determined by most people to not be a security." - Jay Clayton, Chairman of the U.S. Securities Exchange Commission¹

Other "crypto-assets" are most probably securities and their promoters should be held accountable by the current Canadian securities regulation framework. There is no need for additional regulation.

The orientation of the consultation paper is problematic because it packages everything (including Bitcoin) under the vague notion of "crypto-asset". As mentioned above, the emission of new tokens should be treated as security and dealt with using the current CSA regulation framework.

Concerning Bitcoin, the Joint Canadian Securities Administrators / Investment Industry Regulatory Organization of Canada are clearly wandering outside of their jurisdiction. Bitcoin is not a security, it was never a security. Additionally, the negative bias towards Bitcoin expressed by the various public interventions of the CSA members is concerning and should be denounced not only by the members of the emergent Canadian Bitcoin industry but also by the legal community.

"For innovators, controlled economies are dream destroyers. Free markets should be the natural choice of today's innovators, who today are striving to build bright and better futures."

- J. Christopher Giancarlo, Chairman of the U.S. Commodity Futures Trading Commission²

Jonathan Hamel

Founder, [Académie Bitcoin](#)

Associate Researcher, [The Montreal Economic Institute](#)

¹ <https://coincenter.org/link/sec-chairman-clayton-bitcoin-is-not-a-security>

² <https://www.coindesk.com/christopher-giancarlo-cftc-future-of-blockchain>



Comments on Consultation Paper 21402:
Proposed Framework for Crypto-Asset Trading Platforms

TO: Canadian Securities Administrators/Investment Industry Regulatory Organization of Canada
FROM: PARADISO VENTURES INC. O/A Balance
Date: May 15th, 2019

Dear Sir/Madam,

As a federally incorporated fintech business focused on cryptoassets, PARADISO VENTURES INC. O/A Balance (**"Balance"**) respectfully wishes to make the following observations and comments in reply to *Consultation Paper 21402: Proposed Framework for Crypto-Asset Trading Platforms* jointly published by the Canadian Securities Administrators (**"CSA"**) and the Investment Industry Regulatory Organization of Canada (**"IIROC"**) on March 14th, 2019. Allowing room for innovation while ensuring the fair and efficient functioning of our capital markets is a tough balancing act. We hope our contribution will help towards building a tailored framework that will not only bring much needed clarity to ecosystem participants, but also ensure that Canada maintains its reputation on the international stage as a financial markets leader and innovator in this new digital economy.

We address some of the consultation questions below.

1. *Question 1: Are there additional factors not mentioned in the paper that should be considered in making the determination of whether or not a security or derivative might be involved in the trading performed on Platforms?*

We believe the factors enumerated are sufficient in helping make a determination, however further clarification is needed around the criteria of what counts as delivery of crypto assets. To provide some context before explaining our view, we would like to highlight the distinctions between possession, ownership, and control. If a participant generates the private cryptographic key used to access the crypto-asset themselves, they have possession, ownership, as well as control of the asset. If a Platform generates it on their behalf:

- directly: the participant lost both possession, as well as control;
- indirectly (e.g. through a custodial key management system): the participant lost possession, but retains partial or full control.

The matter of ownership comes down to whether or not the Platform passes the full legal title to the client, or whether the right in the bundle get split and held by both the participant as well as the Platform (specified typically in a Platform User Agreement or equivalent document).

As such, if a participant purchases a crypto-asset from a Platform, we expect the following criteria to be met for delivery to have occurred:

- the crypto-asset was delivered to a participant approved digital wallet that they have partial or full control of (i.e. participant controls the asset);
- the participant has first rights and full legal title to the crypto-asset (i.e. participant owns the asset);

- delivery needs to occur within a reasonable time frame as evidenced by an independently verifiable cryptographic proof (confirmed blockchain transaction or signed transaction in a state channel or sidechain that could be closed and broadcast to the blockchain by the participant at any time).
2. *Question 2: What best practices exist for Platforms to mitigate these risks? Are there any other substantial risks which we have not identified?*

We suggest the following best practices for mitigating some of the risks highlighted:

- *Investors' crypto assets may not be adequately safeguarded.* With over 1B dollars worth of crypto-assets lost or stolen from Platforms globally last year, we would see this risk mitigated by Platforms through:
 - full-segregation of digital wallets for each client as evidenced by regular third party audits (i.e. no more pooled wallets where the entire Platform treasury can be lost in one incident);
 - offline (i.e. air-gapped) generation of private keys controlling the wallets, as well as offline management of the key for its entire lifetime (i.e. transactions signing must also be performed offline);
 - adequate disaster recovery and succession planning protocol that are tested and meet the business purpose as well as specified service level agreements, as evidenced by regular third-party audits.

Whether Platforms self-custody or choose to work with a third-party custodian, we see a *SOC 2 Type I (Security)* report as a core minimum competency that should be met by any ecosystem participant providing custodial services.

- *Processes, policies, and procedures may be inadequate.* This risk could be partially mitigated by Platforms requiring personnel have any form of access to Platform's or participants' crypto-assets to pass and be subject to ongoing background and criminal checks. The existence, suitability, and application of processes for ensuring business continuity, and addressing key personnel and regulatory compliance risks can be demonstrated through a qualified opinion provided by a third-party, typically in the form of a SOC report.
- *Investors' assets may be at risk in the event of a Platform's bankruptcy or insolvency.* This risk could be partially mitigated by Platforms that pass the full legal title to the participant and do not keep the participants' assets on their balance sheet. For Platforms that include participants' assets on their balance sheets for rehypothecation, existing risk mitigation strategies in the applicable regulation should be sufficient.
- *Investors may not have important information about the crypto assets that are available for trading on the Platform.* This risk could be partially mitigated by requiring Platforms to publicly disclose their selection criteria through the form of a Digital Asset Selection Framework or equivalent document, as well as their policy for managing hard and soft forks, as well as airdrops in a Fork Policy or equivalent document.
- *Investors may not have important information about the Platform's operations.* This risk could be partially mitigated by requiring Platforms to publicly disclose the ownership, possession, and control parameters around the participant's crypto-assets (as per the definitions in the answer to Question 1 above) in their User Agreement or an equivalent document.
- *Conflicts of interest may not be appropriately managed.* This risk could be partially mitigated through requiring Platforms that act as market makers or trade as principal to publicly disclose so in their User Agreement or an equivalent document.

- *Investors may purchase products that are not suitable for them* partially mitigated by Platforms that keep any information displayed to participants as general, historical, and impersonal in nature. For Platforms that offer financial and investment advice, existing risk mitigation strategies in the applicable regulation should be sufficient.
- *Manipulative and deceptive trading may occur* mitigated through the implementation of existing monitoring requirements in the applicable regulation, and regular reporting to a regulation services provider.
- *There may not be transparency of order and trade information* mitigation strategies in the existing regulation should be sufficient, for the Platforms where this is applicable.
- *System resiliency, integrity and security controls may be inadequate* though we are aware there currently are challenges in obtaining such reports, we believe the correct way to mitigate these risks is through requiring platforms to demonstrate the existence of appropriate controls by obtaining a qualified opinion (e.g. SOC for Cybersecurity) from a third-party auditor or cybersecurity firm.

At the time of this writing we do not identify any other substantial risks that would require mitigation, other than the ones already highlighted in the paper.

3. *Question 3: Are there any global approaches to regulating Platforms that would be appropriate to be considered in Canada?*

Proving and tracking ownership of a digital file through a cryptographically linked series of transactions recorded in a ledger secured via a proof of work consensus mechanism is a fundamental computer science breakthrough. When such digital file is a cryptographic key controlling a scarce resource with a finite supply and mathematically encoded emission schedule (e.g. Bitcoin), that resource can be best classified as a digital commodity, thus in our view the approach taken by the Securities Commission in Malaysia is not appropriate. The question of whether or not a Platform is dealing in digital commodities or securities such as a derivative comes down to a test of delivery (see the answer to Question 1). The CFTC's approach in the United States to the proposed interpretation of the term "actual delivery" is something the Canadian provincial regulators could mirror.

4. *Question 4: What standards should a Platform adopt to mitigate the risks related to safeguarding investors' assets? Please explain and provide examples both for Platforms that have their own custody systems and for Platforms that use thirdparty custodians to safeguard their participants' assets.*

We hope to see the following standards adopted by Platforms or any ecosystem participant involved in the act of doing crypto-asset custody:

- one or more sets of fully segregated wallets are maintained for each participant;
- participant's assets are potentially split multiple digital wallets to prevent very large amounts being controlled by one individual cryptographic key;
- the cryptographic keys controlling the digital wallets should be generated offline and managed offline for the lifetime of the key, on dedicated hardware (e.g. Hardware Security Modules) that have achieved a rating of FIPS 140-2 Level 3 or higher;
- access to the digital wallets by employees should be restricted based on role, following the principle of least-privilege;
- the cryptographic keys should be stored in bank grade vaults that are access controlled, monitored, and guarded 24/7;

- access to the digital wallets should be regulated using a per-wallet encryption scheme and one-time passwords for access to signing transactions;
- transactions should require the coordinated actions of multiple employees of both the participant, as well as multiple employees;
- access to funds as well as other relevant operations should be recorded on immutable, tamper-proof logs residing outside of the organization, and made available to the participant for auditing purposes;
- adequate disaster recovery and succession planning protocols that are tested and meet the business purpose are in place, as evidenced by SOC2 report done by an auditing firm;
- their corporate headquarters should not store or contain crypto-assets of material value;
- employees should pass and be subject to ongoing criminal and credit background checks.

Unfortunately Canada currently lacks a dedicated solution that meets the above criteria, and as such most Platforms are forced to work with foreign custodians (e.g. BitGo, Gemini Custody, Kingdom Trust, Coinbase Custody). Our aim at Balance is to bring such a solution to the Canadian market in the near future.

5. *Question 5: Other than the issuance of Type I and Type II SOC 2 Reports, are there alternative ways in which auditors or other parties can provide assurance to regulators that a Platform ~~has~~ complies to ensure that investors' crypto assets exist and are appropriately segregated and protected, and that transactions with respect to those assets are verifiable?*

Although we would like the case to be otherwise, after spending close to two years building a custody solution, we've come to regard a SOC2 report as a requirement in demonstrating the core competencies needed to provide crypto-asset custodial services. Most approaches we've seen attempted in the space around providing cryptographic proof of funds are either immature or can be easily spoofed.

6. *Question 6: Are there challenges associated with a Platform being structured so as to make actual delivery of crypto assets to a participant's wallet? What are the benefits to participants, of Platforms holding or storing crypto assets on their behalf?*

Actual delivery of crypto-assets is a challenge due primarily to the operational complexity involved in maintaining fully-segregated wallets for each participant. However, we do not see any benefits to participants in Platforms holding crypto-assets on their behalf, rather we regard this as a historical artifact. As the space gained momentum, some of the early solutions and processes had to be unfortunately stretched past their limit and kept in operation to this day. We hope this to change as more infrastructure pieces get built and brought to market, such as dedicated custodian and wallet management platforms.

7. *Question 13: Under which circumstances should an exemption from ~~the report~~ to provide an ISR by the Platform be considered? What services should be included/excluded from the scope of an ISR? Please explain.*

Given the risk and extremely sensitive nature of the business, we believe the custodial aspect of Platforms should be included in the scope of an independent systems review.

8. *Question 14: Is there disclosure specific to trades between a Platform and its participants that Platforms should make to their participants?*

We believe Platforms that act as market makers or trade as principal should publicly disclose it to their participants in their User Agreement or an equivalent document.

9. *Question 16: What type of insurance coverage (e.g. theft wallet, coldwallet) should a Platform be required to obtain? Please explain.*

We would expect Platforms to obtain insurance at least for their hot or warm wallets. Insurance for the assets kept offline in cold wallets is debatable, if the appropriate controls and policies are put in place to protect against external threats, human error, and misuse of insider access, as evidenced by a SOC 2 report.

10. *Question 17: Are there specific difficulties with obtaining insurance coverage? Please explain.*

While there is interest from both Platforms and brokers to put insurance policies in place, most underwriters lack the appropriate models for quantifying risk. As such most Platforms end up insuring just the hot or warm wallets, as insurance for the cold wallets is either impossible or prohibitively expensive to get.

11. *Question 18: Are there alternative measures that address investor protection that could be considered equivalent to insurance coverage?*

While there are other measures that can be put in place to address investor protection and mitigate risk (e.g. split large amounts of cryptoassets across multiple digital wallets controlled together as a logical unit by the participant), they cannot unfortunately be considered equivalent to insurance coverage.

The management team at Balance hopes you found our comments and feedback insightful. We're grateful to be part of the process and have the opportunity to have our views considered, and are available to provide any further clarifications on our comments. Please do not hesitate to contact us.

With respect,

George Bordianu
Co-founder & CEO
PARADISO VENTURES INC. O/A Balance



May 15, 2019

VIA ELECTRONIC EMAIL

British Columbia Securities Commission
Alberta Securities Commission
Financial and Consumer Affairs Authority of Saskatchewan
Manitoba Securities Commission
Ontario Securities Commission
Autorité des marchés financiers
Financial and Consumer Services Commission (New Brunswick)
Superintendent of Securities, Department of Justice and Public Safety, Prince Edward Island
Nova Scotia Securities Commission
Securities Commission of Newfoundland and Labrador
Superintendent of Securities, Northwest Territories
Superintendent of Securities, Yukon
Superintendent of Securities, Nunavut

The Secretary
Ontario Securities Commission
20 Queen Street West
22nd Floor, Box 55
Toronto, Ontario M5H 3S8
Fax: 416-593-2318
comments@osc.gov.on.ca

Me Anne-Marie Beaudoin
Corporate Secretary
Autorité des marchés financiers
800, square Victoria, 22e étage
C.P. 246, tour de la Bourse
Montréal (Québec) H4Z 1G3
Fax : 514-864-6381
Consultation-en-cours@lautorite.qc.ca

IIROC
Victoria Pinnington
Senior Vice President, Market Regulation
Investment Industry Regulatory Organization of Canada
Suite 2000, 121 King Street West
Toronto, Ontario M5H 3T9
vpinnington@iiroc.ca

Re: Proposed Framework for Crypto-Asset Trading Platforms (“the Proposal”)

Aquanow develops technology-enabled liquidity, execution, and market intelligence solutions for businesses that use digital assets for trading or commerce. Aquanow consolidates global

liquidity from major marketplaces and delivers it to investors through a single point of access to provide a better trading experience.

Aquanow is pleased to take this opportunity to provide our comments on the consultation paper (“Consultation Paper”) regarding the Proposal by the Canadian Securities Administrators (“CSA”) and Investment Industry Regulatory Organization of Canada (“IIROC”) to establish a framework that provides regulatory clarity to Platforms, addresses risks to investors (“Investors”) and creates greater market integrity.

We applaud the efforts of CSA and IIROC to establish a regulatory framework in response to the rapid growth of the digital assets in recent years. In light of the recent events with Platforms in both domestic and international markets, it is clear that regulatory oversight is needed to protect Participants, and gain the confidence of retail and institutional investors beyond the early adopters who are currently participating.

3. Are there any global approaches to regulating Platforms that are appropriate to be considered in Canada?

We are advocating for a balanced regulatory approach that gives entrepreneurs both the flexibility and incentive to create innovative solutions while protecting Canadian Investors. Due to the global nature of this new industry, overregulation could potentially create regulatory arbitrage. Also important is regulatory clarity that will give entrepreneurs the confidence to establish and grow businesses in Canada without fear of drastic regulatory changes that could destroy their businesses.

6. Are there challenges associated with a Platform being structured so as to make actual delivery of crypto assets to a participant’s wallet? What are the benefits to participants, if any, of the Platforms holding or storing crypto assets on their behalf?

Due to the nature of onchain digital asset transactions which require a period of time to be validated, Platforms may experience operational challenges facilitating timely execution of trades and delivery of assets. Participants may choose to custody assets with a Platform for convenience purposes, or to reduce latency time to process a trade. Most self-custody solutions require a reasonably high level of technical proficiency to use in their current form, where errors made by the Investor often result in an irreversible loss of their investment which may be another reason why a Participant would choose to store their digital assets on the Platform.

7. What factors should be considered in determining a fair price for crypto assets?

The fair price for digital assets should be based around the same best execution principles that are required in the trading of traditional assets. In order to do so, a Platform must be able to demonstrate that it considers the prices set in the most important global markets and can demonstrate that Investor trades were matched to the best available trade. Regulators should monitor the variance between global average prices and the prices quoted on domestic Platforms and promote Canadian spot prices that are competitive with the global markets. Furthermore, fair price should consider the “all in” cost of a potential trade including deposit/withdrawal and any other processing fees. Currently it could be challenging for Investors

to compare Platforms for the purpose of making an educated decision about where to place their trades.

8. Are there reliable pricing sources that could be used by Platforms to determine a fair price, and for regulators to assess whether Platforms have complied with fair pricing requirements? What factors should be used to determine whether a pricing source is reliable?

Due to the fragmented nature of the digital asset markets, Platforms and regulators must take multiple factors into account in order to determine a fair price. Some assessment considerations include liquidity of a particular venue, jurisdiction and the regulatory oversight that governs a particular venue. Until a best execution standard has been established, we believe the onus is on the Platform to communicate their best execution strategy and provide sufficient data to substantiate best execution based on their own methodology. As the industry matures, we believe the Platforms and regulators will agree on a best execution standard that delivers fair pricing to Canadians.

9. Is it appropriate for Platforms to set rules and monitor trading activities on their own marketplace? If so, under which circumstances should this be permitted?

We believe it is necessary for Platforms to monitor trading in order to identify potentially manipulative or abusive trading activities. However, it is important to establish common practices that will uphold the principles of fair access and prevent conflicts of interest.

10. Which market integrity requirements should apply to trading on Platforms? Please provide specific examples.

We advocate for trade execution surveillance to monitor trading, identify misconduct, and handle disciplinary actions when required. Furthermore, we believe in compliance reviews of Platforms to ensure that proper know-your-client (“KYC”) procedures are being followed to protect the integrity of the ecosystem.

11. Are there best practices or effective surveillance tools for conducting crypto asset market surveillance? Specifically, are there any skills, tools or special regulatory powers needed to effectively conduct surveillance of crypto asset trading?

The most important tool for digital asset surveillance is high quality data, which is unstructured in nature. In order to effectively conduct trading surveillance, regulatory powers need an aggregate view of the highly fragmented market. When this can be achieved, regulators will be able to see when and where Investors are being forced into systematically disadvantaged position.

12. Are there other risks specific to trading of crypto assets that require different forms of surveillance than those used for marketplaces trading traditional securities?

The first risk we identified is wash trading which has become a common practice used on many Platforms in order to inflate unaudited market share. The second risk relates to trading that

happens outside of displayed venues. These trades cannot be easily monitored as they are seldomly reported and it may result in the trades executed at large discounts or premiums of the consolidated market price.

13. Under which circumstances should an exemption from the requirement to provide an ISR by the Platform be appropriate? What services should be included/excluded from the scope of the ISR? Please explain.

This rapidly evolving industry is characterized by new technologies and business models emerging on a regular basis. We believe that the industry will benefit from a simple framework that will put investor protection first while at the same time encouraging entrepreneurs and young companies to continue innovating.

14. Is there disclosure specific to trades between a Platform and its participants that Platforms should make to their participants?

Platform operators should be required to disclose their relationship with the Participants they interact with, whether that be an agency relationship working on behalf of a client, or counterparty. Many Investors are under the impression that the Platform they interact with is an agency when in fact is a counterparty in their trade.

15. Are there particular conflicts of interest that Platforms may not be able to manage appropriately given current business models? If so, how can business models be changed to manage such conflicts appropriately?

The handling of the market making function should be carefully considered. The lack of oversight has created a situation where many Platforms operators are the sole market maker on the Platform, or where the Platform operator is working together with a market maker towards a common goal of Platform profitability with little regard for the fair pricing of client trades. Some Platform operators that advertise themselves as “exchanges” may restrict “outside” market makers from providing liquidity or make it very frictional – we believe transparency is important in these situations.

17. Are there specific difficulties with obtaining insurance coverage? Please explain.

It is currently very difficult to obtain insurance coverage due to lack of availability or willingness from insurance providers.

20. What, if any, significant differences in risks exist between the traditional model of clearing and settlement and the decentralized model? Please explain how these different risks could be mitigated.

Decentralized exchanges present some unique risks that are not present in centralized models. Although counterparty risk is eliminated through the use of a smart contract, there is also no way to know who your trade is being matched to. This presents a difficult situation for Investors

and regulators to manage compliance risks. Gaming risk such as front running is also present on decentralized exchanges, and much more difficult to prevent.

Conclusion

An effective regulatory framework for digital assets should foster innovation while maintaining the integrity of the Canadian markets. Increased competition coupled with fair market access will reduce the influence of bad actors and improve the trading experience for Canadians.

We applaud the Canadian regulators for starting an open dialogue about these issues and thank you for the opportunity to provide our comments on the proposed framework. Please feel free to contact us with any questions or requests for clarification.

Respectively submitted,



Phil Sham

Chief Executive Officer

Aquanow

May 15, 2019

The Secretary Ontario Securities Commission
20 Queen Street West 22nd Floor, Box 55
Toronto, Ontario M5H 3S8
Fax: 416-593-2318
comments@osc.gov.on.ca

Me Anne-Marie
Beaudoin Corporate Secretary Autorité des marchés financiers
800, square Victoria, 22e étage
C.P. 246, tour de la Bourse
Montréal Québec, H4Z 1G3
Fax : 514-864-6381
Consultation-en-cours@lautorite.qc.ca

Victoria Pinnington Senior Vice President,
Market Regulation Investment Industry Regulatory Organization of Canada
Suite 2000, 121 King Street West
Toronto, Ontario M5H 3T9
vpinnington@iiroc.ca

Consultation Paper 21-402: Proposed Framework for Crypto-Asset Trading Platforms

Tritum is extremely supportive of global regulatory efforts to bring clarity, and certainty to digital asset markets. We strongly advocate our domestic market regulators jointly recognizing that this growing segment is replete with extremely new and novel characteristics, and is also evolving at extreme speed.

We would like to highlight that we are most interested in seeing Canada provide a balanced framework of regulations providing sufficient participant protections, orderly market liquidity, transparency and overall market certainty. The digital asset industry is fully global and capable of expediently migrating to jurisdictions which offer the most attractive regulations. As such, we strongly support requirements and standards which are fairly attainable for both traditional and digital-first service providers being capable of meeting in operating their businesses. Canada has a formidable global base of digital ledger talent, and history of lost opportunities to foreign jurisdictions when we could easily be a world leader in embracing the capabilities these innovations enable.

To be clear Tritum is not supportive of efforts of various market stakeholders to obfuscate, deny service to, circumvent, or otherwise cast doubt or uncertainty onto the digital asset industry which has thus far been a chronic issue due to either stakeholder self-interest or general poor comprehension regarding the opportunities to improve financial systems which this technology can enable, be it for securities or non-securities.

Concerning the aforementioned, we wish to emphasize that a new approach to establishing the taxonomy of digital assets, some of which exhibit features not previously contemplated in traditional financial services regulations. On that basis, Tritum also strongly suggests guidance regarding a lexicon amongst the industry to identify and agree upon the treatment of very different categories of instruments, such as digital ledger enabled securities vs. non-national “currency” instruments and the unique considerations or applicability of existing rules for each.

Within the existing cryptocurrency services industry, Tritum agrees with, and supports the CSA and IIROC dissection of the functions performed by many of the service providers in the digital asset industry wherein they offer products or services which closely resemble traditional financial services such as broking and custody, but are vertically integrated into a single provider which may be fraught with conflicts of interest and may have a conflict of interest. We believe it is in the public interest to bring as much transparency into these situations where they exist, and apply controls or prohibitions to such operators to either eliminate the opportunities for conflict of interest or excessive stacked risk.

This includes the separation of the functions of ATS-like order matching from managing proprietary market making desks, and the functions of deposit taking institutions. We are also strong supporters of co-ordinated or consolidated audit trails in order to ensure maximum traceability and certainty for banks processing funds via these institutions and eliminate any reasons for reticence to provide full service banking.

Within the legacy securities industry, we note that the adoption of the novel enablements of digital ledger technology for existing financial services and electronic representations of instruments are manifold, and can be best equated to the de-materialization of paper certificates-based securities to the first iteration of electronic clearing such as CDS and DTCC’s first systems. Those changes were embraced and quickly demonstrated their worth to the markets. With due care and consideration for the systemic risks of changing mission critical infrastructure, the ability to reduce points of friction, settlement time, and rent-seeking intermediation in the middle and back office functions via this technology cannot be ignored. For the sake of Canada’s institutional and private investors.

Given this consultation paper, we focus our final thoughts on the existing cryptocurrency market place and sentiments expressed both by legacy crypto currency incumbents as well as forthcoming clean sheet, regulatory approval-seeking entrants. Tritum believes the single biggest immediate issue which should be addressed by CSA and IIROC will be the management of the transition from an ambiguously regulated environment to a fully regulated one. We seek further information regarding the fair and equal treatment of new entrants who we expect may be initially required to meet a



TRITUM

higher standard of compliance prior to commencement versus legacy providers who may be able to operate continually during a transition period in a non-compliant manner while remediating their operations.

Sincerely,

John Willock

Jim Andriopoulos

CEO, Tritum Inc.

Head of Risk Management, Tritum Inc.

coinsquare

May 15, 2019

SENT BY ELECTRONIC MAIL

British Columbia Securities Commission
 Alberta Securities Commission Financial and Consumer Affairs
 Authority of Saskatchewan
 Manitoba Securities Commission
 Ontario Securities Commission
 Autorité des marchés financiers
 Financial and Consumer Services Commission (New Brunswick)
 Superintendent of Securities, Department of Justice and Public Safety, Prince Edward Island
 Nova Scotia Securities Commission
 Securities Commission of Newfoundland and Labrador
 Superintendent of Securities, Northwest Territories
 Superintendent of Securities, Yukon
 Superintendent of Securities, Nunavut

c/o The Secretary
 Ontario Securities Commission
 20 Queen Street West
 22nd Floor, Box 55
 Toronto, Ontario M5H 3S8
 Fax: 416-593-2318
 Via: comments@osc.gov.on.ca

Me Anne-Marie Beaudoin
 Corporate Secretary
 Autorité des marchés financiers
 800, square Victoria, 22e étage
 C.P. 246, tour de la Bourse
 Montréal (Québec) H4Z 1G3
 Fax : 514-864-6381
 Via: Consultation-encours@lautorite.qc.ca

IIROC
 Victoria Pinnington
 Senior Vice President, Market
 Regulation
 Investment Industry Regulatory
 Organization of Canada
 Suite 2000, 121 King Street W.
 Toronto, Ontario M5H 3T9
 Via: vpinnington@iiroc.ca

Re: Consultation Paper 21-402 *Proposed Framework for Crypto-Asset Trading Platforms*

Coinsquare Capital Markets Ltd. (hereinafter “Coinsquare” or “we”) appreciates the opportunity to submit feedback to the Canadian Securities Administrators and the Investment Industry Regulatory Organization of Canada (the “Regulators”) in connection with Consultation Paper 21-402 *Proposed Framework for Crypto-Asset Trading Platforms* (the “Paper”). We are committed to participating in the establishment of a regulatory compliant environment for crypto-asset trading platforms (“Platforms”) in Canada, and we share the overarching goal of the Regulators to establish a framework that provides regulatory certainty, addresses investor risks and promotes market integrity.

We commend the Regulators for their thoughtful and proactive approach to this matter. Furthermore, we agree in principle with the approach of the Regulators to base the proposed framework on the current framework applicable to dealers and marketplaces in Canada.

1. *When evaluating a token to determine if it is a security, are there factors in addition to those noted above in Part 2 that we should consider?*

We acknowledge that the way in which the trading of a crypto-asset occurs on a Platform will impact the assessment of whether the investor's contractual right to the crypto-asset constitutes a security. To that end, the factors listed in the Paper are instructive.

With respect to the underlying crypto-asset, Coinsquare respectfully submits that the determination of what constitutes an investment contract and thus a security is addressed by the four-pronged test set out in the seminal case of *Pacific Coast Coin Exchange v. Ontario (Securities Commission)*, [1978] 2 S.C.R. 112 ("Pacific Coast"). Specifically, we note that one of the factors in the Pacific Coast test is whether there is an "expectation of profit", and the majority of crypto-asset trading occurring today on Platforms is speculative in nature. An additional factor that should be considered is whether the crypto-asset is widely accepted as a payment method and treated as a currency or is otherwise not a security pursuant to the Pacific Coast test. Circumstances such as a crypto-asset having a distributed development community or utility value should be considered. We expect that this approach will promote regulatory certainty in the market.

2. *What best practices exist for Platforms to mitigate these risks? Are there any other substantial risks which we have not identified?*

To the extent that Platforms enable the trading of crypto-assets where the investor's contractual right to the crypto-asset constitutes a security or where the crypto-asset is in itself a security, they should be subject to the same requirements as existing regulated securities dealers and marketplaces. For every risk noted in the Paper, a dealer/marketplace standard should be applied. Such standards not only serve to promote a level "playing-field" amongst Platform operators and market participants, but they also serve to provide regulatory certainty and protections for existing and new industry participants.

3. *Are there any global approaches to regulating Platforms that would be appropriate to be considered in Canada?*

The global approaches set out in the Paper (as well as in other jurisdictions including Gibraltar and Bermuda) provide helpful guidance for consideration in Canada. However, due to the close alignment between Canadian and U.S. markets, we suggest that the Regulators strongly consider the approach of the U.S. Securities Exchange Commission, whose position is that Platforms that are trading in crypto-assets that are securities ought to register with the Financial Industry Regulatory Authority as a broker-dealer. An overarching focus of the Regulators should be harmonizing the regulations for Platforms across multiple jurisdictions.

4. *What standards should a Platform adopt to mitigate the risks related to safeguarding investors' assets? Please explain and provide examples both for Platforms that have their own custody systems and for Platforms that use third-party custodians to safeguard their participants' assets.*

There is no perfect solution with respect to the custody of crypto-assets and therefore we urge the Regulators to take a balanced and pragmatic approach. We submit that the Regulators should not be too prescriptive, as different custodians have different procedures. Instead, we recommend the Regulators set out minimum standards for custody and as the crypto-asset market evolves, enhance the standards and publish best practices. At present, best practices include holding the majority of crypto-assets in an offline wallet (“cold storage”), requiring multiple signatures to access and move crypto-assets as well as keeping the private key on a computer or hardware device that has never been on the internet and which is physically secured in a vault.

To the extent possible, existing regulation and standards applicable to marketplaces and dealers should govern how a custody arrangement is structured and operated. That said, we agree that allowances must be made to address the unique characteristics of crypto-assets. To this end, Part 14.5.2 of Division 3 of the Companion Policy to National Instrument 31-103 *Registration Requirements, Exemptions and Ongoing Registrant Obligations* is instructive in that it provides that:

“[w]e recognize that in limited cases, it may not be feasible to hold certain asset types at a qualified custodian. For example, bullion requires a custodian that is experienced in providing bullion storage and custodial services, and is familiar with the requirements relating to the physical handling and storage of bullion. Such a custodian may not meet the definition of a qualified custodian. In those cases, we expect a registered firm that would otherwise be subject to subsection 14.5.2(2), (3) or (4)...to exercise due skill, care and diligence in the selection and appointment (where applicable) of the custodian. This can involve the registered firm reviewing the facilities, procedures, records, insurance coverage and creditworthiness of the selected custodian.”

In the view of Coinsquare it makes sense to specify minimum custodial standards to bolster public confidence in crypto-assets. The Regulators should consider establishing robust standards for safekeeping programs. Such programs should include minimum internal control reports, compliance testing, and special capital requirements or insurance to protect crypto-assets (if financially feasible - see our responses to Questions 16 and 17).

While we appreciate that the crypto-asset community may protest such requirements for adding cost and friction to an ideally frictionless blockchain ecosystem, until such time when all fraud and bad behavior can be removed from the industry, leveraging minimum standards and controls should be required.

5. *Other than the issuance of Type I and Type II SOC 2 Reports, are there alternative ways in which auditors or other parties can provide assurance to regulators that a Platform has controls in place to ensure that investors' crypto-assets exist and are appropriately segregated and protected, and that transactions with respect to those assets are verifiable?*

We believe that the issuance of SOC 2 Type I and Type II Reports as an industry standard for assessing operational readiness and controls would be appropriate for initial and ongoing operations. However, exemptive relief will be necessary at the outset because SOC 2 Type II Reports require at least a year of operations and many Platforms and custodians are relatively new to the industry. We strongly believe that ongoing oversight, akin to the oversight provided by a Regulatory Services Provider such as IIROC, is also necessary to ensure a “non-static” approach to compliance and supervisory oversight.

6. *Are there challenges associated with a Platform being structured so as to make actual delivery of crypto-assets to a participant's wallet? What are the benefits to participants, if any, of Platforms holding or storing crypto-assets on their behalf?*

There is no specific challenge associated with the transfer of crypto-assets from a Platform to a third-party wallet. However, “centralized” Platforms and OTC desks (albeit on a short term basis) must custody the crypto-assets or have an intermediary custody the crypto-assets to ensure each participant has sufficient funds to execute on a specific trade. Most, if not all Platforms have the ability to facilitate the actual delivery of crypto-assets to a participant’s wallet relatively quickly after a trade has been executed (however, note that crypto-assets may be temporarily withheld by a Platform in order to comply with anti-money laundering or Know Your Customer laws). The main benefit to participants of storing their crypto-assets on a Platform is that they do not have to manage their own wallet, which would require them to be responsible for storing their own private keys. We believe that the tendency for participants to keep assets on a Platform is rooted in convenience, particularly for frequent traders that are impacted by high confirmation times and mining/transaction fees associated with “on-chain” transactions and for participants who lack the technological savvy.

7. *What factors should be considered in determining a fair price for crypto-assets?*

The determination of what constitutes “fair price” should be based on a comparison of posted transparent prices on regulated marketplaces. This is consistent with the concept of “best price” on “protected marketplaces”.

As is the case with traditional equity markets, “best price” is premised on the available best bid/ask on marketplaces that are subject to the same or similar regulatory oversight.

In today’s crypto-asset market, Platforms, while competing on price, do so in the absence of any obligation to ensure that systems, processes and operations meet minimum regulatory standards and protocols. The lack of regulatory compliant systems used by Platforms creates an uneven playing field insofar as Platforms that have invested in security, systems and oversight are at a competitive disadvantage when pricing against Platforms that have significantly lower overhead and controls.

In the view of Coinsquare, the determination of what constitutes fair (best) price should be premised on an equity market structure construct - meaning that prices should be based on the best available

bid/ask on a regulated marketplace. The pricing available on unregulated Platforms should not be afforded the same protections as those prices quoted on regulated Platforms. Failure to do so is a failure to “price in” factors such as counterparty, operational and compliance risk.

Furthermore, some Platforms operate exclusively as crypto-asset Platforms, without a fiat on or off ramp. Such Platforms do not afford participants the opportunity to “monetize” back to fiat without a secondary trade on a separate Platform that enables fiat conversion (subjecting the participant to additional cost). These crypto-asset Platforms operate as a “crossing network”, and as such, should be limited to “putting up trades” at prices that are equal to or better than those prices determined by protected regulated marketplaces.

8. *Are there reliable pricing sources that could be used by Platforms to determine a fair price, and for regulators to assess whether Platforms have complied with fair pricing requirements? What factors should be used to determine whether a pricing source is reliable?*

Per our response to Question 7 above, reliable pricing sources should be determined exclusively from regulated marketplaces. To the extent that global regulators take differing approaches to the regulation of crypto-assets in their respective jurisdictions, the Regulators should focus on those global markets that afford investors at least the same level of protection and oversight as mandated for Canadian Platforms to arrive at a “consolidated national (global) best bid/offer”.

9. *Is it appropriate for Platforms to set rules and monitor trading activities on their own marketplace? If so, under which circumstances should this be permitted?*

Platforms should be required to monitor trading activities on their markets. Specifically, Platforms should be obligated to have policies, procedures and controls in place to identify and prevent manipulative and deceptive methods of trading and comply with all applicable marketplace requirements as set out in the Universal Market Integrity Rules (“UMIR”). To ensure that such monitoring is conducted in a robust manner, Platforms should be required to engage a regulation services provider (such as IIROC) to conduct market surveillance.

10. *Which market integrity requirements should apply to trading on Platforms? Please provide specific examples.*

Per our response directly above, it is the view of Coinsquare that Platforms should be held to the same standards of traditional equity marketplaces, where applicable. Allowances should be made for specific nuanced elements of Platforms (i.e. some Platforms may operate outside of traditional market hours or even on a continuous 24 hour cycle), however it is our view that compliance with at least the following provisions of UMIR should be required:

- Part 2 - Abusive Trading
- Part 3 - Short Selling
- Part 4 - Frontrunning
- Part 5 - Best Execution

- Part 6 - Order Entry and Exposure
- Part 7 - Trading in a Marketplace
- Part 8 - Client-Principal Trading

11. *Are there best practices or effective surveillance tools for conducting crypto-asset market surveillance? Specifically, are there any skills, tools or special regulatory powers needed to effectively conduct surveillance of crypto-asset trading?*

See our response to Question 9 above. Presently a number of widely-used equity marketplace surveillance providers have customized crypto-asset surveillance tools (i.e. Nasdaq SMARTS).

12. *Are there other risks specific to trading of crypto-assets that require different forms of surveillance than those used for marketplaces trading traditional securities?*

The majority of surveillance systems in use today by traditional equity marketplaces contain most of the core surveillance alerts applicable to Platforms, with slight nuances to account for the fact that most Platforms operate on a 24 hour basis. As noted in our response to Question 11 above, surveillance vendors such as Nasdaq SMARTS have already leveraged existing protocols to account for these differences.

13. *Under which circumstances should an exemption from the requirement to provide an ISR by the Platform be considered? What services should be included/excluded from the scope of an ISR? Please explain.*

It is our view that all Platforms be required to conduct and complete a full-scale ISR with any exceptions being very narrow in scope (i.e. to accommodate for the fact that many Platforms are new and have not yet been able to complete a full-scale ISR). The majority of Platforms in existence today are “home-grown”, and built on proprietary systems which may be functionally incomplete such that the safety of crypto-assets cannot be guaranteed. These proprietary systems have generally not been fully tested by an independent third-party under crypto-asset market conditions, such as periods of high growth or volatility.

For those Platforms that leverage well established third-party systems (i.e. cloud-based infrastructure, trade matching engines and surveillance tools developed by traditional equity market providers), increased reliance on third-party attestations and testing should be afforded.

14. *Is there disclosure specific to trades between a Platform and its participants that Platforms should make to their participants?*

Investors should be afforded the same level of disclosure currently required of marketplaces and dealers in Canada.

15. *Are there particular conflicts of interest that Platforms may not be able to manage appropriately given current business models? If so, how can business models be changed to manage such conflicts appropriately?*

Platforms should model their operations and corporate structures in a manner that is similar to traditional marketplaces and dealers. At present, the vast majority of Platforms are structured in a manner such that they both accept/manage and execute a client order in a “single platform” structure. This form of organization creates a myriad of potential conflicts that require significant internal measures.

To this end, it is our view that Platforms should bifurcate their role as a dealer and marketplace. Specifically, Platforms should operate as an IIROC dealer with respect to the acceptance and handling of client orders for crypto-assets but the matching of such orders should be conducted on a regulated marketplace.

This arrangement is commonplace in the traditional equity market structure, with a number of dealers operating a proprietary marketplace. As a dealer, a Platform would be required to consider (better) prices on other regulated marketplaces prior to routing orders to its own marketplace.

16. *What type of insurance coverage (e.g. theft, hot-wallet, cold-wallet) should a Platform be required to obtain? Please explain.*

We believe that the type of insurance coverage a Platform should be required to obtain should be no greater than the type of insurance coverage currently required for traditional IIROC broker dealers. This type of coverage would cover, among other things, insolvency, any loss through dishonest or fraudulent acts of employees, etc. We however note that reduced insurance coverage should be appropriate with respect to crypto-assets held in “cold storage”, and a “reserve model” where assets are held as a percentage of client liabilities should be required for crypto-assets held in a “hot wallet”. Insurance in other industries (such as banking) does not provide full coverage for participants. We believe that the issuance of SOC 2 Type I and Type II Reports to a custodian provides Regulators the assurance that clients’ assets are sufficiently protected without the need for insurance.

17. *Are there specific difficulties with obtaining insurance coverage? Please explain.*

With the current state of the insurance market, it is extremely difficult and expensive for Platforms to obtain any type of insurance (“hot wallet”, “cold storage”, theft insurance or otherwise). Very few insurance providers are willing to insure crypto-asset Platforms, and those that are willing to insure place high premiums that “price-out” many Platforms from purchasing insurance. While we support the Regulators’ approach, we believe the Regulators should take a further look at the insurance market prior to mandating any type of insurance.

18. *Are there alternative measures that address investor protection that could be considered equivalent to insurance coverage?*

By requiring Platforms to register as an IIROC dealer, they would presumably fall under the mandate of the Canadian Investor Protection Fund.

19. *Are there other models of clearing and settling crypto-assets that are traded on Platforms? What risks are introduced as a result of these models?*

At present there is no centralized clearinghouse for crypto-assets. While blockchains are uniquely well suited given their ability to record transactions in an immutable manner, blockchains are not, at present, well suited to the management and reconciliation of bi-lateral transactions by discrete parties. This invariably leads to the need for transacting parties to have assurances and recourse in the event of contra-side failure to deliver/settle. In traditional equity markets, the process of clearing/settlement and custody are closely intermingled concepts - such is not the case with crypto-assets.

In respect of crypto-assets, custody, and the movement between hot- and cold-wallets is the critical point of differentiation from traditional clearing and settlement. In the absence of a centralized clearinghouse, the ability to rely on a counterparty's credit, financial viability, and regulatory status (read as integrity) takes on increased prominence.

While Coinsquare is a vocal advocate for Platforms to generally be subject to the same regulatory requirements applicable to traditional dealers and marketplaces as it relates to trading and oversight, owing to the nature of how crypto-assets are transferred and "stored", traditional market structure is not instructive.

In light of the above, we are of the view that the manner in which clearing/settlement and custody is conducted in the crypto-asset space requires a fundamental paradigm shift. We agree with the Regulators that an exemption from the requirement to report and settle trades through a clearing agency should be considered. We submit that Platforms be regulated as dealers and marketplaces with centralized custody provided by third-party entities. By limiting direct participants to regulated dealers and marketplaces, participants have the ability to manage and account for net flows of crypto-assets through a "closed loop ledger" while concurrently limiting the unnecessary movement of crypto-assets in and out of custody. As the Paper notes, Platforms acting as IIROC dealers will also be required to have policies, procedures and controls in place to address the risks of settling transactions on an internal ledger. Lastly, since participants have the ability to withdraw crypto-assets to their own wallets, where such transaction would immediately be posted on a public ledger, the need for a clearing house is less prevalent.

20. *What, if any, significant differences in risks exist between the traditional model of clearing and settlement and the decentralized model? Please explain how these different risks may be mitigated.*

See our response to Question 19 above.

21. *What other risks are associated with clearing and settlement models that are not identified here?*

See our response to Question 19 above.

22. *What regulatory requirements, both at the CSA and IIROC level, should apply to Platforms or should be modified for Platforms? Please provide specific examples and the rationale.*

See our response to Question 19 above.

Dear CSA Members,

Re: CSA's Proposed Framework for Crypto-Asset Trading Platforms

Thank you for the opportunity to submit our feedback on the Proposed Framework for Crypto-Asset Trading Platforms. We recognize that a new and innovative industry involving an unregulated asset class that does not fit neatly into a pre-existing asset definition is challenging for regulators committed to protecting consumers. The ongoing unwinding of QuadrigaCX, leaving thousands of consumers unsure about the status of their holdings, underscores the need to set a bare minimum of standards for Platforms that wish to provide crypto asset trading and custody services to the public.

While most existing crypto assets are not securities, the Platforms themselves operate in a similar fashion to securities exchanges and many of the same best practices that apply to securities brokers and exchanges may indeed be applicable to crypto exchange Platforms. Indeed, the industry has attracted the interest of securities professionals whose skill set transfers well to crypto asset trading.

Nevertheless, it's important to slow-walk the process of applying regulations to an innovative industry with a global presence so as not to invite regulatory arbitrage, where service providers such as trading Platforms and token issuers do business everywhere but Canada, leaving law-abiding Canadian consumers and businesses out of participating in a nascent industry, and giving extrajurisdictional scofflaws an advantage.

Arguably, fraud remains an issue in the regulated securities industry, despite the existence of applicable regulations. Therefore, these regulations should be judged by their overall effect, and not hastily applied.

Attached is our feedback to the proposed framework. We hope you find it helpful. If you have any follow up questions regarding our feedback, we are happy to help.

Sincerely,

The Ludo Group
Adrian Sischin, Lara Wojahn, Cloudesley Hobbs, Jason Dearborn

1. Are there factors in addition to those noted in Part 2 that we should consider?

Yes

The origins of a digital asset would be a risk factor if the digital asset is originating in Canada, for example, as opposed to originating outside the jurisdiction. Disclosing the origin of digital assets helps investors assess risk.

The outcome should be a request to legislators - overtly asking for clarification. Failure to do this will inevitably result in courts determining the status. If these instruments are securities it could be argued that Security Panels may be the best arbitrators for disputes. Failing to have the clarity from the legislation will result in the courts making the decisions without the investigatory processes, such as this current exercise, resulting in a patchwork of pan-Canadian decisions which would seemingly be binding. The Parliament of Canada began investigating these matters in 2014. The process of regulators and self regulatory agencies reacting in 2019 is demonstrative that elements will move too quickly and courts will have matters before them upon which must make binding decisions.

Secondly, the design of current platforms in the industry matches actual properties with the cryptocurrencies or tokens being digitally present on the platforms. This is akin to a farmer's market where the actual produce is present. These exchanges or brokerages are not representing assets, which could clearly be representative of a security, but rather the property itself. The following paragraph warns that "securities legislation may apply" however no list of what is a security or not is provided. This approach is at odds with the direct intent of Consumer Protection legislation. The ambiguity cannot be explained but rather is being presented by design. This has born results of being harmful to Canadians - the Quadriga receivership affecting 115,000 creditors being the most salient example.

Produce a list of what are deemed to be securities to prevent the abrogation of the responsibilities of the security regulators. If properties exist outside the list report it to the proper legislative body so the Canadian's elected representatives may address the matter.

2. What best practices exist for Platforms to mitigate the risks outlined in Part 3? Are there any other significant risks which we have not identified?

FAQ section on websites, complete disclosure documents available for download that address any conflict or confluence of interests.

All fees should be disclosed conspicuously.

The rules of the Platform should be disclosed conspicuously, including timing and trading limits.

Market manipulation is addressed through third party analysis (Blockchain Transparency Institute) already performed and available to the public - these reports should be disseminated and referred to on the Platform's website. Platforms that allow trading should be required to belong to an SRO that uses member fees to monitor trading and report on manipulation. See: <https://finance.yahoo.com/news/blockchain-transparency-institute-launches-self-210030112.htm>

!

SROs should be set up to set standards for pricing and disclosure, such as determining the information provided to customers in quarterly account statements.

Recordkeeping requirements should apply across Platforms and they should be required to have secure systems and backups. Records must be kept for a certain period of time, such as 6 years.

Capitalization requirements should only be imposed on business models where the customers' assets are held in omnibus or commingled accounts. Where customers' assets are segregated and not used by the Platform for use in its operations, no capitalization requirements should apply.

All Platforms should be required to send written account statements to customers at least quarterly. The information in these statements should be standardized and all fees paid to the Platform should be disclosed in plain english.

New categories of qualified investors is needed for crypto assets to encourage safe adoption of new technology. Canada has an opportunity to drive adoption by setting new definition of

qualified crypto investors that are in line with the spirit and ideals of democratizing investments in projects. For example - projects where investments are less than \$10k could be accepted based on the investment size from triggering qualified investor status. There are currently global projects that carve out Canadian participation, while European participation is allowed, due to the more liberal approach to qualified investor definitions in the European Union.

One oversight in the list is the lack of fork protocols and ownership rights. A fork in a blockchain occurs when a copy of the blockchain is released with minor changes in code but where the contents of the parent blockchain wallets coins are recorded in the new fork. The previous private keys which activated the wallets from the parent blockchain wallet will work in the new forked wallet. This potentially allows for an equivalent number of new forked coins to be claimed by the former wallet holder.

If wallets on exchanges are parts of accounts and the property of the Platform, the Platform has control and the rights of the new fork coins, unless it publishes a policy to the contrary. Therefore, each Platform should have a fork policy outlined in the user agreement.

3. Are there any global approaches to regulating Platforms that are appropriate to be considered in Canada?

See Estonia as one of the leaders in adopting regulations.

<https://www.cointelligence.com/content/estonia-cryptocurrency-trading-licensing/>

4. What standards should a Platform adopt to mitigate the risks related to safeguarding investors' assets? Please explain and provide examples both for Platforms that have their own custody systems and for Platforms that use third-party custodians to safeguard their participants' assets.

As regards the veracity of custody, the National Institute of Standards and Technology in the USA has standards for generating public and private cryptographic keys - NIST Special

Publication 800-133 Recommendation for Cryptographic Key Generation - to which a custodian's key generation process could be compared.

5. Other than issuance of Type I and Type II SOC 2 Reports, are there alternative ways in which auditors or other parties can provide assurance to regulators that a Platform has controls in place to ensure that investors' crypto-assets exist and are appropriately segregated and protected, and that transactions with respect to those assets are verifiable?

Establishment of an SRO that has a division to specifically deal with this issue that is unique to the virtual currency industry is the best approach as traditional approaches are not suitable. Furthermore, the established finance industry is dominated by large, well-capitalized companies and discourage competing startups without large capital backing, generally out of Silicon Valley, known for anticompetitive practices.

Canada is a smaller market and entrants to the space generally do not have large war chests to develop the sorts of systems that can satisfy Type I and II SOC 2 reports.

6. Are there challenges associated with a Platform being structured so as to make actual delivery of crypto assets to a participant's wallet? What are the benefits to participants, if any, of the Platforms holding or storing crypto assets on their behalf?

The benefits for participants when Platforms hold or store crypto assets on their behalf is they are accessing a fully automated private key storage system that is not subject to human error, which has caused assets to be locked away forever. Nevertheless, these Platforms should be able to demonstrate infallible systems for generating and safeguarding private keys.

7. What factors should be considered in determining a fair price for crypto assets?

It will entirely depend on the type of coin or token. A token that is backed by an asset, such as gold or a sovereign currency, should be priced in accordance with that asset, and the liquidity of the token. Establishment of market makers go a long way to set price discovery.

A pure convertible cryptocurrency will have price discovery using authentic transactions between arm's length buyers and sellers. Given its global presence, the price of an established cryptocurrency such as bitcoin is easily determined. Using an average of listings on various trusted exchanges at a certain time is the best way to determine price. Arbitrage between Platforms both within a jurisdiction and globally has been reduced to single points due to the efficiency of the bitcoin market.

On the other hand, a newly issued coin may be subject to pump and dump schemes, similar to newly issued shares. New coin or token issues - particularly those that are not backed by a tangible asset - could be accompanied by notices that the value is not determinable and that they are purely speculative investments.

8. Are there reliable pricing sources that could be used by Platforms to determine a fair price, and for regulators to assess whether Platforms have complied with fair pricing requirements? What factors should be used to determine whether a pricing source is reliable?

As in any fair market, the price of an asset will not be set by a Platform, but by the supply and demand of the asset. The price is what an informed buyer is willing to pay, and what a seller is willing to take. As with some securities, there may not be liquidity if there is too much of a spread between the "bid and ask". Market transparency as shown on Platforms or other tools that demonstrate bona fide transactions between arm's length market participants is the best way to determine reliable pricing.

As the security token market matures, we will see pricing of the tokens determined in the same way securities are priced - vis a vis the underlying asset, venture or commodity.

9. Is it appropriate for Platforms to set rules and monitor trading activities on their own marketplace? If so, under which circumstances should this be permitted?

Platforms are already required to conduct customer identification procedures to ensure the identity of its participants and to continually check its customer list against OFAC SDN lists and other lists. This is not yet required by FINTRAC, but by banks with which the Platforms must

have accounts in order to process payments. Banks also require Platforms to have transaction monitoring in place to detect suspicious transactions.

In the event a Platform is listing centralized coins or security tokens with identifiable insiders, it makes sense for the Platform to prohibit insiders from trading tokens over which the insider has control and access to nonpublic material information.

Rules should be agreed upon by all Platforms, preferably via an SRO and applied across all participants. There should be well-reasoned rationale for each rule and the rule should be monitored for its efficacy and compliance and revisited regularly. Platforms, for example, could set rules limiting the value of a trade if it is determined to not be in the trader's or public interest. Requiring confirmation before executing a trade, similar to that which exists on online discount securities trading platforms, should be standard.

10. Which market integrity requirements should apply to trading on Platforms? Please provide specific examples.

Different tokens types will require different market integrity requirements.

Tokens that are traded globally, with no central control, do not require much market integrity and, if restrictions were applied, Canadian traders would be unfairly impacted compared to those in other jurisdictions.

Tokens that act more like securities will require market integrity rules that apply to trading securities.

Trading for all assets should be transparent across all Platforms and across all jurisdictions.

11. Are there best practices or effective surveillance tools for conducting crypto asset market surveillance? Specifically, are there any skills, tools or special regulatory powers needed to effectively conduct surveillance of crypto asset trading?

Digital asset market surveillance can be performed using many of the same tools used for securities exchanges. They also have the benefit of the blockchains, which is a publicly

available database showing transactions, which can be paired by date and amount to specific trades.

Specialized blockchain analysis organizations such as Elliptic or Chainalysis do blockchain analysis that can trace transactions. This would be useful for forensics and auditing in the event of suspected market manipulation or money laundering.

Established Platforms that operate in the US market employ 3rd party market surveillance service providers that provide real-time and forensic surveillance.

Ideally, all Platforms that execute trades would share surveillance data - both within Canada and extra-jurisdictionally - to detect and deter manipulation and other fraudulent behavior.

12. Are there other risks specific to trading of crypto assets that require different forms of surveillance than those used for marketplaces trading traditional securities?

There are fewer risks associated with crypto assets because it solves the double-spending problem.

13. Under which circumstances should an exemption from the requirement to provide an ISR by the Platform be appropriate? What services should be included/excluded from the scope of the ISR? Please explain.

ISRs can be prohibitively expensive for small companies and their requirements can be overly onerous and inapplicable. It is recommended that the ISR model be flexible and dependent on the level of complexity and risk of the Platform business model.

14. Is there disclosure specific to trades between a Platform and its participants that Platforms should make to their participants?

Trade details can be disclosed such as whether a Platform is trading as an agent or principal. The time of the trade and price should be disclosed.

15. Are there particular conflicts of interest that Platforms may not be able to manage appropriately given current business models? If so, how can business models be changed to manage such conflicts appropriately?

When Platforms trade as a dealer on their own account, this is an important service to create and contribute to liquidity in the marketplace, similar to the role of market makers in traditional securities markets. This is not necessarily a conflict of interest, as long as this role is disclosed and the price paid is transparent, fair and equitable.

16. What type of insurance coverage (e.g. theft, hot-wallet, cold-wallet) should a Platform be required to obtain? Please explain.

Certain platforms do not maintain client hot wallets. In such case insurance should not be required. A more important part is disclosure of risks associated with different types of wallets. Transparency and education are important.

17. Are there specific difficulties with obtaining insurance coverage? Please explain.

Yes but is expected that global adoption and competition will make this easier as time goes by. From an entrepreneurial perspective, the insurance may not be effective as this could be provided with many limitations that could make this economically not feasible, and in reality it could be used for marketing purposes and have a counter - productive effect for clients / investors. Example: very few companies have currently such insurance. The premiums are high. Having insurance does not lead to certainty of providing protection to clients. Insurance scarcity may be looked by platforms at this time as a marketing differentiator as a primary objective

18. Are there alternative measures that address investor protection that could be considered that are equivalent to insurance coverage?

Alternative measure: A recent solution from Austria is a card with enhanced security features, card produced by a government body Austrian State Printing House. In Canada such a card could be printed by the Canadian Mint.

Here is the actual wallet: <https://www.cardwallet.com/en/home/>

The investor protection is achieved by providing the investor the actual card loaded with digital assets - and the investor is the only one who can store and access the assets. Also private key generation is done by a reputable organization / government body - i.e. Royal Canadian Mint.

19. Are there other models of clearing and settling crypto assets that are traded on Platforms? What risks are introduced as a result of these models?

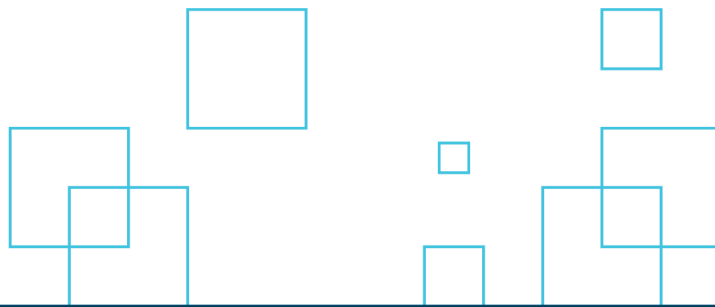
Yes - real time brokerage where client is virtually placing an order - similar with making purchases on e-commerce websites. There is a risk on the broker side that needs to absorb volatility of a quoted asset for which the client has not send funds after the order was placed. This translates into higher prices vs. sending the money in advance, but offers a much higher protection for clients.

20. What, if any, significant differences in risks exist between the traditional model of clearing and settlement and the decentralized model? Please explain how these different risks could be mitigated.

Complete decentralization may not provide sufficient KYC / AML protection and has not evolved to the point that provides a frictionless AML controls. The concern would be higher in the area of money laundering rather than settlement. Additional concerns are around custody.

21. What other risks could be associated with clearing and settlement models that are not identified here?

Identity and security are key elements that require ongoing improvements. If either is compromised, this leads to vulnerabilities and increased risk with criminals continuing to exploit virtual currencies to support illegal activities.



The Secretary
Ontario Securities Commission
20 Queen Street West
22nd Floor, Box 55
Toronto, Ontario M5H 3S8 Fax: 416-593-2318
comments@osc.gov.on.ca

Me Anne-Marie Beaudoin
Corporate Secretary
Autorité des marchés financiers
800, square Victoria, 22e étage
C.P. 246, tour de la Bourse
Montréal (Québec) H4Z 1G3
Fax : 514-864-6381
Consultation-en-cours@lautorite.qc.ca

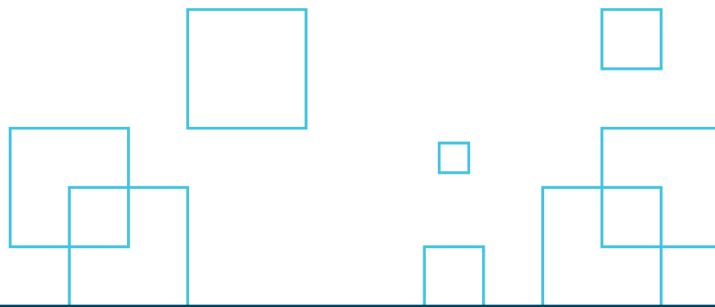
IIROC
Victoria Pinnington
Senior Vice President, Market Regulation
Investment Industry Regulatory Organization of Canada
Suite 2000, 121 King Street West
Toronto, Ontario M5H 3T9
vpinnington@iroc.ca

May 15, 2019

Dear Madams and Sirs:

**Re: Joint Canadian Securities Administrators/Investment Industry Regulatory
Organization of Canada - Consultation Paper 21-402 - Proposed Framework for
Crypto-Asset Trading Platforms**

We would like to thank the Joint Canadian Securities Administrators (CSA) and the Investment Industry Regulatory Organization of Canada (IIROC) for preparing the Proposed Framework



for Crypto-Asset Trading Platforms¹ and for inviting industry stakeholders to participate in this important consultation.

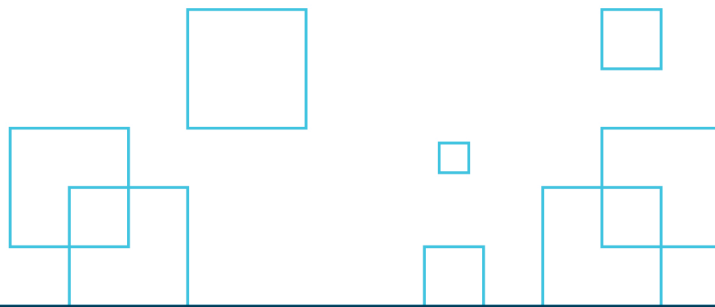
The Chamber of Digital Commerce Canada (the “Chamber”) provides dedicated support for Canada’s emerging and rapidly growing blockchain ecosystem. Today, the Chamber represents some of the most significant companies operating in the blockchain and digital asset industry in Canada. Our mission is to promote the acceptance and use of digital assets and blockchain-based technologies.

As an initiative of the Chamber of Digital Commerce, the largest global trade association representing over 200 companies working in the digital asset and blockchain industry, we are able to provide unprecedented global coordination to support the growth of Canada’s blockchain community. Through education, advocacy, and working closely with policy makers, regulatory agencies, and industry, we are helping to develop an environment that fosters blockchain and digital asset innovation, jobs, and investment across Canada. As such, the Chamber and its members have a significant expertise and interest in ensuring that Canada can support the blockchain ecosystem so that it continues to grow and thrive.

Indeed, the transformative potential of blockchain, digital asset, and distributed ledger technologies (“DLT”) presents tremendous cross-sectoral and economic advancement opportunities that have been recognized globally by government and industry alike. Fundamentally, the technology reshapes the ownership of assets, how we interact with each other digitally, and how we transfer value. As a result, the ways in which companies in all sectors conduct business - from financial services, digital identity and privacy, healthcare, insurance, intellectual property, real estate, commerce, and supply chain management, among others - are being rapidly transformed and establishing a new Internet infrastructure dedicated to the digital exchange of value.²

¹ Canadian Securities Administrators, Joint Canadian Securities Administrators/Investment Industry Regulatory Organization of Canada Consultation Paper 21-402 Proposed Framework for Crypto-Asset Trading Platforms, https://www.osc.gov.on.ca/documents/en/Securities-Category2/csa_20190314_21-402_crypto-asset-trading-platforms.pdf.

² Deloitte, The Internet of Value-Exchange, <https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/Innovation/deloitte-uk-internet-of-value-exchange.pdf>.

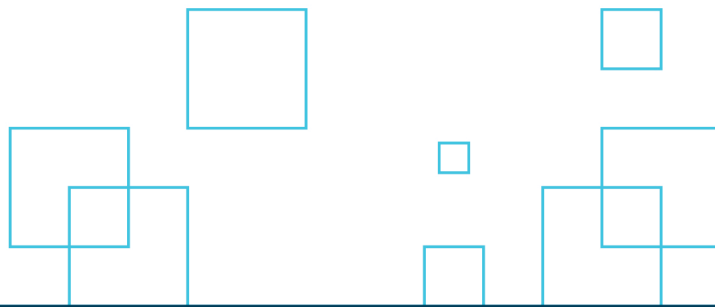


This shift, as Canadian regulators know, is causing significant challenges for current regulatory and policy frameworks. While there are aspects of the digital asset and DLT landscape that might fit under existing law, policy, and regulation, it remains the case that the broader systemic shift and innovation that is occurring, and in particular with regard to “crypto-asset trading platforms,” demands holistic study and review with industry experts at the table. In reviewing the existing legal and regulatory framework, policymakers must be cognizant of the innovative aspects of this technology which transcend existing regulatory frameworks applicable to financial services, securities and commodities and carefully evaluate the extent to which it is appropriate to base new policy responses on traditional models, such as the Proposed Platform Framework.

The Chamber, its members, and industry allies - including financial services companies, technology companies, law firms, multinational consulting firms, crypto-exchanges, startups, academics, and other industry stakeholders - have prepared the following response to the Consultation. We suggest ongoing and collaborative dialogue as we carefully work with Canadian regulators to establish a path forward that is in the best interest of Canadian digital asset investors, innovators, and the general public who stand to benefit from participation in this rapidly growing global crypto-asset market.

Regulators must be cognizant of the potential unintended consequences that could result from over-reaching terminology and interpretation. Such consequences could be harmful not only to industry by creating confusion and red tape while stifling innovation and driving business out of Canada, but also to regulators by creating an unworkably broad mandate, or a mandate that directly conflicts with other Canadian legislation (such as the anti-money laundering regulation expected later this year). Consumer and commercial interests alike suffer where there is a misalignment of incentives and a lack of education. Such pitfalls can best be avoided through ongoing dialogue, which may take the form of a task force of experts to work with government policy makers and regulators to fully study and review each distinct aspect of “crypto-exchange” platforms and the broader global token regulatory framework and objectives. Where appropriate guidance is established, it should be published in a timely and transparent manner, that is coordinated with other policymakers, legislation, and guidance.

For the purposes of this Consultation reply, the Chamber has prepared general comments that should be considered throughout. Further, we are grouped questions together and provided detailed replies under each of the heading in the Consultation Paper. Finally, we have highlighted some specific challenges that deserve further consideration and have provided the following recommendations:

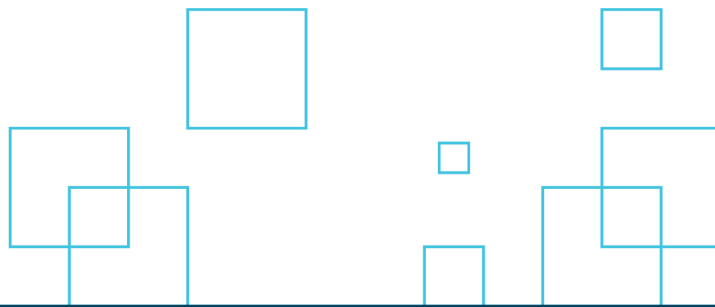


1. Recognize that not all digital assets are securities and avoid broad characterization of tokens as securities by starting with the assumption that a token or digital asset may not be a security, commodity or derivative.
2. Establish meaningful industry dialogue, input, and collaborative consultations to create effective and appropriate regulatory regimes for the global, digital marketplace.
3. Establish a task force of experts to work with federal and provincial government policy makers and regulators to fully study and review each distinct aspect of “crypto-exchange” platforms and the broader global token regulatory framework and objectives.
4. Develop objective investor and consumer education tools to help inform the public.
5. Take the time necessary to research and review the global blockchain ecosystem, considering all policy and legislative perspectives, to design and support a competitive blockchain ecosystem in Canada.
6. Coordinate with other policy makers and regulators, including the Department of Finance, FINTRAC, and the Canada Revenue Agency (CRA), to ensure that regulations are aligned, consistent, and not confusing or overly burdensome to industry.
7. Publish timely and transparent guidance, including guidance related to digital assets that are not considered to be securities, commodities, or derivatives.
8. Take a principles-based, technologically-neutral approach to regulation and policy to foster innovation.

The Chamber and its members look forward to ongoing and regular discussions with the CSA, IIROC, and the appropriate provincial and federal policy makers and regulators.

General Consultation Comments

As a matter of general comment, the Chamber offers the following feedback in an effort to assist regulators and policy makers as they move through the work ahead in relation to digital asset trading platforms (hereafter “digital asset trading platforms”).



1. Not All Digital Assets Are Securities

At its heart, blockchain is a database technology. As with any database technology, it can be used to create and track digital representations of assets (including natively digital goods). The financial services applications of blockchain include value transfer and the creation of digital tokens³ that may be used to represent traditional securities and other traditional financial instruments. It would be too limiting, however, to only consider these applications of the technology. Any consideration of digital assets, DLT, and blockchain technology must recognize the broad array of uses for tokens as well as assets that can be digitized and transacted in on blockchains. Simply creating a digital representation of an asset does not change the asset's character or nature, nor should it change the asset's treatment under law. The Consultation assumes, in some respects, that all participants in this ecosystem are "investors". They are not, nor will they be, as the ecosystem evolves beyond its current applications. While many holders of digital assets do so for investment or speculative reasons, many also hold digital assets for their utility value. These types of holders are expected to increase in number as the blockchain ecosystem evolves beyond its current applications.

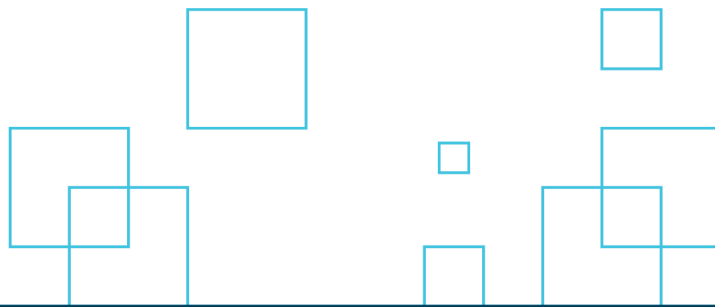
2. Establish Meaningful Industry Dialogue, Input, and Collaborative Consultations to Create Effective and Appropriate Regulatory Regimes

Canada and Canadians have pioneered some of the most widely used and exciting digital asset projects to date, including Ethereum,⁴ a platform on which many other digital assets have been built. As early as 2014, the Canadian government was conducting in-depth analysis of emerging digital asset classes. In their 2015 report,⁵ the Standing Senate Committee on Banking, Trade and Commerce recommended that "The federal government, in considering any legislation, regulation and policies, create an environment that fosters innovation for digital currencies and their associated technologies. As such, the government

³ Digital tokens are transferable units generated within a distributed network that tracks ownership of the units through the application of blockchain technology. Chamber of Digital Commerce, Understanding Digital Tokens: Market Overviews and Proposed Guidelines for Policymakers and Practitioners, <https://digitalchamber.org/token-alliance-whitepaper/>.

⁴ Founder Vitalik Buterin and many early team members are Canadian. Much of the early work took place in Canada, however, the project's foundation is now headquartered in Switzerland. Ethereum, <https://www.ethereum.org/>.

⁵ Senate Canada, Digital Currency: You Can't Flip This Coin! Report of the Standing Senate Committee on Banking, Trade, and Commerce, <https://sencanada.ca/content/sen/Committee/412/banc/rep/rep12jun15-e.pdf>.



should exercise a regulatory “light touch” that minimizes actions that might stifle the development of these new technologies.” In addition, the Canadian federal government⁶ and many provincial governments⁷ have taken up the call to “reduce red tape.” The key to success of such initiatives is industry consultation to assist with the evaluation of the effectiveness and potential impact of regulation in advance of its drafting and implementation.

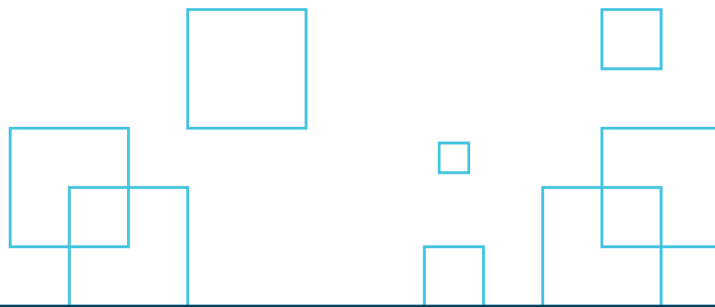
As with all transformative technological innovation, it can be difficult to determine what aspects of the innovation to promote as well as the appropriate regulatory scope, fit, and strategy. Global courts, regulators and policy makers are actively considering a variety of ways to approach digital assets and digital asset exchanges. Striking an appropriate balance between protecting consumers and investors on the one hand, while allowing them access to new and highly innovative emerging markets on the other hand, is difficult. The risk related to an error in regulatory judgement is also high - overregulation will stifle or displace digital asset innovators and investors in Canada, and ineffective regulation and regulation with unintended harmful consequences for industry innovators and investors will also do the same.

To appropriately support and regulate digital asset innovation, it is critical that policy makers and regulators understand digital asset technology and the various iterations of these technologies in an expert capacity. Achieving such an understanding will take time and will require regulators and policy makers to establish transparent, meaningful, multi-stakeholder working groups and collaborative dialogue to ensure that they are informed and working in a proactive manner to support both the growth of this highly valuable innovative sector, and to help guide the sector to embed best practices and standards into everyday operations. Meaningful consultation with industry players must occur on an ongoing basis, and not only as “point in time” or procedural exercises.⁸

⁶ Treasury Board of Canada Secretariat, Forward Regulatory Plan: 2019 to 2021: amending the Red Tape Reduction Regulation, <https://www.canada.ca/en/treasury-board-secretariat/corporate/transparency/acts-regulations/forward-regulatory-plan/forward-regulatory-plan-2019-2021/amending-red-tape-reduction-regulations.html>.

⁷ Ontario Government, Red Tape Challenge, <https://www.ontario.ca/page/red-tape-challenge>.

⁸ For example, the Office of the Privacy Commissioner (OPC) has been widely recognized for their success engaging industry, setting early standards and balanced regulation. The Canadian approach to data and privacy law was foundationally established with businesses at the table. More recent revisions to privacy laws and regulations in Canada are showing the long-term benefit of such a committed and engaged process, as awareness for privacy best practices is reasonably widespread across sectors, and there continues to be ongoing and meaningful dialogue with industry and Canadians. Heavy-handed, prescriptive regulation was not implemented at the outset of big data technology innovation, but rather, a relationship and respectful dialogue



The Chamber respectfully submits that the most effective regulatory results will be achieved through ongoing supportive and collaborative dialogue, rather than through a process that attempts to overlay or extend rules designed for incumbent, paper-based systems onto new systems born in the digital age. We strongly encourage provincial policy makers, the CSA, IIROC and its members to establish regular dialogue with industry, working groups, and a collaborative study of core questions, concerns and interests of all stakeholders in the digital-asset, and more broadly blockchain, technology industries to ensure the right regulatory balance is struck.

3. Investor and Consumer Education is Needed

Investor, consumer, and public education in relation to innovative new technologies and platforms, including digital-asset trading platforms, is needed, regardless of which stakeholder group is being considered in this process. By working with industry to gain a deeper understanding of emerging platforms, policy makers and regulators will be able to better support and provide principles-based public and consumer education tools.

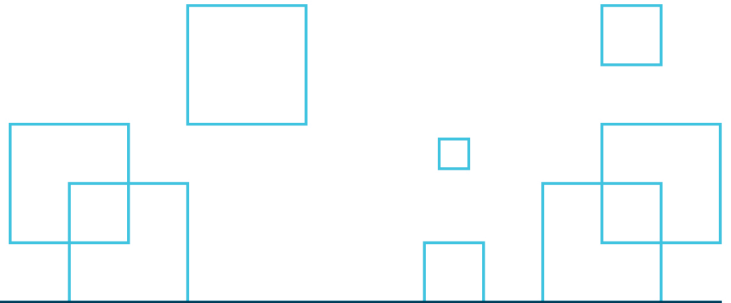
Proactive and objective public education is particularly important in the case of nascent industries such as ours, where the pace of change is rapid. It is noteworthy that education in this regard may diverge from traditional investor education. While providers, including the Canadian Securities Institute, have demonstrated an interest in digital assets,⁹ most course materials, including materials related to advisory designations, have not been updated to include training related to digital assets.

We applaud efforts taken by the securities regulators to date to educate consumers, which have included engaging websites.¹⁰ We encourage continued efforts in this regard, including educational materials designed to assist financial and investment advisors who may be answering questions about digital assets. The Chamber would be pleased to assist with these efforts.

between industry, regulators and policy makers was established and has subsisted for the last 15 years serving all stakeholder interests.

⁹ Canadian Securities Institute Research Foundation, Haskayne's Alfred Lehar awarded professorship to study the impact of blockchain technologies on capital markets, https://www.csi.ca/student/en_ca/news/news/pdf/NR-CSIRF-Lehar_Press-Release-February.pdf.

¹⁰ Ontario Securities Commission, Get Smarter About Crypto, <https://getsmarteraboutcrypto.ca/>.



4. Further Research and Review is Necessary to Develop Comprehensive Standards

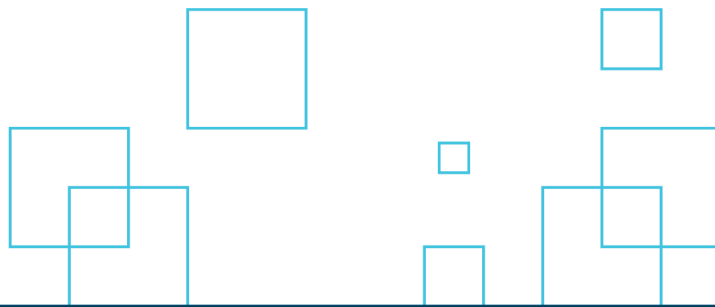
In the Consultation paper, it is noted that “although DLT may provide benefits, global incidents point to digital assets having heightened risks related to loss and theft as compared to other assets.”¹¹ The Consultation goes on to warn of “novel features that create risk to investors and our capital markets that may not be fully addressed by the existing regulatory framework.” The greater concern we see is that there has been one platform in Canada, Quadriga CX, that was ill-managed and caused harm to its users, which included Canadians, due to improper corporate governance and poor business decisions. Companies, regardless of sector, must have systems in place to mitigate risk to their stakeholders and ensure appropriate governance measures are in place. However, we caution against developing a new and broad regulatory framework in response to risks alone. Further establishing regulatory framework, ahead of holistic study of the cumulative legal, regulatory, policy, and economic landscape relating to the digital asset and blockchain ecosystem in Canada stands to introduce significant risk of industry and ecosystem disruption and interference impacting those who want to participate in the digital asset market - whether as innovators, purchasers, investors, or other industry participants that stand to benefit from new forms of commerce and digital engagement.

In February 2019, the Bank of Canada released a Staff Discussion Paper entitled, “Crypto “Money”: Perspective of a Couple of Canadian Central Bankers,” which discusses a number of important questions regarding the risk versus benefit assessment from the perspective of a central bank.¹² The Paper highlights the importance of the contemplative discourse in relation to monetary policy in Canada and states that there is no clear threat level to address, but rather significant research and broad policy work to complete to establish a clear path forward. The paper expressly states that, “while cash is a public good, a number of important policy and design questions need to be answered [to assess what would] be in the public interest. Clearly the implications for the broader financial system, especially deposit-taking institutions, need to be assessed in conjunction with other benefits and risks....”¹³ Of note, on May 2, 2019, the Central Bank of Canada and the Monetary Authority of Singapore

¹¹ Investment Industry Regulatory Organization of Canada, IIROC Notice: Joint CSA/IIROC Consultation Paper 21-402 Proposed Framework for CryptoAsset Trading Platforms, http://www.iroc.ca/documents/2019/196069ad-9053-4d8b-8022-a8e11a6c4385_en.pdf.

¹² Staff Discussion Paper 2019 - 01: Crypto “Money”: Perspective of a Couple of Canadian Central Bankers (February 2019): <https://www.bankofcanada.ca/wp-content/uploads/2019/02/sdp2019-1.pdf>.

¹³ P.23, Staff Discussion Paper 2019 - 01: Crypto “Money”: Perspective of a Couple of Canadian Central Bankers (February 2019): <https://www.bankofcanada.ca/wp-content/uploads/2019/02/sdp2019-1.pdf>.



successfully completed the first ever cross-border and cross currency payments using central bank-issued digital currencies.¹⁴

The Chamber is a strong proponent of engaged policy dialogue and research designed to help advance policy relating to digital assets, the platforms upon which they are exchanged, and the manner in which they fit into existing systems. The Chamber suggests that the CSA/IIROC take a similar, measured approach to Platform regulation as the Bank of Canada is taking toward monetary policy applicable to digital assets. Risk should be assessed alongside reward and regulatory overreach should be avoided with a view to minimizing future jurisdictional challenges, stifling innovation and market chill.

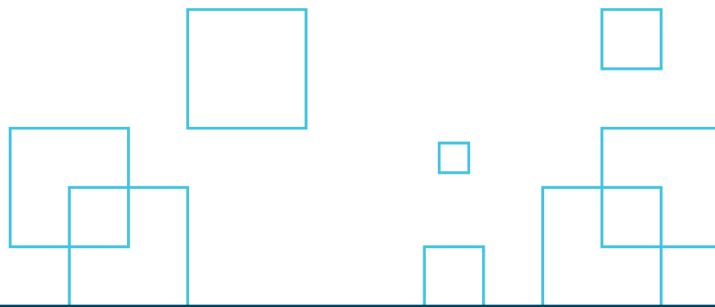
5. Regulatory Clarity for Tokens that Are Securities and those that Are Not Is Essential, Recognizing that Not All Tokens Are Securities

One of the most striking developments in the blockchain ecosystem is the emergence of token technology platforms and their transformative potential.¹⁵ The evolution of the tokenized economy is just one unique facet among the many transformative and positive possibilities that blockchain technology represents for government, businesses, and consumers. Blockchain technology will improve many aspects of our lives, much of which will be fueled through the distribution and use of digital tokens. Yet, the versatility of tokens has proved a challenge for regulators globally. The sheer number of unique characteristics that tokens may represent means that much work remains to be done to understand their potential and functionality.

In the current blockchain ecosystem, the development of digital tokens that can represent numerous things, from a currency, to a commodity, a security, title to property, identity, provenance, and many others, has created the need to interpret existing laws that may no longer adequately govern the new features of this technology. Further, a token may initially represent one functionality, such as a security, and then shift and represent another, such as a commodity. When it comes to the regulatory treatment of a token, this very versatility can be confounding. The fact that other countries are recognizing the potential of this technology,

¹⁴ Coindesk, “Central Banks Settle Cross Border Payments with Blockchain for the First Time” (May 2, 2019): <https://www.coindesk.com/central-banks-settle-cross-border-payments-with-blockchain-for-first-time>.

¹⁵ In some cases these are referred to as “crypto-exchange” platforms, but not all platforms would be categorized in this manner within the meaning or possibly intent being addressed by the CSA-IIROC Consultation.

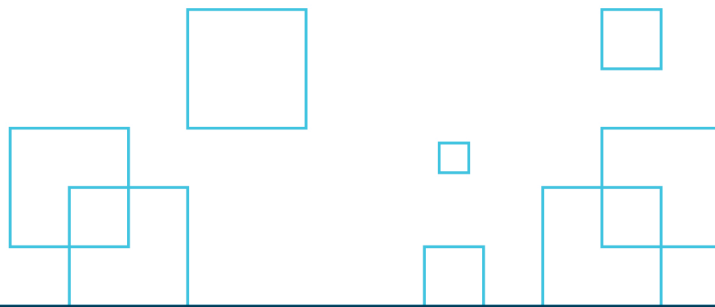


and developing regulatory systems to welcome it, renders the problem more urgent. Terminology and function-based assessment is critical when setting any policy and regulatory framework, and it is important to highlight that this is one of the fundamentally more pressing issues relating to digital tokens. Put another way, there is still no agreed upon nomenclature or framework that clearly establishes what is absolutely inside or outside the scope of securities and financial services regulation and policy, causing difficulty for all stakeholders that want to assess compliance and trust factors associated with token exchange platforms and token issuers. The Consultation does not squarely address the issue of how to characterize digital asset token uses nor does it establish the distinction between different types of token platforms.¹⁶ For example, people who buy different types of digital assets and use them as currency are not investors, and would not be considered investors if they were to do the analogous act of exchanging common Canadian dollars for foreign currency.

Industry participants noted that in relation to their engagement with existing regulatory sandbox initiatives, industry participants noted that in relation to their engagement with existing regulatory sandbox initiatives, CSA staff generally started from the premise that the proposed token in question was a security, instead of being open-minded to the possibility that some tokens are not securities. CSA staff often jumped right to the issue of what, if any, exemptive relief from securities regulation would be appropriate to permit the project to move forward. This may have resulted, in part, from a difference in understanding between some of the participating businesses and regulators. The former entered the program expecting that they would receive guidance, including guidance on whether or not securities legislation was applicable. The latter approached the initiative with a view to applying securities legislation to the participating projects, granting injunctive relief where it may be prudent to do so. In addition, participating businesses note that there appears to be little coordination with other Canadian regulators or with industry. While clarity will be beneficial to the ecosystem as a whole, the benefit of such clarity will be lost if the positions are overly restrictive or likely to be challenged on the basis of being an incorrect application of law. Guidance relating to whether or not a token is a security must recognize the breadth of possible permutations that exist, as well as other potentially applicable laws.

The importance of appropriate guidelines that take into account the myriad of applications for tokens has been raised in numerous global fora. For example, the Chamber and its Members

¹⁶ Legal expert Addison Cameron-Huff articulates this point well. Cameron-Huff further brings forward inherent assumptions, and the challenges and risks that are related to these assumptions, as drafted into the narrative of the CSA -IIROC Consultation Paper: <http://www.cameronhuff.com/blog/csa-iiroc-consultation-2019-assumptions/index.html>.



have produced several thought leadership pieces in this regard, including “Understanding Digital Tokens: Market Overviews and Proposed Guidelines for Policymakers and Practitioners.”¹⁷ This resource, developed within the Chamber’s Token Alliance working group consisting of more than 450 participants, makes clear that there is a need to recognize the myriad of tokens that exist and that will emerge beyond securities tokens, such as utility tokens and other types of digital assets that are not securities.

As CSA and IIROC are aware, digital tokens are used for:

- Identity verification;
- Payment for services and goods;
- Crowdfunding purposes, and may represent a right in a future product, but do not represent an interest in the underlying company;
- Video game platforms (in-game gold, armour, etc.) which can often be bought and sold on secondary markets or transferred between players; and,
- Access to membership or loyalty program benefits, and effectively replace a membership card to serve as proof of payment for access to services or perks.

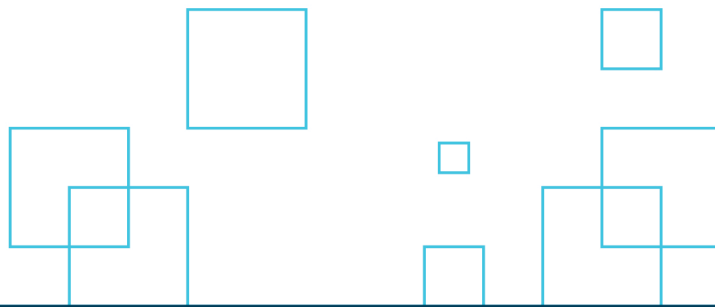
In cases where a token is not a security, the Chamber has made specific recommendations for policy guidelines and governance, including the types of information that should be disclosed and when, and practices that should be clearly prohibited (for example, promises of financial return).¹⁸ We believe that Canadian securities regulators should continue the publication of relevant policy positions and decisions, similar to those that have been published by the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) on their website.¹⁹ In each case, they consider the facts, context, and legislation at the time, and provide their analysis publicly.

We have seen government policies have profound effects on the development of digital asset exchange platforms and digital asset innovation and adoption. The Chamber recommends that policy makers and regulators across Canada aim to develop supportive policy and

¹⁷ Chamber of Digital Commerce, Understanding Digital Tokens: Market Overviews and Proposed Guidelines for Policymakers and Practitioners, <https://digitalchamber.org/token-alliance-whitepaper/>.

¹⁸ Chamber of Digital Commerce, Understanding Digital Tokens: Market Overviews and Proposed Guidelines for Policymakers and Practitioners, <https://digitalchamber.org/token-alliance-whitepaper/>.

¹⁹ FINTRAC, FINTRAC interpretation notices and policy interpretations, <http://www.fintrac.gc.ca/guidance-directives/overview-apercu/FINS/1-eng.asp>.



regulatory guidance so that businesses in Canada focusing on digital asset innovation can confidently develop their business strategies and compliance roadmap to stay competitive globally.

Responses to Specific Consultation Questions

The general comments should be considered in relation to the questions below, in addition to the specific responses to each.

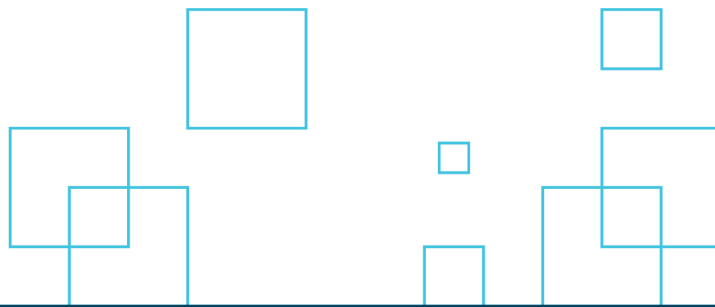
1. Are there factors in addition to those noted above that we should consider [relating to digital-asset exchange platforms]?

Definitions and terminology, such as “platform” for example, need to be clearly and contextually defined in all consultations, policy, and proposed frameworks going forward to mitigate the risk of establishing unclear and overly broad rules that may discourage innovation and / or result in unintended damage to businesses that should not be targeted.

Establishing regulation too early in an innovative sector also presents risk. The industry is working hard to establish its own best practices, not least given the significant financial investments that have been made to drive progress to date. If the CSA moves forward to crystalize today’s best practices prematurely, they may be out of date in short order.

The Consultation acknowledges that, “at least some of the well-established digital assets that function as a form of payment or means of exchange on a decentralized network, such as bitcoin, are not currently in and of themselves, securities or derivatives. Instead, they have certain features that are analogous to existing commodities such as currencies and precious metals.” We note that the Consultation stops short of exploring transactions that function as a “form of payment or means of exchange” - we believe these transactions require further clarification.

Chamber members The Chamber members submit that most Canadian Platforms do not offer trading in security tokens, but rather sell bitcoin, ether and other leading cryptocurrencies which are not securities in spot transactions. These types of Platforms are money services businesses (MSBs) and should be regulated as such. The federal Department of Finance recognized this in 2014, when Bill C-31 proposed to amend the PCMLTF to add definitions for “virtual currency” and “dealers in virtual currency” and to regulate dealers in virtual currency as MSBs. It took the Department of Finance four years to



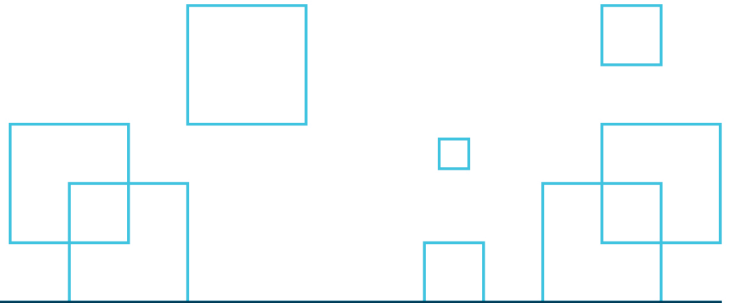
publish the draft regulations in early 2018, and the final regulations which were scheduled to be adopted in the fall of 2018 are still on hold. Many Canadian Platforms have applied to FINTRAC for registration as MSBs but have been turned down or have had to change their business model to include fiat currency trading in order to be subject to MSB regulation. For the vast majority of Platforms, MSB regulation is appropriate and should address many investor protection concerns regarding digital assets, including ensuring that purchasers of cryptocurrencies are subject to identity verification requirements and transactions in cryptocurrencies are subject to reporting and recordkeeping requirements under Canadian anti-money laundering laws.

The Chamber proposes that exchanges dealing in virtual currencies should be considered Money Services Businesses, and not Brokers or Dealers in securities, a position that seems to have growing support in Canada.

There are a number of factors, beyond investment contracts, that should be assessed to determine what may constitute a security in the tokenized world. The definitions section in the *Ontario Securities Act* lists many factors that may not be appropriate or suited to determine what qualifies as a security or activities regulated by securities regulation. Coordinated industry discussions are necessary to determine the depth and breadth of applicability of current definitions in *the Ontario Securities Act*. We encourage coordination between federal and provincial policy makers and regulators to ensure industry does not get conflicting guidance.

Finally, the Proposed Framework states, “the CSA wishes to remind market participants that any person or company advertising, offering, selling, or otherwise trading or matching trades in digital assets that are securities or derivatives, or derivatives that are based on digital assets to persons or companies in Canada, or conducting such activities from a place of business in Canada is subject to securities legislation in Canada.” In Canada, we have seen a similarly proposed piece of regulation as part of the Proceeds of Crime Money Laundering and Terrorist Financing Act (the “PCMLTFA” or the “Act”). The particular regulation proposes that those “directing services” to Canadians will be considered foreign money services businesses, and therefore captured under the Act and regulated. A business is seen to be “directing services” to persons or entities in Canada if it meets at least one of the following three criteria:

1. The business undertakes marketing and advertising directed at persons or entities in Canada;



2. The business maintains a Canadian website (e.g., with “Canada” in the name, a .ca domain name); or,
3. The business is listed on a Canadian business directory.

In the case of the Canadian regulatory environment, this therefore leaves open a loophole for foreign entities operating in this space but “passively” providing services to Canadian customers, *i.e.*, through word of mouth and reputation. In the digital asset economy, direct advertising isn’t the norm. Customers are obtained through word-of-mouth and reputation rather than direct advertising in magazines, papers, and similar publications. As a result, this gives foreign entities an “out” from the regulation based on the current definition. It should be noted further that we are aware of many examples of Canadians using services of platforms that would not meet the proposed requirements based on the above. We acknowledge that Part 5.1 states that exemptive relief may be considered for those located outside of Canada and regulated by a foreign regulator “in a manner that is similar to domestic oversight.” Further discussion is required to understand what this would entail and how this would be assessed, particularly given the rapidly shifting regulatory environment we currently see across the globe, relative to the virtual asset space. It is imperative to ensure that Canadian exchanges and platforms are not disadvantaged by exemptive relief granted to foreign exchanges and platforms.

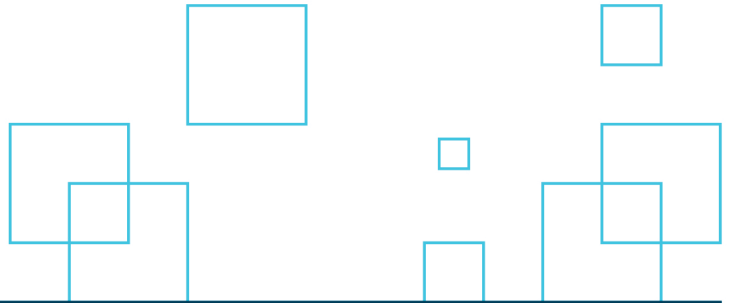
Finally, it is important for regulators to be aware that the vast majority of players in the blockchain ecosystem aren’t in Canada. Almost all of the exchanges cited in the Consultation operate abroad. If Canada creates rules that put Canadian exchanges or other businesses at a competitive disadvantage then not only will Canada have no exchanges, but Canadians will also be carved out of this market.

Risks, Custody and Verification of Assets

2. What best practices exist for Platforms to mitigate these risks? Are there any other substantial risks which we have not identified?

3. Are there any global approaches to regulating Platforms that would be appropriate to be considered in Canada?

There are no leading global approaches as of yet. Further study is required and the following regimes should be researched and considered as they demonstrate a nuanced approach to the classification of digital tokens.

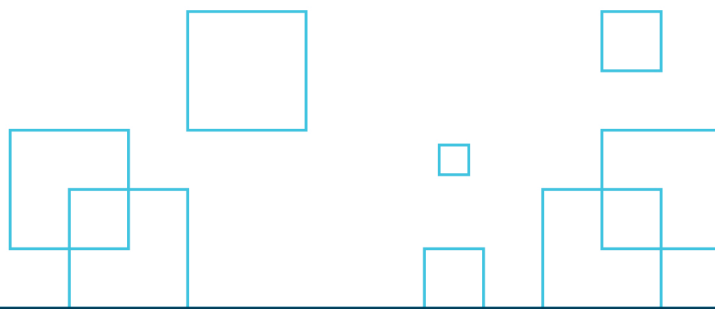


1. **Japan:** Japan requires that digital currency exchange businesses manage customer's funds or digital currency separate from their own. The state of this must be verified by CPAs or accounting firms. They must have a contract with a designated dispute resolution center with digital currency expertise. They must keep accounting records of its digital currency transactions and submit a report of these annually to Japan's Financial Services Agency. A group of exchange businesses formed a self-regulatory body which all registered exchange businesses must join.

2. **Switzerland:** Switzerland has defined tokens into three categories: i) payment tokens (digital currencies) which are used as a means of payment or value transfer; ii) utility tokens which provide digital access to applications or services through the blockchain; and, iii) asset tokens which are assets such as a debt or equity claim and are analogous to equities, bonds and derivatives. Tokens received in an "ICO" generally qualify as securities. They define securities as certified or uncertified securities, derivatives and intermediated securities which are capable of mass standardized trading.

3. **Bermuda:** Bermuda is working to develop themselves as a destination for utility tokens, tokenized securities and coin offerings. They are creating a digital currency association with a defined code of conduct and rules of operation. The group will be self-governing. Utility tokens are not a security unless there is a promise of future value. There is a working group directed by the minister of National Security which is tasked with ensuring that Bermuda's regulations are conducive for the development of digital currencies. The group's members include individuals from a variety of government ministries, a bank, a law firm, the National AML Committee, and the Bermuda Business Development Agency. The group is self-governing. They have previously consulted the public for opinions on digital asset regulation and what those regulations should be.

4. **Australia:** INFO 225 gives guidance around a number of aspects considered in this Framework. Guidance is given around the legal status of ICOs and digital-assets, considerations for when an ICO could be an offer of a financial product, when a platform for secondary trading of ICO tokens or other digital-assets could become a financial market, and guidance around how prospective ICO issuers and digital-asset businesses can obtain informal assistance from the Australia Securities and Investments Commission.



Members also note Malta, Gibraltar, and Mauritius are demonstrating global leadership through its standards setting approach to digital assets and digital asset exchange platforms.²⁰

4. What standards should a Platform adopt to mitigate the risks related to safeguarding investors' assets? Please explain and provide examples both for Platforms that have their own custody systems and for Platforms that use third-party custodians to safeguard their participants' assets.

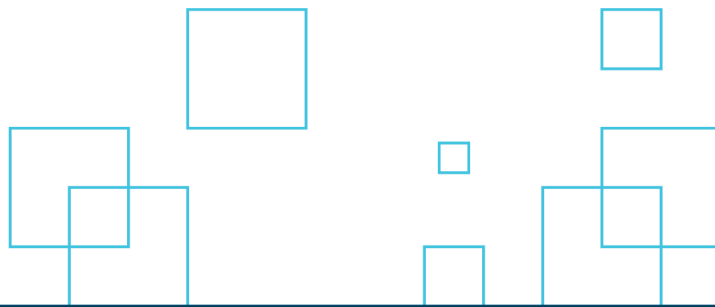
Many platforms are taking proactive measures to ensure they are able to mitigate risk and build successful and sustainable businesses. As business needs have evolved, so too have the number of custody solutions, which we see as a very positive advancement that will attract institutionally managed digital assets that will advance blockchain adoption globally. Industry is demonstrating its commitment to improving innovation at a rapid pace. We encourage regulators and policymakers to acknowledge and applaud positive steps forward.

Some members suggest that securities-centric businesses should be expected to show robust system design, specifically design intended to avoid "single points of failure", as well as to clearly document (and follow) their own processes. However, there are varying schools of thought on the degree to which specific security measures should be known/shared outside of strictly controlled and vetted parties. The argument against a broader sharing of security parameters is the possibility that doing so may expose the platform to an attack vector via a vulnerability made apparent to a potential attacker via descriptions of the security measures in place. Further discussion with industry is required to fully address standards.

5. Other than the issuance of Type I and Type II SOC 2 Reports, are there alternative ways in which auditors or other parties can provide assurance to regulators that a Platform has controls in place to ensure that investors' crypto-assets exist and are appropriately segregated and protected, and that transactions with respect to those assets are verifiable?

It is important that the regulator work with industry to establish expectations regarding the scope of high-level control objectives or system requirements that may be relevant for a securities specific digital asset platform. Some basic controls may include those that would

²⁰ Regulatory Framework for Custodian Services (Consultation Paper):
https://www.fscmauritius.org/media/67493/consultation-paper-custody-of-digital-assets_final.pdf.



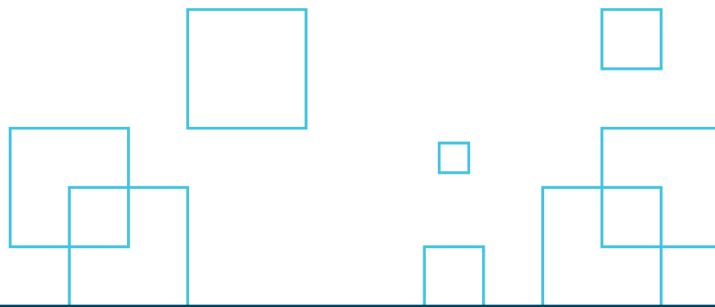
manage and mitigate the custodial risks, including safeguarding of private keys and ensuring that investors' crypto assets exist and are appropriately segregated and protected, and that transactions with respect to those assets are verifiable. In many cases, public blockchains are fully transparent and may be auditable in relatively novel ways that are not possible with traditional assets. Assets in wallet addresses can be viewed at any time. Even in the case of assets that have been designed to be privacy intensive, audit keys can be built into the design of the digital asset in order to allow a type of "view only" access on an as-needed basis. These types of features must be taken into consideration when designing audit processes. In some cases, it may be possible to automate most audit functions relating to the issuance and custody of digital assets.

Many platforms pool assets. It is often impractical and expensive for the platform to create separate digital asset wallets for each user that hold only that user's assets and confirm any and all transaction activity to the asset's underlying blockchain. In such cases, transactions would only be visible on a public blockchain when the platform receives custody of a digital asset, transfers custody of a digital asset, or transfers a digital-asset between different wallets that are controlled by the platform. In other instances, it may be practical for platform operators to maintain segregated wallets for each user and/or to conduct transactions in a manner that is always confirmed to the blockchain of the digital-asset affected by each transaction.

Regardless of whether digital assets are held in pooled or segregated accounts, auditing standards should take into account the degree to which public blockchains can be used to automate audit functions. A reliance on traditional audit standards applied to digitally native assets would be unfortunate if these reduced the ability to harness automation.

Further, as noted by the CPA, regardless of whether a SOC 1 or SOC 2 report is provided, it is not possible to provide a Type II report (*e.g.*, SOC 1 Type II or SOC 2 Type II) until the Platform has been in operation for a reasonable period of time (*e.g.*, 6 months). Consideration should be given when a Type I report will be accepted and what the maximum period of time is that the Platform can operate until a Type II report is required.

The Consultation also notes that Platforms seeking registration as an investment dealer and IIROC membership that plan to provide custody of crypto assets will not only need to satisfy existing custody requirements but will also be expected to meet other yet-to-be determined standards specific to the custody of crypto assets. While standards specific to the relevant risks should be considered, and addressed appropriately, it is important to understand the



unique risks of digital asset platforms and address them in a manner that balances the protection of the public interest and the ability for organizations to innovate in Canada.

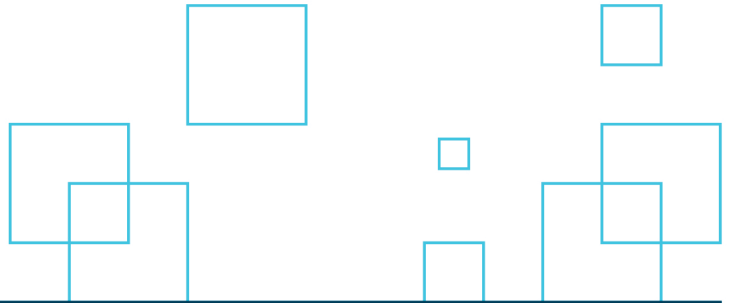
The Chamber urges that options to provide assurance over the design and operating effectiveness of and any controls should be explored with industry at the table, and that the Chamber and its members would welcome the opportunity to participate in these discussions.

6. Are there challenges associated with a Platform being structured so as to make actual delivery of crypto assets to a participant's wallet? What are the benefits to participants, if any, of Platforms holding or storing crypto assets on their behalf?

Best practices for platforms that are considered regulated under securities laws, are still being defined by innovation and industry. Some Members suggest that trading platforms should not hold assets as there is heightened risk for foul play or central failure where the exchange platform also custodies the assets.

Custody is a complex issue, and one on which our membership has not achieved consensus. On one hand, it is important to consider the innovations that are unlocked by technology, including the ability of owners to take full custody of digitally native assets, or to place such assets in a multi-signature smart contract, where both the platform operator and the owner of the asset would be required to sign a transaction in order to move an asset. Such innovation has the potential to greatly increase transparency, efficiency, and auditability. These innovations do carry risks⁵ as well, including the risk of loss of private keys used to sign transactions, and the risk that a smart contract does not function as intended or contains weaknesses in its code which can be exploited. While no member advocated for a strict recreation of existing custody models, which can be expensive, inefficient, opaque, and difficult to audit accurately, a perfect model was not immediately apparent. In some cases, members noted that platform providers may benefit from the use of custodial services, at least in the short term, while alternatives and controls (including audits) matures and technology continues to develop to provide longer term solutions to these problems.

It is noteworthy that the use of technology can allow for more secure transactions without the use of intermediaries, or in some instances, using different types of intermediaries, including automated functions. For example, in a transaction that is conducted on a completely decentralized platform, it would be possible using digital signatures and other electronic controls to validate that certain conditions (cybersecurity-related controls, identification, KYC, etc.) are sufficiently met without necessarily exposing the users' personal information. Such



models in which transactions are private but not anonymous should be explored and encouraged as they can play a significant role in protecting consumers from potentially harmful data and privacy breaches. The Chamber is concerned that the Proposed Platform Framework may stifle these innovations, which are designed to protect personal information and reduce transaction costs, by imposing a traditional model of financial regulation onto Platforms.

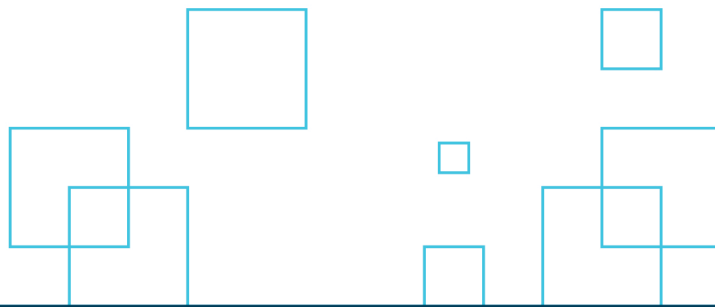
With regard to SOC Reports, members identified alternative options to SOC engagements which, depending on the ultimate audience of the results of such work, could serve as additional assurance that appropriate controls are in place. Establishing internal reporting protocol requirements may be useful. For example, internal controls over financial reporting and data provide factual accounts of performed procedures. Generally, they are used for management and have restrictions on public distribution. There are a variety of frameworks (COSO, CobiT, SOC 2, etc.) that can be utilized in guiding the above work and should be studied more carefully to assess applicability for platforms regulated by securities laws.

Finally, it is important for digital asset users and investors to be able to understand platform terms and conditions regarding the use of their data. The standards set out in the General Data Protection Regulation (GDPR) are instructive in this regard, requiring that a reasonable user can understand how platforms collect and use their data. Similar principles can be applied in order to create more effective real-time disclosures relating to the use of funds, investment choices, and fees.

These disclosure principles apply to the parameters that exist when taking custody of their own digital assets. It is widely believed that the single greatest challenge to delivery and self-custody is user error. In some instances, it may be preferable for users that are not technically savvy to have platforms remain in custody of their digital assets. It is expected that, given time, wallets that are both user-friendly and secure will emerge. In the meantime, risk-based education should continue. Where possible, platforms should implement real-time safeguards, such as double-checking a wallet address, and displaying short and clear disclosures where a user requests to take custody of their own funds.

Price Determination

7. What factors should be considered in determining a fair price for crypto assets?



When considering price discovery, the activity that is confirmed to a digital asset's public blockchain should be taken into consideration where possible. This may include the volume of trading activity and the rates at which a digital asset has been traded for other digital assets (which is possible in some cases without the use of an intermediary). In such instances, the information is publicly accessible and easily verifiable. It may even be possible and desirable to automate some information aggregation and publication processes.

Where transactions or transaction information are not publicly available, clear guidelines should be developed to help platforms report complete and accurate information, including how such information should be calculated and disclosed. Here, again, it may be possible to automate many of the discovery functions based on predefined regular inputs from platforms at regular intervals.

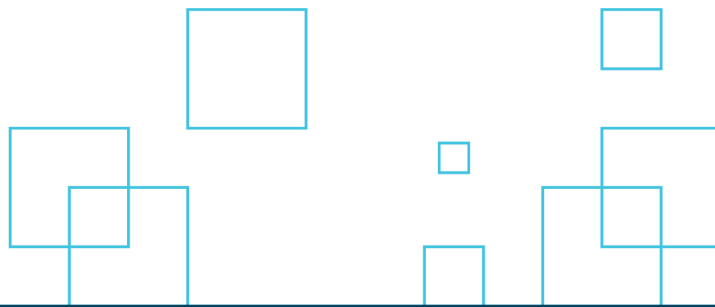
We recommend working closely with the industry to understand the nuances of pricing and price disclosures. This may include transactions that take place via over the counter (OTC) units connected to platform providers, as well as the impact of platform providers in jurisdictions outside of Canada, as well as traditional futures markets that have implemented products related to digital assets.

8. Are there reliable pricing sources that could be used by Platforms to determine a fair price, and for regulators to assess whether Platforms have complied with fair pricing requirements? What factors should be used to determine whether a pricing source is reliable?

The fair and transparent pricing of digital assets continues to be the subject of much speculation and some academic study.²¹ We agree that this is an important issue. We recommend that, rather than providing strict guidelines relating to how price discovery should/must be done, there be instead strict prohibitions against deceptive and manipulative practices. We believe that this approach would continue to foster innovation while punishing "bad actors" within the ecosystem.

It was noted that where a tangible asset guarantees or is represented by a digital asset, there should be clear and timely financial audits related to the underlying asset (for example, real property). Material misrepresentations should have appropriate consequences, in particular

²¹ For example: John M. Griffin and Amin Shams, *Is Bitcoin Really Un-Tethered?*, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3195066.



where these meet the standard for negligence or malice. Finally, practices such as inflated or misleading transaction volumes on platforms should also be prohibited. Trading volume that represents trades made by the platform itself (and not by a user) should be explicitly excluded from the exchanges' trading volume, as should trades conducted by third parties (including bots) for the sole purpose of creating volume on a platform and/or affecting prices on a platform.

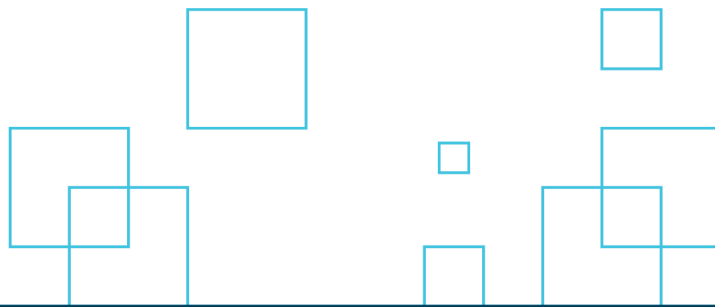
Of note, price discovery, transparency, and lack of self-dealing are important, however, digital asset trading is a global activity. Pricing is not set by the Canadian marketplace, but rather is set globally. Most exchanges make use of "liquidity pools" (*i.e.*, trading on their own account with other exchanges in order to fulfill orders) or rely on people running arbitrage bots to ensure that large orders can be processed quickly without too much slippage. Users want this to happen because they want to be able to trade on Canadian exchanges, rather than using foreign exchanges that have substantially more volume. Unlike traditional exchanges, most digital asset trading being done by Canadians is not occurring in Canada and therefore cannot be regulated by Canadian regulators. Efforts to regulate extraterritorially is futile and more likely to result in an erosion of the competitive position of Canadian exchanges, further offshoring of digital currency trading activity.

As discussed above, the Proposed Framework may apply both to platforms that operate in Canada, and to those located outside of Canada that have Canadian participants. Clear guidance in relation to any applicable exemptions/relief is required. If there is an expectation that exemptions will be granted to operators in jurisdictions that are deemed to have sufficient regulatory regimes in place in their home or operating countries, it would be desirable for Canadian regulators to publish and maintain an up-to-date list of such jurisdictions. In addition, the conditions under which exemptions/relief would be withdrawn from a particular platform operator should be clear (for instance, if there were egregious compliance issues in the home or operating country).

Finally, it would be imperative to ensure that Canadian exchanges and platforms can comply to these regulatory requirements to ensure Canada can maintain a competitive global position and participate in this growing and highly valuable marketplace.

Surveillance of Trading Activities

9. Is it appropriate for Platforms to set rules and monitor trading activities on their own marketplace? If so, under which circumstances should this be permitted?



10. Which market integrity requirements should apply to trading on Platforms? Please provide specific examples.

11. Are there best practices or effective surveillance tools for conducting crypto asset market surveillance? Specifically, are there any skills, tools or special regulatory powers needed to effectively conduct surveillance of crypto asset trading?

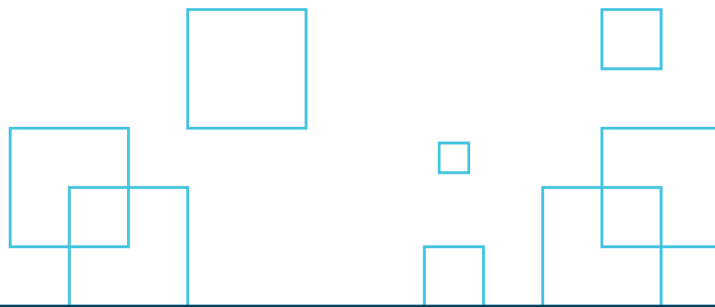
12. Are there other risks specific to trading of crypto assets that require different forms of surveillance than those used for marketplaces trading traditional securities?

This question can be addressed along two dimensions: the actions that platforms take in terms of monitoring and oversight, and the monitoring and oversight of the platforms themselves.

On the first dimension, the Chamber is aware that digital asset platforms are starting to monitor customer activity and monitoring for suspicious behavior. They are manually, or through combinations of manual and automated methods, identifying types of behavior and indicators of suspicion that require further consideration and engagement with regulators and other authorities. The typologies of what suspicious behavior looks like in the context of digital asset transactions is beginning to be better understood and documented. A number of these typologies are new and different to a fiat environment. While this monitoring activity is not currently a regulatory requirement in Canada, a number of platforms and companies are focusing their resources on such activities in an effort to proactively identify and mitigate the threat of their platforms being used for money laundering or illicit behaviour. Tools created by companies such as CipherTrace and Chainalysis are powerful blockchain analytics tools which can be effective in tracing digital assets throughout the blockchain. The industry is anticipating federal regulations for anti-money laundering to establish surveillance requirements. The Chamber recommends that provincial regulators align any surveillance requirements with the upcoming federal changes.

Once “virtual currency dealers” are regulated as MSBs, they will be subject to regulatory oversight by FINTRAC, which is expected to include reporting and surveillance measures appropriate for such Platforms. The Chamber expects that FINTRAC oversight will be sufficient for most Platforms that are not trading in securities.

With respect to market manipulation, this responsibility currently sits with the Compliance Officer and is done on a proactive basis. Certain companies are building indicators and surveillance protocols into the training provided to members of their internal compliance team.



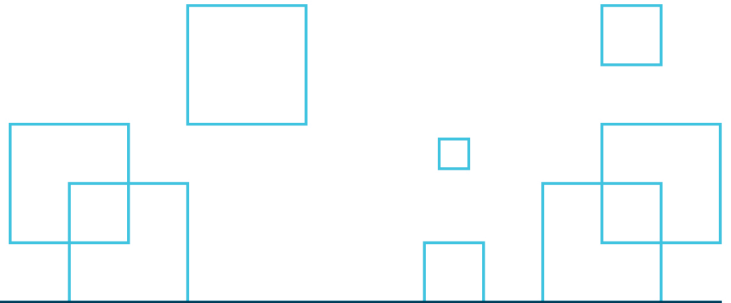
There are also mainstream monitoring tools that provide surveillance capability to fiat financial organizations and are now increasingly turning their attention to FinTech and digital asset-related businesses, such as Irisium.

Members felt that the scope of surveillance best practices should ideally include both functional activities and their supporting technology elements. For example, the scope should include the processing of transactions along with the systems (infrastructure, software, people, processes, data, procedures, etc.) that support the delivery of processing of transactions.

On the second dimension, the application of systems such as IIROC's market surveillance system²² may be useful in some instances, the development of such tools as they relate to digital assets should take into consideration the types of data that are publicly available, and the ability to automate certain oversight functions. Industry leaders in blockchain analysis technologies are already emerging, and it will be of great importance to work with such companies, as well as consulting with the industry, to ensure that technologies are appropriately leveraged for efficiency. In order to be effective in this aim, there is a need to understand the current state of technology, as well as innovations which are continuously emerging. The ideal system must be robust and flexible enough to interface with data sets that are built in accordance with different technological standards.

It will be equally important to define the boundaries of the application of such oversight, which relates back to the need for comprehensive guidance in relation to the taxonomy of tokens and other crypto assets. Similarly, it will be important to clearly define exclusions, lest there be an expectation that provincial regulators are tasked with the monitoring of a volume of data that does not present a risk commensurate to such monitoring (such as in-game gold, or rewards points).

²² Investment Industry Regulatory Organization of Canada, IIROC and Nasdaq unveil state-of-the-art market surveillance technology to enhance oversight of Canada's capital markets, http://www.iroc.ca/documents/2019/0f12e531-e281-4fd7-8958-9ff0e6930037_en.pdf.



Systems and Business Continuity Planning

13. Under which circumstances should an exemption from the requirement to provide an ISR by the Platform be considered? What services should be included/excluded from the scope of an ISR? Please explain.

At this stage, it remains difficult to advise on this question as the level of decentralization of a given platform, for example if someone has a fully decentralized platform, it may mean that an ISR may not be feasible. The Chamber recommends that an industry and regulator working group be established to further discuss how to approach ISRs and the related questions regarding business continuity planning.

Conflicts of Interest

14. Is there disclosure specific to trades between a Platform and its participants that Platforms should make to their participants?

15. Are there particular conflicts of interest that Platforms may not be able to manage appropriately given current business models? If so, how can business models be changed to manage such conflicts appropriately?

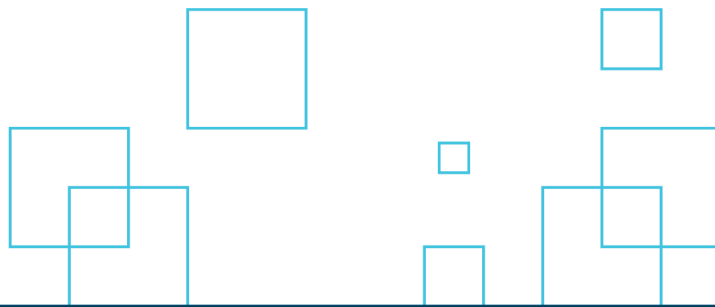
Platforms should provide clear and concise real-time disclosures, whether or not these are related to any conflicts of interest. Clear guidance should be issued describing the circumstances that create a conflict of interest, as well as the expected resolution and disclosure. Members did not believe that there were insurmountable conflicts of interest but did express a desire for clear guidance in this regard.

Insurance

16. What type of insurance coverage (e.g. theft, hot-wallet, cold-wallet) should a Platform be required to obtain? Please explain.

17. Are there specific difficulties with obtaining insurance coverage? Please explain.

We believe that the standards in this regard should be no greater than those established for traditional broker dealers and custodians. Insurance in other industries (including the banking industry) does not provide full coverage for investors. The Canadian Deposit Insurance



Corporation (CDIC) covers only the first \$100,000 in eligible deposits at any one member institution for any single depositor.²³ Significant exclusions from eligible deposits exist, including mutual funds, stocks, bonds, and accounts denominated in foreign currencies. In addition, some account types are exempt. It does not make sense to hold digital asset platforms to a higher standard than the standard that is applicable to Canadian banks. Finally, it is worth noting that in instances where a platform does not take custody of digital-assets on behalf of its users, insurance may not be necessary.

There is a relatively strong consensus that the challenges in the current environment would make it difficult to mandate insurance outside of a publicly administered insurance scheme.

17. Are there specific difficulties with obtaining insurance coverage? Please explain.

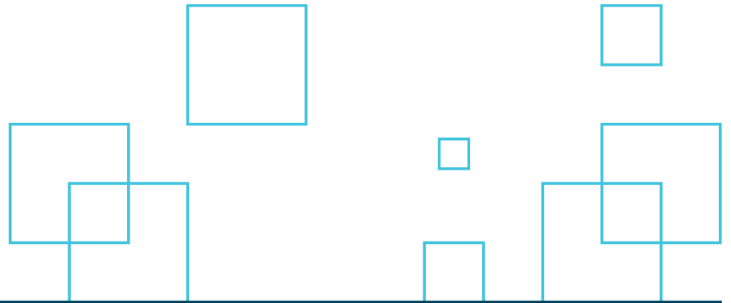
Our members raised concerns over the fact that there are currently very few insurance providers willing to insure digital assets, or companies that deal in digital assets. Anecdotally, companies that deal in digital assets have reported significantly higher premiums, including premiums for insurance products (such as Directors' and Officers' liability insurance) that are unrelated to digital assets. Where insurance is obtained, buyers have expressed doubts about the nature of the coverage, and whether or not the insurer has understood the underlying digital assets sufficiently enough to allow appropriate insurance contract parameters. In short, the industry is not currently well-served. While we support insurance as a best practice, we recommend a cautious approach to requiring specific coverages, in particular where markets are limited and cost-prohibitive.

This is not a uniquely Canadian issue. Earlier this year, BitGo, a company that acts as a custodian (among other functions), announced that it had acquired insurance covering some of the digital assets that it holds at a significant expense.²⁴ This announcement quickly attracted the ire of an underwriter, who went on to discuss in-depth the nuances of what may and may not be covered.²⁵

²³ Canada Deposit Insurance Corporation, What's Covered?, <https://www.cdic.ca/about-deposit-insurance/whats-covered/>.

²⁴ <https://blog.bitgo.com/bitgo-sets-the-standard-for-insurance-coverage-and-transparency-4cf93446bbd7>.

²⁵ Ian Allison, Underwriter Claims Crypto Custodian BitGo Exaggerated Insurance Coverage, <https://www.coindesk.com/crypto-custodian-bitgo-exaggerated-insurance-coverage-underwriter-claims>.



18. Are there alternative measures that address investor protection that could be considered equivalent to insurance coverage?

Ideas proposed included devising an insurance scheme (similar to CDIC) in which platforms were required to participate, with reasonable premiums and strict parameters. This type of scheme may be useful, even if not mandatory, in the short term in order to provide insurance markets for digital asset platforms that are struggling to find market fit.

Further, it may be possible for platforms to institute a form of self-insurance by maintaining fiat balances in amounts equivalent to digital assets held on behalf of users in hot wallets (which are connected to the internet and can be used to conduct transactions) at all times.

Regulators should work with industry participants, both platforms and insurance companies, to better understand the types of risks that can be insured and those which cannot. Regulations should be tailored to meet the needs of investors, platforms and insurance companies in order to create standards that will reduce the cost of insurance in the overall industry. Without standards, platforms and insurance companies will have to engage in bespoke insurance policies that will be costly to obtain and require a lengthy underwriting process.

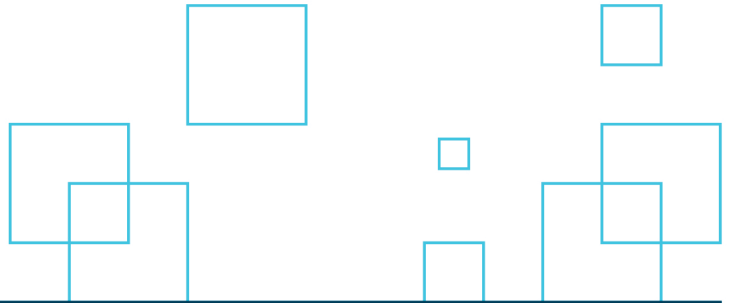
Clearing and Settlement

19. Are there other models of clearing and settling crypto assets that are traded on Platforms? What risks are introduced as a result of these models?

20. What, if any, significant differences in risks exist between the traditional model of clearing and settlement and the decentralized model? Please explain how these different risks may be mitigated.

Where transactions are confirmed on a blockchain, settlement can be automated and almost instantaneous, creating an immutable public record of the settled transaction, and allowing for transactions that involve fractions of a unit or share. Taken together, these characteristics indicate that there are significant advantages that can be offered over traditional settlement methods.

The Chamber recommends that an industry and regulator working group be established to further discuss how to approach related questions regarding settlement and clearing.



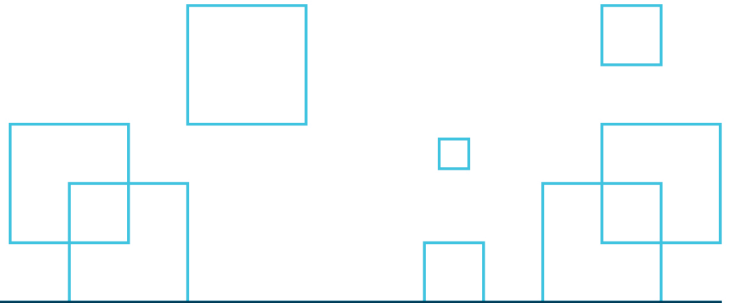
21. What other risks are associated with clearing and settlement models that are not identified here?

With regard to significant differences in risk that exist between traditional and decentralized clearing, members commented that decentralized exchanges should be subject to KYC/AML compliance measures that fit with and reflect their business models. The Chamber commented on Canada's proposed KYC/AML Proposed Regulations last Fall and encourages the CSA and IIROC to review the comments submitted, as they provide relevant considerations at length in relation to this topic.²⁶

It is also worth considering that new models for digital identity and digital transaction security will dramatically enhance the security for these types of trades. Decentralized exchanges should be encouraged to support a model where the trade instruction, which is digitally signed for all digital asset trades by the User's Private Key, also include:

1. Evidence in the form of a digital signature of a manifest of the system that protected the Private key, and support verification that the Cyber controls are operating correctly as part of the transaction execution. This attestation process will assure the controls required by the user are in place and working.
2. Evidence in the form of a digital signature of a manifest of the compliance requirements are fully satisfied prior to the execution of a transaction. Third party compliance service providers could provide one time use validation tickets that all of the steps for compliance were satisfied, and the compliance ticket could then be consumed by the execution of the trade.
3. Integration of privacy and protection of personal identifiable information. The new models should consider that it is possible to execute a private trade between known parties without the exchange knowing the parties, but trusting a third party service that "knows" the parties. Digital assets have the ability to enable a new model of private, but not anonymous, transactions that will meet the true needs of protecting customers and their PII.

²⁶ Chamber of Digital Commerce, Comments of the Chamber of Digital Commerce on the Regulations Amending Certain Regulations Made under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act, 2018 (the "Proposed Regulations") published in the Canada Gazette on June 9, 2018, <https://digitalchamber.org/wp-content/uploads/2018/09/Canada-AML-Proposed-Regulation-Comment-Letter-Chamber-of-Digital-Commerce.pdf>.



It is important that FinTech innovation is given space to evolve generally and specifically in relation to online transactions, as paper trade instructions are quickly becoming irrelevant and outdated.

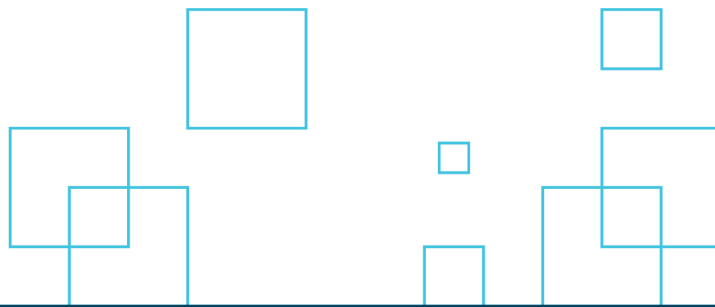
Exchanges should be encouraged to support digitally signed instructions that are built on secure technology. This may include:

- Securely stored private keys in hardware with strong device controls;
- “What You See is What is Signed” technology such as global platform TUI 1.0 standard for trusted display;
- User consent using secure PIN or biometric authentication such as EU PSD2 Cyber security requirements for consumer e-commerce;
- Verified trust protocol attesting that systems are operational and working as expected.

Finally, platforms are currently unable to achieve Delivery vs Payment (“DVP”) settlement. DVP settlement is a requirement for many brokers, funds and other regulated investment entities to participate in trading on an Exchange or Marketplace. To date, there is no known system where digital assets can settle for fiat currency in a DVP fashion. The primary reason for this, correctly identified by the Consultation Paper, is a lack of clearing agents or clearinghouses with the technical capability to facilitate DVP settlement. This creates several risks not identified in the Consultation paper.

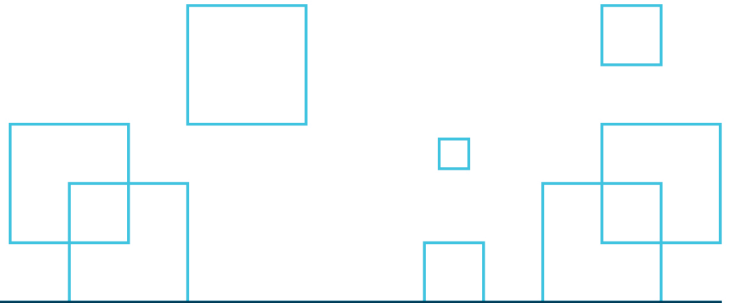
First, platforms, in their current configuration, require participant’s deposit fiat (or digital assets) on the Platform, or must setup margin facilities, prior to trading. This introduces counter-party risk and/or credit risk that does not exist today in regulated Marketplaces. Second, the lack of DVP settlement precludes many brokers or trustees from participating on these platforms because they are prohibited from taking on this type of risk when dealing with client assets. This introduces an “opportunity cost” risk as many investors who choose to work exclusively with brokers would not be able to access digital assets on platforms. The lack of DVP also prevents pension funds and mutual funds from participating on the platforms, again excluding large segments of the Canadian investing public. Rather than relying on exemptive relief, regulators should form working groups with current market infrastructure participants to explore settlements systems. An example of how DVP settlement could be achieved is described below.

Certain digital assets, such as bitcoin, operate on a blockchain, *i.e.* the Bitcoin blockchain, that possesses the technical capabilities required to create a DVP-like settlement. However,



key market infrastructure is required in order to create this system, chiefly banking and custody services that have access to the SWIFT payment system. In such a system, if the Platforms and the clearing agency had access to banking services, or even accounts at the same bank, the clearing agency could operate an escrow service to facilitate DVP settlement. The system would work as follows. Retail Investor could place an order through their registered representative, *i.e.* their broker, who in turn would place an order to purchase bitcoin on a participating platform. Similar to today, during a “net settlement” period, typically between 4:00 PM EST and 6:00 PM EST, automated systems from both the platform and broker would match their trades and agree on an amount of fiat to be sent to the platform from the broker’s custodian and an amount of bitcoin to be sent to the clearing agent from the platform’s custodian. Instructions would be sent to the clearing house via SWIFT or some other messaging service with the amounts, bank accounts and bitcoin wallet addresses participating in the transaction. The platform’s custodian would then initiate a multi-signature transaction and broadcast that transaction to the bitcoin blockchain. The clearing agent, having already received the instructions from the custodian, is able to “listen” to the Bitcoin blockchain (through their own node) and when the fiat funds arrive in the clearinghouse bank account, the clearing agent signs the bitcoin transaction and broadcasts the signed transaction to the Bitcoin blockchain. Simultaneously, the clearing agent releases the fiat funds to the platform’s custodian, achieving near DVP settlement as both participants receive their funds and digital assets simultaneously. If either party fails to deliver either fiat funds or digital assets the clearing agent cancels the transaction or delivers the missing asset to complete the trade. Regulators should form a working group to further explore such a solution with the aim of defining standards so that dealers, brokers, platforms, custodians and clearing agents could participate in roles similar to how they currently operate.

Underpinning many of the issues with clearing and settlement, however, is the inability for platforms to obtain access to banking services. So long as digital assets remain in regulatory limbo, banks will face significant difficulty providing banking services. Regulators should form a working group with both banks and digital asset industry stakeholders to develop operating standards for companies that wish to deal and/or accept payment in digital assets. Without such standards, banks will be unable to judge the risks that both platforms as well as other digital asset participants pose to their own operating model. Given the strict regulatory standards that oversee banks, it will continue to be extremely difficult to provide banking services. Banks must have clear regulatory guidance to know when a digital asset platform is operating in a manner that complies with rules and regulations. Banks cannot be making such assessments on their own because each bank will have to determine their own standards, resulting in a different set of rules for each institution. Ultimately, this will create even more



challenges for other regulatory bodies, such as OSFI and IIROC, who would have to determine and review if each bank's unique set of guidelines is sufficient. Such a scenario appears contradictory to the public position of the Ontario government and the OSC which has been recently mandated to reduce regulatory burden, and even created the Burden Reduction Task Force.

Applicable Regulatory Requirements

22. What regulatory requirements, both at the CSA and IIROC level, should apply to Platforms or should be modified for Platforms? Please provide specific examples and the rationale.

In all instances, consultation with the industry should occur in order to ensure effective implementation. Particular care should be given to functionality that is enabled by technology, including:

- Users' ability to hold assets without a third-party custodian,
- The ability to automate audit-related functions,
- The ability to conduct testing and verification using publicly available data (in the case of public blockchains),
- Platforms' ability to deliver real-time disclosures and warnings, and
- Different types of crypto-assets and the suitability of requirements to each type.

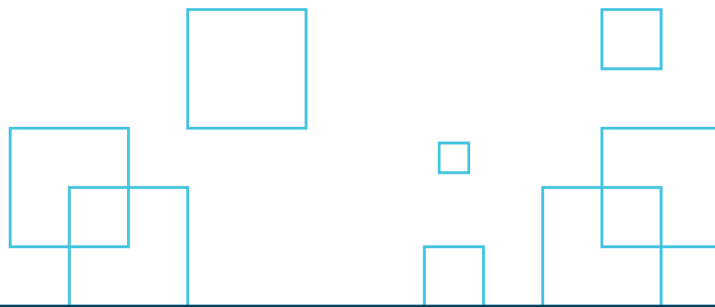
Given the depth and breadth of potential crypto assets a staged approach which first provides clarity in relation to the expectations surrounding digitized or tokenized securities, and the platforms on which they are offered may be the most useful.

The Chamber recommends that an industry and regulator working group be established to further discuss how to approach related questions regarding regulatory requirements at the CSA and IIROC level.

Specific Industry Concerns That Require Attention and Consideration

Bank Accounts and De-risking

For many businesses in Canada, the single greatest barrier to entry is not compliance, technology-related, or other deficiency in vital infrastructure, but instead is obtaining and



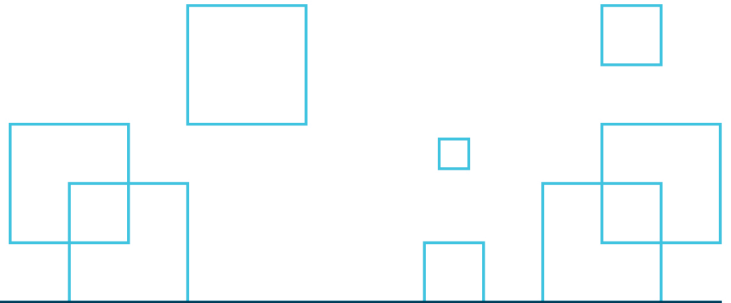
maintaining a stable banking relationship. In one instance, a company obtained a large investment from a consortium which included banks as participant investors. When the investment consortium representative asked the company what they most needed to foster success, the company's CEO confided that they were in need of an operating account in which to deposit the cheque that they had just received. The bank members of the consortium stated that their banks would not open accounts for this type of company as it would contravene the banks compliance and risk policies. In essence, the company was not so high risk that the bank would not invest, but it was too high risk to be able to offer access to a basic banking product. Months of perseverance were required before the company was able to establish a stable banking relationship.

The issue of access to banking is prevalent at both the federal and provincial levels. In some cases, provincial credit unions are prohibited by their service provider from sending electronic funds transfers or wires on behalf of any company that deal in virtual currency. The act of restricting access to stable banking services to these businesses (also known as derisking) creates significant barriers to functions such as audit, insurance, and price discovery. In addition, it may create additional risks for consumers, including the risk that funds become stuck or lost when a relationship is terminated, and the risk that transactions with suppliers in increasingly risky jurisdictions outside of Canada become the norm. In the recent bankruptcy case involving Quadriga CX, a popular Canadian digital currency exchange, the fact that the exchange was insolvent may have been apparent sooner if the exchange had not conducted its affairs through a complex web of payment processors and service providers that are neither as vigilant nor as well-regulated as the Canadian banking sector.

Audits

In many ways, audit markets suffer from similar pitfalls to those suffered in insurance markets. There are not enough qualified personnel, and those that are willing to perform the work charge a premium under current market conditions. In addition, accounting professionals have expressed a need for clarity in order to establish appropriate standards related to digital-assets. We recommend that regulators work closely with one another, as well as with accounting and other relevant oversight bodies for professionals, in order to establish appropriate standards.

Where non-financial audits are being considered (for example security and compliance audits), we encourage clear guidance for service providers, including any relevant regulator expectations related to the scope, methodology, format and content of audit reports (where



applicable). Such guidance is useful in helping professionals to set standards that will be useful to their clients.

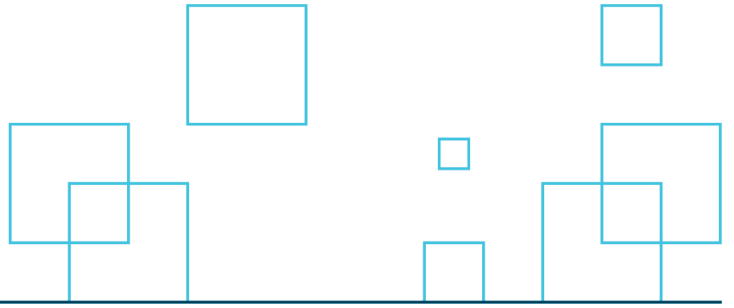
Conclusion & Core Recommendations

The Chamber and its members look forward to working closely with policymakers and regulators across Canada to ensure that Canada’s digital asset and blockchain chain ecosystem is strong and globally competitive.

Providing the clarity required in conjunction with the flexibility to support rapidly-evolving technologies in a nascent industry will require a diligent and nuanced approach. Protecting consumers and the Canadian system are important goals. We should not, however, rush to accomplish such goals at the expense of innovation and opportunity.

As outlined above, we recommend that the CSA, IIROC and relevant policy professionals work to:

1. Recognize that not all digital assets are securities and avoid broad characterization of tokens as securities by starting with the assumption that a token or digital asset may not be a security, commodity or derivative.
2. Establish meaningful industry dialogue, input, and collaborative consultations to create effective and appropriate regulatory regimes for the global, digital marketplace.
3. Establish a task force of experts to work with federal and provincial government policy makers and regulators to fully study and review each distinct aspect of “crypto-exchange” platforms and the broader global token regulatory framework and objectives.
4. Develop objective investor and consumer education tools to help inform the public.
5. Take the time necessary to research and review the global blockchain ecosystem, considering all policy and legislative perspectives, to design and support a competitive blockchain ecosystem in Canada.
6. Coordinate with other policy makers and regulators, including the Department of Finance, FINTRAC, and the Canada Revenue Agency (CRA), to ensure that



regulations are aligned, consistent, and not confusing or overly burdensome to industry.

7. Publish timely and transparent guidance, including guidance related to digital assets that are not considered to be securities, commodities, or derivatives.
8. Where required, take a principles-based, technologically-neutral approach to regulation and policy to foster innovation.

In all cases, regulation and legislation designed to support and strengthen digital asset exchange platforms should be developed in close consultation with industry and supported by detailed and transparent guidance and policy interpretations that can be used by industry in all stages of business from strategy to execution.

We would be happy to provide additional information or answer any questions that you might have in relation to this submission. It is our sincere hope that this consultation is the first in an ongoing dialogue with the industry and that we may serve as a valuable partner in that consultation process.

The Chamber looks forward to ongoing and collaborative dialogue with the CSA and IIROC going forward. Should you have any further questions, we would be pleased to discuss them with you.

Sincerely,



Tanya Woods
Managing Director
Chamber of Digital Commerce Canada



BY ELECTRONIC MAIL: comments@osc.gov.on.ca, consultation-en-cours@lautorite.qc.ca

May 15, 2019

British Columbia Securities Commission
Alberta Securities Commission
Financial and Consumer Affairs Authority of Saskatchewan
Manitoba Securities Commission
Ontario Securities Commission
Autorité des marchés financiers
Financial and Consumer Services Commission of New Brunswick
Superintendent of Securities, Department of Justice and Public Safety, Prince Edward Island
Nova Scotia Securities Commission
Securities Commission of Newfoundland and Labrador
Registrar of Securities, Northwest Territories
Registrar of Securities, Yukon Territory
Superintendent of Securities, Nunavut

The Secretary
Ontario Securities Commission
20 Queen Street West, 22nd Floor, Box 55
Toronto, Ontario M5H 3S8

Me Anne-Marie Beaudoin
Corporate Secretary
Autorité des marchés financiers
800, square Victoria, 22^e étage
C.P. 246, tour de la Bourse
Montreal (Québec) H4Z 1G3

Dear Sirs / Madames:

RE: Consultation Paper 21-402 - Proposed Framework for Crypto-Asset Trading Platforms (the "Consultation Paper")

Thank you for the opportunity to provide feedback to the Canadian Securities Administrators ("CSA") on the Consultation Paper.

Fidelity Clearing Canada ULC ("Fidelity Clearing") is one of Canada's few firms providing execution, clearing, custody and back-office solutions for brokerage firms and portfolio managers. Since 2009, Fidelity Clearing has put its clients and their investors first by working hard to help them achieve their financial goals. We recognize that the CSA is also

committed to improving outcomes for investors and we are pleased to work collaboratively with the CSA toward our shared commitment.

Fidelity Clearing very much supports the CSA in its endeavor to canvass industry guidance on the novel features and risks related to crypto-assets, crypto-currencies and the trading platforms on which they reside. We believe that a fulsome understanding of the crypto trading platforms is necessary to adequately adopt and tailor existing securities regulations.

While we will not be commenting on the Consultation Paper at this time, we continue to maintain a meaningful interest in crypto trading platforms. We are always exploring innovation initiatives to serve the needs of our clients.

We look forward to reviewing the comments on the Consultation Paper and are grateful to the CSA for undertaking such a significant initiative.

Yours very truly,

Fidelity Clearing Canada ULC

“Scott MacKenzie”

Scott MacKenzie
President

May 15, 2019

The Secretary
Ontario Securities Commission
20 Queen Street West
22nd Floor, Box 55
Toronto, Ontario M5H 3S8
Fax: 416-593-2318
comments@osc.gov.on.ca

Me Anne-Marie Beaudoin
Corporate Secretary
Autorité des marchés financiers
800, square Victoria, 22e étage
C.P. 246, tour de la Bourse
Montréal (Québec) H4Z 1G3
Fax : 514-864-6381
Consultation-en-cours@lautorite.qc.ca

IIROC
Victoria Pinnington
Senior Vice President, Market Regulation
Investment Industry Regulatory Organization of Canada Suite 2000
121 King Street West
Toronto, Ontario M5H 3T9
vpinnington@iiroc.ca

To Whom It May Concern:

Re: Joint Canadian Securities Administrators/Investment Industry Regulatory Organization of Canada - Consultation Paper 21-402 - Proposed Framework for Crypto-Asset Trading Platforms

The following comments are submitted in response to Consultation Paper 21-402 (the "**Consultation Paper**"), the joint consultation paper and request for comments published by the Canadian Securities Administrators (the "**CSA**") and Investment Industry Regulatory Organization of Canada ("**IIROC**") on March 14, 2019, with respect to the establishment of a regulatory framework for platforms that facilitate the buying and selling or transferring of crypto assets ("**Platforms**").

Thank you for the opportunity to submit the following comments on the Consultation Paper. I am writing this letter in my personal capacity. My perspective is derived from my experience in legal, regulatory and business consulting in the crypto assets industry, as a core focus area,

and my active engagement in the industry, including through roles at a high tech consultancy and as an independent consultant. I also sit on the Advisory Committee for the Blockchain Program at George Brown College. My perspective is further derived from my professional experiences as a General Counsel in financial services in wealth management, including traditional funds as well as crypto asset investment funds. Given my perspective and professional experience in law, securities regulation, financial services and crypto assets, my goal is to offer a neutral perspective based on an appreciation of the issues and the various stakeholder perspectives involved.

OVERVIEW

I commend the CSA and IIROC on their efforts to facilitate innovation that benefits investors and the capital markets, keep pace with evolving markets, provide regulatory clarity to crypto asset businesses, while addressing investor risk and market integrity. I appreciate the consideration given in the Consultation Paper to the existence of novel features in relation to crypto assets, the desirability of industry tailored rules and the acknowledgement of the existence of operators who would like to comply, who have approached the regulators and who welcome some form of regulatory framework to legitimize their businesses and to help their businesses grow.

There is no shortage of opinions on crypto assets. Some see the industry as defined by investment scams. Others see it as revolutionary, efficient, and more technologically advanced, with significant potential across business and human rights. The underlying distributed ledger technology holds promise also, specifically, for regulators, including in enabling transparency with the future potential to avert or mitigate systemic and other risks.

Notwithstanding the above, the promise of innovation should warrant a balanced and thoughtful approach, but not a complete regulatory free pass particularly where retail investors are involved. Policy-maker consensus, for example, according to the Financial Stability Board, is that financial stability is not a current risk in light of industry size, volume and financial system interconnectedness, at least at this time. However, investor protection objectives and concerns are understandably paramount, including in the aftermath of Quadriga CX.

I am of the view that it is in the best interests of the crypto assets industry and investors for industry to collaborate with regulators and to work towards an appropriate regulatory, governance and accountability framework. I agree that it is necessary to consider appropriate governance models for Platforms and to examine ways to address the risks and governance gaps in the current framework. At the same time, I would urge the CSA and IIROC to consider alternative models for a regulatory framework, including of self-regulation combined with industry certifications.

GENERAL RECOMMENDATIONS

The following represent several general recommendations.

- **Learn from the experiences of other jurisdictions** - The fragmentation of regulatory rules in the United States, for example, between states and between regulators has caused so much frustration that the Token Taxonomy Act has been proposed (and reintroduced) as a solution. It is authored and sponsored by members of Congress, and it appears to have some level of support from blockchain technologies, Washington, D.C.-based think tank, Coin Center. The Token Taxonomy Act seeks to roll back and wipe off the books state cryptocurrency laws including a significant amount of work that was already accomplished to create state legislative regimes, such as the New York State BitLicense (which has been referred to as heavy handed) and the five bills passed in the more permissive state of Wyoming. Canada would not necessarily be invulnerable to similar potential problems arising. There is currently some absence of harmonization in traditional Canadian securities regulatory rules, for example, in the exempt market. Also, such regulatory areas as anti-money laundering could result in confusion where we currently see FINTRAC and the securities regulators all simultaneously enacting or proposing new rules, each of which will implicate business classifications and KYC/ AML expectations. Lack of clarity around business classification under securities regulatory rules could, for example, result in confusion around categorization and compliance with FINTRAC expectations. Problems could arise with inconsistent rules across geographic lines, within Canada as well globally given the global nature of this technology and business economy, or between and amongst regulators within the same jurisdiction (such as the CSA, IIROC, FINTRAC and CRA). A multi-constituent, collaborative dialogue and approach, with the objective of advancing harmonized, clear and consistent rules, will help to avoid problems with incompatible or fragmented rule-making.
- **Consider intervention and/or education in the broader business ecosystem** - As a matter of investor protection, and as a matter of enabling compliance with potential new rules, certain products or services normally required by traditional securities regulatory rules may not be attainable, or reasonably and feasibly attainable, by Platforms. For example, if certain insurance coverage isn't available to Platforms, or is only available to a few of the very largest entities, the rendering of this industry non-compliant, or monopolistic, or pushing business underground, all constitute potential consequences which would be unintended and undesirable. France, as one example, decided that it would be good public policy to require that its banks bank blockchain companies, in a fashion that bears similarity to a comply or explain model. Similar tactics could be considered in Canada for certain critical services. Consideration and investigation of the gaps and deficiencies within the broader business infrastructure and ecosystem, combined with thoughtful and balanced rules, can help to achieve regulatory objectives.

- **Consider the potential for creative alternatives in order to fill business and ecosystem gaps** - On May 7, 2019, Binance, a global cryptocurrency exchange and one of the largest exchanges in the world by trading volume, suffered a large scale hack worth around \$40 million USD in bitcoin, as a result of what was apparently a well orchestrated attack. Binance has confirmed that it will compensate investors fully for all moneys stolen as a result of the attack using the Binance Secure Asset Fund. In July of 2018, Binance announced the creation of its Secure Asset Fund for Users (SAFU) as insurance to protect users in the event of such potential situations. It explained its intention to self-fund the SAFU using 10% of all trading fees earned by Binance. That plan has presumably been effective as it is enabling the full reparation of investors, as a thoughtful and considered solution selected by Binance, amongst several alternatives that it considered. This case could be used to set an example for others to follow, or for industry to implement in an organized and enforced fashion, such as through a third party agency that could establish a similar emergency investor fund, funded by industry, for use in specified emergency cases and where insurance isn't otherwise available to step in.
- **Consider, as an alternative model, formation of a dedicated third party agency** - Illustrations and variations of this concept include Osgoode's Professor Allan Hutchinson discussion, in his response letter, of what he refers to as a QUANGO. He describes and proposes a quasi-autonomous non-governmental organization to function separate from government but have ties to and representation from government, and to have primary and sole responsibility for regulating cryptocurrency.

The Japan model is notable in this regard. Japan granted to the cryptocurrency exchange industry self-regulatory status. Japan provided authority to the self-regulatory body, the Japan Virtual Currency Exchange Association, over rule-making, policing and sanctioning of cryptocurrency exchanges.

There are several reasons why this model - a separate, dedicated agency - would be more beneficial than the traditional regulatory model. A dedicated and specialized entity can stay close and connected to the industry, the technology and the international developments, which is necessary in this evolving, nascent, fast moving and high tech space. If primary authority was instead retained with the CSA and IIROC, will the regulators have adequate resources (including financial and specialized, multi-disciplinary and technical personnel with specific expertise in crypto assets) in order to effectively carry out all initial and ongoing obligations, including monitoring? As noted by Neil Gross in the Comments of the Investor Advisory Panel to the Consultation Paper, regulators will be required to "continually build knowledge and capacity to stay on top of technological innovation and understand its potential impact on investor outcomes and vulnerabilities". The combination of the technical complexity, industry nuances, speed of change and global scale could prove to be very onerous in the context of limited, partial or split resources. And although in terms of size the industry is not systemically

important yet, it is quickly growing. Establishing an appropriate dedicated, self-regulatory body sooner than later would help to stay ahead of market and regulatory needs.

On vision and reasoning, I also agree, in particular, with the comments of James Herhaw on behalf of Crowdmatrix Inc. within their response letter, including but not limited to the following proposal reasoning in advancing the concept of a dedicated federal taskforce and industry specific laws:

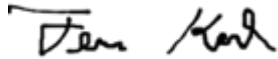
“A federal taskforce to address all the Digital Assets issues would likely be more focused, better funded and better able to interact with other global leaders than the CSA coalition and the IIROC SRO that is funded by an existing subset of private Canadian registrants in the capital markets ecosystem. Developing new federal legislation can utilize existing principles but also consider new approaches to regulation.”

- **Consider including in any new industry regulatory framework relevant reforms that are being implemented or accepted in traditional financial services** - For example, in accordance with the OSC Regulatory Burden Reduction Roundtable, a chief compliance officer (“CCO”) should be allowed to work part-time for more than one smaller firm, so that several firms may share a single experienced CCO. I commend the OSC for engaging in this reform. This is beneficial to any industry and particularly to newer industries, such as crypto assets, which could benefit from flexibility in retaining experienced compliance and regulatory personnel. The alternative, i.e. prior model, can often result in an inferior outcome, not specific to the technology sector but also in financial services. It is not infrequently the case that a CEO, who is also the CCO, and who might have significant business experience but negligible compliance experience, wears multiple hats and must balance the internal conflict in being concurrently, effectively, the “Chief Sales Officer” and the “Chief Compliance Officer”. The foregoing is not intended as a generalization about all CEOs but rather a commentary on the unintended consequences of the traditional one registrant rule and the rule’s not too uncommon impact. Advancing this more innovative and flexible approach can be of great benefit to many industries, including crypto assets.

CONCLUSION

I commend the CSA and IIROC for their community outreach with this Consultation Paper. I support the CSA's objectives in investor protection, market integrity and reducing regulatory uncertainty as articulated in the Consultation Paper. I welcome any opportunities to assist and I am appreciative of being afforded this opportunity to comment. If you require any further information, please do not hesitate to contact me at fern@fermkarsh.com.

Yours truly,

A handwritten signature in black ink that reads "Fern Karsh". The signature is written in a cursive, slightly slanted style.

Fern Karsh

1. Are there factors in addition to those noted in Part 2 that we should consider?

<No Comment>

2. What best practices exist for Platforms to mitigate the risks outlined in Part 3? Are there any other significant risks which we have not identified?

- **Problem:** Individuals have the ability to create Initial Coin Offering (ICO) or Security Token Offering (STO), and platforms have the ability to create initial exchange offerings (IEO)s. Due to their ease of creation, and users inability to determine if projects are real, creates many risks. One risk is the ICO/IEO/STO founders have many tokens and can use them to pump and dump a platform's market. Another risk is ICO/IEO/STO founders create a fake company and use their worthless cryptocurrency to purchase other cryptocurrency or fiat.
 - **Potential Solution:** On regulated platforms only allow approved cryptocurrencies. An "approved cryptocurrency" could be different depending on: if the cryptocurrency is centralized or decentralized, that cryptocurrencies consensus mechanism, and likelihood that the founders (if the cryptocurrency was centralized) are creating a real product.
- **Problem:** An exchange could be initiating trades between itself to create transaction volume on that exchange.
 - **Potential Solution:** Internal controls must be in place and used, users of the exchange must be verified, and parties related to the exchange must be identified.
- **Problem:** Exchanges keep user data on site, and may not have appropriate safeguards to secure that information (Driver licences, utility bills, etc.)
 - **Potential Solution:** Using a service like Verified.Me to confirm a user rather than sending sensitive information to an entity that might not have proper security in place to store user data.
- **Problem:** Some cryptocurrencies are susceptible to a 51% attack. That is why most cryptocurrency exchanges have a minimum confirmation height for a deposited cryptocurrency before it can be traded on that exchange.
 - **Potential Solution:** Before a cryptocurrency is accepted for trading on an exchange there should be a minimum amount of confirmations. The amount of confirmations for each cryptocurrency should be different, and based on a type of economic model (i.e. if the cost of a 51% attack is \$1 million dollars based on the amount of confirmations needed, network hashing power and current price, then total deposits over x amount being confirmed by the exchange should take longer so that an attack

would be more costly than the benefit that would be received from the attack.). The amount of confirmations needed for each cryptocurrency should be dynamic and conservative.

- Problem: Banks submit suspicious transaction reports to FINTRAC for fiat transactions; however, there is no reports submitted for suspicious cryptocurrency transactions. This has the potential for people in illicit activities to wash their money through a platform.
 - Proper regulation and infrastructure needs to be in place to deal with these types of transactions, but a potential short-term solution could be to:
 - #1 – Only allow current transactions to the platform where the 2nd prior transaction is more than a day old, and transactions where the 2nd prior transaction is less than a day old to not accept the transaction to the platform. This will prevent individuals from creating multiple addresses in order hide the source of the cryptocurrency right before they post the transaction to the exchange. Some exceptions that could shorten this time could be “when received from an approved exchange that is follow these regulations” also some things that could increase the time might be “When crypto assets were involved in a mixing service or atomic swap”.
 - #2 – Also have a reporting page where investors can indicate crypto assets have been stolen or were involved in a fraud. This will be tricky to manage as people could use this site to mess around with legitimate crypto assets. Therefore, the identity of the individual would need to be known, proof of ownership (can be proved by signing addresses where incident happened from), and a report of what happened.
- Problem: To my knowledge bank accounts involved in cryptocurrency activities cannot be opened in Canada, and owners of exchanges open bank accounts in other countries to get around this problem. This causes many issues, as an exchange in Canada that has Canadian assets do not hold those assets in Canada.
 - Potential Solution: Provide a way for platforms to hold funds in Canada
- Problem: As mentioned there are no suspicious transaction reports for cryptocurrencies, and the source of an asset is just as important when talking about fiat as it is when talking about cryptocurrencies.

For example, if someone received fiat for human trafficking, we would want to treat cryptocurrency received for human trafficking in the same way. This is a direct causality (i.e. proceeds of human trafficking = cryptocurrencies).

However, we also need to think of indirect causality when discussing this topic (i.e proceeds of human trafficking were used to create a cryptocurrency mining facility, and this mining facility produces newly minted cryptocurrencies).

- Potential solution: Source of cryptocurrencies would need to be provided and could potentially be audited. So there would need to be some potential regulations around this auditing process.
- Problem: Retailers may accept cryptocurrencies for goods and services, but allow cryptocurrencies from illicit services. The retailer might then try to sell the cryptocurrencies on the platform and the platform rejects the transaction.
 - Potential solution: If a retailer uses a cryptocurrency payment processor that payment processor could be responsible to have KYT, and reject cryptocurrency from an illicit source.

Many of the above problems echo the report “Why We Fail to Catch Money Launderers 99.9 percent of the Time” released on May 7, 2019:

https://www.cdhowe.org/sites/default/files/attachments/research_papers/mixed/Final%20for%20release%20e-brief_291_web%20%28003%29.pdf

3. Are there any global approaches to regulating Platforms that are appropriate to be considered in Canada?

<No Comment>

4. What standards should a Platform adopt to mitigate the risks related to safeguarding investors’ assets? Please explain and provide examples both for Platforms that have their own custody systems and for Platforms that use third-party custodians to safeguard their participants’ assets.

Some applicable standards to consider, are those of the Cryptocurrency Certification Consortium: <https://cryptoconsortium.org> located at: <https://cryptoconsortium.github.io/CCSS/> (Full disclosure I have my CBP from this body).

5. Other than issuance of Type I and Type II SOC 2 Reports, are there alternative ways in which auditors or other parties can provide assurance to regulators that a Platform has controls in place to ensure that investors’ crypto-assets exist and are appropriately segregated and protected, and that transactions with respect to those assets are verifiable?

To determine the minimum amount of cryptocurrency an exchange controls, and the amount of liability the exchange has from holding its customers cryptocurrencies a Proof-of-Reserve may be performed. Auditors performing normal audit testing with proof-of-reserve testing could provide assurance. Proof-of-reserve only works from an assurance standpoint if all cryptocurrencies offered by an exchange are reviewed at the same point in time. More information on proof-of-reserve can be found at:

- a. https://www.lopp.net/pdf/princeton_bitcoin_book.pdf “Bitcoin and Cryptocurrency Technologies” Pages 115 to 118
- b. <https://www.kraken.com/proof-of-reserves-audit>

6. Are there challenges associated with a Platform being structured so as to make actual delivery of crypto assets to a participant’s wallet?

The question depends of the services the platform provides. If a platform only offers crypto to crypto trading there is no challenge in structuring an exchange to allow an investor to send crypto from their wallet to receive another type of crypto directly to that investor’s wallet. However, for crypto to fiat transactions this does pose challenges as a centralized party is needed to store and distribute the fiat of the investors.

What are the benefits to participants, if any, of the Platforms holding or storing crypto assets on their behalf?

1. There is the benefit of convenience in allowing an investor to store their assets on a platform. If the investor did not want to store their cryptocurrencies on an exchange, they would need to create an address for that particular cryptocurrency, and then need to safe guard it (i.e. create a backup of the private key/seed, and physically secure it against thief).
2. If the assets are kept on a platform the investor can react quicker to market changes.
3. History has shown that storing cryptocurrencies on a platform is less safe than an individual personally holding their cryptocurrencies.

7. What factors should be considered in determining a fair price for crypto assets?

<No Comment>

8. Are there reliable pricing sources that could be used by Platforms to determine a fair price, and for regulators to assess whether Platforms have complied with fair pricing requirements? What factors should be used to determine whether a pricing source is reliable?

<No Comment>

9. Is it appropriate for Platforms to set rules and monitor trading activities on their own marketplace? If so, under which circumstances should this be permitted?

<No Comment>

10. Which market integrity requirements should apply to trading on Platforms? Please provide specific examples.

<No Comment>

11. Are there best practices or effective surveillance tools for conducting crypto asset market surveillance? Specifically, are there any skills, tools or special regulatory powers needed to effectively conduct surveillance of crypto asset trading?

In addition to know your customer (KYC), there is surveillance software that allows for know your transaction (KYT). KYT can allow exchanges to reject cryptocurrency from address or known illicit activities or frauds.

12. Are there other risks specific to trading of crypto assets that require different forms of surveillance than those used for marketplaces trading traditional securities?

At this time not all cryptocurrencies have surveillance software. This creates a risk of not being able to track some cryptocurrencies.

13. Under which circumstances should an exemption from the requirement to provide an ISR by the Platform be appropriate? What services should be included/excluded from the scope of the ISR? Please explain.

<No Comment>

14. Is there disclosure specific to trades between a Platform and its participants that Platforms should make to their participants?

<No Comment>

15. Are there particular conflicts of interest that Platforms may not be able to manage appropriately given current business models? If so, how can business models be changed to manage such conflicts appropriately?

<No Comment>

16. What type of insurance coverage (e.g. theft, hot-wallet, cold-wallet) should a Platform be required to obtain? Please explain.

<No Comment>

17. Are there specific difficulties with obtaining insurance coverage? Please explain.

<No Comment>

18. Are there alternative measures that address investor protection that could be considered that are equivalent to insurance coverage?

<No Comment>

19. Are there other models of clearing and settling crypto assets that are traded on Platforms? What risks are introduced as a result of these models?

<No Comment>

20. What, if any, significant differences in risks exist between the traditional model of clearing and settlement and the decentralized model? Please explain how these different risks could be mitigated.

<No Comment>

21. What other risks could be associated with clearing and settlement models that are not identified here?

<No Comment>

22. What regulatory requirements (summarized at Appendices B, C, and D), both at the CSA and IIROC level, should apply to Platforms or should be modified for Platforms? Please provide specific examples and the rationale.

<No Comment>

Roger Miller

May 15, 2019

BY EMAIL

British Columbia Securities Commission
Alberta Securities Commission
Financial and Consumer Affairs Authority of Saskatchewan
Manitoba Securities Commission
Ontario Securities Commission
Autorité des marchés financiers
Financial and Consumer Services Commission (New Brunswick)
Superintendent of Securities, Department of Justice and Public Safety, Prince Edward Island
Nova Scotia Securities Commission
Securities Commission of Newfoundland and Labrador
Superintendent of Securities, Northwest Territories
Superintendent of Securities, Yukon
Superintendent of Securities, Nunavut

Dear Sirs/Mesdames:

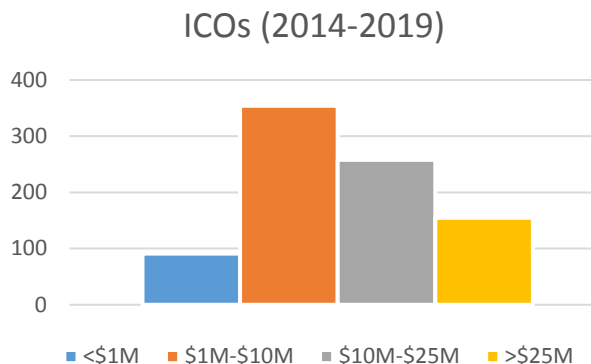
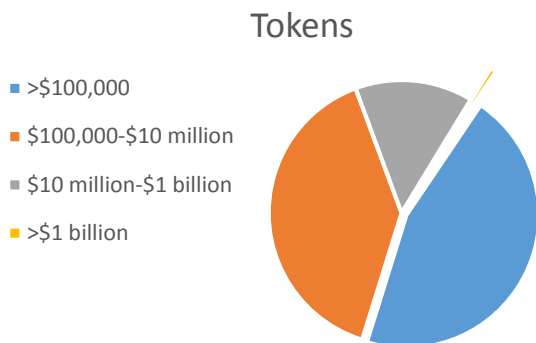
Re: **Joint Canadian Securities Administrators/Investment Industry Regulatory Organization of Canada
Consultation Paper 21-402 Proposed Framework for Crypto-Asset Trading Platforms**

First and foremost, we wish to thank the Canadian Securities Administrators (“CSA”) and the Investment Industry Regulatory Organization of Canada (“IIROC”) for the opportunity to comment on how the regulatory environment should govern crypto-token trading platforms.

SoapBox is a video distribution platform driven by blockchain technology. It is constructed around an expansive peer-to-peer network where content creation, storage and delivery is handled by a community incentivized by receiving tokens mined in a unique blockchain network. By either creating its own trading platform or allowing a third-party trading platform, SoapBox allows the tokens in its ecosystem to be exchanged for fiat currency. Given our business model, we welcome a better regulatory understating of how to affect or partner with trading platforms to allow for a seamless monetization experience for our community.

Before we comment on the questions posed by the CSA/IIROC, we would like to raise some issues we feel are relevant.

Market Capitalization Distribution of all Crypto-Tokens



The charts above show i) the current market capitalization of tokens currently in circulation and ii) the number of ICOs that have been issued in ranges shown.

Both charts suggest that most circulated tokens are relatively modest in value. This is important because regardless of how media has sensationalized the ramp-up of crypto-tokens and the related security breaches, the market in comparison is more tempered (outside of some known outliers such as Bitcoin).

In that vein, we feel there should be proportionate application of scrutiny from the regulatory authorities depending on the market capitalization of the token. A one-size-fits-all approach will stifle innovation in the crypto-asset area and allow beneficial projects to die out in their infancy. It will also cause platforms to seek out other less-stringent jurisdictions and possibly endanger investor proceeds.

Classification of Offerings as distributions of securities

We ask the regulatory authorities to better define the test concerning when an offering of utility tokens constitutes a distribution of securities. Much like a publisher pre-sells an upcoming book or an event pre-sells early bird tickets to a concert, there are instances where an initial offering of utility tokens does not invoke securities legislation. In fact, instead of seeking funding, an ICO’s primary motivation can be to create a network of users.

There is also no guidance from the authorities on whether subsequent offerings of a utility token where the token is established also classifies as a distribution of securities.

Question 1 - Are there factors in addition to those noted above that we should consider?

- i) As the case in *Pacific Coast Coin Exchange v. Ontario Securities Commission*, [1978] 2 S.C.R. 112, there should be clear distinction between full and partial delivery subject to conditions. The courts were clear that in the latter case, it involved an investment contract.
- ii) If there is delivery it is important to assess who bears the pricing risk between the trade and settlement – the Platform or its participant. We should point out that given the inherent nature of crypto-token transactions, there is a market-governed transaction cost that may fluctuate before settlement.

Question 2 – Question 4

No comment.



Question 5 - Other than the issuance of Type I and Type II SOC 2 Reports, are there alternative ways in which auditors or other parties can provide assurance to regulators that a Platform has controls in place to ensure that investors' crypto-assets exist and are appropriately segregated and protected, and that transactions with respect to those assets are verifiable?

A significant amount of effort and time is required to obtain a Type II Report—including receiving a Type I Report first. Furthermore, the paper does not comment on which principles the Type II Report should be assessed on, but we assume at least Security and Availability. As stated in the paper, this type of audit will be challenging given the infancy of most of the Platforms.

As stated earlier in our response, we are of the position that there be a tiered system of compliance to such requirements, depending on the market capitalization of the token, the complexity of the crypto-token, the number of existing ledgers and velocity of transactions and the number of token participants.

Question 6 - Are there challenges associated with a Platform being structured so as to make actual delivery of crypto assets to a participant's wallet? What are the benefits to participants, if any, of Platforms holding or storing crypto assets on their behalf?

The inherent problem revolves around private keys. If the key is stolen or lost, the participant could possibly lose the crypto-token and the associated value. Much like cash, it can be challenging to prove chain of custody after the fact.

In the same way a bank is a safer venue for money, we believe it is safer to keep the tokens in the Platform, specifically its internal or external custodian, than to keep the crypto-token in a home computer.

Question 7 - What factors should be considered in determining a fair price for crypto assets?

- i) Utility – With respect to utility crypto-tokens, the fungibility of the token into a portfolio of services lends itself to better price determination on a Platform. The more niche the service, the less likely a utility crypto-tokens will be embraced by users which will affect price.
- ii) Mining Difficulty/Coin Circulation - It is important to understand the scarcity of the tokens whether artificially set or the cost of mining. For instance, the current operational cost of mining one bitcoin is approximately between \$4,000 to \$6,000 USD. The hardware required to mine is approximately \$150,000 USD. Disclosure on mining activity is key for price determination.
- iii) Transaction Speed/Cost – Depending on how expensive or cheap the transaction fee is will determine the attractiveness of crypto-tokens trading and therefore price discovery.
- iv) Regulations – While both giving confidence to the market, regulations can also strangle the market and therefore cause poor price discovery.
- v) Macro Factors – external factors such as the economy, prices of other crypto-tokens and market speculation will affect price.

Question 8 - 15

No comment

Question 16 - What type of insurance coverage (e.g. theft, hot-wallet, cold-wallet) should a Platform be required to obtain? Please explain.

Crime, Errors & Omissions and Cybersecurity insurance coverage should be considered for the custodian (internal or external). The exchange portion of the Platform would presumably be more resistant to widespread fraud, human error or data breaches.



Question 17 - Are there specific difficulties with obtaining insurance coverage? Please explain.

Traditional insurance coverage might be difficult to obtain. As with the Type I/II Reports given that each token has its own peculiarities, startups in this area might find insurance carriers unwilling to cover or charging too high an insurance premium.

Question 18 – Question 22

No comment

Conclusion

SoapBox would like to thank the CSA and IIROC again for the consultation to the proposed framework. It is key that the regulators give more certainty to the market and give comfort to both investors and the financial services industry in how crypto-tokens are to be incorporated into the securities framework.

If you require any clarification or further comments, please contact us at info@soapbox.net

SoapBox Network Inc.





TO: Canadian Securities Administrators
Investment Industry Regulatory Organization of Canada

FROM: DV Chain, LLC

DATE: May 15, 2019

RE: Joint Canadian Securities Administrators/Investment Industry Regulatory Organization of Canada Consultation, Paper 21-402 *Proposed Framework for Crypto-Asset Trading Platforms* (March 14, 2019)

Dear Sir/Madam:

This letter is offered in response to the Joint Canadian Securities Administrators (“CSA”) /Investment Industry Regulatory Organization of Canada (“IIROC”) Consultation (Paper 21-402 Proposed Framework for Crypto-Asset Trading Platforms) (the “Proposal”). DV Chain, LLC, a CSA’s request for comments on their Consultation Paper 21-402, the “Proposed Framework for Crypto-Asset Trading Platforms”. The undersigned at DV Chain, LLC (“DV Chain”), a proprietary cryptocurrency trading desk and an affiliate of Independent Trading Group (ITG) Inc., a registered IIROC dealer (“ITG”), respectfully offer the following comments addressing the questions posed in the Proposal.

PART 2 – Nature of crypto assets and application of securities legislation

DV Chain agrees that the determination of a crypto asset’s categorization as a security, derivative, commodity, or alternative investment asset, is essential to understand the appropriate regulatory framework which should be applied to the specific facts and circumstances. As such, in addition to the factors enumerated in the Proposal, DV Chain wishes to expound on the list with the following:

As early as 2013, the U.S. Commodity Futures Trading Commission (the “CFTC”) has promulgated both formal guidance and agency rulings that bitcoin and other virtual currency is a commodity.¹ Various US federal rulings and statements by other US regulators, i.e. the Securities and Exchange Commission (the “SEC”) and the Financial Crimes Enforcement Network (“FinCEN”) have extrapolated from CFTC guidance to affirm this classification to encompasses any digital representation of value (a “digital asset”) that functions as a medium of exchange, and any other digital unit of account that is used as a form of a currency (i.e., transferred from one party to another as a

¹ *In re Coinflip, Inc., d/b/a Derivabit, and Francisco Riordan*, CFTC Docket No. 15-29, 2015 WL 5535736, [Current Transfer Binder] Comm. Fut. L. Rep. (CCH) ¶ 33,538 (CFTC Sept. 17, 2015) (consent order); *In re TeraExchange LLC*, CFTC Docket No. 15-33, 2015 WL 5658082, [Current Transfer Binder] Comm. Fut. L. Rep. (CCH) ¶ 33,546 (CFTC Sept. 24, 2015) (consent order).

medium of exchange); may be manifested through units, tokens, or coins. Notably, this excludes certain utility tokens which may be deemed securities.

Per the US Commodity Exchange Act (the “CEA”), the CFTC has broad regulatory jurisdiction over “retail commodity transactions.”² A retail commodity transaction may be excepted from CEA section 2(c)(2)(D) (and thus not subject to CEA sections 4(a), 4(b), and 4b) if actual delivery of the commodity occurs within 28 days of the transaction.³

The Canadian parallels to US regulation are quite clear. More specifically, the Ontario Securities Commission (“OSC”) Rule 91-506, 2 (1) (d), which discusses a *product’s determination (if securities legislation applies)*, states that a contract or instrument is prescribed not to be a derivative if it is (quoting in pertinent part):

a contract or instrument for delivery of a commodity other than cash or currency that,

- (i) is intended by the counterparties, at the time of execution of the transaction, to be settled by delivery of the commodity, and*
- (ii) does not allow for cash settlement in place of delivery...*

In Canada, like in the US, if a commodity is not intended to be delivered, at the time of execution, it is deemed to be a derivative and therefore applicable securities legislation applies. It is clear, in both the spirit of the rule and accepted practice, that for a commodity that is intended to be delivered (such as gold, silver, platinum, palladium, diamonds, etc.), securities legislation would not apply, and the commodity would be treated as a spot commodity product. Therefore, a crypto asset that is intended to be delivered, would not be a derivative and should not be subject to securities legislation (i.e. treated no different than gold, silver, platinum, palladium, diamonds, etc.).

The meaning of “delivery” for crypto assets is an area which needs further explanation. This is best illustrated by comparing a crypto asset (like bitcoin) to a traditional commodity (like gold). If a client buys gold from an online platform, and that gold is:

- delivered (within a reasonable time frame) to a client approved vault;
- the client has first rights (and legal title) to the specific quantity of gold he/she just purchased which is now being held in that vault;
- (and further evidence of legal title is demonstrated by segregation of the client’s gold from the firm’s own assets and routine third-party audits of the vault to ensure physical existence of such gold),

then the gold has met the delivery requirement such that it is clearly a commodity and securities legislation does not apply.

Similarly, if a client buys bitcoin from an online platform, and that bitcoin is:

² CEA section 2(c)(2)(D)(i) captures any such retail transaction “entered into, or offered ... on a leveraged or margined basis, or financed by the offeror, the counterparty, or a person acting in concert with the offeror or counterparty on a similar basis.”

³ 7 U.S.C. 2(c)(2)(D)(ii)(III)(aa).

- delivered (within a reasonable time frame) to a client approved wallet, evidenced by an “on-chain transaction”⁴, (preferably) in cold storage, and custodied by a third party;⁵
- the client has first rights (and legal title) to the specific quantity of bitcoin he/she purchased which is now being held in that wallet (or cold storage facility);
- (and further evidence of legal title is demonstrated by segregation of the client’s bitcoin from the firm’s own assets and routine third party audits of the wallet and cold storage to ensure “physical” existence of such bitcoin),

then the bitcoin, similar to gold, has met the delivery requirement such that it is clearly a commodity and securities legislation would not apply.

PART 3 – Risks related to Platforms

DV Chain agrees with the CSA’s comprehensive list of risks related to crypto asset platforms and has several comments responding to the question of best practices to mitigate such risks:

- **Investors’ crypto assets may not be adequately safeguarded.** DV Chain believes this risk has the potential to jeopardize the legitimacy of the entire crypto industry. One way to mitigate this risk is to require all online trading platforms to contract custodial services to a third party who can demonstrate adequate processes and procedures to safeguard their clients’ assets and be subject to routine (annual) audits, unless the platform can demonstrate adequate processes and procedures itself. For example, if an online trading platform is holding more than \$10,000,000 in clients’ assets, then it should be required to have a SOC2 Type1 report, demonstrating its minimum required competency. There are three crypto-custodians today that have obtained this minimum requirement, meaning that there are auditing firms performing this function. Furthermore, all third party custodians holding more than \$10,000,000 in clients’ assets should also be SOC2 Type1 certified.
- **Processes, policies and procedures may be inadequate.** With respect to the processes, policies and procedures for safeguarding clients’ assets, it is essential to create best practices, as discussed above. DV Chain also believes online trading platforms with more than \$10,000,000 of assets⁶ should have an annual financial audit, testing the adequacy of the firm’s accounting procedures and controls. With respect to more standard business processes, policies and procedures, DV Chain believes the industry will weed out those participants without adequate processes and procedures, leaving only institutional, professional firms in the space.
- **Investors’ assets may be at risk in the event of a Platform’s bankruptcy or insolvency.** All online platforms must record their clients’ assets separate and totally segregated from the Firm’s own assets. Furthermore, the Client Agreements must clearly state that all clients’ have full title to their assets. If investors wish to risk trading with online trading platforms that are

⁴ Where the crypto assets are held at a third party custodian and wallet service provider, and a transaction is done between two or more clients within the same custodian, then no “on-chain” transaction is required because its neither efficient nor practical (just like if gold was traded between two or more clients using the same vault, only an entry to the books and records of the vault provider is made).

⁵ To be discussed in more detail later, although we believe the custody function for Bitcoin, which is analogous to the vault function for gold, should be performed by a trusted third party custodian and wallet service provider, we believe it is not 100% necessary.

⁶ Clients’ assets held by themselves or on behalf of their clients with a third party custodian.

operating in foreign jurisdictions, they can if they wish, but they are subject to the perils of doing so; notwithstanding, there must be legal reach to prohibit foreign online trading platforms from doing business in Canada that do not comply with our new standards.

- **Investors may not have important information about the crypto assets that are available for trading on the Platform.** DV Chain agrees that platforms should maintain standard evaluations for all crypto assets they provide access to. The evaluation should include a description of the crypto asset and references to its backing project. Platforms should also provide clear policy around the handling of forks, airdrops and other events of relevance to these assets.
- **Investors may not have important information about the Platform's operations.** DV Chain believes the safekeeping of all clients' assets is of upmost importance. Simple disclosure describing the custody and wallet process, which we've already explained above, should be mandatory. Trading fees along with other ancillary fees (such as deposit fees, withdrawal fees, etc.) are all relatively easy to ascertain and usually posted on existing online crypto trading platform websites. If fees are not disclosed and/or the fees are too high, investors already have sufficient choices in the marketplace and ultimately, like in the FX business, (with everything else equal) the platforms with the best prices and cheapest fees will prevail.
- **Investors may purchase products that are not suitable for them.** DV Chain's view, similar to that of any traditional commodity business, provided there is no misleading information, it is "buyer beware".
- **Conflicts of interest may not be appropriately managed.** In the crypto asset trading industry, just like any traditional commodity trading business, for example the buying and selling of cars, small boats, physical food products such as dairy, meat, or even agricultural products, trading as principal is both accepted and fair. It is very common for the "middleman" Commodity Trader to take on principal risk and buy the goods in advance (whether it's a car, a small boat, tons of cheese or meat) in anticipation of selling it shortly thereafter to their client at a profit. This isn't disclosed, it is simply expected. Similarly, in the crypto asset space that are not securities or derivatives, there are many OTC trading desks that exclusively trade as principal. It is common and well understood. The clients (or Investors or counterparties) to the OTC trading desk all understand this fact and can easily compare prices with other OTC desks to ensure they are receiving fair prices. It is our view that online crypto trading platforms, which are analogous to an electronic OTC crypto trading desk, should simply disclose that they may be acting as principal on some of their clients' transactions.
- **Manipulative and deceptive trading may occur.** The CSA and the CFTC have already reminded the crypto trading industry that the provisions of their legislation relating to fraud, market manipulation, and misleading statements apply to the underlying commodities (i.e. Bitcoin or any crypto asset that is deemed to be a commodity). Said another way, the rules are already set. A RSP (such as IIROC) can be delegated the responsibility of enforcing these rules to prohibit illegal activities such as spoofing, wash trading, layering, banging the close, etc., and it's our recommendation for that to be the case. To be more specific, it is our recommendation that the monitoring be self-administered, with routine (monthly) reporting of transactions to the RSP to ensure compliance with existing rules.
- **There may not be transparency of order and trade information.** In the trading of physical commodities, there is no requirement to provide order and trade transparency. So, in instances when it is determined that the online crypto trading platform is trading crypto assets that are

deemed to be a commodity (and not a security or a derivative), then we believe there should be no requirement for ensuring the client has “efficient price discovery”. Just like trading gold, or silver, or cars, or small boats, or any physical commodity, it is up to the buyer (or seller) to ensure they are getting fair prices. We believe that online crypto trading platforms should make it easy for clients to understand the prices they are paying but not necessarily the prices that everyone else is paying; however, having said that, most online trading platforms already make visible the prices and volumes of all clients’ trades. It has become an industry norm. If they fail to do so, customers will not trust the platform and ultimately the platforms that do not disclose all their clients’ trade data will either struggle with perpetually low volumes or go out of business.

- **System resiliency, integrity, and security controls may be inadequate.** As described above, it is imperative to safeguard clients’ crypto assets (and personal data) from theft. We believe the solutions already mentioned help sufficiently mitigate this risk.

PART 4 – Regulatory approaches in other jurisdictions

It is very important to take a global eye to securities and derivatives regulators when determining the right approach for Canada. The SEC and the CFTC together have taken a very pragmatic and eloquent approach. If the crypto asset is a commodity, then a delivery test must be met for the crypto asset not to be deemed a derivative (and therefore subject to CFTC, or in Canada, provincial security legislation). The discussions and examples published by the CFTC, on what it means to deliver a crypto asset, are very specific and easy to understand. For asset determination, DV Chain believes the Canadian regulators should mirror that of the SEC and the CFTC.

One area where DV Chain believes that Canada can set the global best-practice, is in the custody of crypto assets. DV Chain believes creating a standard for all online trading platforms, or any crypto related business that holds in excess of \$10,000,000 of clients’ assets, should have their processes for safeguarding such assets subject to passing a SOC2 Type1 audit, and eventually a recurring SOC2 Type2 audit. Furthermore, because DV Chain believes the safeguarding of clients’ assets is the single most important issue that all crypto industry participants need to address, DV Chain recommends *that all custodian service businesses for crypto, that is deemed to be a commodity, should be restricted to either an IIROC dealer, a trust company, or a bank.* This is consistent with the current Canadian requirements to custody securities. This would mean that all IIROC dealers, trust companies, or banks that wished to offer crypto commodity custody services, would need to have their custody solution SOC2 Type 1 certified.

PART 5 – The Proposed Platform Framework

5.1 Overview of the Proposed Platform Framework

DV Chain agrees with everything the CSA has outlined, and offers clarification on the following points:

- As described above, if the online crypto trading platform is only trading crypto assets determined to be commodities (and not securities or derivatives), then the assets and the platform listing the assets would not be subject to securities regulation.
- However, even where the crypto asset is a commodity, when such commodities are held on behalf of clients and exceed \$10,000,000, the firm acting as the custodian should have a SOC2, Type1 certification, **with the ultimate goal of within 12-18 months, that all such custodian services only be provided by either an IIROC dealer, a trust company, or a bank.**

With respect to Question 5, DV Chain believes a SOC2 Type1 certification is superior to ensure the safeguarding of clients' crypto assets for the following reasons:

1. BitGo and Gemini have already obtained such certification;
2. (At least) two other reputable crypto custodians are in the process of receiving the same certification;
3. Among the main industry participants, a SOC2 report is the gold standard; and
4. KPMG, Deloitte, and other major auditing firms have built specific businesses within their practice to perform such an audit, at fairly reasonable prices, offering any firm the ability to maintain compliance.

With respect to Question 6, while there are challenges to make actual delivery of crypto assets to a client's wallet, by implementing several simple processes, firms can overcome these challenges. For example, the costs and administration to book every single transaction "on the native chain" (i.e. for Bitcoin, Ethereum, etc) to verify delivery is extremely expensive and time consuming. However, by batching and delivering trades "on-chain" within a reasonable time frame, and creating an omnibus accounting system to record all the transactions, (containing a master account and client sub-accounts integrated with the custodian/wallet service provider), ensures all clients' assets are fully segregated and ultimately delivered and verifiable "on-chain".

The benefits to participants for platforms, or other third party custodians, storing participants' crypto assets on their behalf are highly analogous to the benefits of banks storing participants' fiat assets on their behalf. Properly designed, certified and accountable custodial solutions (as we've advocated for throughout this commentary) provide participants with audit trails, access recovery and convenient asset access and transfer ability while maintaining tight security standards. Participants who wish to store their crypto assets themselves, and in effect act as their own crypto asset bank, should be free to do so. However, DV Chain believes most participants do not want to, nor should be forced to, act as their own crypto asset bank. **The benefits to participants of Platforms holding crypto assets on their behalf versus a third party custodian are so minimal, and simply put, should not be allowed unless their systems and processes are SOC2 certified, and then eventually only permitted within an IIROC Dealer, a Trust Company, or a Bank.**

In response to Questions 7 and 8, DV Chain believes that existing, recognized ATSs and exchanges offering crypto securities and/or derivatives will need to publish trading data, and online trading platforms will need to ensure that their clients received a fair price. However, the lack of liquidity for most crypto securities, should they become popular, and their underlying assets, (e.g. real estate tokens), will make compliance with ensuring fair price execution for their clients increasingly difficult.

In response to Questions 9 and 10, for crypto assets determined to be commodities (not securities or derivatives), it is appropriate for platforms to monitor trading activities on their own platforms. Market abuse and manipulation rules, however, are already set forth by global regulators. The CSA in Canada and CFTC in the US retain jurisdiction over commodity transaction as they relate to *fraud, market manipulation, and misleading statements*. A regulation service provider (“RSP”), (such as IIROC) may be delegated authority for enforcing these rules, but ultimately, the monitoring be self-administered, with routine (monthly) reporting of transactions to the RSP to ensure compliance with existing rules. Specific rules and integrity requirements (for trading commodity crypto assets) should prohibit spoofing, wash trading, layering, and fraud. This not dissimilar to how market manipulation is monitored today in some physical commodity markets.

In response to Question 11, existing solutions for traditional assets classes such as equities or in-house custom solutions already using by experienced proprietary trading firms can be easily adapted to monitor illegal trading behavior for crypto assets.

In response to Question 12, No; one type of trading behavior to explicitly monitor is “round robin” wash trading. There is a large incentive for crypto exchanges to show volume, such that near-riskless trading among a small number of participants (i.e. “round robin” wash trading) is a means to fictitiously inflate volume.

In response to Question 13, for online trading platforms that only trade crypto assets (not securities or derivatives), DV Chain recommend that all custody (ensuring security against hacks and other cyber-attacks), should be only conducted by a SOC2 Type1 certified entity, *with the 12-18 month goal of custody only permitted within a IIROC dealer, trust company or bank*.

In response to Questions 14 and 15, like in traditional commodity trading, principal trading is both accepted and fair. It is very common for the “middleman” commodity trader to take on principal risk and buy the goods in advance (whether it’s a car, a small boat, tons of cheese or meat) in anticipation of selling it shortly thereafter to a third party at a profit. This isn’t disclosed, it is simply expected. Similarly, in the crypto asset space, there are many OTC trading desks that exclusively trade as principal. Counterparties to the OTC trading desk understand this fact and can easily compare prices with other OTC desks to ensure they are receiving fair prices. DV Chain believes online crypto trading platforms are analogous to *electronic* OTC crypto trading desks, and should simply disclose that they may be acting as principal on some of their clients’ transactions.

In response to Questions 16 and 17, custodians should acquire insurance, at least for the values typically kept in their hot/warm wallet. The need for insurance for assets held in cold storage is debatable, especially if the custodian is SOC2 certified.

In response to Question 18, an inherent safeguard that offers investor protection in the event of bankruptcy, but not theft, is segregation of clients’ assets as discussed earlier. DV Chain recommends that all online trading platforms segregate all clients’ funds from firm assets.

In response to Question 19, for crypto assets that are neither a security nor a derivative, the clearing and settlement requirement for marketplaces would not apply.

In response to Question 20, for crypto assets that are settled (i.e. delivered) on a decentralized model or simply not through a centralized clearing entity, the key risk is ensuring *delivery* versus

payment. For online trading platforms that settle and deliver the traded crypto assets to its clients, the *payment* is made when the client deposits fiat or cryptocurrency as the means to purchase a crypto asset. The *delivery* (and settlement) of the crypto asset purchase is confirmed via receipt of the crypto asset at the custodian, verifiable “on-chain” by anyone running a node, including the custodian, and should be delivered (and settled) within a reasonable time frame (*e.g. CFTC mandates within 28 days*).

DV Chain thanks the CSA and IIROC for considering its views on the Proposed Framework for Crypto-Asset Trading Platforms. We welcome the opportunity to discuss our views with you in greater detail. Please do not hesitate to contact the undersigned at (647) 496-9450 with any questions the CSA or its staff might have regarding this letter.

Respectfully submitted,

/s/ Dino Verbrugge

Dino Verbrugge
Co-Founder
DV Chain, LLC



Wednesday, May 15, 2019

Delivered Via Email:

comments@osc.gov.on.ca; consultation-en-cours@lautorite.qc.ca; vpinnington@iiroc.ca

Investment Industry Regulatory Organization of Canada
British Columbia Securities Commission
Alberta Securities Commission
Financial and Consumer Affairs Authority of Saskatchewan
Manitoba Securities Commission
Ontario Securities Commission
Autorité des Marchés Financiers
Financial and Consumer Services Commission of New Brunswick
Superintendent of Securities, Department of Justice and Public Safety, Prince Edward Island
Nova Scotia Securities Commission
Securities Commission of Newfoundland and Labrador
Superintendent of Securities, Northwest Territories
Superintendent of Securities, Yukon
Superintendent of Securities, Nunavut

The Secretary
Ontario Securities Commission
20 Queen Street West
22nd Floor, Box 55
Toronto, Ontario M5H 3S8
Fax: 416-593-2318
comments@osc.gov.on.ca

Me Anne-Marie Beaudoin
Corporate Secretary
Autorité des marchés financiers
800, Square Victoria, 22e étage
C.P. 246, Tour de la Bourse
Montréal (Québec) H4Z 1G3
Fax : 514-864-6381
Consultation-en-cours@lautorite.qc.ca

Victoria Pinnington
Senior Vice President, Market Regulation
Investment Industry Regulatory Organization of Canada
Suite 2000, 121 King Street West
Toronto, Ontario M5H 3T9
vpinnington@iiroc.ca

**Re: Joint Canadian Securities Administrators/Investment Industry Regulatory Organization of Canada
– Consultation Paper 21-402 – *Proposed Framework for Crypto-Asset Trading Platforms***

The Investment Industry Association of Canada (“IIAC”) would like to submit its comments regarding the proposed framework for crypto-asset trading platforms. You will find below general comments from the IIAC and its industry members, followed by answers to the consultation questions listed in the joint proposal. We remain available for further discussions.

The IIAC and its mandate

The IIAC is the national association representing the position of 118 IIROC-regulated Dealer Member firms on securities regulation, public policy and industry issues. We work to foster a vibrant, prosperous investment industry driven by strong and efficient capital markets.

Therefore, the IIAC believes that, to maintain a prosperous investment industry, a crypto-asset regulatory regime should be merged with the current regulatory framework in Canada through the Investment Industry Regulatory Organization of Canada (“IIROC”). Crypto-asset trading platforms must be held to the same standards as IIROC-regulated entities. We believe that a different or non-existent regulatory regime would create regulatory arbitrage and would be detrimental to Canadian investors.

The IIAC represents IIROC-regulated broker dealers. Our members' clients know they are dealing with entities that comply with a stringent CSA/IIROC regulatory framework. Clients understand that this stringent regulatory framework protects them. A similar framework should be implemented for crypto-assets.

Main objective of the regulatory framework: Investor protection

The regulatory framework for crypto-assets should have the main objective of protecting investors. We believe that a stringent regulatory regime and regulatory oversight will not only protect investors but may also bring more credibility to crypto-assets - which Canadians seem to want. We believe that no Canadian investor should have to worry about being in the next QuadrigaCX saga.

Do "investors" understand crypto-assets and related risks?

In this submission letter, the IIAC will refer to Canadians transacting in crypto-assets as "investors" even if we would not necessarily categorize crypto-assets as "investment products". The investment firms we represent exist to help investors reach their investment goals. By contrast, crypto-assets are often seen as being purely speculative products with few investment properties.

Our members believe that, for many Canadians, crypto-assets are just "another investment product". Clients do not seem to properly understand the crypto products, the trading platforms, the risks and the current lack of regulation. For example, we do not believe that Canadians know:

- that no platform is recognized as an exchange or is authorized to operate as a marketplace or broker dealer in Canada;
- that most platforms currently operate without insurance coverage for investors' assets;
- that there are no regulated clearing agencies for crypto-assets (securities or derivatives).

The fact that over 200 platforms offer over 2000 crypto-assets without any regulatory oversight proves that global customers are interested in these innovative products but may not fully understand the risk associated with these crypto-assets. We doubt that investors, if clearly told that they will send money to an unregulated platform, would choose to do so. Investors must better understand the risk of crypto-assets before they decide whether or not to trade them. In any case, a stringent regulatory framework is required.

The IIAC believes that the current consultation is therefore an important step in the right direction with respect to protecting the Canadian public. Having our Canadian regulators collaborate with foreign regulators is also the only way crypto-assets will be properly regulated since innovation has no physical boundaries.

IIROC-regulated investment firms: True benefits to investors

The IIROC-regulated firms we represent must meet numerous stringent rules and regulations to ensure clients are properly protected. Our members are used to implementing internal controls, monitoring such controls, maintaining documentation and being inspected by regulatory agencies. Our members' clients feel safe investing their savings with our members and we believe clients should also be protected when dealing in crypto-assets - if and when they chose to do so. We believe IIROC is well positioned to regulate crypto-assets if amendments are made to the way it currently regulates broker dealer activities. Furthermore, we are supportive of marketplaces and dealers registering with IIROC to prevent crypto-asset regulatory arbitrage.

Proper framework: Theory and practice

As the consultation paper clearly states, the crypto platforms can be a mix of marketplace, broker dealer, clearer and custodian. Our members believe that using the existing rules and regulations as a basis for the framework is proper and accurate.

We also believe that amendments will need to be done to certain rules to apply to crypto-asset platforms and to the way they are to be implemented by these platforms. We also believe that regulators will need to change the way in which they perform their regulatory role. Regulators may need a different type of resource, such as employees with extensive technology and regulatory knowledge. However, the main objective for the rules, regulations and their regulatory surveillance should remain unchanged: The protection of the Canadian public.

In theory, all stakeholders could possibly agree on a theoretical framework that would provide customer protection through privacy, data protection, fair value, and safeguard against fraud. Platform executives (such as the Chief Compliance Officer and Ultimate Designated Person in the current IIROC-regulated environment) should be required to successfully pass certain amended regulatory exams and should possibly certify that the platform is, to the best of their knowledge, in compliance with rules and regulations.

In practice, the innovative technology being used by these crypto-asset platforms and the innovative processes they use (such as hot or cold wallets) complicate our recommendation-making process. Unfortunately, we may not have the extensive technology knowledge and experience required to properly recommend detailed regulatory/surveillance actions for such an innovative technology environment.

Proper framework: Implementation by trading platforms

We believe that trading platforms should come up with proper ways of mitigating the risk identified by the regulators. This can be done if collaboration between the parties (platforms and regulators) truly exists. We believe the Canadian regulatory sandboxes may be the best places to discuss risks (identified by regulators) and controls.

Proper framework: Surveillance by regulators

The IIAC believes that trading platforms should comply with market integrity rules, when applicable to crypto-assets. We also believe that the monitoring and surveillance performed by regulators must follow the same general guidelines that currently exist for marketplaces, broker dealers, clearing agencies. We believe the regulator should perform regular inspections of the platforms, investigations when needed, should have access to complete data to perform proper surveillance and identify possible market manipulation and fraud. The regulator should also monitor the risk adjusted capital (or similar calculation) and review monthly early warning signals to assess the platform's financial health. Furthermore, the regulator should not be in a conflict of interest with the trading platform in order to provide fair and just surveillance.

Insurance coverage for asset protection

We believe that crypto-assets, in hot and cold wallets or any other method of custody, should be protected through insurance coverage. Furthermore, we believe that a fund similar to the Canadian Investor Protection Fund ("CIPF") should provide protection for crypto-assets held by clients if the crypto-asset trading platform becomes insolvent.

Harmonization on a global level

A main issue is the discrepancy between the global reach of these platforms (the internet is everywhere) and the limited jurisdictional powers of our Canadian regulators. The IIAC has previously mentioned a similar issue regarding foreign (and fraudulent) binary option trading platforms that were targeting Canadian investors. Since our Canadian regulators do not have a global reach, collaboration and harmonization between international regulators is required to protect investors. Furthermore, if Canadian clients cannot be properly protected when trading on a foreign platform, should we accept foreign platforms in Canada?

Consultation questions

1. Are there factors in addition to those noted above that we should consider?

No comments.

2. What best practices exist for Platforms to mitigate these risks? Are there any other substantial risks which we have not identified?

No comments.

3. Are there any global approaches to regulating Platforms that would be appropriate to be considered in Canada?

No comments.

4. What standards should a Platform adopt to mitigate the risks related to safeguarding investors' assets? Please explain and provide examples both for Platforms that have their own custody systems and for Platforms that use third-party custodians to safeguard their participants' assets.

The standards related to safeguarding crypto-assets are the same whether the platform custodies directly or indirectly. Crypto-assets must be properly safeguarded. We believe that technology experts would be better positioned to recommend controls for these platforms.

5. Other than the issuance of Type I and Type II SOC 2 Reports, are there alternative ways in which auditors or other parties can provide assurance to regulators that a Platform has controls in place to ensure that investors' crypto-assets exist and are appropriately segregated and protected, and that transactions with respect to those assets are verifiable?

We believe that SOC 2, Type I and Type II Reports should be required – but may need to be amended to apply to crypto-assets.

6. Are there challenges associated with a Platform being structured so as to make actual delivery of crypto assets to a participant's wallet? What are the benefits to participants, if any, of Platforms holding or storing crypto assets on their behalf?

No comments.

7. What factors should be considered in determining a fair price for crypto assets?

Based on our understanding of crypto-assets, determining a fair price may be tricky for a multitude of products. We believe that the bid and ask (offer and demand) should be the basis of fair value for a lot of crypto-assets that do not derive their value from “standard” products.

8. Are there reliable pricing sources that could be used by Platforms to determine a fair price, and for regulators to assess whether Platforms have complied with fair pricing requirements? What factors should be used to determine whether a pricing source is reliable?

No comments.

9. Is it appropriate for Platforms to set rules and monitor trading activities on their own marketplace? If so, under which circumstances should this be permitted?

The IIAC has submitted previous comment letters regarding conflicts of interest between a marketplace and its regulator. Such regulator monitors trading activities on a marketplace while regulatory staff is possibly being remunerated based on the volumes traded on the marketplace. Industry members have stated, on more than one occasion, their serious concerns with a proposed governance structure where regulator and marketplace would ultimately report to the same board members.

We once again wish to state that a marketplace can set its own commercial rules (for example, on new products they wish to list) but should not, under any circumstances, have its trading activities monitored by a related party. The reputation and integrity of the Canadian market, of its industry participants, as well as the protection of investors are at stake.

10. Which market integrity requirements should apply to trading on Platforms? Please provide specific examples.

We believe that market integrity requirements should apply to crypto-asset platforms. These platforms should provide fair and orderly markets and should not tolerate market manipulation or market fraud. They should also maintain risk management processes, supervisory controls, policies and procedures manuals, disaster recovery plans/business continuity plans and should document these processes and controls.

We also believe that, at least initially, these platforms should not permit dark trading or short selling activities, and should not extend margin to their clients.

11. Are there best practices or effective surveillance tools for conducting crypto asset market surveillance? Specifically, are there any skills, tools or special regulatory powers needed to effectively conduct surveillance of crypto asset trading?

Platform regulators will need to have a new set of skills. Regulators will need to hire technology experts who fully understand the technology used by the crypto-asset trading platforms. As for surveillance tools, they should be able to analyze data from different products in order to identify suspicious patterns.

12. Are there other risks specific to trading of crypto assets that require different forms of surveillance than those used for marketplaces trading traditional securities?

No comments.

13. Under which circumstances should an exemption from the requirement to provide an ISR by the Platform be considered? What services should be included/excluded from the scope of an ISR? Please explain.

No comments.

14. Is there disclosure specific to trades between a Platform and its participants that Platforms should make to their participants?

Platforms must be transparent and provide clear trade and fee information to its clients, similar to other marketplaces. Clients should be made aware whether they traded against the inventory of the platform or against another client. We believe that strong disclosure requirements for dealers that trade against their clients should be implemented. Platforms should also disclose conflicts of interest.

We recommend strong risk disclosure language be included at account opening for crypto-assets since their volatility and risk can be in excess of volatility currently experienced with other products.

Firms should also consider implementing a specific Know-Your-Client (KYC) section and an appropriateness test for crypto-assets, given volatility and possible low liquidity.

15. Are there particular conflicts of interest that Platforms may not be able to manage appropriately given current business models? If so, how can business models be changed to manage such conflicts appropriately?

Platforms should not be allowed to monitor their own trading activities (see answer to question #9 above) as we would consider this a significant conflict of interest.

16. What type of insurance coverage (e.g. theft, hot-wallet, cold-wallet) should a Platform be required to obtain? Please explain.

Since insurance companies hire professional risk assessors, they may be better positioned to identify specific risks in the crypto-asset space.

17. Are there specific difficulties with obtaining insurance coverage? Please explain.

There are probably difficulties for platforms to obtain insurance coverage. We believe that if insurance coverage for platforms becomes a regulatory requirement, insurance companies will quickly expand their offering to protecting crypto-assets. Insurance companies should be involved in the discussions.

18. Are there alternative measures that address investor protection that could be considered equivalent to insurance coverage?

We are unaware of such measures. However, we believe that the CIPF should be involved in the current discussions. We believe that the CIPF or a similar type of fund should cover crypto-assets in the case of bankruptcy/insolvency if the platforms are to be regulated by IIROC.

19. Are there other models of clearing and settling crypto assets that are traded on Platforms? What risks are introduced as a result of these models?

We are unaware of other clearing and settling models. That being said, we believe that platforms should comply with the existing regulatory framework. They need to have updated policies and procedures manuals and controls to mitigate the different types of risk (operational, custody, liquidity, investment and credit).

20. What, if any, significant differences in risks exist between the traditional model of clearing and settlement and the decentralized model? Please explain how these different risks may be mitigated.

No comments.

21. What other risks are associated with clearing and settlement models that are not identified here?

No comments.

22. What regulatory requirements, both at the CSA and IIROC level, should apply to Platforms or should be modified for Platforms? Please provide specific examples and the rationale.

The IIAC and its members believe that the existing regulatory framework should generally apply. We believe some modifications will be needed to properly assess and monitor risk for crypto-asset trading platforms. We also believe that these platforms should regularly (monthly) inform their regulators of their financial health. A monthly financial report (“MFR”) as well as an annual audited report, similar to that of IIROC-regulated dealers, should be implemented. Platforms should be required to provide a calculation similar to the risk adjusted capital (“RAC”) calculation of IIROC-regulated dealers, including margin amounts and non-allowable assets, in order to help the regulator assess the platforms’ financial health. Early warning tests should also be put in place for these platforms.

Conclusion:

The IIAC and its members would like to thank the CSA and IIROC for drafting this consultation paper.

The Canadian public seems to have adopted crypto-assets, and therefore must be protected. Canadians should be able, if they wish to do so, to trade crypto-assets on regulated platforms that will properly safeguard their assets.

Canadians should be made aware, by clear and simple disclosure, that crypto-assets can be risky and speculative in nature and may not be a proper investment vehicle.

In order to properly protect investors, the IIAC and its members believe crypto-assets should be regulated by IIROC.

IIROC is well-positioned to become the regulator of crypto-asset platforms in Canada since it already regulates listed equities and fixed income products, and is not, as a regulator, in a conflict of interest with a marketplace.

Furthermore, we believe that the Canadian marketplace will be better protected by a regulator that has access to trading data for all products (versus regulators that try to maintain market integrity by performing surveillance solely on crypto-assets).

We believe that further consultations will be needed between the different stakeholders to keep pace with innovation and, as such, please note that the IIAC and its members, as always, remain available for further consultations.

Yours sincerely,



Annie Sinigagliese
Managing Director
Investment Industry Association of Canada
asinigagliese@iiac.ca



May 15th, 2019

BY ELECTRONIC MAIL ONLY TO:

comments@osc.gov.on.ca, Consultation-en-cours@lautorite.qc.ca, vpinnington@iiroc.ca

**Ontario Securities Commission
Investment Industry Regulatory Organization of Canada**

**The Secretary
Ontario Securities Commission
20 Queen Street West, Suite 1903, Box 55
Toronto, Ontario M5H 3S8**

**Me Anne-Marie Beaudoin
Corporate Secretary
Autorité des marchés financiers
800, square Victoria, 22e étage
C.P. 246, tour de la Bourse
Montréal (Québec) H4Z 1G3**

**Victoria Pinnington
Senior Vice President, Market Regulation
Investment Industry Regulatory Organization of Canada
Suite 2000, 121 King Street West
Toronto, Ontario M5H 3T9**

INCLUDES COMMENT LETTERS

Eric Gu, Chief Executive Officer
www.viewfin.com
eric.gu@viewfin.com



To Whom It May Concern,

ViewFin Canada is a one-of-a-kind alliance of independent Fintech consulting firms that extends our network and expertise for blockchain solutions globally. We've also partnered with **TulipEx**, a digital assets management platform that will be launching within the next few weeks. Together, we would like to present our comments related to the: **Consultation Paper 21-402 Proposed Framework for Crypto-Asset Trading Platforms**.

We were able to respond to questions: 1, 2, 3, 8, 11 and 15.

1. Are there factors in addition to those noted above that we should consider?

We should consider further compliance factors. Most algorithms are setup with risk criteria. We'd say it's imperative for fintech firms to have solid compliance standards clearly outlined in the manual, prior to entering the market.

2. What best practices exist for Platforms to mitigate these risks? Are there any other substantial risks which we have not identified?

The compliance manual should have a list of indicators of suspicious activity, a flowchart on what to do step by step can help mitigate the risk. This should be periodically updated as the industry is rapidly evolving.

3. Are there any global approaches to regulating Platforms that would be appropriate to be considered in Canada?

A Know Your Customer (KYC) process that is consistent with global standards, evaluating the risks of platforms that operate in higher risk jurisdictions. There are many jurisdictions to learn from, countries in Asia are currently wrestling with these issues as well.

Eric Gu, Chief Executive Officer

www.viewfin.com

eric.gu@viewfin.com



8. Are there reliable pricing sources that could be used by Platforms to determine a fair price, and for regulators to assess whether Platforms have complied with fair pricing requirements? What factors should be used to determine whether a pricing source is reliable?

Pricing Sources will depend on the Crypto currency being traded. The MVIS CryptoCompare Bitcoin Index(MVBTC) maintained by MV Index Solutions GmbH(MVIS). MVIS is a index provider based in Frankfurt Germany and is regulated as an Index administrator by the German financial regulator (BaFin).

MVIS complies with EU benchmark regulations in relation to pricing and conforms with International Organization of Securities organization. We believe reliable pricing for Crypto Currencies is in early days and that over time with regulation, more index providers will start tracking them bringing more legitimacy.

In addition to MVIS, the Chicago Mercantile Exchange (CME) has started to publish CME CF Bitcoin Reference Rate as well as the Ethereum Reference Rate and Real-Time Index. CME Group has developed standardized cryptocurrency references rates and real-time indices with the methodology and rules publishes transparently online:
(<https://www.cmegroup.com/education/bitcoin/cme-cf-cryptocurrency-reference-rate-methodology.html#4-methodology-and-rules>)

11. Are there best practices or effective surveillance tools for conducting crypto asset market surveillance? Specifically, are there any skills, tools or special regulatory powers needed to effectively conduct surveillance of crypto asset trading?

We believe similar to the Canadian markets that a system of Broker or Client ID's be implemented for Crypto Exchanges. This can help mitigate price manipulation and wash trading that can be common in Crypto. Participants on the exchange should be able to see Time & Sales data of executions as well as level 2 data. Designated Market Makers should have their own unique broker code so that market participants can identify that a trade executed with a registered market maker.



15: Are there particular conflicts of interest that Platforms may not be able to manage appropriately given current business models? If so, how can business models be changed to manage such conflicts appropriately?

We believe disclosure is the best way to handle conflicts of interest. TMX and CSE publish Exchange rules online for their clients so that they know how their orders are handled and are bound by Best Execution requirements from the regulator. Crypto Exchanges/Platform's should be governed the same way.

Furthermore TSX openly discloses their policy regarding Market Making (<https://www.tsx.com/trading/toronto-stock-exchange/order-types-and-features/market-maker-program>). It shows the responsibilities of the market maker in relation to Minimum Guaranteed Fill (MGF) Facility and clearly defines their role in the marketplace. The illiquidity of the Crypto Market requires the added liquidity that regulated market makers can provide.

TSX continuously monitors the performance of all Market Makers with respect to their ability to contribute to the overall market in terms of creating liquidity, depth and continuity. Market Makers are assessed on their ability to call a 2-sided market (i.e. spread maintenance), their efforts to line the book with reasonable depth (i.e. liquidity), and their overall participation in trading of the security. We believe first that disclosure should be made to clients and that relationships be disclosed.

Apart from market making, Payment For Order Flow is a concern. Similar to SEC rule 606 in the U.S. Brokers are required by the Securities and Exchange Commission (SEC) to disclose its policies with respect to payment for order flow. According to the SEC, payment for order flow may include monetary payment, reciprocal agreements, services, property, or any other benefit that results in remuneration, compensation, or consideration to a broker-dealer in return for routing of customer order flow and includes exchange rebates and credits

By adopting these proposals to publish exchange rules, regulate exchange market making activity and disclosing Payment for Order Flow compensation, we believe that Crypto platforms regulated in Canada will have an unrivaled regulatory environment to prosper in.

Eric Gu, Chief Executive Officer

www.viewfin.com

eric.gu@viewfin.com



We would like to sincerely thank you for the opportunity to provide our comments. Please do not hesitate to contact us with any questions or concerns you may have.

Thank you.

ViewFin Canada Compliance Team

Adnan Tahir, Chief Compliance Officer - TulipEx
adnan@viewfin.com

Eric Gu, Chief Executive Officer
www.viewfin.com
eric.gu@viewfin.com

May 15, 2019

VIA EMAIL

British Columbia Securities Commission
Alberta Securities Commission
Financial and Consumer Affairs Authority of Saskatchewan
Manitoba Securities Commission
Ontario Securities Commission
Financial and Consumer Services Commission (New Brunswick)
Superintendent of Securities, Department of Justice and Public Safety, Prince Edward Island
Nova Scotia Securities Commission
Securities Commission of Newfoundland and Labrador
Superintendent of Securities, Northwest Territories
Superintendent of Securities, Yukon
Superintendent of Securities, Nunavut

c/o The Secretary

Ontario Securities Commission

20 Queen Street West
22nd Floor, Box 55
Toronto, Ontario M5H 3S8
Fax: 416-593-2318
comments@osc.gov.on.ca

M^e Anne-Marie Beaudoin
Corporate Secretary

Autorité des marchés financiers

800, square Victoria, 22e étage
C.P. 246, tour de la Bourse
Montréal (Québec) H4Z 1G3
Consultation-en-cours@lautorite.qc.ca

Ms. Victoria Pinnington
Senior Vice President, Market Regulation
Investment Industry Regulatory Organization of Canada
Suite 2000, 121 King Street West
Toronto, Ontario M5H 3T9
vpinnington@iiroc.ca

Dear Sirs/Mesdames:

Re: CSA/IIROC Request for Comments to Joint Consultation Paper 21-401

The Jersey Company welcomes the opportunity to comment on Joint Consultation Paper 21-401 dated March 14, 2019 (the “Paper”).

The Jersey Company is a Canadian capital markets and growth company consultancy, with active projects related to the application of distributed ledger technology to securities issuance and trading globally. We are pleased to share our insights below.

The Paper’s broad topic is Crypto-Asset Trading and Platforms, and while we have worked with participants in *cryptocurrency* businesses, our more-relevant expertise is in digital securities and thus our comments hereunder are confined to considerations regarding the trading of “Digital Securities” – transactions of assets traditionally regarded as securities, but using underlying technology and methods similar to those used in cryptocurrency markets. In our Comment we distinguish these assets as **Digital Securities** and to the referenced common underlying technologies and methods as **Crypto Token Systems**.

Utility Token Offerings often masquerade as Asset Offerings

We feel it is useful to first touch on the growing practice of issuing and trading so-called Utility Tokens - a category of transactions leveraging Crypto Token Systems similar to those underpinning cryptocurrencies and Digital Securities, and an area which is often conflated with those Digital Assets discussed in the Paper.

These Utility Tokens are generally contracts based on a service (as-distinct from an ownership right) to be provided by the issuer. In addition to their use of Crypto Token Systems, these Utility Tokens are sometimes exchangeable for Digital Securities or cryptocurrencies or may be marketed as such or in combinations with either.

The issuance of Utility Tokens by corporates has created confusion among investors. We applaud the efforts of Canadian regulators to date in issuing warnings to the public¹. In our view, it is important to confidence in regulated markets that Canadian issuance of Utility Tokens continues to be monitored by CSA members, and that such activity be understood by Canadians as separate and distinct from regulated crypto asset markets. We urge continued broad communication and clarification to the investing public.

On Crypto Currencies and Digital Securities

Your Paper considers the issuance and trading of digital non-fiat “currencies” and the issuance and trading of Digital Securities (defined as securities generally in various provincial securities acts), and there are clearly overlaps, grey areas and sometimes hybrids among these. But while both cryptocurrencies and Digital Securities leverage similar underlying technologies and methods, the two markets are at their cores generally quite distinct. For example:

¹ Notably CSA Staff Notice 46-308 at https://www.osc.gov.on.ca/en/SecuritiesLaw_csa_20180611_46-308_securities-law-implications-for-offerings-of-tokens.htm

1. *There exist different legacy market structures for currencies (including cryptocurrencies) versus securities (including Digital Securities).*
 - For example, the inherent value of currencies holdings is typically based on possession of the instrument (effectively, bearer instruments), whereas most securities are contractually-described ledged or certificated structures. This difference of bearer status is a contributor to several differences in investor risk, market structure and regulatory considerations.
 - Digital Securities structures include a ‘manager’ of the asset represented by the security, and that manager (eg; issuer) plays a central role in the market structure.

Several other market structure differences also contribute to the distinctness of each market, and many of these legacy differences survive as we move to a digital world.

2. *Generally, Digital Security ecosystems employ a central authority model while cryptocurrencies are decentralized - often by definition - creating significantly differing oversight challenges.*
3. *There are differing implementations of similar technology which distinguish cryptocurrency markets from those for Digital Securities:*
 - As one example, many Digital Security marketplaces are built on a permissioned and/or proprietary network managed by a central authority, while cryptocurrencies generally exist over decentralized, open networks and thus rely more-heavily on the cryptographic security features of their technology;
 - In another example, Digital Security ecosystems generally make more-advanced use of Smart Contract technology than cryptocurrencies.

Other architectural, technological and workflow choices are often distinct markers of cryptocurrency markets vs those designed for Digital Securities.

Taken together, the differences enumerated above and other identifiers allow us to categorize current and proposed blockchain-based issuance and trading solutions into one or the other category (Cryptocurrency or Digital Security), with perhaps a smaller subset occupying the aforementioned “grey areas”².

² We acknowledge that financial innovation has and continues to create seeming hybrids, including bundling one asset inside another (for example currency futures) or providing for the morphing of one to another (utility tokens with a triggered conversion right). We agree with the CSA that offerings need to be evaluated on their own facts, but feel that on inspection, most offerings can be reduced to discrete and recognizable securities, currencies or utility tokens, even when marketed together.

Why Digital Securities

You, the Paper's sponsors, collectively oversee much of Canada's securities activity, maintaining fair and orderly markets and protecting investors. In managing a market environment which is worthy of the public's trust, you also facilitate capital formation, and thus contribute significantly to improving Canada's economy.

In a manner analogous to our collective experience of digital correspondence (such as email) replacing letter-writing, Digital Securities hold the promise of significantly better record-keeping and vastly improved auditability, searchability & transparency regarding securities transactions and participants.

These attributes contribute significantly to the regulatory and public policy objectives above. With a shift to Digital Securities, regulators could achieve real-time insights into the detailed actions of individual investors, intermediaries, custodians, clearers, depositors and issuers seen *collectively*, reviewing actions industry-wide - again in real time - by any machine-sortable parameter. Better still, machines could programmatically review activity details that are unavailable today, across the myriad players involved in any transaction or series of related transactions, among all the players whose information now is held in incompatible databases. Issuers could better-reach and better-inform investors whose ownership was registered electronically. Intermediaries could adhere to faster and higher compliance and customer-service standards.

Once Canada achieves clarity on a framework for Digital Securities issuance and trading, follow-on regulations could support imagined innovation such as securitization of asset types that are otherwise difficult to regulate; fractional ownership; improved exempt market mechanisms and liquidity; tenured voting; and more. Doing so would greatly increase the efficiency of capital deployment for Canadians and the Canadian economy and supporting growing and competitive financial and digital industry sectors in Canada – all while improving compliance, oversight and confidence in our markets and financial activity.

But just as digital correspondence brought new challenges (such as spam, phishing and more), Canada needs to be thoughtful as it moves along with the rest of the world to capitalize on the benefits of Digital Securities-based capital markets.

Canada and the World:

The CSA/IROC Consultation Paper comes at a notable moment for Digital Securities. 2018's global mini-bubble of unregulated Initial Coin Offering activity demonstrated both the opportunity and the potential for investor abuse as cryptocurrency platforms and methods were hurriedly redeployed to raise money selling (real or imagined) assets. Regulators worldwide took note and took action.

More recently, several smaller-economy jurisdictions have encouraged regulated issuance of Digital Securities through "light" regulation, leveraging interest in the benefits of Digital Securities issuance to attract capital markets activity where historically interest was light.

But asset owners strongly prefer jurisdictions where robust legal frameworks provide critical additional protections, and Canada and the US are top-rated in this regard. With the SEC and FINRA maintaining an

indefinite “hold” on any blockchain-based new- or continuing-member applications, Canada – already home to a competitive capital markets industry and a booming digital economy - has an opportunity to extend and improve its position among the world’s preferred capital markets jurisdictions by modifying its existing successful securities regulation model to support Digital Securities.

As described above, it is our view that Canadian regulation of cryptocurrencies markets and Platforms will differ from the regulation of Digital Security markets and Platforms. A framework for regulating Digital Security Platforms is achievable by extending the existing regulatory framework for securities regulation. We sense that establishing (a necessary) regulatory framework for cryptocurrency Platforms will take the authors into new territory, requiring significant learning and discovery, consultation and likely, significant new regulation appropriate to a very different market.

Recommendation. *It is our recommendation that IIROC and the CSA pursue an oversight model and methods which de-couple the work of (a) creating a framework for crypto-currency trading from the work of (b) modifying existing securities regulation to address the subtle differences arising from the use of blockchain technology for securities trades, addressing any outliers as exceptions, thus allowing Canadian issuers and investors to benefit without unnecessary delay.*

Questions posed by the Consultation Paper

Our responses to the questions specifically posed in the Consultation Paper follow:

General Questions

1. Are there factors in addition to those [facts & circumstances of how trading occurs on Platforms] noted above that we should consider [in determining applicability of securities regulation]?

Speaking specifically to the issuance and trading of Digital Securities, we believe the existing criteria regarding applicability of securities regulations can and should apply equally to identifying (traditional) securities activities and Digital Securities activities.

3. Are there any global approaches to regulating Platforms that would be appropriate to be considered in Canada?

Not directly.

As-mentioned, it is our view that Canada is uniquely positioned as a jurisdiction with well-developed and attractive regulatory and legal foundations upon which to build. While we encourage a global view, we would urge caution in adopting approaches from those jurisdictions where accommodative policies seem primarily intended to outweigh the structural advantages of Canada and similar countries.

Nor do we consider the US approach helpful. There, securities regulators have effectively halted new initiatives, offering few insights regarding direction or timeline for issuance or trading of Digital Assets, providing little which is instructive or could be recommended for Canada.

Potential Investor Risks, Risk Mitigation and Investor Protection

2. *What best practices exist for Platforms to mitigate these [described] risks? Are there any other substantial risks which we have not identified?*

In our view, new or evolving entities seeking approval to issue or trade Digital Securities in Canada can expect considerable opportunities, and those opportunities are sufficient to outweigh any burden of compliance with existing requirements. We feel that existing securities issuance and trading regulations should, with *in most cases* only slight adjustments, be sufficient to achieve the broad policy objectives of the regulators.

We identify below three areas where this “only slight adjustments” approach may be insufficient:

- a) **Safeguarding Investors’ assets.** While the current custodial model for IIROC brokers represents a good starting point, there is an extra hurdle for clearers to demonstrate possession and control of assets when those assets are represented by code on a public network. Specifically, challenges exist in proving a negative: insuring the custodial holder or holders of a token’s key(s) can prove that no duplicate(s) exist(s).

Leveraging the central authority attribute of Digital Securities, markets, we have seen several models emerge whose approach to this issue is credible, but regulatory approval of these models is a new step.

In our view, demonstrating an appropriate level of possession and control is more-difficult in the decentralized implementations typical of cryptocurrency

- b) **Processes, Policies.** The existing securities framework in Canada is a workable framework for Digital Securities in Canada. But those procedures will necessarily be different in some respects for Digital Securities and the assets they might eventually securitize.

Chief Compliance Officers and overseeing regulators will need to match these changes with training of review staff in order to conduct reviews and audits which are both relevant and meaningful in an emerging Digital Securities industry. In our view this is a significant, not incremental, undertaking (which learning incidentally will also prepare staff for parallel challenges in oversight of all Digital Assets, ie; including cryptocurrency and Digital Securities).

- c) **Security.** Significant parts of the cryptocurrency market arose from - and maintain - a hacker culture. The underlying technology of most Digital Security issuance and trading systems employs Crypto Token Systems which are highly-similar to - and thus seemingly accessible by/ attractive to - crypto hackers.

Registrants pursuing a Digital Securities business model should expect a greater vulnerability to, and targeting by, cyber attacks, and regulators should require more-advanced cyber (and physical) security programs.

We feel the balance of the Risks referenced in the Paper can be addressed through small changes existing securities regulations which should apply and are generally appropriate to Digital Securities.

Some Platforms may wish to operate both as a Digital Securities Platform (issuing or trading Securities in a digital form) and a Cryptocurrency Platform (by pricing and settling those securities trades in a non-fiat cryptocurrency). In our view this amalgam needs to conform both with rules for trading Digital Securities as well as with those for cryptocurrency trading and settlement, meeting the higher standard where there is overlap.

4. What standards should a Platform adopt to mitigate the risks related to safeguarding investors' assets? Please explain and provide examples both for Platforms that have their own custody systems and for Platforms that use third-party custodians to safeguard their participants' assets.

Currently, institutional investors engage institutional Custodians for custody, while retail investors look to their brokers for securities custody. Those brokers in some cases engage a “clearing” broker to provide services including custody, to the introducing broker and end investor.

All of these organizations are Participants in CDS, who provide Participants custodial services for (CDS-eligible) securities.

While Digital Securities are similar to traditional securities, their nature creates those issues regarding assurance of possession and control previously discussed. We believe that several emerging solutions are improving that assurance, and we expect more, and believe there are already models which combine safeguards which deliver a level of assurance equal to or better than existing custody infrastructures.

Separately, we feel that “back office” systems and practices to identify fraudulent transactions may vary on a firm-to firm basis, and suggest regulators consider limiting digital securities trading & custody to a “two-party” system: Institutional broker/Custodian or Introducing Broker/ Carry Broker, for some period, or at minimum, setting high standards for self-custody:

- This would provide a period of separation of people & processes and a time of some duplication of compliance oversight, during which internal best practices and audit skills of Compliance and regulatory staff can develop to accommodate and oversee a dependable self-custody model.
- We also note that practically, many firms who may wish to engage in Digital Securities trading may introduce Digital Securities clearing later, and rely on a few emergent

Digital Securities Clearing Brokers, concentrating expertise development for the new technology.

In a final note on custody, we believe that the types of custodial services such as those provided by CDS and CDCC to their Participants could remain largely as-is while introducing a regulatory framework for issuance and trading of Digital Securities: we do not perceive an immediate industry need to couple a move by such organizations to “Digital Asset-Ready” (although we note that there are benefits of introducing similar technologies in this area, in our understanding these are largely decoupled).

6. Are there challenges associated with a Platform being structured so as to make actual delivery of crypto assets to a participant's wallet? What are the benefits to participants, if any, of Platforms holding or storing crypto assets on their behalf?

In our view, securities investors are not interested in maintaining wallet technology. In fact, our recommendation would be to make bearer-version Digital Securities not permitted, to the extent that such an action could be made compatible with existing permissive Canadian law regarding bearer securities.

5. Other than the issuance of Type I and Type II SOC 2 Reports, are there alternative ways in which auditors or other parties can provide assurance to regulators that a Platform has controls in place to ensure that investors' crypto-assets exist and are appropriately segregated and protected, and that transactions with respect to those assets are verifiable?

The Jersey Company has a long history of providing institutional investors expert review of broker controls. It has been our experience that diligent evaluations of brokers’ competence and controls decreases both costs and risks, and that there is considerable opportunity for improvement in the securities industry generally.

With regard to the specific challenges or opportunities in auditing the controls and processes of brokers engaging in offering and trading Digital Securities, we would offer the following areas for consideration:

- Regulatory, third-party and/or in-house adoption of Smart Contract audits with specific focus on anti-fraud controls;
- We have worked with third parties who offer independent and ongoing cyber security evaluation services to government and industry and note that the area is one of ongoing significant improvement and innovation.
 - Given the profile and technological dependence of firms using Crypto Token Systems, we feel that Platform’s ISRs should specifically and publicly describe types of continuous cyber security testing the firm is conducting, and that results of this testing should be made privately available to regulators;

- We suggest that regulators consider engaging such a service (alternatively or in addition to the data received indirectly above), and regularly report on overall industry cyber security in a report card format, thus encouraging continued improvement.

14. Is there disclosure specific to trades between a Platform and its participants that Platforms should make to their participants?

Due to the nature of Digital Securities and their transparent blockchain-based record of ownership, a Platform handling many orders has access to more information (and one might reason, more tools to collect and analyse that information) and thus can realize significant information asymmetries. Barring suitable deployment of masking or similar tools, we feel that principal trading should not be allowed.

15. Are there particular conflicts of interest that Platforms may not be able to manage appropriately given current business models? If so, how can business models be changed to manage such conflicts appropriately?

Digital Security Platforms may have significantly-more investor information, including holdings information of previous investors (wallets), and may easily develop the capabilities to devise derivative information. Regulators should strongly consider the ramifications of Platforms' use or sale of this unique information, and should be certain that Privacy policies are adequate and enforced.

18. Are there alternative measures that address investor protection that could be considered equivalent to insurance coverage?

In our view, Digital Securities which are legally identical to CIPF-covered assets should receive equivalent CIPF protections to equivalent non-digital securities.

Rules and Surveillance

9. Is it appropriate for Platforms to set rules and monitor trading activities on their own marketplace [rather than retaining an RSP]? If so, under which circumstances should this be permitted?

We believe that Platforms are brokers of financial services and agree that they should be subject to obligations of NI 31-103 and (subject to allowed exemptions) Digital Securities Platforms generally should become an IIROC Dealer Member, adhering to the Dealer Member Rules providing investor protection and ensuring confidence in Canada's markets. We note that some Platforms' businesses models may fit better in the current Exempt Market regime, and that some number of models may offer compelling benefits yet not fitting precisely into existing frameworks, requiring some adjustment to their business models and/or limited rule exemptions (from RSPs) in order that these "edge case" Platforms operate within a framework which is substantially-similar to existing securities dealers.

While the full text of Canada’s Universal Market Integrity Rules (UMIR) may not apply to trading some new instruments on new Platforms, many trading rules are common to all well-run markets. Examples include prevention of manipulative & deceptive trading, banning front running, proper handling of client orders (including timely exposure, consistent use of relevant markers), fair & consistent availability of quote and trade information and more. In our view, it is important that Platforms adhere to the accepted standards in these fundamental aspects, and we believe an independent RS provider should continue to be required.

But there are clearly trading rules which may be unique to individual Platforms (for example, how client orders will be handled with respect to time, or size, etc.) or with respect to customer participation (an example here might include institutional-only or IIROC-registrant only marketplaces).

We also understand that practically, there may be no competent independent authority able to provide ‘full’ market oversight of some aspects of Platforms’ trading of some new asset classes (an illustrative example might include digital token-based fractional ownership of sports cars), and that the current model of marketplace membership in IIROC, with full compliance with UMIR, may be impractical.

We encourage IIROC to contemplate RSP relationships which would support a hybrid model where IIROC can contribute oversight of common trading rule while the Platform or a third party – after review and approval by the appropriate regulators – provides surveillance of those asset- or marketplace-specific rules and activities.

Whether in-house or third party, we would expect to see governance of these surveillance organizations achieved in such a manner as to allow them to operate independently/at arms-length from the core Platform. As with RS providers, such Platforms’ surveillance organizations should be regularly audited by the overseeing securities commission.

10. Which market integrity requirements should apply to trading on Platforms? Please provide specific examples.

Please see our response to Question 9, above.

11. Are there best practices or effective surveillance tools for conducting crypto asset market surveillance? Specifically, are there any skills, tools or special regulatory powers needed to effectively conduct surveillance of crypto asset trading?

The attributes of Digital Securities bring significant opportunities to greatly improve market surveillance. In fact, they provide significant inherent advantages in other regulatory surveillance activities as well. But as most major jurisdictions are on the cusp of approving Digital Securities (and in many cases, the technologies, architectures and processes which will be approved are as-yet not confirmed), there are no significant third party offerings known to us as being developed or being marketed. Once regulators provide clarity on the technologies they will approve, we expect significant growth of Digital Securities surveillance tools, including in-

house development, with both types spurred by the breadth of shared knowledge about Crypto Token Systems.

A recent interesting proposal from the Federal Reserve Bank of Boston illustrates our views and describes the addition of a regulatory node to Crypto Token networks³. While the possible consequences of such a system require deliberation, we feel this illustrates the sort of enhanced supervision we envision as the market and surveillance matures.

Please also refer to our comments regarding Smart Contract audit tools for additional views on surveillance tools.

13. Under which circumstances should an exemption from the requirement to provide an ISR by the Platform be considered? What services should be included/excluded from the scope of an ISR? Please explain.

We can think of no circumstance in which an ISR as contemplated in NI 21-101 at 12.2(1) should not be required, except for the provision included at 12.4(2), given the likelihood that early Digital Securities systems will trade a few unique securities. A different standard may be appropriate.

Indeed, we offer in this Comment Letter suggestions for more transparency in ISR reporting.

We note that this question and our response provide a good example of our view: that often only minimal changes are needed to most existing securities regulation in order to allow for the issuance and trading of Digital Securities in Canada.

Other Questions

The remaining questions include those which are more-relevant to cryptocurrency trading. We have no comments to make on these questions:

7. What factors should be considered in determining a fair price for crypto assets?

We have no comment on this question.

8. Are there reliable pricing sources that could be used by Platforms to determine a fair price, and for regulators to assess whether Platforms have complied with fair pricing requirements? What factors should be used to determine whether a pricing source is reliable?

We have no comment on this question.

12. Are there other risks specific to trading of crypto assets that require different forms of surveillance than those used for marketplaces trading traditional securities?

We have no comments on this question beyond those already provided.

³ The Boston Fed's paper is available at <https://www.bostonfed.org/-/media/Documents/one-time-pubs/2019/blockchain-white-paper.pdf>

16. *What type of insurance coverage (e.g. theft, hot-wallet, cold-wallet) should a Platform be required to obtain? Please explain.*

We have no comment on this question.

17. *Are there specific difficulties with obtaining insurance coverage? Please explain.*

We have no comment on this question.

19. *Are there other models of clearing and settling crypto assets that are traded on Platforms? What risks are introduced as a result of these models?*

We have no comment on this question.

20. *What, if any, significant differences in risks exist between the traditional model of clearing and settlement and the decentralized model? Please explain how these different risks may be mitigated.*

We have no comment on this question.

21. *What other risks are associated with clearing and settlement models that are not identified here?*

We have no comment on this question.

22. *What regulatory requirements, both at the CSA and IIROC level, should apply to Platforms or should be modified for Platforms? Please provide specific examples and the rationale.*

We have no comments on this question beyond those already provided.

Conclusion

We are greatly encouraged by your work to date, as represented by the Consultation Paper and congratulate you on the initiative. The Paper is a significant step in establishing a clear regulatory framework for Digital Assets in Canada and follows a policy-development protocol which has brought Canada respect for advancing well thought-out regulations.

We believe that innovative new Platforms for issuing and trading both Cryptocurrencies and Digital Securities hold significant promise and opportunity for Canadian investors, issuers and the Canadian economy overall. But we do not believe that the similarities in underlying technologies, nor some applicants' practice of conflating assets and currencies, recommend that Canada should pursue a single framework for regulating cryptocurrencies and Digital Securities.

Speaking from our experience with Digital Securities and with Canada's securities regulations, we are confident that Canada's existing securities issuance and trading framework provide excellent foundations upon which to create a framework for the regulation of Digital Securities Platforms. And we believe Canada is well-positioned to benefit significantly from the accomplishment of such a regulatory framework for Digital Securities.



We hope that you find our comments – on a topic that is broad, complex and fast-moving - contribute to your thinking on a framework, and we look forward to next steps.

On behalf of The Jersey Company,

A handwritten signature in black ink, appearing to read "Robert Young".

Robert Young

MANAGING PRINCIPAL



T: +1 416 300 0110

E: Robert.Young@TheJerseyCo.com

W: www.TheJerseyCo.com





TD Securities
TD Bank Group
Ernst & Young Tower
222 Bay Street, 7th Floor
Toronto, Ontario M5K 1A2

Investment Industry Regulatory Organization of Canada
British Columbia Securities Commission
Alberta Securities Commission
Financial and Consumer Affairs Authority of Saskatchewan
Manitoba Securities Commission
Ontario Securities Commission
Autorité des marchés financiers
Financial and Consumer Services Commission (New Brunswick)
Superintendent of Securities, Department of Justice and Public Safety, Prince Edward Island
Nova Scotia Securities Commission
Securities Commission of Newfoundland and Labrador
Superintendent of Securities, Northwest Territories
Superintendent of Securities, Yukon
Superintendent of Securities, Nunavut

via e-mail

May 15, 2019

Re: Joint CSA/IIROC Consultation Paper 21-402 Proposed Framework for Crypto-Asset Trading Platforms

Dear Sirs and Mesdames:

TD Securities welcomes and appreciates the opportunity to comment on the Joint CSA/IIROC *Proposed Framework for Crypto-Asset Trading Platforms* (the Proposed Framework).

TD Securities is a leading securities dealer in Canada and a top ranked block trader in Canadian equities and options based on dollar value and shares traded. TD Securities also acts as the execution broker for TD Waterhouse, the largest direct investing brokerage firm in Canada.

BACKGROUND

A cryptocurrency is a digital or virtual currency designed to work as a medium of exchange. It uses cryptography to secure and verify transactions as well as to control the creation of new units of a cryptocurrency. Essentially, cryptocurrencies are limited entries in a database that no one can change unless specific conditions are fulfilled. The challenges going forward from a Regulatory perspective would entail the operational requirements intended to protect participants from the counterparty and other risks associated with Platforms, such as requirements for market integrity, market surveillance, fair pricing, custody, clearing and settlement, disclosure of conflicts of interest, and systems and business continuity planning.

CSA/IIROC QUESTIONS:

- 1) Are there factors in addition to those noted above that we should consider?

TD Securities believes there are 4 clear categorizations to be examined:

1) Coins or Cryptocurrencies – These would include digital currencies such as Bitcoin whereby encryption techniques would be used to regulate the generation of currency units and thus the verification of the transfer of fund. This would be operated independently of a Central Bank. Items such as Stable coins/Bank coins could be issued by Financial Institutions or other credible Global entities where hypothetically every Fiat currency could one day become a cryptocurrency.

2) Utility tokens (ICO's/Crowdfunding tokens) – Utility tokens are services or units of services that could be purchased. These tokens can be compared to API keys which could be used to access these services.

3) Security Tokens – These would be tokens that could represent shares of a business that has Cashflow. In addition, considering the recent SEC announcement, "any tokens that cannot pass the Howey Test" should be considered a Security and fall under the 1934 Securities Exchange Act.

4) Asset backed Tokens – An asset backed token is a blockchain token that has a link with an object with economic value. This object would be tangible or intangible (e.g. Property vs Patent). The asset backed token would help to digitize an asset and the information would be recorded via blockchain. This asset-based token could then easily be transferred to whoever decides to buy the property.

2) What best practices exist for Platforms to mitigate these risks? Are there any other substantial risks which we have not identified?

TD Securities believes and has outlined below other substantial risks that have not been identified previously.

- *Multi signature wallets (hot wallets vs cold wallets)*
- *Segregation of accounts (client vs proprietary)*
- *Regular technical and financial audits*
- *Regular security tests (pen test)*
- *Decentralized Exchanges*
- *Governance committees*
- *Better KYC/AML (more automated solutions, compliance layers on top of blockchains)*
- *Third party reports on Platform volumes and trading data*
- *Moving platforms to non-offshore jurisdictions*
- *Higher security reviews of staff*
- *Investments into 3rd party custody services (e.g. Bitgo)*

3) Are there any global approaches to regulating Platforms that would be appropriate to be considered in Canada?

TD Securities has identified the following potential Global approaches to regulating platforms that could be considered appropriate to be used in Canada. In NY and in Singapore they issue something called "bit-licenses" to operate while in Singapore they are in the process of issuing security token licenses for exchange operator. The process in NY is an application that gets vetted before licenses are issued. In Singapore, applicants must go thru their sandbox and clear the sandbox requirements before a license is issued. Other countries like Japan are also moving towards the license-based model for crypto exchanges. A fine balance needs to be put in place as the harder and onerous the application process is, the likelihood that technology companies will move to jurisdictions with lower barriers of entry. The application process needs to be prudent, balanced and fair not overly burdensome for the sake of slowing done technology.

- 4) What standards should a Platform adopt to mitigate the risks related to safeguarding investors' assets? Please explain and provide examples both for Platforms that have their own custody systems and for Platforms that use third-party custodians to safeguard their participants' assets

TD Securities believes mitigating the risks relating to safeguarding an Investors' Asset is of the utmost importance. Some of the steps TD Securities would support and enact would be platforms that are completely decentralized so there would be no impropriety of any "middle men" to hold private keys or assets. Regular reporting on transactions both on and off exchange will be vital and would tie into regular audits (Security, technical/code and financial, Internal and External etc.) that would greatly assist in minimizing risk. Finally, an enhanced and robust Risk Management program which would set the terms of Limit setting, notifications and Circuit Breakers.

- 5) Other than the issuance of Type I and Type II SOC 2 Reports, are there alternative ways in which auditors or other parties can provide assurance to regulators that a Platform has controls in place to ensure that investors' crypto-assets exist and are appropriately segregated and protected, and that transactions with respect to those assets are verifiable

TD Securities would look to implement alternative ways such as 3rd party custodians as well as other tools to look into various transactions. This can transpire via Blockchain data startups as well as specialized skillsets that comprehend Blockchain, Crypto and other Emerging Technology that are with Regulators such as those like MAS in Singapore, that has a Special team dedicated to this as well as the SFC team in Hong Kong to ensure that investors' crypto-asset exist and are appropriately segregated and protected.

- 6) Are there challenges associated with a Platform being structured to make actual delivery of crypto assets to a participant's wallet? What are the benefits to participants, if any, of Platforms holding or storing crypto assets on their behalf?

TD Securities believes that most platforms that control and retain assets on behalf of their clients would be part and parcel for the issues we have observed and be the best way forward. This would be done to establish and create platforms that decentralize or segregate assets with a 3rd party custodian. There would be no issues in securing a platform that makes delivery of client assets efficient. This would require that the platform hold the assets until payments are delivered. The best solution would be to segregate this service (i.e. settlement/clearing) thru a 3rd party custodial service or for TD Securities to be completely decentralized from the platform.

- 7) What factors should be considered in determining a fair price for crypto assets?

TD Securities believes there would be a threefold factor approach in determining a "fair price" for crypto assets:

- 1) 3rd party reference data (reliable/vetted) is of utmost importance.*
 - 2) a matching engine for the bid/offer that is fair and transparent and*
 - 3) good liquidity with a mix of flows (Institutional, Retail, Liquidity Providers and Market Makers etc.).*
- This would be a catalyst and incentivize that pricing would be conducted in the proper fashion and not be viewed as predatory.*

- 8) Are there reliable pricing sources that could be used by Platforms to determine a fair price, and for regulators to assess whether Platforms have complied with fair pricing requirements? What factors should be used to determine whether a pricing source is reliable?

TD Securities believes there are several external sources that can be used to determine whether a pricing source is reliable. The most obvious source would be Bloomberg as it is the global bellwether for reliable sources and feeds which encompasses absorbing data from 2-3 globally large exchanges such as Coinbase, Kraken and Bitstamp, Coinmarketcap.com would also be a reliable and credible source. Having large data providers in the current traditional financial ecosystem as well as the traditional exchanges participating in developing the next digital financial system would also manifest and establish a good partnership to consider for Regulators globally. Finally, for less liquid assets, Poloniex could be a good platform to reference. Poloniex was acquired by Circle, which is a Goldman Sachs backed Crypto platform.

- 9) Is it appropriate for Platforms to set rules and monitor trading activities on their own marketplace? If so, under which circumstances should this be permitted?

TD Securities disagrees with the concept of platforms being able to set rules and having the ability to monitor trading activities on their own marketplace. TD Securities believes that 3rd Party Surveillance would be a more comprehensive and well-rounded model. There are many platforms throughout the World, particularly in China where trading volumes are not transparent, therefore the accuracy cannot be verified. In terms of setting trading rules, currently traditional exchanges are not regulated in terms of their daily transaction activities. They form their own rules that best fit the needs of their customers/members. Perhaps looking at a "membership" system would help platforms manage the operation and subsequently police the various players versus an open-door onboarding policy where anyone can trade post proper KYC.

- 10) Which market integrity requirements should apply to trading on Platforms?
Please provide specific examples.

TD Securities believes there are 5 key market Integrity requirements that should apply to trading on Platforms:

- 1) Daily reporting on Funds, Transactions and Volumes.*
- 2) Daily reconciliation between reported data and 3rd party data.*
- 3) Proper Segregation of Accounts and proof of Funds.*
- 4) Regular and robust Audits, both Internal and External and*
- 5) Proper documentation of KYC/AML for all clients.*

- 11) Are there best practices or effective surveillance tools for conducting crypto asset market surveillance? Specifically, are there any skills, tools or special regulatory powers needed to effectively conduct surveillance of crypto asset trading?

TD Securities has observed that new startups within the Cryptocurrency field have recently established systems that offer Reporting and Surveillance tools for 3rd parties. One is Blockchain.com which offers an API that allows clients to view network level transactions, wallets etc. Another is Etherscan.io which is an

equivalent and alternative to Blockchain.com which allows clients to observe the transaction history, wallets/addresses and the total supply of Ether. These are just a couple, of examples TD Securities believes could be used as tools that could be used to effectively conduct surveillance for crypto asset trading.

- 12) Are there other risks specific to trading of crypto assets that require different forms of surveillance than those used for marketplaces trading traditional securities?

TD Securities notes concerns for risks applicable to big off exchange marketplaces for trading cryptocurrencies such as Bitcoin and Ethereum. Transactions are conducted wallet to wallet, bank to bank and TD Securities postulates that this would be extremely risky unless a client is dealing with a trusted counterparty. Currently, there is no proper infrastructure at the moment to enable robust monitoring, surveillance and reporting for this flow.

- 13) Under which circumstances should an exemption from the requirement to provide an ISR by the Platform be considered? What services should be included/excluded from the scope of an ISR? Please explain

TD Securities feels the only circumstance whereby an exemption from the requirement to provide an ISR by the Platform would be one where the platform is a fully operational, distinctly decentralized exchange where there would be no middle entity of people managing assets or funds.

Currently, crypto exchanges are immediately compromised when they hold their customers private keys (i.e. passwords). In order to be secure and risk free, exchanges need to move more towards a fully decentralized system with multi signature wallets playing a big part in the transactions. This would ensure that private keys are held at each end point rather than a middle man, in this case the exchange. All transactions are done peer to peer and the decentralized exchange or DEX only matches and settles the transactions without having to hold private keys. This is the future state that the Canadian Regulators should strive towards in terms of enabling players in the Canadian market. A fully decentralized exchange with customers using an integrated multi sig wallet solution is the only structure that could warrant a provision or exemption to the ISR.

- 14) Is there disclosure specific to trades between a Platform and its participants that Platforms should make to their participants?

TD Securities believes that at a minimum, Platforms should create and establish a fully vetted 3rd party source report on trading volumes and public audit reports (monthly or quarterly) on all funds. As well, it is the belief of TD Securities that an Annual security report be made public to user – example: Penetration testing on the networks which would be very useful for transparency and would garner goodwill and confidence from the public.

- 15) Are there particular conflicts of interest that Platforms may not be able to manage appropriately given current business models? If so, how can business models be changed to manage such conflicts appropriately?

TD Securities believes there are certain conflicts of interests that platforms are not managing currently given the prevailing business models. Currently there are still many platforms that do not accurately and suitably segregate customer funds from their own business funds. As well there is a lack of proper established procedures that helps to clarify and avoid Front Running of customers' orders. Finally, secure and protected procedures need to be established as Private keys that allow for access to client wallets are being mishandled and not properly handled.

Regular 3rd party/independent financial, operational and security audits would be a good gauge to ensure that players are consistently improving/enhancing their fiduciary duties as well as strengthening good corporate governance. Within the current banking model, similar checks and balances are put in place with respect to security on infrastructure, financial audits and governance checks on change control and process models.

16) What type of insurance coverage (e.g. theft, hot-wallet, cold-wallet) should a Platform be required to obtain? Please explain.

Currently, there is not mechanism where any viable issuer is prepared and willing to underwrite cryptocurrency platforms. TD Securities gives credence to the belief that the best insurance policy would be a durable and unyielding security framework to help mitigate against the potential for hacks and thefts, which 9 times out of 10 occur due to an internal breach. A considerable number of platforms also do not have the basic and fundamental skillset to establish a cohesive and qualified "short term" money market/treasury functions to ensure funds are suitably managed in terms of continuing and ongoing cash inflows and outflows.

17) Are there specific difficulties with obtaining insurance coverage? Please explain.

Currently, Insurance Coverage is not offered in the industry yet. TD Securities believes this is primarily due to the technicalities and vulnerabilities of businesses to hackers. Until this is compelling and serious progress in securing existing businesses. Insurers, as such, are not willing to underwrite policies significant scope and volumes.

18) Are there alternative measures that address investor protection that could be considered equivalent to insurance coverage?

It is the belief of TD Securities that constructing and investing in decentralized platforms eliminating the necessity for other "middle" entities managing assets and funds would be the best alternative to address investor protection as a thorough equivalent to insurance coverage. This would alleviate and mitigate the necessity for insurance as a sound and vigorous Decentralized Exchange with a fully integrated multi sig wallet would make hacking an extremely remote possibility given the resources required to attack such an infrastructure.

19) Are there other models of clearing and settling crypto assets that are traded on Platforms? What risks are introduced as a result of these models?

TD Securities is of the opinion that due to size of scale problems for a good deal of major Blockchains (e.g. Ethereum) the concept of developing and promoting decentralized exchanges would require greater energy and potency than a centralized exchange relying upon off chain procedures. This would create for the necessity to match orders off the "main" chain and then subsequently bring back those matched

order for settlement. Ultimately the process would be united to 1) order book matching off chain and 2) settlement on the chain. TD Securities believes the risks are yet to be seen as there are currently only a handful of decentralized exchanges that are active presently.

20) What, if any, significant differences in risks exist between the traditional model of clearing and settlement and the decentralized model? Please explain how these different risks may be mitigated

Currently the key difference with decentralized settlement, trades are cleared in real time whereas in the traditional function, settlement normally takes effect on a T+ basis with matching trades and payments transpiring in manual and costly manner. The occurrence of a higher degree of human error is a possibility whereas the decentralized model would automate and help to streamline the process.

21) What other risks are associated with clearing and settlement models that are not identified here?

The other risks associated with the clearing and settlement models that have not been identified would include:

- 1) Security. TD Securities would consider this one of the greater risks whether it is user access, human error and fraud (creating bogus and fabricated accounts).*
- 2) Having the settlement process transpire in "real time" over a blockchain permits and facilitates mitigation from any and all potential human related risks that is widely seen in today's markets.*
- 3) The costs associated with clearing and settlement would dramatically decrease and*
- 4) when assets move faster, payments move faster thus creating a higher turnover on the network(s) ultimately beneficially benefitting Money Managers, businesses, investors and overall users.*

22) What regulatory requirements, both at the CSA and IIROC level, should apply to Platforms or should be modified for Platforms? Please provide specific examples and the rationale

The regulator requirements TD Securities believes should apply to Platforms would be:

- 1) Mandatory Audits (Internal and External),*
- 2) Mandatory Reporting,*
- 3) Compulsory Internal training for employees and management at various start-ups,*
- 4) Mandatory "white hat" and "black hat" security tests (pen test) and*
- 5) a potential "Licensing" requirement as an option.*

CONCLUSION

We thank the regulators for its work on this framework proposal as Crypto-Assets are an important and growing area of interest across the globe. TD Securities welcomes any questions IIROC or CSA staff may have with respect to these comments.

Joint Canadian Securities Administrators/Investment Industry Regulatory Organization of Canada

Consultation Paper 21- 402 – KNØX INDUSTRIES Response

PART 2 - Nature of crypto assets and application of securities legislation

Question 1: Are there factors in addition to those noted above that we should consider?

Ans:

In some cases, the responsible entity or trustee may elect to provide self-custody, but must be able to demonstrate that the assets are held separately from its own assets and meet capital requirements.

Benefits of appointing a custodian include:

- ▶ Ensuring assets are properly segregated from the assets of other trusts
- ▶ Safeguarding asset portfolios to protect investors
- ▶ Enabling the responsible entity/trustee and trust manager to concentrate on managing the fund
- ▶ Assisting with the marketing of the fund to investors by increasing investors' confidence
- ▶ Demonstrating corporate governance
- ▶ Protecting investors' assets in the event of an insolvency event of the responsible entity/trustee
- ▶ Utilizing the custodian's scale to minimize transaction costs and operational efficiency

In addition to traditional custodian services, depicted above, modern custodians of digital assets provide security and safekeeping of assets, which requires additional controls.

In today's market place, the following factors need to be considered:

- a) The design and orchestration of the technology involved in digital asset safekeeping is a highly specialized endeavour.
- b) Organizations engaging in a number of activities are simultaneously undertaking digital asset safekeeping.

Given the current environment and understanding of digital assets, specialized organizations which understand and can demonstrate adequate implementation of requisite controls can be relied on to provide modern custodial services. Just the same, if self-custody is implemented, it should be expected to meet the same level of stringent controls. Due to the specialized nature of the activity and the advantages of appointing a specialized custodian, the industry should be encouraged to segregate custodial services from others.

PART 3 - Risks related to platforms

Question 2: What best practices exist for Platforms to mitigate these risks? Are there any other substantial risks which we have not identified?

Ans:

Risks are best mitigated by ensuring implementation and practice of identified controls, which are monitored, reported on, and audited by a third party. The best way to assert controls are designed and operating effectively is by obtaining an insurance policy via regulated insurance companies.

The act of obtaining an insurance policy mitigates risks in two very important ways:

1. It allows for the issuance of insurance claims in the event of losses, making customers whole.
2. Insurance companies are currently the most knowledgeable third parties regarding the design and implementation of a rigorous set of controls. This is no surprise considering they are accepting the transfer of the underlying risk.

Insurance providers must on a periodic basis assure themselves that all operational controls are in order, including internal and/or external controls; both qualitative and/or quantitative. Thus, the act of obtaining insurance is a higher marker for safety than any other controls (i.e. SOC2, COSO, ITIL, etc) and provides a degree of security to those whose assets are insured under custody. By enforcing insurance coverage on custodial services, regulators will enable effective and tested controls which in turn provide lower overall risk to the customer's digital assets under custody.

The safe-keeping of customer funds by entities that have not undergone the rigorous process of obtaining an insurance policy is a substantial unidentified risk.

PART 4 - Regulatory approaches in other jurisdictions

Question 3: Are there any global approaches to regulating Platforms that would be appropriate to be considered in Canada?

Ans: There are many other global approaches with arising regulatory frameworks in the space of digital custody and fintech. One of the ones that we have looked into is Autorité des Marchés Financiers (AMF) in France. As of April 11th, 2019, AMF has adopted the PACTE draft Bill (action plan for business growth and transformation). This law will establish a framework for fundraising via the issuance of virtual tokens (ICOs) and digital assets services providers (DASP). Under this bill, there are two focus areas: 1) optional visa regime for ICOs and 2) optional license for digital assets services providers.

PART 5 - The Proposed Platform Framework

5.2.1 Custody and verification of assets

Question 4: What standards should a Platform adopt to mitigate the risks related to safeguarding investors' assets? Please explain and provide examples both for Platforms that have their own custody systems and for Platforms that use third-party custodians to safeguard their participants' assets.

Ans:

As indicated in previous answers, it is highly recommended that regulators discourage self-custody until organizations develop the knowledge and technology required to be able to provide insured custodial services.

In most cases, the best route for any Platform will be to appoint a third party custodian that is adequately insured.

Question 5: Other than the issuance of Type I and Type II SOC 2 Reports, are there alternative ways in which auditors or other parties can provide assurance to regulators that a Platform has controls in place to ensure that investors' crypto-assets exist and are appropriately segregated and protected, and that transactions with respect to those assets are verifiable?

Ans:

In our experience, working extensively with both the insurance industry and consulting firms in the current climate, the issuance of SOC 2 Type I and Type II reports is not an adequate marker of safety.

As indicated above, at the current moment, based on our experience, entities from the insurance industry are the third parties best fit to assess the design and implementation of a set of controls in digital asset custody.

In addition to the advantages stated above, insurers have shown themselves capable of learning and adapting to the level of controls expected at a faster pace than any other third parties. They can thus be expected to steadily increase the safety of the industry as a whole.

Many organizations are generating SOC2 reports by using smaller third party consulting practices not recognizable on the market while the big 4 consulting firms are still establishing benchmarks for SOC2 controls that will apply to digital custody services. Should SOC2 reports mature to the point that they are useful markers of safety, their issuance may be recommended. At the moment, however, we do not believe that obtaining such a report is indicative of a sound operation.

The best way of assuring regulators that a Platform has an adequate level of controls is by way of obtaining an insurance policy that transfers the most critical risks. In such a way, regulated third parties who are willing to expose capital to these risks are vetting the safety of any Platform.

Question 6: Are there challenges associated with a Platform being structured so as to make actual delivery of crypto assets to a participant's wallet? What are the benefits to participants, if any, of Platforms holding or storing crypto assets on their behalf?

Ans:

In many cases, a Platform's operation requires holding or storing assets on a participant's behalf. In cases where this is not required, it is recommended that participants be given the right to hold the assets on their own terms.

However, in the many cases where a Platform's operation requires that it hold or store assets on a participant's behalf, regulators should be assured that the assets are safely stored. The recommendation for most cases is for the Platform to appoint an insured third party custodian that meets the stringent levels of safety expected.

5.2.2 Price determination

Question 7: What factors should be considered in determining a fair price for crypto assets?

Ans:

In our opinion, the best demonstrated pricing of digital assets has been shown in the pricing of futures contracts traded on the CME and CBOE. For example, the CME CF Bitcoin Real Time Index (BRTI) and the the CME CF Bitcoin Reference Rate (BRR).

The methods used are in alignment with SEC requirements, and the generation of agreeable reference rates for other products should be welcomed by the industry.

Question 8: Are there reliable pricing sources that could be used by Platforms to determine a fair price, and for regulators to assess whether Platforms have complied with fair pricing requirements? What factors should be used to determine whether a pricing source is reliable?

Ans:

See Question 7.

5.2.3 Surveillance of trading activities

Ans:

We believe that Questions 9 through 12 are important to address. However, we do not presently engage in trading activities and we wish to leave treatment of this area to others.

Question 9: Is it appropriate for Platforms to set rules and monitor trading activities on their own marketplace? If so, under which circumstances should this be permitted?

Question 10: Which market integrity requirements should apply to trading on Platforms? Please provide specific examples.

Question 11: Are there best practices or effective surveillance tools for conducting crypto asset market surveillance? Specifically, are there any skills, tools or special regulatory powers needed to effectively conduct surveillance of crypto asset trading? ?

Question 12: Are there other risks specific to trading of crypto assets that require different forms of surveillance than those used for marketplaces trading traditional securities?

5.2.4 Systems and business continuity planning

Technology and cyber security are key risks for Platforms. For these reasons they will also be required to comply with the systems and business continuity planning requirements applicable to existing marketplaces in Regulation 21-101.

Question 13: Under which circumstances should an exemption from the requirement to provide an ISR by the Platform be considered? What services should be included/excluded from the scope of an ISR? Please explain. ISR = independent system review.

Ans: Third party assessments are recommended and should continue to be a requirement. Independent system reviews are already a part of insurance market efforts. Insurance policies are priced partly on the basis of such reviews. It is highly recommended that the scope of services be defined by insurance markets in the interim, with others such as consulting services set to follow.

5.2.5 Conflicts of interest

Question 14: Is there disclosure specific to trades between a Platform and its participants that Platforms should make to their participants?

We do not presently engage in trading activities and we wish to leave treatment of this area to others.

Question 15: Are there particular conflicts of interest that Platforms may not be able to manage appropriately given current business models? If so, how can business models be changed to manage such conflicts appropriately?

Ans:

Beyond the worries surrounding safe-keeping, entities engaging in self-custody may produce conflicts of interest that need to be carefully considered. As such, the appointment of a third party custodian is the best recommended practice at the moment, until such time as the full set of conflicts of interest are understood and appropriately accounted for in entities wishing to engage in self-custody of digital assets.

5.2.6 Insurance

Question 16: What type of insurance coverage (e.g. theft, hot-wallet, cold-wallet) should a Platform be required to obtain? Please explain.

Ans:

As indicated above, we believe that obtaining an insurance policy is one of the best ways to both safeguard participants and assure regulators that a Platform has implemented an adequate set of controls.

The risks transferred should include, at a minimum, theft and loss of assets, including internal collusion within the entity safekeeping digital assets. Obtaining such insurance ensures the client that operational and security controls have been tested and continue to be monitored by the insurance provider. In most cases, companies obtaining insurance policies are obtaining either inadequate levels of insurance, inadequate range of coverage, or both.

Question 17. Are there specific difficulties with obtaining insurance coverage? Please explain.

Ans:

Exceedingly few firms have designed and implemented the rigorous set of controls necessary to safely store digital assets. Most of these firms, including those capable of obtaining SOC Type I or Type II reports, would fail to secure an insurance policy due to the stringency of controls expected. It is for this reason that the capability to obtain and renew an insurance policy remains the best assurance of underlying safety to regulators and participants.

Custodians with adequate controls should have no problem obtaining insurance.

Question 18. Are there alternative measures that address investor protection that could be considered equivalent to insurance coverage?

Ans:

Alternatives may include practices such as the establishment of a reserve fund of cryptocurrencies or digital assets whose prices correlate with those of the digital assets exposed to theft and loss risk. Such reserves should themselves be held in an insured custody arrangement.

5.2.7 Clearing and settlement

Ans: Questions 19-21 are not within the scope of KNØX's operations.

Question 19: Are there other models of clearing and settling crypto assets that are traded on Platforms? What risks are introduced as a result of these models?

Question 20: What, if any, significant differences in risks exist between the traditional model of clearing and settlement and the decentralized model? Please explain how these different risks may be mitigated.

Question 21: What other risks are associated with clearing and settlement models that are not identified here?

5.2.8 Applicable regulatory requirements

Question 22: What regulatory requirements, both at the CSA and IIROC level, should apply to Platforms or should be modified for Platforms? Please provide specific examples and the rationale.

Ans: SOC2 requirements need to be modified for digital custodians before they are deemed fit to assess the safety of any firm engaging in custodial activities. Digital custodians need to mature for SOC2 requirements to be modified and/or updated thereby incorporating/understanding digital custody service needs.



State Street Corporation

James J. Biancamano
Managing Director

600 College Road East
Princeton, NJ 08540

Telephone: 609.580.5313
JBiancamano@statestreet.com

www.statestreet.com

May 15, 2019

Me Anne-Marie Beaudoin
Corporate Secretary
Autorité des marchés financiers
800, rue du Square-Victoria, 22e étage
C.P. 246, Place Victoria
Montréal (Québec) H4Z 1G3
Via email: consultation-en-cours@lautorite.qc.ca

The Secretary
Ontario Securities Commission
10 Queen Street West
22nd Floor, Box 55
Toronto, Ontario M5H 3S8
Via email: comments@osc.gov.on.ca

Victoria Pinnington
Senior Vice President, Market Regulation
Investment Industry Regulatory Organization of Canada
Suite 2000, 121 King Street West
Toronto, Ontario M5H 3T9
Via email: vpinnington@iiroc.org

Re: Proposed Framework for Crypto-Asset Trading Platforms

Dear Madams or Sirs:

State Street Corporation (“State Street”) appreciates the opportunity to respond to the joint Canadian Securities Administrators (“CSA”) and the Investment Industry Regulatory Organization of Canada’s (“IIROC”) Consultation Paper on a Proposed Framework for Crypto-Asset Trading Platforms (“consultation paper”).¹ Specifically, the CSA and IIROC seek feedback as they begin to establish a regulatory framework for platforms facilitating the buying and selling of crypto-assets. This includes requirements regarding the custody of such assets.

¹ See https://www.osc.gov.on.ca/documents/en/Securities-Category2/csa_20190314_21-402_crypto-asset-trading-platforms.pdf.

STATE STREET

Headquartered in Boston, Massachusetts, State Street specializes in the provision of financial services to institutional investor clients, such as pension plans, mutual funds, alternative investment funds, central banks, charitable foundations and endowments. This includes the provision of investment servicing, investment management, data and analytics, and investment research and trading. With \$32.643 trillion in assets under custody and administration and \$2.805 trillion in assets under management, State Street operates in more than 100 geographic markets globally.²

State Street is organized as a United States (“U.S.”) bank holding company, with operations conducted through several entities, primarily its wholly-insured depository institution subsidiary, State Street Bank and Trust Company (“SSBT”). In Canada, State Street provides global custody and local financial services through State Street Trust Company Canada, a Canadian federal trust company and wholly-owned subsidiary of SSBT, the Canadian branch of SSBT and State Street Global Markets Canada Incorporated.

State Street supports the development of a proper regulatory regime for digital assets, such as crypto-assets (including crypto-currencies, utility tokens and security tokens, hereinafter referred to as “digital assets”) which will assist platforms that facilitate the buying and selling, or the transferring, of digital assets. In our view, the participation of institutional investors in this new asset class will only materially develop to the extent that the market structure for digital assets improves and the regulatory framework is clarified.

As described in more detail below, we strongly believe that custody banks should be involved in ensuring the proper safekeeping of digital assets; that minimum safeguards and standards should be established for platforms engaged in the buying and selling of digital assets; and efforts should be made to expand the availability and affordability of insurance for digital assets.

I. Use of Regulated Custodial Entities

State Street recommends that the custody of digital assets should be limited to regulated custodial entities, such as banks and trust companies. As emphasized in the consultation paper, some digital assets platforms are hybrid in nature and perform several functions similar to those of various market participants, including custodians. This includes the self-custody of investors’ assets or systems which give the platform control over investors’ assets. We are concerned that platforms that engage in the buying or selling of digital assets may not have sufficiently robust systems in place to mitigate risks and ensure the safety and soundness of assets. Most notably, some digital asset platforms may not segregate investor assets from their own, a practice that is central to the proper safekeeping and control of assets.

Regulated custodial entities, such as State Street, specialize in the safekeeping and administration of investment assets, and already have well established processes and controls in place to safeguard assets. Similarly, custodial entities have the necessary experience and expertise to develop policies, procedures and controls for digital assets as the regulatory regime evolves. Moreover, regulated custodial entities routinely segregate investors’ assets from their own, and perform in-depth know-your-customer and anti-money laundering assessments. We believe that there should be no exceptions from these core practices when guarding against the misappropriation of digital assets.

² As of March 31, 2019.

In our view, key areas of consideration required for the custody of digital assets include: (1) information systems and technology; (2) the operating model; and (3) the manner in which digital assets are reflected in the underlying distributed ledger technology (“DLT”) and the requisite controls over DLT. For example, to mitigate the risk of misallocation and malicious transfers, controls should be put in place to approve transactions which are appropriately managed via either infrastructure and/or layers of software. The operating model should, in turn, delineate responsibilities, escalation procedures and business continuity plans. It also should control what final users/beneficial owners are permitted to do with digital assets (*e.g.* prevent the selling or transferring of digital assets to facilitate illicit activities).

As such, regulated custodial entities are, in our view, better positioned to support the custody of digital assets than other market entities, such as trading platforms.

II. Establish Minimum Standards for the Custody of Digital Assets (Question 4)

As a threshold matter, we believe that platforms for digital assets that engage in custody should be subject to the same regulations and principles which apply to other financial market infrastructures, as outlined by the Committee on Payment and Settlement Systems and the International Organization of Securities Commissions.³ This includes principles around: credit and liquidity risk management; settlement and settlement systems; default management; operational and business risk management; access; efficiency; and transparency.

In addition, State Street recommends the establishment of minimum operating standards for the custody of digital assets. As mentioned in the consultation paper, a significant risk to digital assets is that they are not adequately safeguarded in today’s operational environment. We therefore support the adoption of a set of minimum standards which address:

- Segregation of assets;
- Data privacy and cybersecurity;
- Verification of assets, including multi-signature authorizations for transactions, with rotating permissions; hyper-secure (*i.e.* complete end-to-end) encryption of private keys; and enhanced control protections, including physical access to wallets and security protocols for private keys; and
- Development of a standardized settlement cycle, reconciliation requirements and dispute adjudication procedures.

III. Minimum Insurance Coverage Availability (Questions 16, 17, and 18)

Finally, State Street strongly supports efforts to promote the availability of more affordable, minimum insurance coverage for digital assets. The consultation paper discusses the difficulty and high costs for platforms to obtain insurance due to the lack of consistent regulatory guidance around the custody of digital assets, the limited number of insurance providers and the high risk of cyber-attacks.

³ Committee on Payment and Settlement Systems Technical Committee of the International Organization of Securities Commissions- Principles for financial market infrastructures. April 2012. Available at <https://www.bis.org/cpmi/publ/d101a.pdf>.

STATE STREET

State Street agrees with this assessment. The lack of transparency and the difficulty in assessing security of digital assets drives increased costs which are exponentially higher than insurance rates for traditional assets. We suggest that the CSA and IIROC encourage the development of innovative insurance solutions for digital assets.

For example, insurance intermediation platforms have been recently introduced to the market which could provide a unique solution for crypto-assets. Platforms can offer these products which permit the use of digital tokens for premiums, thus allowing the platform itself to provide insurance to its clients. In effect, the insurance platform acts an intermediary between clients and the traditional insurance market, leading to decreased insurance costs for users and increased levels of protection.

Furthermore, we recommend, that all insurance products for digital assets cover the following:

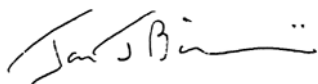
- Third-party hacking and the theft of private keys;
- Insider (*i.e.* employees) hacking and theft of private keys;
- System breakdowns; and
- The death or incapacity of a keyholder.

Conclusion

Thank you once again for the opportunity to respond to the consultation paper. We appreciate the CSA's and IIROC's engagement on this matter and look forward to the opportunity to serve as a resource as the regulatory regime for digital assets evolves to support the needs of the Canadian market.

Please feel free to contact me at JBiancamano@StateStreet.com should you wish to discuss State Street's submission in further detail.

Sincerely,



James J. Biancamano

Consultation questions:**1. Are there factors in addition to those noted above that we should consider?**

A: None

2. What best practices exist for Platforms to mitigate these risks? Are there any other substantial risks which we have not identified?

- there presently exist protocols which have baked into them KYC-based trade restrictions. Those can be extended as needed simply by amending the smart contracts.

- a comprehensive set of rules for the Platforms, and a positive disclosure obligation on the Platforms can go a long distance in mitigating the risks associated with processes, policies and procedures (trade order, conflicts, token security controls, record-keeping, etc.).

- similarly, a standardized (or relatively so) disclosure form can be created that token-issuers must complete and must be kept by the Platform for each token it trades, and that form be provided to each investor prior to completion of any token purchase (complete with a click-box acknowledgement that the form has been read to the investor's satisfaction).

- rules regarding custody can be created. For example, each investor must be clearly presented with the choice to have its tokens stored in its own wallet, or on that of the Platform; Platforms may be allowed to aggregate multiple investors' tokens, but not co-mingle them with Platform's tokens. It may also be determined best that Canadian investors' tokens, if stored by the Platform, must be stored in a cold wallet physically located in Canada.

- an audit function must be introduced with reporting on Platforms' compliance with this set of rules.

3. Are there any global approaches to regulating Platforms that would be appropriate to be considered in Canada?

No comment.

4. What standards should a Platform adopt to mitigate the risks related to safeguarding investors' assets? Please explain and provide examples both for Platforms that have their own custody systems and for Platforms that use third-party custodians to safeguard their participants' assets.

No comment.

5. Other than the issuance of Type I and Type II SOC 2 Reports, are there alternative ways in which auditors or other parties can provide assurance to regulators that a Platform has controls in place to ensure that investors' crypto-assets exist and are appropriately segregated and protected, and that transactions with respect to those assets are verifiable?

No comment.

6. Are there challenges associated with a Platform being structured so as to make actual delivery of crypto assets to a participant's wallet? What are the benefits to participants, if any, of Platforms holding or storing crypto assets on their behalf?

- Speed of completion of trades may be affected if crypto is held in a participant's wallet, if the participant also retains the private key (and not the exchange)
- the participant's wallet may be less secure than that of the exchange, and therefore more prone to hacks, especially in the case of hot wallets
- the participant may be more likely to lose (or have fewer safeguards/redundancies to prevent against the loss of) private keys than an exchange
- for all of the above reasons, it may be preferable to have the Platform store crypto assets on behalf of investors

7. What factors should be considered in determining a fair price for crypto assets?

No comment.

8. Are there reliable pricing sources that could be used by Platforms to determine a fair price, and for regulators to assess whether Platforms have complied with fair pricing requirements? What factors should be used to determine whether a pricing source is reliable?

- Coin Market Cap is widely recognized as a fair resource for a token price. There are also a number of leading exchanges. Often, in M&A transactions, the accepted value of crypto is that as stated in coin market cap, and, should that not be available, the average price of the average in-day price of three leading exchanges.
- Reliability of a pricing source can be assessed based on the degree of variance between the price in question, and that found in the already-accepted authorities. Trading history on a particular exchange may also be a factor in determining price reliability.

9. Is it appropriate for Platforms to set rules and monitor trading activities on their own marketplace? If so, under which circumstances should this be permitted?

- perhaps not initially – if a Platform wants to conduct its own monitoring, it should be required to use an RSP initially, and use its own monitoring system as a duplicate tool. If the 2 regimes yield the same or materially similar results over a stated period of time, then the Platform would have established the case for the use of its own monitoring tool, and the RSP can drop off. However, regulators would retain the right to conduct audits of these Platforms' monitoring systems.

10. Which market integrity requirements should apply to trading on Platforms? Please provide specific examples.

- trading order practices must be implemented – ie: if a bid has several possible matches, it would be paired to the first-posted ask; there would be no discretion as to how trade partners are paired.

11. Are there best practices or effective surveillance tools for conducting crypto asset market surveillance? Specifically, are there any skills, tools or special regulatory powers needed to effectively conduct surveillance of crypto asset trading?

- No comment.

12. Are there other risks specific to trading of crypto assets that require different forms of surveillance than those used for marketplaces trading traditional securities?

- No comment.

13. Under which circumstances should an exemption from the requirement to provide an ISR by the Platform be considered? What services should be included/excluded from the scope of an ISR? Please explain.

- No comment.

14. Is there disclosure specific to trades between a Platform and its participants that Platforms should make to their participants?

- If the Platform is the counterparty to the trade, this must be disclosed.

15. Are there particular conflicts of interest that Platforms may not be able to manage appropriately given current business models? If so, how can business models be changed to manage such conflicts appropriately?

- Many Platforms also issue their own security tokens that would be traded on the Platforms. Platforms would be able to use token supply management to offer price support, and primary token sales by the Platform (from treasury) would always be in conflict to secondary market trades by token holders if both were allowed to occur at the same time. Perhaps it would be necessary to not allow both primary and secondary trades to occur at the same time, meaning that the Platform would have to complete its primary token issuance in order for the tokens to trade on the Platform's secondary market.

16. What type of insurance coverage (e.g. theft, hot-wallet, cold-wallet) should a Platform be required to obtain? Please explain.

- This may be something that the market can decide. Rather than mandate what type of insurance is required, make it mandatory that all Platforms disclose the type and amount of insurance they carry for the benefit of their participants. In that way, participants will select out those Platforms that carry inadequate levels of coverage, and will also select out those that have coverage that is more expensive than they are willing to pay for.

17. Are there specific difficulties with obtaining insurance coverage? Please explain.

- No comment.

18. Are there alternative measures that address investor protection that could be considered equivalent to insurance coverage?

- There could be a form of self-insurance, whether on an individual Platform basis or respecting the industry as a whole, where all Platforms contribute premiums to a central repository, where they are held to compensate participants in cases of loss. The size of premiums assessed against a Platform can be based on trade volume, history of losses (or absence of losses), quality of audit reports, use or non-use of RSP's, whether Platform does or does not maintain custody of crypto, etc.

19. Are there other models of clearing and settling crypto assets that are traded on Platforms? What risks are introduced as a result of these models?

- No comment.

20. What, if any, significant differences in risks exist between the traditional model of clearing and settlement and the decentralized model? Please explain how these different risks may be mitigated.

- No comment.

21. What other risks are associated with clearing and settlement models that are not identified here?

- No comment.

22. What regulatory requirements, both at the CSA and IIROC level, should apply to Platforms or should be modified for Platforms? Please provide specific examples and the rationale.

- No comment.



May 15th, 2019

BY ELECTRONIC MAIL ONLY TO:

comments@osc.gov.on.ca, Consultation-en-cours@lautorite.qc.ca, vpinnington@iiroc.ca

**Ontario Securities Commission
Investment Industry Regulatory Organization of Canada**

**The Secretary
Ontario Securities Commission
20 Queen Street West, Suite 1903, Box 55
Toronto, Ontario M5H 3S8**

**Me Anne-Marie Beaudoin
Corporate Secretary
Autorité des marchés financiers
800, square Victoria, 22e étage
C.P. 246, tour de la Bourse
Montréal (Québec) H4Z 1G3**

**Victoria Pinnington
Senior Vice President, Market Regulation
Investment Industry Regulatory Organization of Canada
Suite 2000, 121 King Street West
Toronto, Ontario M5H 3T9**

INCLUDES COMMENT LETTERS

Eric Gu, Chief Executive Officer
www.viewfin.com
eric.gu@viewfin.com



To Whom It May Concern,

ViewFin Canada is a one-of-a-kind alliance of independent Fintech consulting firms that extends our network and expertise for blockchain solutions globally. We've also partnered with **TulipEx**, a digital assets management platform that will be launching within the next few weeks. Together, we would like to present our comments related to the: **Consultation Paper 21-402 Proposed Framework for Crypto-Asset Trading Platforms**.

We were able to respond to questions: 1, 2, 3, 8, 11 and 15.

1. Are there factors in addition to those noted above that we should consider?

We should consider further compliance factors. Most algorithms are setup with risk criteria. We'd say it's imperative for fintech firms to have solid compliance standards clearly outlined in the manual, prior to entering the market.

2. What best practices exist for Platforms to mitigate these risks? Are there any other substantial risks which we have not identified?

The compliance manual should have a list of indicators of suspicious activity, a flowchart on what to do step by step can help mitigate the risk. This should be periodically updated as the industry is rapidly evolving.

3. Are there any global approaches to regulating Platforms that would be appropriate to be considered in Canada?

A Know Your Customer (KYC) process that is consistent with global standards, evaluating the risks of platforms that operate in higher risk jurisdictions. There are many jurisdictions to learn from, countries in Asia are currently wrestling with these issues as well.

Eric Gu, Chief Executive Officer

www.viewfin.com

eric.gu@viewfin.com



8. Are there reliable pricing sources that could be used by Platforms to determine a fair price, and for regulators to assess whether Platforms have complied with fair pricing requirements? What factors should be used to determine whether a pricing source is reliable?

Pricing Sources will depend on the Crypto currency being traded. The MVIS CryptoCompare Bitcoin Index(MVBTC) maintained by MV Index Solutions GmbH(MVIS). MVIS is a index provider based in Frankfurt Germany and is regulated as an Index administrator by the German financial regulator (BaFin).

MVIS complies with EU benchmark regulations in relation to pricing and conforms with International Organization of Securities organization. We believe reliable pricing for Crypto Currencies is in early days and that over time with regulation, more index providers will start tracking them bringing more legitimacy.

In addition to MVIS, the Chicago Mercantile Exchange (CME) has started to publish CME CF Bitcoin Reference Rate as well as the Ethereum Reference Rate and Real-Time Index. CME Group has developed standardized cryptocurrency references rates and real-time indices with the methodology and rules publishes transparently online:
(<https://www.cmegroup.com/education/bitcoin/cme-cf-cryptocurrency-reference-rate-methodology.html#4-methodology-and-rules>)

11. Are there best practices or effective surveillance tools for conducting crypto asset market surveillance? Specifically, are there any skills, tools or special regulatory powers needed to effectively conduct surveillance of crypto asset trading?

We believe similar to the Canadian markets that a system of Broker or Client ID's be implemented for Crypto Exchanges. This can help mitigate price manipulation and wash trading that can be common in Crypto. Participants on the exchange should be able to see Time & Sales data of executions as well as level 2 data. Designated Market Makers should have their own unique broker code so that market participants can identify that a trade executed with a registered market maker.



15: Are there particular conflicts of interest that Platforms may not be able to manage appropriately given current business models? If so, how can business models be changed to manage such conflicts appropriately?

We believe disclosure is the best way to handle conflicts of interest. TMX and CSE publish Exchange rules online for their clients so that they know how their orders are handled and are bound by Best Execution requirements from the regulator. Crypto Exchanges/Platform's should be governed the same way.

Furthermore TSX openly discloses their policy regarding Market Making (<https://www.tsx.com/trading/toronto-stock-exchange/order-types-and-features/market-maker-program>). It shows the responsibilities of the market maker in relation to Minimum Guaranteed Fill (MGF) Facility and clearly defines their role in the marketplace. The illiquidity of the Crypto Market requires the added liquidity that regulated market makers can provide.

TSX continuously monitors the performance of all Market Makers with respect to their ability to contribute to the overall market in terms of creating liquidity, depth and continuity. Market Makers are assessed on their ability to call a 2-sided market (i.e. spread maintenance), their efforts to line the book with reasonable depth (i.e. liquidity), and their overall participation in trading of the security. We believe first that disclosure should be made to clients and that relationships be disclosed.

Apart from market making, Payment For Order Flow is a concern. Similar to SEC rule 606 in the U.S. Brokers are required by the Securities and Exchange Commission (SEC) to disclose its policies with respect to payment for order flow. According to the SEC, payment for order flow may include monetary payment, reciprocal agreements, services, property, or any other benefit that results in remuneration, compensation, or consideration to a broker-dealer in return for routing of customer order flow and includes exchange rebates and credits

By adopting these proposals to publish exchange rules, regulate exchange market making activity and disclosing Payment for Order Flow compensation, we believe that Crypto platforms regulated in Canada will have an unrivaled regulatory environment to prosper in.

Eric Gu, Chief Executive Officer

www.viewfin.com

eric.gu@viewfin.com



We would like to sincerely thank you for the opportunity to provide our comments. Please do not hesitate to contact us with any questions or concerns you may have.

Thank you.

ViewFin Canada Compliance Team

Adnan Tahir, Chief Compliance Officer - TulipEx
adnan@viewfin.com

INCLUDES COMMENT LETTERS

Eric Gu, Chief Executive Officer
www.viewfin.com
eric.gu@viewfin.com



May 15, 2019

Delivered via email:

comments@osc.gov.on.ca

Consultation-en-cours@lautorite.qc.ca

vpinnington@iiroc.ca

Investment Industry Regulatory Organization of Canada
British Columbia Securities Commission
Alberta Securities Commission
Financial and Consumer Affairs Authority of Saskatchewan
Manitoba Securities Commission
Ontario Securities Commission
Autorité des marchés financiers
Financial and Consumer Services Commission (New Brunswick)
Superintendent of Securities, Department of Justice and Public Safety, Prince Edward Island
Nova Scotia Securities Commission
Securities Commission of Newfoundland and Labrador
Superintendent of Securities, Northwest Territories
Superintendent of Securities, Yukon
Superintendent of Securities, Nunavut

Re: [Consultation Paper 21-402 Proposed Framework for Crypto-Asset Trading Platforms](#)

Thank you for the opportunity to comment on the Consultation Paper 21-402 *Proposed Framework for Crypto-Asset Trading Platforms* (the Consultation Paper) published jointly by the Canadian Securities Administrators (CSA) and the Investment Industry Regulatory Organization of Canada (IIROC, and together with the CSA, the Regulators), which seeks input from the public regarding how existing regulatory requirements should be adapted for crypto asset exchange platforms operating in Canada or that have Canadian participants.

Payward Canada Inc., together with its affiliates (referred to herein as Kraken), operates an international digital currency exchange and custody platform. As an industry leader, Kraken supports efforts to ensure that the crypto marketplace is fair and orderly. That said, it is important to recognize, as the Regulators have done, the difference between crypto assets that are securities under existing Canadian law and crypto assets that operate solely as a form of payment, which we refer to herein as crypto currencies. For the reasons explained below, we believe that exchange platforms on which crypto currencies are traded (Exchanges) should not be substantively regulated under the framework applicable to securities or derivatives.

We wish to provide input on several of the consultation questions asked by the Regulators. The questions below reflect the numbering in the Consultation Paper.

Part 2. Nature of crypto assets and application of securities legislation

Question 1. Are there factors in addition to those noted [in Part 2 of the Consultation Paper] that we should consider?

The assertion of jurisdiction over Exchanges is premised on the concept that even if a crypto currency is not itself a security, the contractual arrangement between an Exchange user (whom we refer to as a customer) and the Exchange operator may be deemed to be a security (or derivative). This premise implies that a customer's interests or holdings on the Exchange are fundamentally different than the assets underlying the holdings, giving rise to risks that are separate and apart from those inherent to the asset itself. We respectfully disagree. This premise is faulty with respect to reputable¹ Exchanges. As described below, most reputable exchanges operate as custodians or bailees. As such, the assets are legally owned by the customer and not the Exchange operator. This means, critically, that the customer's interest is not *derived* from the underlying asset - it IS the underlying asset. The application of a securities law framework, accordingly, is both unnecessary and inappropriate to this structure.

Operation of Exchanges. Exchanges typically hold customers' assets on their behalf, which assets are not used to fund the operations of the Exchange operator. Although there are of course variations in the market, Exchanges typically hold customers' crypto assets in an omnibus wallet, which may consist of numerous addresses.² All transactions are typically done "off chain," which means that ownership changes are represented only on the books and records of the Exchange. Only when virtual currency is transferred off of the Exchange (or onto the Exchange) are transactions broadcast to the underlying public network. Models for fiat funding vary and include: (a) fiat held in segregated omnibus bank accounts held for the benefit of clients, and (b) fiat held in individual client-owned bank accounts over which the Exchange has contractual rights.

Indicia of Direct Ownership. Although each Exchange may describe its operating model differently, there are a few key elements that suggest that the assets held by an Exchange are owned by the customers directly, as opposed to underlying a derivative interest:

1. Contractual terms indicating that the relationship is in the nature of a custodial relationship;
2. Customer has the right to dispose of the assets at any time by transferring them off of the Exchange;
3. Contractual terms governing escheatment of the underlying asset; and

¹ Throughout this Letter, we will refer to "reputable" Exchanges. In general, these Exchanges are those defined in the March 19, 2019 presentation of Bitwise Asset Management, Inc. ("Bitwise") to the Division of Trading and Markets of the U.S. Securities Exchange Commission, in connection with NYSE Arca, Inc.'s proposed rule filing to list and trade shares of the Bitwise Bitcoin ETF Trust (the "Bitwise Presentation"). See <https://www.sec.gov/comments/sr-nysearca-2019-01/srnysearca-201901-5164833-183434.pdf>. As discussed in more detail in this Letter, the Bitwise Presentation identified ten exchanges that formed a uniform, highly connected market with extremely limited deviations in price. Other features of these Exchanges are described in the Bitwise Presentation.

² Although crypto currencies belonging to different customers may be held in a single wallet for operational purposes, each customer's holding is separately accounted for on the books and records of the Exchange. Accordingly, customers' holdings are not "pooled" in a traditional sense, as the participants do not hold a percentage interest in a pooled fund and their holdings do not fluctuate with the holdings of other customers.

4. With respect to bank accounts holding customer funds, titling of the bank account as a “for the benefit of” (FBO) or “custodial” account, or similar wording.

One final indicia of direct ownership relates to market valuation. In general, if the market price of a crypto asset held on an Exchange is consistent with the market price of that same crypto asset at other Exchanges, that is strong evidence that the “interest” offered by the Exchange is the underlying asset. In other words, features that are unique to an interest held at a particular Exchange, such as lack of redeemability, value guarantees or exposure to a pool of assets, should be reflected in the pricing of the interest. Accordingly, where the price of an interest held at an Exchange is generally aligned (and not just correlated) with the value of the corresponding crypto asset on the broader market, it is likely that the customer’s interest is in the underlying asset.

We have set forth below commentary specific to the factors identified by the Regulators in connection with the securities law analysis.

- **whether the Platform is structured so that there is intended to be and is delivery of crypto assets to investors**
- **if there is delivery, when that occurs, and whether it is to an investor’s wallet over which the Platform does not have control or custody**

If customers cannot obtain actual delivery of crypto currency held on an Exchange, that may be an indicia that the customers’ interests are derivative in nature (i.e., that the customers have a financial instrument tied to the value of the underlying asset, but not the asset itself). That said, we believe that the factors, as described in the Consultation Paper, place too much emphasis on how delivery currently occurs as opposed to the customer’s *right* to delivery to an address controlled by the customer. This is important because customers may elect to hold assets “on platform”.³ Assets held on platform generally are still available for delivery to an address controlled by the customer, which should be the key criteria. Specifically, most reputable Exchanges permit customers to remove crypto currency from the Exchange at any time.

- **whether investors’ crypto assets are pooled together with those of other investors and with the assets of the Platform**

Clearly, comingling of assets where the Platform operator uses customers’ assets for its own funding could be an indicia of a security interest. That said, we caution the Regulators about concluding that there is pooling among customers based solely on the storing of multiple customers’ crypto currencies in a single wallet. This omnibus structure is common at Exchanges and reflects operational and security requirements rather than actual co-ownership of assets. Specifically, although a single address may hold crypto currencies in omnibus, the internal records of an Exchange will reflect client ownership on an individual basis.

Part 3. Risks Related to Platforms

³ Customers may elect to hold assets on a platform where the platform holds the private key for numerous reasons, as described in more detail in response to Question 6.

Question 2. What best practices exist for Platforms to mitigate these risks? Are there any other substantial risks which we have not identified?

The Consultation Paper identifies numerous risks, including risks relating to safeguarding of private keys, risks relating to specific assets, conflicts of interest and market manipulation. We have provided feedback on certain identified risks below.

- **Investors' crypto assets may not be adequately safeguarded.**

As the Exchange marketplace evolves, there is increasing demand for assurances about internal controls. In response, many Exchanges are in the process of pursuing SOC certification to assure customers and other stakeholders of the effectiveness of internal controls. As with other risks described below, the way that each Exchange addresses internal controls will be a key competitive differentiator going forward. Although some Exchanges may elect not to pursue SOC certification, we believe that the trend is in the direction of greater controls and transparency. As the public demands greater assurances regarding internal controls, the market will respond accordingly and this risk will diminish.

- **Each crypto asset has its own functions, associated rights and risks.**
- **Investors may not have important information about the crypto assets that are available for trading on the Platform.**
- **Investors may purchase products that are not suitable for them.**

This risk is premised on the idea that government (and Exchanges, for that matter) is in a better position to assess an individual's risk tolerance than the individual. Regulators have often used a "suitability" model that is based on income or assets, thereby denying many financially or technologically sophisticated investors the ability to invest in accordance with their risk appetite. Even a more complex and nuanced approach to suitability runs afoul of the general ethos of the crypto industry, which supports broad, fair access to stores of value. Rather than focusing on how to "protect" people from themselves, we advocate for educating people - and allowing them to make smart decisions that meet their own requirements and risk tolerances.

- **Conflicts of interest may not be appropriately managed -- There may be conflicts of interest between the Platform's operator and participants who access the Platform, including the inherent conflicts of interest where Platforms act as market makers and trade as principal.**

There have been numerous assertions of conflict of interest at Exchanges, most of which represent a misunderstanding of the mechanics of crypto currency exchanges. These purported conflicts of interest include: (1) proprietary trading by Exchanges on their own venues, (2) trading by Exchange employees on the basis of non-public information, and (3) receipt of payment for listing.

Proprietary Trading by Exchange. Although proprietary trading could have the impact of confusing customers about the depth of liquidity on an Exchange, it can function to stabilize otherwise thin and volatile markets. Specifically, some Exchanges may conduct limited proprietary trading to add liquidity to their markets, allowing customers to receive a better price than would be otherwise available. It is important to note that an Exchange doing such proprietary trading does not “step in front of” its clients, thereby depriving them of the ability to transact. The order book determines which orders are matched, so if a customer has a lower offer or higher bid, those orders will be matched first.

Trading on Insider Information. Unlike traditional securities markets where there is a significant amount of material nonpublic information generated, such as in the case of pending mergers, earnings announcements and divestitures, information about decentralized networks is inherently public. There is no “Bitcoin” company that holds secret Bitcoin information; all of the information about the network (such as a proposed fork) is both publicly determined and publicly available. Material nonpublic information in the crypto currency marketplace is generally limited to advance knowledge of an Exchange’s listing or delisting of a crypto currency (which likely would only move the market price for a very thinly traded asset). This risk is addressed by both Exchange prohibitions on insider trading and the enforcement of laws regarding the same.

Receipt of Payment for Listing. Although Kraken does not accept listing fees, listing fees need not represent a meaningful conflict of interest. Listing fees are common for securities marketplaces and can be quite large.⁴ Although some Exchanges may generate revenue from listing fees, in many cases listing fees are assessed merely to cover the cost of supporting a new crypto currency (such as development of secure wallet solutions). The problem with listing fees arises if there is an expectation that Exchanges make merit-based decisions about the value of a particular crypto currency (beyond the ability to support it and the market demand for the asset). In that case, it can easily appear that the potential revenue from the listing fee outweighs the merit-based decision to list the asset. This is one of many reasons that we believe that Exchanges should not be in the business of making merit-based assessments of crypto currencies and should clearly disclose the same.

- **Manipulative and deceptive trading may occur -- Platforms may be susceptible to manipulative and deceptive trading given the market volatility, lack of reliable pricing information for crypto assets, the fact that they trade 24 hours daily and the fact that trading on many Platforms is not currently monitored.**

In conjunction with a proposed rule change to list and trade shares of the Bitwise Bitcoin ETF on NYSE Arca, Bitwise Asset Management presented an extensive analysis⁵ of the global Bitcoin market, showing that it was far more orderly and less subject to manipulative trading tactics than previously understood. Specifically, the analysis concluded that of the approximately \$6 billion in reported Bitcoin volume per day, 95% is fake and/or non-economic wash trading. By applying various analyses to trading information,

⁴ For example, NYSE imposes a minimum listing fee of \$150,000 the first time an issuer lists a class of common shares. See Section 902.02 of the Listed Company Manual.

⁵ See Bitwise Presentation, *supra* note 1.

such as trade size histograms (which look at the percentage of volume by each trade size bucket), trade volume by time (which looks at when trades occur) and spreads, the authors of the analyses concluded that a significant number of Exchanges were reporting false volume.⁶ Critically, of the ten Exchanges that were not deemed suspicious (of which Kraken was one), Bitcoin prices were nearly uniform, indicating that any deviations were quickly arbitrated.⁷ This means that market manipulation on any of the “true” Exchanges would be prohibitively expensive (and practically impossible) as it would be necessary to manipulate the price on all of the “true” Exchanges at the same time, lest the profits from the manipulation be arbitrated away.

Regarding the assertion that the 24-hour trading cycle contributes to the risk of market manipulation, we would argue the contrary. The fact that there are not artificial obstacles to trading (i.e., when the market is open) enhances price discovery, thereby reducing the risk of market manipulation.

- **System resiliency, integrity and security controls may be inadequate.**

Security is clearly the most significant risk in the industry. The reputational costs of a hack are enormous, as are the direct costs of the hack itself. The magnitude of this risk has the effect, however, of closely aligning the interests of the Exchange and its customers. An Exchange that doesn’t earn its customers’ trust is unable to succeed in the market. In fact, the race to prove security represents a functioning market - providing customers the security they require at a cost they are willing to bear. To this point, immediately after Mt. Gox, major Exchanges launched auditing initiatives to reassure customers that they had reserves supporting customer balances.⁸ Accordingly, we believe that this risk is largely addressed by the functioning marketplace for Exchange services. Moreover, as the market continues to evolve, we believe that security differentiators will become more significant from a competitive perspective.

Question 6. Are there challenges associated with a Platform being structured so as to make actual delivery of crypto assets to a participant's wallet? What are the benefits to participants, if any, of Platforms holding or storing crypto assets on their behalf?

As described above, retail customers often prefer to hold their crypto assets in wallets controlled by the Exchange. Exchanges have technology and security resources that individuals simply don’t have. It still takes some level of technical sophistication to establish a secure wallet, particularly a multi-signature wallet. Beyond establishment of the wallet, most individuals are unable to meet the same level of security standards established by the large Exchanges. Finally, maintaining assets at an Exchange allows customers to retrieve the asset if the customer can identify himself or herself sufficiently. In contrast, if the customer loses his or her private key to a personal wallet, the crypto currency is irretrievable.

⁶ An Exchange may exaggerate its volume to attract listing fees for new coins.

⁷ “Average deviations from the aggregate price for the ten exchanges is well within the expected arbitrage band when you account for exchange level fees (~ 30 basis points), volatility and hedging costs,” Bitwise Presentation.

⁸ See *Kraken Bitcoin Exchange Passes Proof-of-Reserves Cryptographic Audit*, Nermin Hajdarbegovic (March 24, 2014).

From a privacy perspective, any requirement that Exchanges settle trades through delivery to segregated wallets would have significant implications, potentially revealing participants' holdings, trades and counterparties.

In addition, the maintenance of crypto assets on Exchanges facilitates a clearance and settlement model that offers significant risk reduction over securities clearance and settlement. Whereas the securities market is built on layers of intermediaries, none of which hold the actual underlying securities but rather hold "securities entitlements" or other contractual rights, the crypto market is built on exchanges of actual assets. Specifically, Exchanges hold the actual assets that are transacted, effectively eliminating rehypothecation risk and settlement risk generally. Accordingly, whereas the intermediated securities model concentrates settlement risk by adding layers of potential claims to an asset, the disintermediated crypto asset model eliminates settlement risk by removing such layers. The trade is the settlement.

Part 5.2.3 Surveillance of Trading Activities

Question 9. Is it appropriate for Platforms to set rules and monitor trading activities on their own marketplace? If so, under which circumstances should this be permitted?

Question 10. Which market integrity requirements should apply to trading on Platforms? Please provide specific examples.

Question 11. Are there best practices or effective surveillance tools for conducting crypto asset market surveillance? Specifically, are there any skills, tools or special regulatory powers needed to effectively conduct surveillance of crypto asset trading?

Question 12. Are there other risks specific to trading of crypto assets that require different forms of surveillance than those used for marketplaces trading traditional securities?

In order for the industry to continue to flourish, marketplaces must be fair and orderly. Deceptive practices, like wash trading and spoofing, have the potential to undermine the integrity of the market, and accordingly, we believe it is incumbent on Exchanges to monitor their marketplaces for this type of activity. That said, crypto currency marketplaces have a number of characteristics that make market manipulation particularly unlikely. As described in the Bitwise Presentation, low transaction costs together with near-zero transportation costs mean that the bitcoin market (as an example) is a "textbook definition of an arbitrable good".⁹ In fact, pricing for bitcoin among a series of ten exchanges shows that the exchanges trade as a uniform, highly connected market with very limited average deviations from the aggregate price. In other words, among exchanges with real transactions, price discrepancies are quickly arbitrated, meaning that to effectively manipulate the market, someone would need to manipulate numerous exchanges globally - which would be prohibitively expensive.

With respect to the Consultation Paper's questions regarding best practices, the industry employs a mix of market surveillance solutions developed in-house and commercial products adapted from the securities marketplace. Kraken is happy to speak directly to the Regulators about its views on the various solutions available in the industry.

⁹ See page 19 of the Bitwise Presentation, *supra* note 1.

In addition to surveilling for market manipulation, we also believe that it is important that our employees cannot take advantage of nonpublic information that may impact the price of a virtual currency, such as a proposed listing on our Exchange. Because fair access is fundamental to the industry, we believe that Exchanges should monitor for employee trading that violates this principal. To this end, Kraken has adopted a Market Fairness policy that prohibits insider trading.

Part 5.2.6 Insurance

Question 16. What type of insurance coverage (e.g. theft, hot-wallet, cold-wallet) should a Platform be required to obtain? Please explain.

Question 17. Are there specific difficulties with obtaining insurance coverage? Please explain.

Question 18. Are there alternative measures that address investor protection that could be considered equivalent to insurance coverage?

Insurance coverage for cyber-theft/hacking continues to be extremely expensive and does not provide a significant degree of protection for customers, so many Exchanges may elect to “self-insure” or maintain capital sufficient to cover losses. We think that allowing the market to decide as to the right mix of insurance and security will yield the best results as long as the market has adequate information for the determination. Moreover, we expect that as the industry continues to evolve, Exchanges will elect different approaches, and that the market will dictate the appropriate balance between different means of protecting assets.

Conclusion

The crypto asset industry has the potential to give people greater control over their assets and greater privacy for their transactions. Fundamental to delivering on this potential is a clear and sensible legal framework. We appreciate that regulators globally are working to create this framework to ensure that the industry operates in a safe manner that does not stifle innovation. As we have described above, the industry is maturing, and the expectations of the public with respect to security, transparency, auditability and controls are driving positive changes. Without the cudgel of regulation, Exchanges are developing proof-of-reserve techniques, obtaining SOC certifications and enhancing their security and internal controls. As more Exchanges embrace these features, the competitive expectations for all of the Exchanges increase - for the better.

Imposing a security law framework on crypto currency Exchanges would neither achieve the goal of regulatory clarity, nor protect Canadian consumers. Rather it would add a level of complexity that would force Canadian Exchanges to move off-shore, which would reduce rather than enhance the protections for Canadian consumers.

We would be remiss if we did not acknowledge the few unreputable fringe Exchanges, whose operations have posed risks to their users and the industry in general. These businesses exist, unfortunately, in all industries. We caution the Regulators from addressing specific abuses in the crypto marketplace with broad-brush rules designed for other marketplaces (like securities markets). Rather, we advocate for continuing thoughtful engagement with the industry and the application of existing laws to address any wrongdoing.

Thank you for the opportunity to comment on the Consultation Paper. If you have any questions on our comment letter, please feel free to contact us at the email address separately provided.



CPA

CHARTERED
PROFESSIONAL
ACCOUNTANTS
CANADA

COMPTABLES
PROFESSIONNELS
AGRÉÉS
CANADA

Chartered Professional Accountants of Canada
277 Wellington Street West Toronto ON CANADA M5V 3H2
T. 416 977.3222 F. 416 977.8585
www.cpacanada.ca

Comptables professionnels agréés du Canada
277, rue Wellington Ouest Toronto (ON) CANADA M5V 3H2
T. 416 204.3222 Téléc. 416 977.8585
www.cpacanada.ca

May 15, 2019

The Secretary
Ontario Securities
Commission 20 Queen
Street West
22nd Floor, Box 55
Toronto, Ontario M5H 3S8
Fax: 416-593-2318
comments@osc.gov.on.ca

Me Anne-Marie Beaudoin
Corporate Secretary
Autorité des marchés financiers
800, square Victoria, 22e étage
C.P. 246, tour de la Bourse
Montréal (Québec) H4Z 1G3
Fax : 514-864-6381
Consultation-en-cours@lautorite.qc.ca
[IIROC](#)

Victoria Pinnington
Senior Vice President, Market Regulation
Investment Industry Regulatory Organization of Canada
Suite 2000, 121 King Street West
Toronto, Ontario M5H 3T9
vpinnington@iiroc.ca

Investment Industry Regulatory Organization of Canada
British Columbia Securities Commission Alberta Securities Commission
Financial and Consumer Affairs Authority of Saskatchewan
Manitoba Securities Commission
Ontario Securities Commission Autorité des marchés financiers
Financial and Consumer Services Commission (New Brunswick)
Superintendent of Securities, Department of Justice and Public Safety, Prince Edward Island
Nova Scotia Securities Commission
Securities Commission of Newfoundland and Labrador Superintendent of Securities,
Northwest Territories
Superintendent of Securities, Yukon Superintendent of Securities, Nunavut

Dear Sirs/Mesdames:

Subject: Joint CSA/IIROC Consultation Paper 21-402 Proposed Framework for Crypto-Asset Trading Platforms

Chartered Professional Accountants of Canada (CPA Canada) appreciates the opportunity to comment on the Joint Canadian Securities Administrators (CSA) / Investment Industry Regulatory Organization of Canada (IIROC) Consultation Paper 21-402 *Proposed Framework for Crypto-Asset Trading Platforms* (Consultation Paper) which seeks feedback on how requirements may be tailored to establish a framework that provides regulatory clarity to platforms that facilitate the buying and selling or transferring of crypto assets (Platforms).

We support the joint CSA/IIROC initiative to provide greater regulatory certainty and appropriately regulate Platforms in a market that continues to evolve, while endeavoring to facilitate innovation that benefits investors and our capital markets.

CPA Canada is one of the largest national accounting bodies in the world representing more than 210,000 members. CPA Canada conducts research into current and emerging business issues and supports the setting of accounting, auditing and assurance standards for business, not-for-profit organizations and government. CPA Canada also issues guidance and thought leadership on a variety of technical matters, publishes professional literature and develops education and professional certification programs.

In formulating our response on specific aspects of the Proposed Platform Framework referred to in the Consultation Paper, we have drawn on our knowledge of audit and assurance practices and unique challenges related to auditing crypto assets. We also solicited input from our extensive network of volunteers representing members from accounting firms with expertise in the areas of crypto assets, blockchain, and system and organization controls (SOC) reporting.

Overall Comments

We see continued interest in blockchain technology and foresee a future filled with digital asset transactions. From this perspective, this consultation is extremely important, and the issues raised in the Consultation Paper are critical for investor protection.

Emerging financial technology is a key area of focus for CPA Canada. We believe transparent and auditable crypto asset trading and custodial services are critical, and that the accounting profession plays a vital role in building public confidence in these areas.

CPA Canada is committed to supporting our members and other stakeholders in the blockchain and crypto asset ecosystem by working with industry experts, the CSA, academia, and accounting and auditing and assurance standards setters through our various committees and working groups. Some

of our recent educational initiatives include publications on blockchain technology¹, accounting for cryptocurrencies² and auditing cryptocurrencies³.

We also wish to highlight a recently formed Crypto-Asset Auditing Working Group, facilitated by CPA Canada and Auditing and Assurance Standards Board (AASB) staff, which includes representatives from the Canadian Public Accountability Board (CPAB), CPA provincial practice inspection, and the auditing firms. The purpose of this working group is to discuss issues related to the application of Canadian Auditing Standards (CASs) in the crypto asset industry and develop relevant non-authoritative guidance for audit practitioners.

Responses to Consultation Questions

After reviewing the specific questions in the Consultation Paper, we have elected to provide a response to question 5 only:

5. Other than issuance of Type I and Type II SOC 2 Reports, are there alternative ways in which auditors or other parties can provide assurance to regulators that a Platform has controls in place to ensure that investors' crypto-assets exist and are appropriately segregated and protected, and that transactions with respect to those assets are verifiable?

Background Information

In Canada, SOC 2 reports are issued based on engagements performed under Canadian Standard on Assurance Engagements (CSAE) 3000, *Attestation Engagements Other Than Audits or Reviews of Historical Financial Information* and with use of the AICPA's Trust Services Criteria (TSC) for Security, Availability, Processing Integrity, Confidentiality, and Privacy. SOC 1 reports are issued in Canada based on engagements performed under CSAE 3416, *Reporting on Controls at a Service Organization* as well as CSAE 3000. These standards are included in the "Other Canadian Standards" section of the *CPA Canada Handbook - Assurance*. Herein, we will refer to SOC 1 and SOC 2 reports for simplicity.

The Importance of Establishing Relevant Controls

Before determining the assurance approach, it is vital to first identify the controls required at a Platform to mitigate the risks related to Platforms (i.e., those identified in Part 3 of your Consultation Paper and any additional risks identified through consultation). It is important that you establish expectations regarding the scope and/or a baseline set of high-level control objectives (i.e., control objectives are opined upon in a SOC 1 report) or system requirements (i.e., system requirements are opined upon in

¹ <https://www.cpacanada.ca/en/business-and-accounting-resources/audit-and-assurance/canadian-auditing-standards-cas/publications/impact-of-blockchain-on-audit>

² <https://www.cpacanada.ca/en/business-and-accounting-resources/financial-and-non-financial-reporting/international-financial-reporting-standards-ifs/publications/accounting-for-cryptocurrencies-under-ifs>

³ <https://www.cpacanada.ca/en/business-and-accounting-resources/audit-and-assurance/canadian-auditing-standards-cas/publications/cryptocurrency-audit-considerations>

a SOC 2 report) that may be relevant in a controls assurance engagement for a Platform. The baseline control objectives/system requirements (herein referred to as ‘controls’) expected may include, among others, those that would be intended to manage and mitigate the custodial risks, including safeguarding of private keys and ensuring that investors’ crypto assets exist, are appropriately segregated and protected, and that transactions with respect to those assets are verifiable.

In addition to traditional custodial risks, there are unique risks that need to be addressed for Platforms such as client authentication, address verification, transaction approvals and multi-signature implementation, key management, asset verification, currency due diligence, and fork management. Another important consideration is whether there are controls in place that address completeness of balances and transactions, and more specifically the risk of “off-chain” transactions not being recorded by the Platform.

The SEC’s Custody Rule is one example of how you may specify what is appropriate from a control scoping standpoint without being too prescriptive. Custody is only one aspect of the Platform’s services that may need to be expanded upon to include critical control requirements that may be relevant depending on what services are being offered by the particular Platform.

Once you have established the scope and/or baseline of controls expected, options to provide assurance over the design and operating effectiveness of those controls can be explored. We would appreciate the opportunity to provide input on alternatives once that baseline has been established. CPA Canada’s Crypto-Asset Auditing Working Group is currently exploring which risks and controls at a custodian (i.e., service organization) of crypto assets are relevant to the user-entity’s⁴ financial reporting. Although the scope of controls at a custodian relevant to audits of user-entity financial statements may differ from the scope of controls expected by you as the regulator, our research could inform the development of your Platform Framework and we would be happy to share our findings when they are ready.

The Consultation Paper notes that Platforms seeking registration as an investment dealer and IIROC membership that plan to provide custody of crypto assets will not only need to satisfy existing custody requirements but will also be expected to meet other yet-to-be determined requirements specific to the custody of crypto assets. We agree that requirements specific to the relevant risks should be established. It will be important to understand the unique risks and address them appropriately to balance the protection of the public interest and the ability for organizations to innovate in Canada.

Contemplation of SOC Reports

The Consultation Paper notes that you are contemplating requiring SOC 2, Type I and II Reports for a Platform’s custody system, and if they use third-party custodians, to ensure that the third-party custodians have SOC 2, Type I and II Reports. While we agree that one way to provide assurance on such controls may be through the issuance of SOC 2 reports, not all SOC 2 reports have the same scope of controls. If the SOC 2 report does not cover the scope of controls you expect, then it will not

⁴ A user-entity is an entity that uses a service organization and whose financial statements are being audited.

provide the assurance you are seeking.

For example, a minimum scope SOC 2 report may cover only those controls required to meet the Security category of the TSC and would exclude the additional criteria and controls for system Availability, Processing Integrity, Confidentiality, and Privacy. While it seems unlikely that the securities and investment industry regulators would require a SOC report on confidentiality and privacy controls (which is not an independent assurance reporting requirement for traditional asset exchanges), it is possible you may expect SOC 2 reports for some or all Platforms to address relevant aspects of security, processing integrity and possibly availability. If this is the case, it may be appropriate that the SOC 2 report for a Platform cover the criteria for Security, Processing Integrity, and possibly Availability.

In addition, you may wish to require specific regulatory controls for such Platforms (see the 2018 SOC 2 Description Criteria⁵ and 2017 Trust Services Criteria⁶ for details) to help ensure the controls covered in the SOC 2 report meet your expectations. For example, there may be specific control requirements related to client acceptance, transaction processing, and custody that may not be covered by the generic Processing Integrity criteria from the TSC.

As an alternative to SOC 2 reporting, you may consider if a SOC 1 report, with the appropriate scope and control objectives, may be sufficient in addressing regulatory expectations for controls assurance. SOC 1 reports are often used to provide controls assurance for traditional custody and exchange services, so it is unclear why they may not also be suitable for Platforms, provided the appropriate scope and control objectives are covered.

It may be possible to develop a set of regulatory requirements for Platforms that could be used as either System Requirements for SOC 2 reporting, or Control Objectives for SOC 1 reporting, and allow the exchange to decide whether to obtain a SOC 1 or SOC 2 report.

Platform Readiness

Regardless of whether a SOC 1 or SOC 2 report is provided, it is not possible to provide an unqualified opinion in a Type II report (e.g., SOC 1 Type II or SOC 2 Type II) until the Platform has been in operation for a reasonable period of time (e.g., 6 months). Consideration should be given when a Type I report may be accepted initially, and what the maximum period of time is that the Platform can operate until a Type II report is required; or if some scope limitations in the service auditor's opinion may be acceptable for an initial Type II report on a new Platform.

It is also important to consider if effective controls were in place from the commencement of crypto-asset activities, not just the audit year- or period-end. For example, if a wallet was created without appropriate safeguards over the private key, it may be difficult for an auditor to conclude whether all

⁵<https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/dc-200.pdf>

⁶<https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/trust-services-criteria.pdf>

relevant controls were designed, implemented and operating effectively.

Alternative Assurance Options

CSAE 3000

An alternative way in which auditors or other parties could provide assurance over a Platform's controls (other than SOC 1 and SOC 2 reporting) may be by performing an engagement under CSAE 3000, which could potentially provide assurance on a wide variety of relevant subject matter that may include but not necessarily be limited to controls, transactions, balances, regulations, etc. as long as suitable reporting criteria can be defined.

CSAE 3000 engagements may include, for example, an audit of a service organization's description of its controls and the suitability of design and operating effectiveness of those controls. This type of engagement is currently accepted for entities providing traditional exchange or custodial services, however we are aware of scrutiny in the market with this type of report since the scope can vary significantly. The viability of this option depends on the availability of appropriate criteria and controls to promote consistency and quality in reporting.

Another factor to consider is that CSAE 3000 engagements can provide reasonable assurance (i.e., the level of assurance obtained by an audit) or limited assurance (i.e., the level of assurance obtained by a review), as defined in CSAE 3000. You may consider what level of assurance you require (reasonable assurance, limited assurance or possibly no assurance through an Agreed-Upon Procedures engagement – see below) prior to finalizing your Proposed Platform Framework.

Agreed-Upon Procedures (AUP) Engagement⁷

While Question 5 in this Consultation Paper asks for alternative ways in which auditors or other parties can provide assurance, you may also wish to consider AUP engagements. AUP engagements do not provide assurance but may still be a viable option depending on the objectives of the Proposed Platform Framework. As an example, this is the type of engagement performed in Japan with respect to customer asset segregation for virtual currency exchange (VCE) service providers. With the enactment of the amended Payments Services Act in April 2017 in Japan, VCE service providers are now subject to financial statement audits and segregation of funds audits, with the segregation of funds audits being performed using the Segregation of Funds AUP Guidance⁸.

⁷ In Canada, AUP engagements are currently performed under one of the following standards: Section 9100, *Reports on the Results of Applying Specified Auditing Procedures to Financial Information Other than Financial Statements* or Section 9110, *Agreed-Upon Procedures Regarding Internal Control Over Financial Reporting*

⁸ <https://kmra-cpa.com/en/financial-statement-audits-of-virtual-currency-traders-2/>

We appreciate the opportunity to participate in this consultation and would be happy to meet to discuss our comments further. Please do not hesitate to contact Taryn Abate, Director, Research, Guidance and Support (tabate@cpacanada.ca) or myself.

Yours truly,



Gordon Beal, CPA, CA, M. Ed
Vice-President, Research, Guidance & Support
Chartered Professional Accountants of Canada

GLOBAL DIGITAL FINANCE

May 15, 2019

To: **Joint Canadian Securities Administrators/ Investment Industry Regulatory Organization of Canada (IIROC)**

Re: **Consultation Paper 21-402 on the Proposed Framework for Crypto-Asset Trading Platforms**

Dear Joint Canadian Regulatory Team,

We support efforts by global standard setters, national authorities and regulators to consult and work with the nascent global digital/virtual asset industry.

To that end, we are hereby providing input to the **Joint Canadian Securities Administrators/Investment Industry Regulatory Organization of Canada Consultation Paper 21-402 on the Proposed Framework for Crypto-Asset Trading Platforms**.¹

The input has been drafted and led by the GDF Advisory Council.

About GDF

Global Digital Finance (“[GDF](#)”) is a not-for-profit industry body that promotes the adoption of best practices for crypto and digital assets and digital finance technologies through the development of conduct standards, in a shared engagement forum with market participants, policymakers and regulators.

Established in 2018, GDF has convened a broad range of industry participants, with 300+ global community members—including some of the most influential digital asset and token companies, academics and professional

¹ https://www.osc.gov.on.ca/en/SecuritiesLaw_csa_20190314_21-402_crypto-asset-trading-platforms.htm

services firms supporting the industry. GDF is proud to include Circle, ConsenSys, DLA Piper, Diginex, Hogan Lovells and R3 as patron members.

The GDF Code of Conduct is an industry-led initiative driving the creation of global best practices and sound governance policies, informed by close conversations with regulators and developed through open, inclusive working groups of industry participants, legal, regulatory and compliance experts, financial services incumbents and academia. Code principles undergo multiple stages of community peer review and open public consultation prior to ratification.

Consultation Inputs

1. Are there factors in addition to those noted in Part 2 that we should consider?

We suggest that more elaboration is added as to why each of these factors cited are determinative as to the remit of securities law, as several of these factors do not appear determinative under the laws of other jurisdictions.

We refer in this regard for example/ comparison to the interpretation given under UK law in the **FCA Guidance on Crypto Assets** that can be accessed [here](#).

2. What best practices exist for Platforms to mitigate the risks outlined in Part 3? Are there any other significant risks which we have not identified?

The list appears comprehensive.

We also refer you to the GDF paper on **Crypto Asset Safekeeping and Custody** that can be accessed [here](#), in case it may be helpful.

3. Are there any global approaches to regulating Platforms that are appropriate to be considered in Canada?

The IOSCO website contains a more comprehensive list of measures taken by various markets. We would note, for example, the tailored frameworks of **France, Malta, Abu Dhabi, Bahrain, Gibraltar, Bermuda and Bahamas**.

It appears that mostly non-G20 countries have adopted tailored frameworks that create more reasonable room for innovation to take root. This may be

due to the fact that these countries have less legacy regulation in place and, therefore, more room to create and adopt more tailored frameworks.

While evaluating which licensing regime to apply for, reputable platforms consider amongst others the following factors:

- Is the regulator genuinely embracing Fintech innovation, actively engaging with it and seeking to adopt a balanced approach to regulation?
- Is the approach of the jurisdiction towards innovation welcoming/ positive or instead mostly punitive/ enforcement driven/ negative?
- Is there a tailored regime or tailored guidance for crypto assets and, if so, does it match the characteristics and the needs of the crypto asset industry?
- Does the tailored regime allow retail investors to buy and sell crypto assets on platforms?
- Does a transaction tax apply and what is the tax treatment of crypto assets in the country?

We welcome the fact that the **Proposed Platform Regime** seems to take into consideration many of the above.

4. What standards should a Platform adopt to mitigate the risks related to safeguarding investors' assets? Please explain and provide examples both for Platforms that have their own custody systems and for Platforms that use third-party custodians to safeguard their participants' assets.

We refer you to the GDF paper on **Crypto Asset Safekeeping and Custody** that can be accessed [here](#), in case it may be helpful.

5. Other than issuance of Type I and Type II SOC 2 Reports, are there alternative ways in which auditors or other parties can provide assurance to regulators that a Platform has controls in place to ensure that investors' crypto-assets exist and are appropriately segregated and protected, and that transactions with respect to those assets are verifiable?

We refer you to the GDF paper on **Crypto Asset Safekeeping and Custody** that can be accessed [here](#), in case it may be helpful. It mentions SOC 2 reports, amongst others. We would note for completeness that while SOC 2

reports are commonly requested in the traditional financial markets, it has not excluded the existence of material control issues.

6. Are there challenges associated with a Platform being structured so as to make actual delivery of crypto assets to a participant's wallet? What are the benefits to participants, if any, of the Platforms holding or storing crypto assets on their behalf?

Crypto exchanges typically have no settlement period (no T+2) as settlement is instant. The balance is immediately credited to the user's balance on the Exchange's internal ledger and immediately becomes available to withdraw. This could be viewed to constitute actual delivery.

If the proposal is to transfer funds to an address specific to the customer's account on the Exchange, this would be challenging. It would result in a massive increase in on-chain transactions, which would be accompanied by transaction fees, and this increase in transactions could also/ further increase fees. It would also likely increase the number of UTXOs, which is not great for blockchain throughput optimization for applicable coins.

7. What factors should be considered in determining a fair price for crypto assets?

We make reference in this regard to the recent Bitwise submission.²

We would also note that GDF recently started a working group on market integrity, that will report back at the July 2019 GDF mini-summit.

8. Are there reliable pricing sources that could be used by Platforms to determine a fair price, and for regulators to assess whether Platforms have complied with fair pricing requirements? What factors should be used to determine whether a pricing source is reliable?

There is no set standard yet. It could conceptually be a weighted-average across a number of "reputable" Exchanges that provide full trade history and order book data in real-time and have good depth of book. Good depth of book is more helpful than trading volume as volume can easily be boosted fraudulently as many studies have demonstrated.³

Brave New Coin has a few indices that are supported by NASDAQ.⁴

² <https://www.sec.gov/comments/sr-nysearca-2019-01/srnysearca201901-5164833-183434.pdf>

³ See footnote above.

⁴ <https://bravenewcoin.com/enterprise-solutions/indices-program/blx>

9. Is it appropriate for Platforms to set rules and monitor trading activities on their own marketplace? If so, under which circumstances should this be permitted?

Under most national laws other than those of Canada, ATS and MTF must implement their own surveillance systems.

At current the industry is engaging similar market integrity surveillance vendors to those used in traditional asset classes, as these vendors have extended their solutions to apply the market misconduct rule set to crypto assets.⁵

10. Which market integrity requirements should apply to trading on Platforms? Please provide specific examples.

In order to conduct effective surveillance, retaining a complete order audit trail for all orders and trades is necessary.

11. Are there best practices or effective surveillance tools for conducting crypto asset market surveillance? Specifically, are there any skills, tools or special regulatory powers needed to effectively conduct surveillance of crypto asset trading?

There are a number of different vendor options, but in-house programs can be built as well with the requisite expertise.

As noted above, at current the industry is engaging similar market integrity surveillance providers to those used in traditional asset classes.

12. Are there other risks specific to trading of crypto assets that require different forms of surveillance than those used for marketplaces trading traditional securities?

In addition to traditional market integrity surveillance, the crypto asset industry has seen the emergence of specialised surveillance tools focussed on tracking the movement of assets through the crypto asset addresses. We refer in this regard to the latest **GDF submission to FATF** that can be accessed [here](#) as in it we provide more insight into these tools.

⁵ See here relevant news:

<https://www.apnews.com/99e1f16676704fc28ca39867be8b7f1a> ;
<https://business.nasdaq.com/mediacenter/pressreleases/1728735/gemini-to-launch-market-surveillance-technology-in-collaboration-with-nasdaq>

An earlier GDF letter to FATF that can be accessed [here](#) also listed in its Annex various types of systems used in the crypto asset industry based on a survey conducted by GDF.

13. Under which circumstances should an exemption from the requirement to provide an ISR by the Platform be appropriate? What services should be included/excluded from the scope of the ISR? Please explain.

We refer you to the GDF paper on **Crypto Asset Safekeeping and Custody** that can be accessed [here](#), in case it is helpful. It mentions security audits, amongst others.

14. Is there disclosure specific to trades between a Platform and its participants that Platforms should make to their participants?

While market practice is diverging in this regard, Exchange should probably disclose if they are trading as principal, or if there are formal market maker agreements.

15. Are there particular conflicts of interest that Platforms may not be able to manage appropriately given current business models? If so, how can business models be changed to manage such conflicts appropriately?

Exchanges often act as a “one-stop-shop”, where the Exchange acts as issuer, listing venue, custodian, prime broker, settlement agent and/or market maker. Without legal separation, “chinese walls” and tailored policies and procedures, conflicts may arise.

For example, practices are diverging in respect to access by proprietary desks to customer information, and arrangements around firms making markets on it's own Exchange.

Additional conflicts of interest may also arise when an Exchange or other VASP issues a crypto asset and may have an incentive to see it more widely-adopted or see the price rise.

16. What type of insurance coverage (e.g. theft, hot-wallet, cold-wallet) should a Platform be required to obtain? Please explain.

We list below important types of insurance in the context of the crypto market. We, however, caveat this by what is said under 17 below about the difficulties obtaining material insurance coverages.

- Cyber insurance can be used to protect against impacts of potential damages to their computer systems (outages, failures, etc.), along with business interruption coverage to compensate for lost revenues related to these outages.
- Crime insurance can be used to cover both own and customers assets stored both online and offline.
- Specific to offline storage, incremental insurance coverages may be available in the specie market.
- Directors & Officers and Errors & Omissions coverages may be used to protect their Directors and Officers against potential claims related to actions taken by that Platform, for example in the face of an uncertain and evolving regulatory landscape.

17. Are there specific difficulties with obtaining insurance coverage? Please explain.

There are some difficulties obtaining material insurance coverages as the global insurance market for crypto assets is limited in capacity and maturity. Large insurance companies are reluctant to price the risk, due to the small size of the overall market.

In addition, to the limited capacity in the global insurance market, costs are quite high vis-a-vis like coverages for traditional assets. Further, many nascent companies in the space are also limited by their own balance sheet and budget for insurance spend.

As a result, the industry is looking to facilitate a syndicate to address some of the above points, such as balance sheet size.

18. Are there alternative measures that address investor protection that could be considered that are equivalent to insurance coverage?

Key is best in class security infrastructure (both hot and cold storage measures).

19. Are there other models of clearing and settling crypto assets that are traded on Platforms? What risks are introduced as a result of these models?

Centralized crypto Exchanges do not utilize clearing services since trades are all completed in-house.

20. What, if any, significant differences in risks exist between the traditional model of clearing and settlement and the decentralized model? Please explain how these different risks could be mitigated.

Most crypto Exchanges are centralized and as indicated above, do not utilize clearing services since trades are all completed in-house.

For Decentralized Exchanges (DEX), the risks concern the difficulty of recourse in case funds are lost, as well as risks of bugs in the smart contracts.

21. What other risks could be associated with clearing and settlement models that are not identified here?

Other areas still subject to technology evolution and study include: immutability of the blockchain and how settlement finality is/can be achieved.

22. What regulatory requirements (summarized at Appendices B, C, and D), both at the CSA and IIROC level, should apply to Platforms or should be modified for Platforms? Please provide specific examples and the rationale.

We apologize but we have not been able to study or comment in detail on the full standing law. We are happy to conduct a **Community Survey** in case the joint regulators would like to receive more industry input on specific topics/ areas of industry knowledge/ expertise.

Other comments

Canadian participants

We note the following language:

“The Proposed Platform Framework will apply to Platforms that are subject to securities legislation and that may not fit within the existing regulatory framework. It will apply both to Platforms that operate in Canada and to those that have Canadian participants.”

We do not believe that Canadian regulators will be reasonably able to monitor compliance with “and to those that have Canadian participants” and propose this be removed.

Margin

We took note of the following language:

“To reduce the risks of potentially manipulative or deceptive activities, in the near term, we propose that Platforms not permit dark trading or short selling activities, or extend margin to their participants. We may revisit this once we have a better understanding of the risks introduced to the market by the trading of crypto assets.”

Many platforms offer margin trading and derivatives, including several for many years already. Not allowing margin trading and derivatives may stifle the industry and may prevent hedging. Similarly short selling is important for price discovery.

Maybe as an alternative approach IIROC could consider limiting these activities to Platforms with adequate controls and surveillance solutions.

Internal Ledger

We note the following language:

“As indicated above, we understand that on some Platforms, transaction settlement occurs on the Platform's internal ledger and is not recorded on the distributed ledger. We are considering whether an exemption from the requirement to report and settle trades through a clearing agency is appropriate. In these circumstances, Platforms will still be subject to certain requirements applicable to clearing agencies and will therefore be required to have policies, procedures and controls to address certain risks including operational, custody, liquidity, investment and credit risk.”

We welcome the consideration of an exemption.

DEX

We note the following language:

“Some Platforms may operate a non-custodial (decentralized) model where the transfer of crypto assets that are securities or derivatives occurs between the two parties of a trade on a decentralized blockchain protocol (e.g. smart contract). These types of Platforms will be required to have controls in place to address the specific technology and operational risks of the Platform.”

As for DEX, it may be hard for IIROC to determine where it operates from. IIROC may need to add criteria defining this.

PFMI

We note the following language:

“NI 24-102 also sets out the ongoing requirements applicable to recognized clearing agencies. This includes the requirement to meet or exceed applicable principles as set up in the April 2012 report Principles for financial market infrastructures published by the Committee on Payments and Market Infrastructure and the International Organization of Securities Commissions (PFMI). The PFMI cover all areas associated with activities carried out by a clearing agency: systemic risk, legal risk, credit risk, liquidity risk, general business risk, custody and investment risk and operational risk. Clearing agencies are required to:

- have appropriate rules and procedures on how transactions are cleared and settled, including when settlement is final;*
- minimize and control their credit and liquidity risks;*
- have rules that clearly state their obligations with respect to the delivery of securities traded; and*
- identify, monitor and manage the risks and costs associated with the delivery of crypto assets, including the risk of loss of these crypto assets.”*

We apologize but we have not been able to study or comment in detail on the PFMI. We are happy to conduct a **Community Survey** in case the joint regulators would like to receive more industry input on specific topics/ areas of industry knowledge/ expertise. Nevertheless, we would hereby like to share the high level thoughts in respect to the consideration of application of the PFMI:

1. The PFMI were drafted after the Global Financial Crisis when, pursuant to the learnings from the collapse of Bear Stearns and Lehman Brothers and the near collapse of other leading financial institutions, a decision was made that OTC derivatives caused systemic risk and should be centrally cleared, leading in turn to CCPs becoming increasingly “systemic”. In comparison, the crypto asset industry is currently very small, nascent and not “systemic”. Seen from this perspective, applying the PFMI appears premature.
2. Crypto assets clear instantly. As such, there is no context of a CCP. This means that the PFMI cannot be considered relevant in full and that, instead, a tailored approach may need to be developed in consultation with the industry.

We hope you may find this helpful. Please do not hesitate to contact us at www.gdf.io.

GDF



OCTONOMICS

CONSULTATION PAPER 21-402 COMMENTS

Framework for Crypto-Asset Trading Platforms jointly proposed by CSA & IIROC

Presented to

British Columbia Securities Commission
Alberta Securities Commission
Financial and Consumer Affairs Authority of Saskatchewan
Manitoba Securities Commission
Ontario Securities Commission
Autorité des marchés financiers
Financial and Consumer Services Commission (New Brunswick)
Superintendent of Securities, Department of Justice and Public Safety, Prince Edward Island
Nova Scotia Securities Commission
Securities Commission of Newfoundland and Labrador
Superintendent of Securities, Northwest Territories
Superintendent of Securities, Yukon
Superintendent of Securities, Nunavut

Elisabeth Préfontaine, MBA, CFA, CAIA
FOUNDER OF OCTONOMICS

Individual citizen initiative

This text is not about defending a commercial interest. This text is about philosophy, ethics and fundamental beliefs. It is also about preventing a disadvantageous position for all Canadians in terms of property rights, liberty and free speech.

Funding

This document received no funding. It is an individual contribution from Octonomics' founder, Elisabeth Préfontaine. The author is not bound to providing more work beyond the submission of this paper. Tips and donations are welcomed and can be expressed in BTC. Thank you in advance as your identity or location will not be known.



About the author

In over 25 years of work experience, Elisabeth has witnessed a broad spectrum of transformations in financial technologies. In fact, she is one of the few who can claim to have both traded a physical coupon bond in a bank branch and also bitcoins.

She witnessed the birth of online banking while employees of financial institutions were still using an intranet and she also took part in Bank of Montreal's attempt at creating the world's first virtual bank in the late 1990's. Early 2000, she migrated towards capital markets where spent five years on the sell-side of a swap and of a bond trading desk. Then in the mid 2000's, and for over ten years, she actively contributed to foster the market's understanding of ETFs as a technological platform transformation for investment funds. She is the former Head of Wealth Sales for BlackRock in Canada.

Her academic profile includes the CFA and the CAIA designations and also both a Bachelor's degree and an MBA from *Université du Québec à Montréal*.

Disclosure

The author discloses a diversified portfolio composed of traditional assets, alternatives and bitcoin.

Language

Even though the initiative originated from Quebec, this paper is presented in English. This is to ensure it is understood by rest of Canada without having to increase production costs. With funding, an official French translation could be produced under Octonomics' sole approval or supervision.

Caution

Bitcoin is a technological experiment with a successful ten-year track record. As in any journey, it should be understood that there is no guarantee of success. But ignoring may be just as hazardous.

Bitcoin is a trailblazer.

Introductory Remarks

On March 14 2019, the Canadian Securities Administrators (CSA) and the Investment Industry Regulatory Organization of Canada (IIROC) have jointly proposed a framework for crypto-assets trading platforms called Consultation paper 21-402¹ and are seeking feedback from the financial technology community, market participants, investors and other stakeholders.

This is the context under which Octonomics, an independent research firm, is submitting this paper. Octonomics' comments cover Bitcoin specifically and not the plethora of so called crypto-assets. Should securities regulators find elements brought forward in this document applicable to other crypto-assets, a clear stance and definition would be welcomed.

As it stands, the Canadian securities regulators (IIROC and CSA) do not distinguish between the various types of crypto-assets and they bundle 2000+ different "things" into one big category and 200+ platforms as one big type. This lack of nuance is problematic as it paints an entire industry with the same brush, it stigmatizes entrepreneurs, complexify banking relationships and may mislead the public. Canadian securities regulators must state, in plain English, what they are after and what they consider to be a security in the crypto-asset realm. This seems like a logical first step before attempting any regulatory initiative.

However, when it comes to Bitcoin, the securities regulators are outside the scope of their jurisdiction and the first section of this paper aims at making that demonstration. This paper will also highlight a way for securities regulators to influence the development of Bitcoin-platforms without stepping outside of their jurisdiction. Parallels with gold and real estate will be used to demonstrate that securities regulators did not have to regulate gold or real estate trading platforms to allow their inclusion in investment funds structure. Gold and real estate are not securities. Yet, they were included in regulated financial products.

Bad actors such as exposed by the recent QuadrigaCX debacle are harmful to the entire industry. However, cases of frauds, incompetence, data breaches and critical errors are not solved by additional layers of regulation. If it was the case, if regulators had such mighty powers, software viruses, phishing attack, credit card frauds and personal ID theft would no longer exist.

The point is, technological solutions, good education on the subject and skin in the game are the best mechanisms to combat bad actors because participants have a vested interest in preventing what could be detrimental to the emerging Bitcoin industry. Hackers are not stopped by regulation. They are surely not desirable, but they nevertheless play a crucial role; they poke holes at weaknesses. They identify vulnerabilities more effectively than the most zealous regulators could.

Protection of the public and security/safety progress don't happen because meetings, discussions and consultation papers are produced about how things should be. Things are. Technology is not the enemy. Lack of skin-in-the-game is.

¹ https://www.osc.gov.on.ca/en/SecuritiesLaw_csa_20190314_21-402_crypto-asset-trading-platforms.htm (04/08/2019)

Table of Content

1. BITCOIN IS NOT A SECURITY

1.1 Bitcoin never was a security	4
1.2 What is Bitcoin? Bitcoin is text	6
1.3 The general understanding of bitcoin is “digital gold”	7
1.4 How is the U.S. SEC and the U.S. CFTC treating bitcoin?	8

2. THE COMMERCE OF (NON-SECURITIES) VALUABLES

2.1 Individuals buying/selling/storing physical gold	9
2.2 Investment funds buying/selling/storing physical gold	11
2.2.1 ETF investing in gold (American example)	11
2.2.2 Investment Trust investing in gold (Canadian example)	12
2.2.3 ETF investing in Real Estate Investment Trust (American example)	13
2.2.4 ETF investing in Real Estate Investment Trust (Canadian example)	14
2.3 Collateral loans	15
2.4 Summary	16

3. PREOCCUPATIONS

3.1 Multi-dimensional & open-ended regulatory struggle	17
3.2 Stigmatization	19
3.3 There is regulation	21
3.4 Double standard (1) - Volatility	23
3.5 Weak educational content	25
3.6 Double standard (2) - Accountability	30

4. THE CRUX OF THE ISSUE

4.1 Problem: Custodial exchanges & the misuse of funds	32
4.2 Solution: Vires in Numeris	33
4.3 Unintended consequences	34

Conclusion	35
------------------	----

1. Bitcoin is not a security

Bitcoin is a broad topic and links together many disciplines such as cryptography, game theory, monetary theory, monetary history, economics, computer science, network dynamics, thermodynamics and information theory. The present section shall be understood as a demonstration that Bitcoin, Bitcoin-related dealings, trading, and applications unequivocally sit outside the scope of the securities or derivatives legislation. This demonstration should make the case as to why the proposed framework for crypto-assets trading platform by the Consultation paper 21-402 does not apply to Bitcoin.

1.1 Bitcoin never was a security

Here is a brief but straightforward explanation as to why Bitcoin was not a security from the start.

Monetary capital

- No monetary capital was raised to develop Bitcoin.
- There was never a bitcoin Initial Coin Offering (ICO).
- There was no investment of capital from a founder.
- There was no premine (i.e. founders keeping a portion of the tokens for themselves).
- There is no bounty program, or free tokens offered to “promoters”.
- No capital was spent to promote its launch.
- Growth was entirely organic.
- Bitcoin was born out of an 8-page idea.²
- The early-stage was sustained by volunteers.
- Bitcoin is not debt; Bitcoin is not equity. Bitcoin is Bitcoin.

Value

- Bitcoin is a bearer instrument. It solves for the double spending problem in the digital world.
- Bitcoin is functional since its inception and has an up time of 99.9837111434%³ since then.
- Bitcoin has no financial statements.
- Bitcoin doesn't share security-like attributes such as a profit-sharing interest.
- The currency bitcoin has unique characteristics where individuals can express personal preference (see section 1.3)
- The market has spontaneously attributed value to it.
- The price is market driven. The value of one bitcoin is one bitcoin
- The network effect of Bitcoin has value: its community, its users, its developers.
- The proof-of-work has value. It is an expensive monument of immutability.
- The stability at the base layer has value.
- The transparency and predictability of Bitcoin's monetary policy has value.
- The self-regulating mechanism embedded in bitcoin has value.
- Bitcoin is its own and we are still early in the discovery of its full potential.

² <https://bitcoin.org/bitcoin.pdf> (04/15/2019)

³ <http://bitcoинуptime.com/> (05/12/19 at 12H14 EST)

Decentralization

- Bitcoin is not a common enterprise. It is a network.
- Bitcoin is a decentralized system recording sequence of transactions with 80,000+ nodes⁴
- Bitcoin is not a company. There is no authority in charge, no management team, no CEO, no head office, no sales team, no tech support line.
- It is not centrally planned in an effort to deliver an eventual product. Bitcoin exists.
- No one person (or entity) controls the network or the protocol or can change the rules.
- No2X⁵ is a specific event that proved, in real life, bitcoin's decentralization and uniqueness versus other centralized cryptocurrencies.

Unique phenomenon

- A replica or a bitcoin 2.0 / 3.0 / 4.0 would inevitably be centrally planned.
- That central planning would most likely involve, securities-like characteristics.
- Now that the path to creation is known a 51% attack could be successful in the early days.

This section aimed to demonstrate that Bitcoin is not and never was a security. It is very possibly a one-time phenomenon and draws a line between bitcoin and the rest of so-called crypto-currencies.

We ended up with 2,000+ crypto-currencies because of the Blockchain bubble. A very sticky narrative has developed around the *"technology underpinning bitcoin"*, as if it could be considered in isolation. The market⁶ created the name 'blockchain' which led to marketing narratives and fund-raising pitch decks being created. Much like the "snake-oil" claims of previous centuries, this new technology would solve almost any problem in the world (from lettuce tracking to identity management). This spurred the rise of blockchain projects raising capital through ICOs (initial coin offerings) in a tulip-bulb like mania.

We ended-up with 2000+ so-called crypto-currencies because very few took the time to first understand what, how and why bitcoin is. If organized true data without a central authority is not needed, then a decentralized and open architecture are not needed. This would have helped contrast the Bitcoin's network and infrastructure with Initial Coin Offerings (ICOs) which are an essentially a global venture-capital crowd funding mechanism.

Could there be networks that initially started as an ICO and now are too far advanced and can no longer be considered a security? Perhaps. This will be a definition question that securities regulators will need to answer. But Bitcoin did not start as an ICO.

Understanding the uniqueness of Bitcoin's conception and how it gave life to a digitally native scarce asset is the most direct way to comprehend what makes it different from a security-like vehicle.

⁴ <https://luke.dashjr.org/programs/bitcoin/files/charts/software.html> (05/13/2019)

⁵ <https://www.forbes.com/sites/ktorpey/2019/04/23/this-key-part-of-bitcoins-history-is-what-separates-it-from-competitors/#f864ce8ae5ec> (04/25/2019)

⁶ The term blockchain was not utilized in bitcoin's white paper. The paper rather refers to a chain of blocks.

1.2 What is Bitcoin? Bitcoin is text.

Bitcoin is surely different from anything we have seen before. Some argue that Bitcoin is a form of money, others argue it is a commodity and some simply don't see anything in Bitcoin. However, this does not matter. What matters is that Bitcoin exists and its network and protocol do exactly what they are meant to do, since over ten years. Bitcoin is text, information, speech. It communicates.

"Bitcoin is a distributed ledger system, maintained by a network of peers that monitors and regulates which entries are allocated to what Bitcoin addresses. This is done entirely by transmitting *messages* that are *text*, between the computers in the network (known as "nodes"), where cryptographic procedures are executed on these *messages* in *text* to verify their authenticity and the identity of the sender and recipient of the *message* and their position in the public ledger.

The *messages* sent between nodes in the Bitcoin network are human readable, and printable. There is no point in any Bitcoin transaction that Bitcoin ceases to be *text*.

It is all text, all the time.

"The purpose of Bitcoin is to absolutely verify the ability of the owner a cryptographic key (*which is a block of text*) that can unlock a ledger entry in the global Bitcoin network"⁷

There are deep implications to understanding Bitcoin in such a way as it has ramifications to the fundamental freedoms 2(b) of the Canadian Charter of Rights and Freedoms⁸.

FUNDAMENTAL FREEDOMS

Fundamental freedoms

2. Everyone has the following fundamental freedoms:

- (a) freedom of conscience and religion;
- (b) freedom of thought, belief, opinion and expression, including freedom of the press and other media of communication;
- (c) freedom of peaceful assembly; and
- (d) freedom of association.

Is IIROC, the national **self-regulatory** organization overseeing all investment dealers and trading activity on **debt and equity** marketplaces in Canada, and the CSA, aiming to challenge the Constitutional act of 1982 by trying to legislate software developments, text and messaging systems?

⁷ <https://hackernoon.com/why-america-cant-regulate-bitcoin-8c77cee8d794> (04/15/2019)

⁸ <https://laws-lois.justice.gc.ca/eng/Const/page-15.html> (04/15/2019)

1.3 The general understanding of bitcoin is “digital gold”

The perception of value varies from one individual to the other. Individuals will purchase comic books, preserve them in their original sleeves without ever reading them. Others will purchase figurines, keep them in their original boxes and never play with them. Others will collect vintage cars knowing very well they can only drive one at a time. Other examples include, watches, antique furniture, precious stones, paintings, sculptures, fine jewelry and wine.

The point here is their value is not tied to their use, but rather attached to the perceived value in the eyes of the owner. Gold has a valuation significantly above its industrial or ornamental usage. In today's world, it is unlikely anyone buys a pair of shoes with gold. As such, bitcoin doesn't need to be money (in the transactional definition of the term), but it can be valuable. What these examples have in common is scarcity. Some individuals will own them to store value, to brag, to seduce a mating partner or to speculate on the future price appreciation. Generally speaking, individuals will self-custody them.

I do not have the pretention to define something as complex and broad as bitcoin nor to define its full potential, for one reason: it is the free market that dictates what Bitcoin is. I invite the curious reader to consider these selected texts^{9 10 11 12 13} to realize the depth and uniqueness of the topic. For the first time in the history of mankind, a scarce digital asset exists. Bitcoin is not debt or equity; Bitcoin's infrastructure permits the first digitally native bearer instrument without a central authority. Bitcoin is its own.

The monetary policy of the Bitcoin protocol is crystal clear. Its predictability, its limited supply and its stability at the base layer are valuable attributes. Accordingly, bitcoin is often referred to as “digital gold”^{14 15 16 17 18 19 20}. Therefore, bitcoin can be viewed as a limited-supply consumer goods. It can be argued that bitcoin is;

- rarer than gold since technological innovation cannot increase its actual supply or the speed of production.
- more portable than gold as it can be used over the Internet, ham radio, satellite or paper.
- useful in a way that gold can't be, as bitcoin can be programmed.

⁹ https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2275730 (04/12/19)

¹⁰ <https://blockstream.com/satellite/> (04/12/19)

¹¹ <https://grisha.org/blog/2018/01/23/explaining-proof-of-work/> (04/12/19)

¹² <https://medium.com/@BrandonQuittem/bitcoin-is-a-decentralized-organism-mycelium-part-1-3-6ec58cdcfaa6> (04/12/19)

¹³ The Bitcoin Standard by Saifedean Ammous (04/12/19)

¹⁴ <https://finance.yahoo.com/news/in-quest-for-digital-gold-161310664.html> (04/12/19)

¹⁵ <https://www.youtube.com/watch?v=zveT0W-JCa8> (04/12/19)

¹⁶ <https://dailyhodl.com/2019/04/04/messari-ceo-says-bitcoin-is-digital-gold-30-trillion-wealth-transfer-heading-to-btc/> (04/12/19)

¹⁷ <https://cointelegraph.com/news/british-financial-historian-niall-ferguson-says-bitcoin-is-an-option-on-digital-gold> (04/12/19)

¹⁸ <https://www.adamantcapitalfund.com/bitcoin-digital-gold-or-digital-cash/> (04/12/19)

¹⁹ <https://bitcoinexchangeguide.com/block-one-ceo-brendan-blumer-says-bitcoin-is-the-best-store-of-value-a-real-gold-replacement/> (04/12/19)

²⁰ <https://www.forbes.com/sites/investor/2019/04/16/bitcoin-is-the-new-gold/#4168b883239a> (04/12/19)

The curious reader will probably enjoy the following text: *Shelling Out: The origins of Money, Nick Szabo*²¹. A special consideration must be paid to the concept of unforgeable costliness in the context of the energy consumption as it anchors Bitcoin in the physical world. Proof-of-work (energy consumption), the difficulty adjustment and the monetary policy are important concepts to understand in order to draw parallels and grasp the comparison with digital gold and to unbundle bitcoin from other crypto-assets.

Some won't see any value and won't buy bitcoin. This is simply how a market operates (i.e. where conflicting views meet). It is by the same market mechanism that someone did not invest in Amazon +/- 20 years ago when it was trading in the low double digits. Some saw value beyond a simple online book store, some disagreed, some have been rewarded, some have not.

Bitcoin is neither a debt or an equity instruments and from the start never fit the definition of a security. It can rather be viewed as a consumer goods or a commodity and its dealing, trading and marketplace activities sit outside IROC and CSA's legislative scope.

1.4 How is the U.S. SEC and the U.S. CFTC treating bitcoin?

The U.S. Securities and Exchange Commission (SEC) has stated that Bitcoin is not a security. Here is a video interview²² dated June 6th 2018, where the Chairman of the SEC, Jay Clayton is crystal clear:

"...Cryptocurrencies, these are replacements for sovereign currency, replace the Dollar, the Yen, the Euro with Bitcoin. That type of currency is not a security. Let me turn to what is a security (...)"

The U.S. Commodity Futures Trading Commission (CFTC) has also already stated that:

"Yes, virtual currencies, such as Bitcoin, have been determined to be commodities under the Commodity Exchange Act (CEA)²³"

Why is it that a year later, Canadian securities regulators are still not clearly expressing themselves on the matter? Vague language such as "may represent" is used in their communication. The aim is still unclear and may lead to believe that *all* crypto-assets are targeted by the security's regulatory regime? If Canadian securities regulators were misunderstood, and if Bitcoin's ecosystem is not concerned by 21-402, a clear stance would be welcomed.

²¹ <https://nakamotoinstitute.org/shelling-out/> (04/18/2019)

²² <https://www.cnn.com/video/2018/06/06/sec-chairman-cryptocurrencies-like-bitcoin-not-securities.html> (04/12/19)

²³ https://www.cftc.gov/sites/default/files/idc/groups/public/%40customerprotection/documents/file/oceo_bitcoinbasics0218.pdf (04/18/19)

2. The commerce of (non-securities) valuables

In this section, we will explore the commerce of gold in Canada and will use this example to demonstrate that as long as gold is held outside of an investment structure (such as an ETF or a closed ended investment trust), it sits outside the securities legislation. Different cases involving buy and sell transaction, custodial-relationship and collateralized loans will be presented.

2.1 Individuals buying/selling/storing physical gold

Key Messages

- Individuals are free to own, collect, and speculate on collectibles/store of value.
- Securities regulators do not oversee the dealers or trading activities of such items.
- Asset custody by a third party doesn't change the nature of an asset into an investment contract or a derivative.

In this section, we will address Part 3 of the consultation paper called "Risks related to Platforms". To accomplish this, we will use the example of Kitco Metals Inc.

*"Kitco Metals Inc. is also one of the world's premier **retailers** of precious metals and a leading supplier of refining services, labware for mineral analysis and precision-crafted devices for high-technology manufacturing processes. From our offices in Montreal, New York (Subsidiary) and Hong Kong, we **buy and sell a wide range of precious metal products** in gold, silver, platinum, palladium and rhodium. We also provide metals **for custodial storage programs to individual customers and corporations** the world over."*²⁴

Replacing precious metals with bitcoin will allow to compare very similar business models.

- Kitco is a FINTRAC²⁵ reporting entity.
- Kitco is not subject to securities regulation.
- Kitco is subject to code of law and was held accountable by authorities in this unflattering case²⁶.
- Kitco offers transactional-only services (non-custodial).
- Kitco offers custodial services (allocated storage).
- Kitco is not concerned with suitability of the investment in precious metals.
- Kitco does not have an education obligation about the metals, but does so voluntarily.
- Kitco presents buy or sell prices and the client is free to trade or not at these levels.
- Smaller gold coins trade at a premium versus the bullions. Price and premium can vary between retailers.

²⁴ <http://corp.kitco.com/en/index.html> (04/12/19)

²⁵ <https://www.canada.ca/en/financial-transactions-reports-analysis.html> (05/05/19)

²⁶ <https://www.theglobeandmail.com/report-on-business/industry-news/energy-and-resources/quebec-names-kitco-metals-among-companies-in-alleged-tax-fraud/article15821055/> (05/10/19)

Non-custodial relationship (transactional)

Bob goes to Kitco and exchanges CAD \$1,000 for X amount of gold coins. There is no custodial relationship. Bob gives CAD\$ and received gold coins in exchange from Kitco. He leaves the store with his newly purchased gold coins and self-custodies according to the method of his choosing.

This is similar to a non-custodial bitcoin exchange.

Custodial relationship

Alice goes to Kitco and exchanges CAD \$100,000 for X amount of gold bullions and coins. For reasons of her own, Alice does not wish to custody the gold herself. She considered renting a safety deposit box at a bank but does not like the fact that the bank is not liable for loss or damage occasioned by fire, theft or any other cause. Instead, Alice is considering Kitco's allocated storage program where precious metals bullions can be stored on a segregated and allocated basis. Before entering this custodial relationship, Alice consults the website²⁷ and obtains information about key aspects, such as safeguards, process, policies and procedures, insurance, independent audit and the FAQs regarding the custody of the assets.

To my knowledge, this disclosure of information is not required by a regulatory body. It is rather a market-driven business decision where clearly articulating the safety of the value proposition will set the transparent business apart from a competitor that would not. It seems logical to think that market competitive forces will favor the more credible, transparent and professional businesses.

In Alice's example, the act of dealing with a custodian did not transform her gold into an investment contract or a derivative. This is similar to custodial bitcoin exchanges, where both transactional and custodial services are offered.

²⁷ <https://online.kitco.com/faq/kitco-allocated-storage#faq-What-is-the-Kitco-Allocated-Storage-program?>
(04/14/19)

2.2 Investment funds buying / selling / storing physical gold

Key messages

- Securities regulators oversees securities that invest in gold or real estate.
- Previous regulators have faced similar concerns and have created a time-tested path.
- Securities regulators did not have to regulate the market places or the trading of real estate or gold to allow their inclusion in investment trusts.
- Regulators must not single out some assets with more stringent rules.

2.2.1 ETF investing in Gold (American example)

Except for certain aspects that we will cover later, gold ETFs have already paved part of the way for a bitcoin ETF. An examination of the prospectus²⁸ State Street’s exchange traded funds (ETF) GLD will be helpful because it has considerations pertaining to trading, custody, price determination, valuation, conflict of interest, and the various risks associated with the funds.

GLD was launched in 2004 with \$115 million USD in assets. As of April 15th 2019, the funds asset under management is over \$31 billion USD (the trust claims to own 757,85 tonnes of gold). The funds description provided below explains clearly what barriers it is trying to lower with its offering. A Bitcoin ETFs would want to lower the exact same barriers.

“SPDR Gold Shares represent **fractional, undivided beneficial ownership** interests in the Trust, the **sole assets of which are gold bullion**, and, from time to time, cash. SPDR Gold Shares are intended to **lower a large number of the barriers preventing investors** from using gold as an **asset allocation and trading tool**. These barriers have included the **logistics of buying, storing and insuring gold**. In addition, **certain pension funds and mutual funds do not or cannot hold physical commodities, such as gold**, or the derivatives.”²⁹

15 years ago, regulators and lawyers have already alleviated some of the similar concerns (valuation, safeguarding, liquidity, etc.) that the Consultation paper 21-402 is bringing forward. Thus, this could represent a comparable basis for securities regulators to work from. They have the opportunity to formulate, based on previous work, what is expected from non-securities crypto-assets trading platforms so they can service the needs of a funds structure. The following questions are addressed by GLD’s prospectus:

Custodians / Sub custodians	Factors impacting gold prices
Price Determination	Delivery of required deposits
Price Volatility	Market regulation
Price Manipulation	Etc.

²⁸ <https://www.spdrgoldshares.com/media/GLD/file/SPDR-Gold-Trust-Prospectus-20170508.pdf> (04/14/19)

²⁹ <https://www.spdrgoldshares.com/usa/> (04/14/19)

Noteworthy language from the GLD prospectus has been extracted and provided below to highlight precedents set by regulators who previously had to deal with similar concerns raised by 21-402.

- The value of the gold held by the Trust is determined using the LBMA Gold Price PM. Potential discrepancies in the calculation of the LBMA Gold Price PM, as well as any future changes to the LBMA Gold Price PM, could impact the value of the gold held by the Trust and could have an adverse effect on the value of an investment in the Shares.
- If concerns about the integrity or reliability of the LBMA Gold Price PM arise, even if eventually shown to be without merit, such concerns could adversely affect investor interest in gold and therefore adversely affect the price of gold and the value of an investment in the Shares.
- Crises may motivate large-scale sales of gold which could decrease the price of gold and adversely affect an investment in the Shares.
- The Trust’s gold may be subject to loss, damage, theft or restriction on access
- The Trust may not have adequate sources of recovery if its gold is lost, damaged, stolen or destroyed and recovery may be limited, even in the event of fraud, to the market value of the gold at the time the fraud is discovered.
- Because neither the Trustee nor the Custodian oversees or monitors the activities of subcustodians who may temporarily hold the Trust’s gold bars until transported to the Custodian’s London vault, failure by the subcustodians to exercise due care in the safekeeping of the Trust’s gold bars could result in a loss to the Trust.
- The ability of the Trustee and the Custodian to take legal action against subcustodians may be limited, which increases the possibility that the Trust may suffer a loss if a subcustodian does not use due care in the safekeeping of the Trust’s gold bars.
- The gold bullion custody operations of the Custodian are not subject to specific governmental regulatory supervision.

2.2.2 Investment Trust investing in Gold (Canadian example)

In search of a Canadian equivalent to GLD, the Sprott Physical Gold Trust has been identified as a potential comparable. The investment format is different. GLD is open-ended, PHYS is closed-end and both are regulated by their respective securities regulators and both are available to the general public. PHYS is listed on both the TSX and NYSE Arca. When consulting the prospectus³⁰ of PHYS, a noticeable difference with GLD can be observed. Constraints imposed to the receipt of PHYS prospectus appeared to be much less rigid in Canada than in the U.S. for GLD. Only four risks are identified in PHYS’s prospectus versus 24 in GLD’s. Certain risk factors brought forward in 21-402 such as price determination, price volatility, price manipulation, factors impacting gold price have been explicitly covered in GLD but were not a requirement in Canada. If these risk factors were not required for an investment trust to invest in gold in Canada, why is Bitcoin treated differently?

³⁰ <http://www.sprott.com/media/1443/phys-prospectus-en.pdf> (05/01/19)

2.2.3 ETF investing in Real Estate Investment Trust (American example)

Investment trust also have the possibility to invest in real estate. Just like gold, real estate is not a security. Bitcoin could be compared to a form of “digital real estate” because its supply is limited. Said differently, there is a limited set of Unspent Transaction Outputs (UTXO), known as: the bitcoins.

Real Estate differs from traditional stocks and bonds and comes with special risks and intricacies that are also different than with gold. It is therefore interesting to look at how particular provisions were drafted and included in the prospectus³¹ to reflect these particularities associated with real estate investing. IYR is an example of a U.S. real estate ETF and shares risks that could be applicable to bitcoin;

- Cyber security risks (page 3)
- Market Trading Risk: Absence of Active Market/ Risk of Secondary Listings / Secondary Market Trading Risk (...) (page 5-6)
- Liquidity risks (page 8)
- Regulatory risks (page 9)
- Operational risks (page 9)
- Determination of Net Asset Value (NAV) (page 17)

³¹ <https://www.ishares.com/us/library/stream-document?stream=reg&product=I-DREAL&shareClass=US+Class&documentId=1280409~1280118~926348~1255433~1192007&iframeUrlOverride=%2Fus%2Fliterature%2Fprospectus%2Fp-ishares-us-real-estate-etf-3-31.pdf> (04/23/19)

2.2.4 ETF investing in Real Estate Investment Trust (Canadian example)

A Canadian example is XRE (iShares S&P/TSX Capped REIT index ETF). The prospectus³² is a 180 pages umbrella covering at once, all the products offered by the ETF provider (as opposed to a per product prospectus approach). Risks are presented in a simpler form and the prospectus has been receipt with a “tick the box” approach. For example, risks are presented as follows;

Additional Risks Relating to an Investment in Certain iShares Funds

In addition to the general risk factors applicable to all iShares Funds, there are certain risk factors inherent to an investment in the iShares Canadian Equity Funds, as indicated in the table below:

Additional Risks Relating to an Investment in the iShares Canadian Equity Funds																
	XCG	XCS	XCV	XDV	MEG	XEI	XEN	XFN	XIC	XIT	XIU	XMA	XMD	XRE	XST	XUT
Cease Trading of Securities Risk	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Developed Countries Investments Risk	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
General Risks of Equity Investments	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Income Trust Investments Risks	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Large-Capitalization Companies Risk	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Non-Capitalization Weighted Strategy Risks				✓												
North American Economic Risk	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Sector Risk	✓		✓	✓	✓		✓	✓		✓		✓		✓	✓	✓
Small-Capitalization Companies Risk	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Voting of Index Securities Risk	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

This text pertaining to risk is also available in the XRE prospectus.

XRE. REITs generally are subject to certain risks related to their direct ownership of real estate. Real property investments are affected by general economic conditions, local real estate markets, supply and demand for leased premises, competition from other available premises and various other factors. The value of real property and any improvements thereto may also depend on the credit and financial stability of the tenants and upon the vacancy rates of the property portfolio. There are also certain types of risks relating to the ownership of real estate, generally of a catastrophic nature, such as wars or environmental contamination, which may be either uninsurable or not insurable on an economically viable basis. In addition, environmental laws may render a REIT liable for the costs of removal of certain hazardous substances and remediation of certain hazardous locations. Real estate ownership may also require certain significant expenditures, including property taxes, maintenance costs, mortgage payments, insurance costs and related charges regardless of whether the property is producing any income.

Another example is BMO’s ZRE ETF where in the 242 pages *simplified* prospectus³³ we can also see additional risks relating to investing presented in a “tick the box” framework (page 130).

Based on both gold and REITS prospectuses, it can be noticed that Canadian securities regulators are satisfied with risks being disclosed in a simpler format and did not require explicit definitions. The naming of the risk sufficed.

³² <https://www.blackrock.com/ca/individual/en/literature/prospectus/ishares-index-funds-prospectus-en-ca.pdf> (06/05/19)

³³ https://www.bmo.com/assets/pdfs/gam/bmoam_etfs_prospectus_february-7-2019-en.pdf (06/05/19)

2.3 Collateral loans

Key Messages

- Pledging collateral doesn't change the nature of an asset into an investment contract.
- A lien on an asset is not a derivative or an investment contract.
- Securities regulators do not oversee collateralized loans.

Consultation paper 21-402 (page 2) reads as following:

"However, securities legislation may still apply to Platforms that offer trading of crypto assets that are commodities, because the investor's contractual right to the crypto asset may constitute a security or a derivative. We are evaluating the specific facts and circumstances of how trading occurs on Platforms to assess whether or not a security or derivative may be involved. Some of the factors we are currently considering include:"

The list of factors provided mostly revolve around the concept of custody. As illustrated before, the custodial act of gold (in a bank-held safety deposit box, in a vault at Kitco or through an investment trust's custodian) does not transform gold itself into a security or a derivative. However, the list of factors presented in 21-402 did not include bitcoin-backed lending related cases. In the spirit of making sure this paper covers as many angles as possible, I aim to demonstrate that bitcoin-backed lending does not involve a security or a derivative.

Pledging an asset in exchange for money

For all sorts of reasons, individuals may need to borrow against assets they own. They would pledge these assets as collateral in exchange for fiat currency. Gold, jewelry, electronics, art, special collection, etc., are examples of assets that a lender could accept as collateral. If the loan is not repaid according to negotiated terms, the lender becomes the official owner of the pledged collateral. This is essentially the concept of Pawnbrokers (or collateral loans). Applicable Pawnbrokers regulation comes from governmental regulation (federal/provincial/municipal). Consumer protection right and Criminal code also applies. While other provinces^{34 35} have their own ruling, the Government of Ontario repealed the Pawnbroker Act³⁶ at the beginning of 2019. The Ministry of the Attorney General said³⁷:

"Without the Act, pawnbrokers would no longer be required by provincial legislation to have a municipal business license. Municipalities would determine whether to require a license or otherwise regulate."

Pawnshops and alike concepts such as gold-backed lending^{38 39 40 41} are not regulated by the securities or derivatives regulatory agencies.

³⁴ <https://www.avocat.qc.ca/public/iipretgage.htm> (05/02/19)

³⁵ http://www.bclaws.ca/civix/document/id/complete/statreg/96350_pit (05/02/19)

³⁶ <https://www.ola.org/en/legislative-business/bills/parliament-42/session-1/bill-66#BK4> (05/02/19)

³⁷ <https://globalnews.ca/news/4883939/pawnbrokers-act-bill-66-ontario/> (05/02/19)

³⁸ <https://loanscanada.ca/loans/loans-using-collateral/> (05/02/19)

³⁹ <https://cashgoldcanada.ca/collateral-loans-cash-gold-canada/> (05/02/19)

⁴⁰ <https://loansforjewels.ca/> (05/02/19)

⁴¹ <https://www.cashcanada.com/pawn-buy-sell/gold-and-jewelry/> (05/02/19)

2.4 Summary

Individuals are free to own what they perceive to be of value and retailers are not responsible for suitability assessment of the purchase. Securities regulators do not oversee the dealers or trading activities of collectibles or stores of value. Suitability assessment of non-securities items is not part of the securities regulators' mandate and would represent stepping over individual's personal preference. FINTRAC regulates the commerce of certain type of assets (such as precious metals and stones, real estate and virtual currencies) in the context of preventing money laundering and financing of terrorist activities. Thefts, frauds and misleading statements are already illegal or forbidden and punishable by law. There is no need for a specific regulation on Bitcoin as it is already covered by the actual legal framework.

ETFs and investment trust investing in gold have already answered similar concerns that securities regulators have expressed in 21-402. Regulators should not single out or impose more stringent rules than they would otherwise do for other investment structures. **Securities regulators did not have to regulate the trading and market places of gold or real estate to allow their inclusion in investment trusts.** This is not to advocate in favor of investment trusts investing in crypto, as I believe participants should have the option to participate in bitcoin the way that suits them best. But rather to identify, the zone in which there is an intersection between the two ecosystems and where securities regulators can exert their regulatory framework.

Securities regulators were not concerned with suitability of gold or REITs as an investment but were rather preoccupied with the appropriate risks disclosure in the information conveyed to potential investors. Even though they were confronted with novel and specific risks, these did not prevent their inclusion from investment trusts. Instead, legal language was included in the prospectus to reflect the risks and was drafted in a way that satisfied securities regulators. As demonstrated with the Canadian examples, naming the risk was in certain cases deemed a sufficient disclosure.

This section also demonstrated that the act of custody or the act of pledging an asset as collateral does not change the nature of the asset. Custody and collateral are not an investment or a derivatives contract.

21-402 risk sending the securities regulators in a long and unfruitful process that sits outside their mandate and leading to miss the objective of protecting the consumer. The most direct way securities regulators can influence the industry without creating distortion, unnecessary costs and delays is first to clearly define what is a security within crypto-assets from what is not. Secondly, to focus on the securities vehicle (such as investment trusts) who want to participate in bitcoin or so-called crypto-assets. Securities regulators will be able to assess whether or not the proper disclosures have been achieved in the prospectus in regards to the risks participants would expose themselves to.

Unfortunately, securities regulators in Canada have expressed an unnuanced and negative bias against Bitcoin and cryptocurrencies. This stance has led to unintended consequences that we will cover in the next section.

3. Preoccupations

Consultation paper 21-402 proposes a framework for crypto-asset trading platforms without clearly expressing the type of crypto-assets it is going after or explicitly excluding and defining what are non-securities crypto-assets. The definition of the underlying target is particularly important as securities regulators could be attempting to regulate something that is not under their jurisdiction. This lack of clarity, creates market uncertainty, friction, misinformation and raises several concerns.

3.1 Multi-dimensional & open-ended regulatory struggle

CSA Staff Notice 46-307⁴² outlines how Canadian Securities Laws and 'substance over form' tests may apply to ICOs, crypto asset investment funds and exchanges.⁴³

CSA Staff Notice 46-308⁴⁴ "reiterated the CSA's views, adding that many purported 'utility' tokens were not eligible to be exempt from securities laws, therefore requiring both a prospectus and the registration of the securities issuer."⁴⁵

The following is an extract from 46-307. It gives an example of the lack of clarity the market received:

"For example, if an individual purchases coins/tokens that allow him/her to play video games on a platform, it is possible that securities may not be involved. (...)"

Are securities regulators genuinely not able to state that a sword bought or earned in an online game that could be portable to another game (with perhaps a different value) is not a security?

Are the following crypto-assets considered securities in the context of 21-402 framework?

- Central Bank Digital Currencies (CDBC).
- Stablecoins (fiat-pegged issued coins).
- Token of an online game sword that would be portable/tradeable in multiple online games.
- Tokenized patents, tokenized music rights.
- My own personal individual data.

Do the securities regulators intend to regulate?

- how scientists can monetize their patents?
- how the music industry operates?
- how many swords a kid can own and trade while playing his favorite online games?
- how an individual can exert control and monetization over his/her own individual data?
- Software, AI and IoT economic relationships?

⁴² https://www.osc.gov.on.ca/en/SecuritiesLaw_csa_20170824_crypto-currency-offerings.htm (04/26/19)

⁴³ <https://www.jbs.cam.ac.uk/faculty-research/centres/alternative-finance/publications/cryptoasset-regulation/#.XMMwpZNKjUZ> (04/26/19)

⁴⁴ https://www.osc.gov.on.ca/en/SecuritiesLaw_csa_20180611_46-308_securities-law-implications-for-offerings-of-tokens.htm (04/26/19)

⁴⁵ <https://www.jbs.cam.ac.uk/faculty-research/centres/alternative-finance/publications/cryptoasset-regulation/#.XMMwpZNKjUZ> (04/26/19)

Are the following crypto-assets trading platforms considered by the 21-402 framework?

- Non-custodial exchanges and apps.
- Embedded in other platform (ex: tipping on twitter).
- Social media platforms (ex: Facebook is rumored to have an upcoming coin).
- Integrated in a web browser (ex: content monetization).
- Data market places.
- Smart phones, E2EE messengers, satellites, ham radio, smoke signals, emojis.
- Paper.

If the answers are yes, then Canada will be at a significant disadvantage versus the rest of the world. If the answers are yes, the fundamental objectives pursued have to be questioned. In the end, what will truly be accomplished by 46-307, 46-308 and 21-402 if businesses can't develop in Canada? And what would this mean for software, computer networks and businesses in general going forward?

3.2 Stigmatization

Securities regulators in Canada, have repeatedly and publicly expressed their dislike of cryptocurrencies as a whole. This creates a difficult environment for legitimate entrepreneurs who need banking relationships to conduct their normal business (e.g. pay rent, salaries, insurance, income taxes). Statements such as below demonstrate an *a priori* negative bias.

“Cryptocurrencies facilitate the organization of fraudsters”.⁴⁶

Would the same discourse be held towards the Internet, Wi-Fi, cellular phones, emails, encryption, text messages, pre-paid cards? Because they all facilitate the organization of fraudsters.

This next statement goes along the same lines:⁴⁷

Risk of participating in criminal, terrorist or fraudulent activities or money laundering

Cryptocurrencies have been associated with fraud, money laundering and criminal or terrorist activities.

It is important to distinguish between the crime and the means to commit the crime. Toronto⁴⁸ and Vancouver⁴⁹ real estate have also been associated with money laundering. Have securities regulators issued the same public warning against residential and commercial properties?

Are these claims factual or judgmental?

A study commissioned by the European Parliament’s Policy Department for Citizen’s Rights and Constitutional Affairs⁵⁰ and published in May 2018 offers a documented picture of the situation. Key findings about Virtual Currencies (VCs) include:

- a small number of cases suggest some jihadist and right-wing extremists are using (VCs).
- VC’s currently do not provide substantial benefits over traditional methods.

In 2018, according to Japan Times⁵¹, there were 7,096 on a total of 417,465 suspicious transactions that involved cryptocurrencies. Said differently, from all the suspected cases of money laundering in Japan, only 1,7% were attributable to cryptocurrencies.

Same information has been found in the USA as per this comment from the Office of Terrorist Financing and Financial Crimes:

“Although virtual currencies are used for illicit transactions, the volume is small compared to the volume of illicit activity through traditional financial services.”⁵²

⁴⁶ <https://journalmetro.com/cryptomonnaies/2237877/la-crypto-facilite-lorganisation-des-fraudeurs/> (04/16/19)

⁴⁷ <https://lautorite.qc.ca/en/general-public/investments/bitcoin-and-other-virtual-currencies/> (04/25/19)

⁴⁸ <https://globalnews.ca/news/5080238/toronto-real-estate-money-laundering-opaque-investment/> (04/29/19)

⁴⁹ <https://www.bloomberg.com/news/articles/2019-05-10/billions-in-dirty-cash-helped-fuel-vancouver-s-housing-boom> (05/12/19)

⁵⁰ [http://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU\(2018\)604970_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU(2018)604970_EN.pdf) (04/25/19)

⁵¹ <https://www.japantimes.co.jp/news/2019/02/28/national/crime-legal/cases-money-laundering-linked-cryptocurrency-japan-tenfold-2018/#.XMyc69NKjUZ> (05/03/2019)

⁵² <https://www.judiciary.senate.gov/imo/media/doc/Fowler%20Testimony.pdf> (05/10/2019)

Lastly, and with the intent of presenting an order of magnitude for comparison, the example of Danske Bank will be put forward. While it is one of the most respected financial institutions in Europe, it has been caught last fall in a \$200 billion USD money laundering scandal⁵³ ⁵⁴. At the time of writing these lines, the total bitcoin market cap hovers around \$100 billion USD. This one scandal, from a single financial institution is twice the size of the entire market cap of bitcoin.

In light of these, does Bitcoin deserve such a severe stigma from Canadian securities regulators?

Who deals with PCMLTFA matters in Canada?

FINTRAC, the Financial Transactions and Reports Analysis Center of Canada deals with matters pertaining to Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA). Financial entities such as banks, securities dealers (e.g. IIROC/CSA's members), precious metals dealers and money service businesses (MSBs) are examples of FINTRAC reporting entities⁵⁵.

Late in the summer of 2018, FINTRAC held public consultations across Canada to obtain feedback from the industry about its proposed regulatory framework modifications for MSBs dealing in Virtual Currencies. Legislative modifications are currently pending and are sitting with FINTRAC's working group. The results are expected later this year or early 2020.

The AML / FT compliance requirements for MSBs come from FINTRAC not from IIROC / CSA.

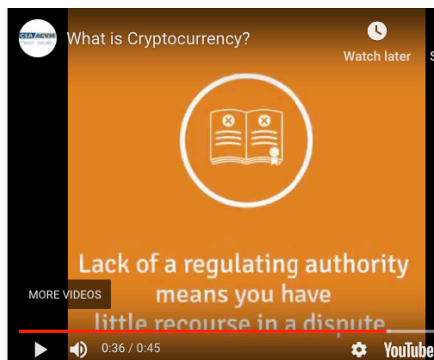
⁵³ [https://moneyweek.com/495970/danske-banks-money-laundering-scandal/\(05/03/2019\)](https://moneyweek.com/495970/danske-banks-money-laundering-scandal/(05/03/2019))

⁵⁴ [https://www.theguardian.com/business/2018/sep/21/is-money-laundering-scandal-at-danske-bank-the-largest-in-history\(05/03/2019\)](https://www.theguardian.com/business/2018/sep/21/is-money-laundering-scandal-at-danske-bank-the-largest-in-history(05/03/2019))

⁵⁵ <http://fintrac-canafe.gc.ca/reporting-declaration/Info/re-ed-eng.asp> (05/13/19)

3.3 There is regulation

Contrary to what is stated in this video⁵⁶ from the Canadian Securities Administrators, there is regulation. Stating that regulation is lacking and that there is little recourse fails to account for important information and may be misleading the public.



First, it misses several points:

- **FINTRAC:** oversees Money Service Business, AML / FT. (regulatory update pending).
- **Code of law / criminal code:** is not nullified by the usage of Bitcoin. Fraud and theft are illegal and punishable by law.
- **Consumer protection right:** is not nullified by the usage of Bitcoin. It may be more difficult to enforce in the context of global businesses but nowadays online reputation is a strong behavioral incentive, possibly more effective than regulation itself to service clients well.
- **Bitcoin has its own embedded rules:** And they are enforced consistently and objectively. This is beautifully described by Spencer Bogart, CFA in his essay *The Internet's Magna Carte Moment: Bitcoin & The Value of Strong Assurances*⁵⁷. An extract can be found below:

"The Bitcoin network, for example is a self-contained, rules-based, self-arbitrating court where valid transactions are clearly defined, objectively verifiable, and unerringly enforced y network participants"

"Bitcoin, for example, offers a self-contained, reliable foundation for property rights in a digital world. The Bitcoin network is a riles-based, self-arbitrating court – it's likely the fairest, most transparent and most predictable court in the world".

"The Bitcoin network is a decentralized institution that defines, monitors and enforces property rights".

It is global in nature (not limited by geography/citizenship), it is clearly defined (no subjective interpretation) and perfectly enforced (objectively and unerringly enforced).

⁵⁶ [https://www.youtube.com/watch?time_continue=16&v=dLPNyHlp8CU\(04/25/19\)](https://www.youtube.com/watch?time_continue=16&v=dLPNyHlp8CU(04/25/19))

⁵⁷ [https://medium.com/blockchain-capital-blog/the-internets-magna-carta-moment-bitcoin-the-value-of-strong-assurances-56fb86887b8a\(04/25/19\)](https://medium.com/blockchain-capital-blog/the-internets-magna-carta-moment-bitcoin-the-value-of-strong-assurances-56fb86887b8a(04/25/19))

Second, it contradicts some of the regulator’s own claims:

- **Securities regulators:** oversee securities offering including ICO’s as stated on their own websites. Please see OSC’s⁵⁸ and AMF’s⁵⁹ website. What is the true message when the securities regulators say there is a lack of regulating authority?

Are ICOs regulated by the AMF?

The AMF regulates ICOs that involve the sale of securities. In Québec, many ICOs are subject to the [Securities Act](#),⁶⁰ mainly because they are considered investment contracts.

CRYPTOCURRENCY OFFERINGS

Cryptocurrency offerings such as initial coin offerings (ICOs) and initial token offerings (ITOs) can provide new opportunities for businesses to raise capital and for investors to access a broader range of investments. Many ICOs and ITOs involve sales of securities. Securities laws in Canada will apply if the person or company selling the securities is conducting business from within Canada or if there are Canadian investors.

- **Securities regulators:** oversee at least one crypto-assets platform in Canada.

Contrary to what is stated on page 1 of the consultation paper 21-402: *“Currently there are no platforms recognized as an exchange or otherwise authorized to operate as a market place or dealer in Canada...”* we can see from AMF’s website that ShakePay Inc. has been delivered a Money Service Business permit⁶⁰ two years ago (2017-04-26). Are we possibly facing a definition problem?

SHAKEPAY INC.	Change de devises Transfert de fonds	2017-04-26
---------------	---	------------

This is an extract from ShakePay website⁶¹.

ShakePay only offers BTC (bitcoin) and ETH (ethereum).

 **Regulatory oversight**

Shakepay is licensed as a Money Service Business by FINTRAC and the AMF to operate in all Canadian provinces and territories

Should we conclude that these two crypto-assets are not considered by consultation paper 21-402? If so why?

Question for IIROC and CSA: Have your members been required to update their PTA (personal trading authorization) procedures to reflect the inclusion of crypto? Because if certain crypto-assets are deemed to be securities, or if your members have access to material non-public information on crypto assets, this could mean they are breaching your very own compliance code.

⁵⁸ <https://www.osc.gov.on.ca/en/our-approach.htm> (04/25/19)

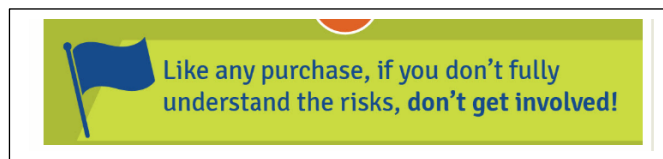
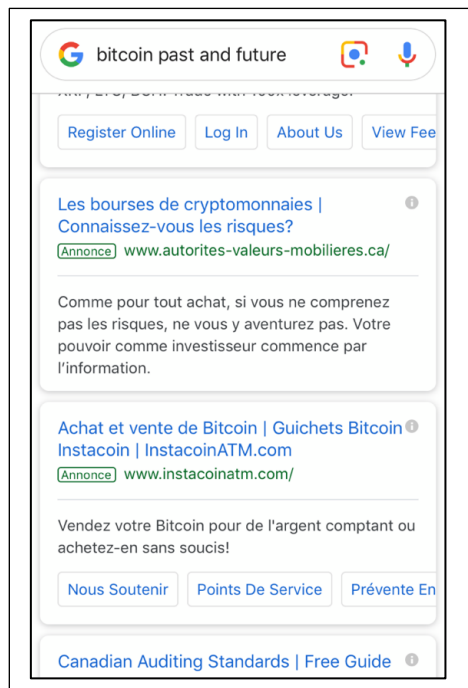
⁵⁹ <https://lautorite.qc.ca/en/general-public/investments/bitcoin-and-other-virtual-currencies/> (04/25/19)

⁶⁰ https://lautorite.qc.ca/fileadmin/lautorite/bulletin/2018/vol15no19/vol15no19_8-3.pdf (04/29/19)

⁶¹ <https://shakepay.co/>(04/29/19)

3.4 Double standard (1) - Volatility

One of the key angles put forward by securities regulators against cryptocurrencies is price volatility. This google ad, shows this is something securities regulators are willing to pay advertisement for⁶².



Don't get involved!⁶³

Volatility risk

The value of a cryptocurrency is determined by the public's interest in it and is based strictly on supply and demand. Media coverage of a cryptocurrency can have a major impact on its value over a short period of time without any official organization or mechanism controlling the volatility. There are also numerous platform or digital exchanges on which digital cryptocurrencies can be negotiated. All such exchanges may offer different prices for the same cryptocurrency.

- *"The value of a cryptocurrency is determined by the public's interest in it and is based strictly on supply and demand"*⁶⁴.
 - Isn't the law of supply and demand an economic tenant underlying all markets?
- *"(..) without any official organization or mechanism controlling the volatility"*.
 - Other than the market itself, what organization or mechanism should "control the volatility"?
 - Are the securities regulators asking for some form of price manipulation?

⁶² Curious of the budget to perform such ad, Octonomics reached out to a firm specialized in google advertising to obtain a quote. The current (04/18/19) price to capture Bitcoin's advertising in Quebec only is +/- 1,400\$ /mth.

⁶³ <https://www.securities-administrators.ca/investortools.aspx?id=1696> (04/25/19)

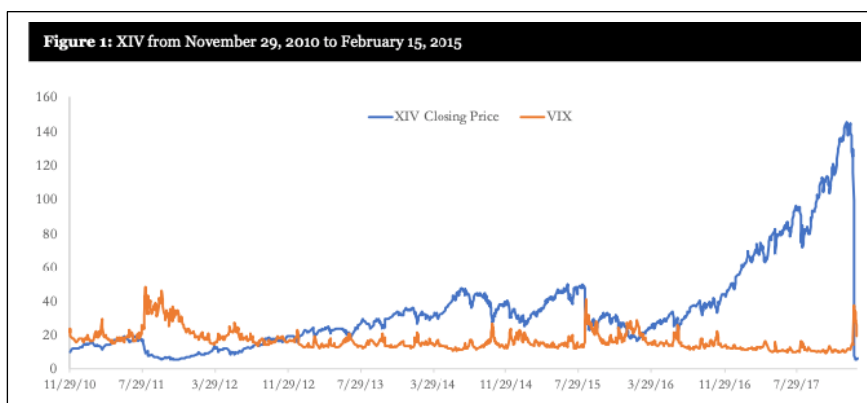
⁶⁴ <https://lautorite.qc.ca/en/general-public/investments/bitcoin-and-other-virtual-currencies/>

The double standard

There are other highly volatile products available to Canadian investors. For example, penny stocks listed on the Venture Stock Exchange or inverse and leveraged ETFs listed on the Toronto Stock Exchange.

What is different about these examples where their high volatility levels don't warrant public warnings from securities regulators?

There is a recent and interesting case of a regulated, prospectus-based volatility product that totally blew up. The product was not listed on Canadian stock exchanges, yet Canadian investors were able to trade it. On February 5th 2018, the Exchange Traded Note (ETN) XIV from Credit Suisse, lost 97% of its value (+/- \$2 billion USD) in a single day⁶⁵. The last trading day occurred two weeks later⁶⁶.



It is worth noting that:

1. People who lost money were on the right side of the trade. They were betting that volatility would go down. And it did. But they lost 97% of their investment in one day.
2. This 2012 lawsuit⁶⁷ showed prior warnings that the product was not functioning properly.
3. The 60+ pages prospectus states: **The long term expected value of your ETN is zero**⁶⁸.

In light of this, should securities regulators also have actively campaigned "if you don't understand the risks, do not get involved" or was the highly complex 60+pages prospectus referring 63 times to a value of zero sufficient to cover the "fully understand the risks" part? Were investors anymore protected because the prospectus said the long-term value is zero?

⁶⁵[https://www.slcg.com/pdf/workingpapers/Material%20Misrepresentations%20in%20XIV%20Prospectus%20Led%20to%20\\$700%20Million%20in%20Losses.pdf](https://www.slcg.com/pdf/workingpapers/Material%20Misrepresentations%20in%20XIV%20Prospectus%20Led%20to%20$700%20Million%20in%20Losses.pdf) (05/04/19)

⁶⁶ <https://www.credit-suisse.com/corporate/en/articles/media-releases/credit-suisse-announces-event-acceleration-xiv-etn-201802.html> (05/04/19)

⁶⁷ <https://www.etfstrategy.com/lawsuit-filed-against-credit-suisse-for-tvix-etns-debacle-relating-to-velocityshares-daily-2x-vix-short-term-etns-66447/> (05/04/19)

⁶⁸ https://www.sec.gov/Archives/edgar/data/1053092/000095010318000969/dp85741_424b2-vix48.htm (05/03/2019)

3.5 Weak educational content

The CSA uses the social media platform Twitter⁶⁹ to target the general public and to share messages. It is interesting to observe the regularity at which the cryptocurrencies warnings efforts are deployed but also that there are days it is the only thing the CSA tweets about.

Various hashtags such as: #bitcoin, #Bitcoin, #ethereum, #ripple, #dash, #litecoin, #initialcoinoffering, #cryptocurrency, #blockchain, #ICO, #cryptoinvestment are used to maximize traction to reach the targeted audience.

Essentially, these sustained warnings point to the same educational content.

1. ICO's^{70 71 72}
2. Cryptocurrencies^{73 74 75}

I will not offer a lengthy comment on the ICO educational pieces because I agree with the essence of the message and because these structures for fundraising very much look like securities and therefore fall under securities legislation. That said, beyond the securities-status recognition, a market observer will realize there is a great deal of unsubstantiated marketing claims floating around. Narratives that don't yet exist are pushed ahead as a *fait accompli* and trendy buzzwords are used lightly and loosely by shady promoters. Transparency, clarity of business model and adequate warnings are often lacking. I think we ended up with a plethora of crypto-assets for the same reasons' capital was raised in Great Britain in 1720 for a great deal of ludicrous projects during the South Sea Bubble⁷⁶. That is the meeting of "get rich quick hopes" and unscrupulous people.

Not all project are intentional scams. Some legit entrepreneurs are sending the message to securities regulators they wish to operate globally without the heavy bureaucratic process-oriented burden the global fragmented securities framework has to offer.

As explained in 1.1, Bitcoin is a different animal and doesn't fit in the securities regulation. The current orientation of the regulators bundling everything into one big category is worrisome.

In 46-307, we can read: *"Any disclosure provided to investors, whether an OM or otherwise, must not be false or misleading. The disclosure must focus on material facts and be relevant, clear, balanced, in plain language and not overly promotional"*.

However, some of the information provided by the securities regulators is inaccurate, misleading and sometimes unfair. In that context and because a broad negative bias has been demonstrated, the next pages will provide comments on the educational content from the CSA in regards to cryptocurrencies.

⁶⁹ https://twitter.com/ACVM_Nouvelles and https://twitter.com/CSA_News (04/25/19)

⁷⁰ <https://www.securities-administrators.ca/investortools.aspx?ID=1697&LangType=1033> (05/04/19)

⁷¹ <https://twitter.com/NSSCommission/status/1123603571004592128/photo/1> (05/04/19)

⁷² <https://twitter.com/MSCCommission/status/1123273331053088768> (05/04/19)

⁷³ <https://www.securities-administrators.ca/investortools.aspx?id=1696> (05/04/19)

⁷⁴ <https://twitter.com/NSSCommission/status/1123241064062648321> (05/04/19)

⁷⁵ <https://www.youtube.com/watch?v=dLPNyHIp8CU> (05/04/19)

⁷⁶ *Extraordinary Popular Delusions and The Madness of Crowds* (by Charles Mackay) p. 33-36

It's obscure:

It's hard to make informed decisions about a cryptocurrency's value without financial statements or other traditional assessment criteria to rely on.



Bitcoin is not only transparent, but the information is abundantly available for free online to whomever wants to invest the time to research, curate, read and learn. The monetary policy, the emission curve, the protocol, the risks, the challenges and many more are exposed in the open.

Gold doesn't have financial statements; it doesn't pay dividend or interest. There are no earnings announcement or management team to gold. Yet, gold's valuation is in the trillions of dollars. Paintings, sculptures and other art work do not have financial statements and their pricing does not rely on traditional assessment criteria. Securities are investments, but investments are not necessarily securities.

Traditional measures such as market cap may not always be useful when it comes to crypto assets. Realized capitalization may offer more accurate insights⁷⁷. Being able to assess network performance, developer's activity, behavior profile of activity and user base are a new set of data forming metrics that are very different from what traditional finance professionals are used to working with.

No backing:

Cryptocurrencies are not backed by a bank or authority.




The "No backing" is presented in the "Risks" section. This should instead be presented in the "Value" section (if there was one). The fact that bitcoin is not backed by a bank or a central authority is part of the core proposition. It is a *raison d'être*. Avoiding pricey rent-seeking intermediaries or corruptible entities with the powers to confiscate, debase or misuse the asset are example of Bitcoin's mission. Bitcoin's white paper⁷⁸ published over 10 years ago is clear about the "no central authority" (see section 6).

⁷⁷ <https://newwebsite.coinmetrics.io/realized-capitalization/> (05/10/2019)

⁷⁸ <https://bitcoin.org/bitcoin.pdf?> (04/25/19)


It is complex:
It can be difficult, confusing and time-consuming to withdraw cryptocurrency, often requiring several intermediaries.



This statement both unfair and inaccurate. Unfair because anything someone does for the first time may seem to be difficult or confusing. It's called a learning curve and yes, it is time-consuming. For those old enough to remember the pre-internet era and the launch of online banking, most will recall how difficult, confusing and time-consuming it felt. Most of us are now quite familiar with it but it did not happen day one.

As far as withdrawal often requiring "several" intermediaries, it is inexact and fails to recognize the peer-to-peer nature and the various ways to withdraw (or utilize) bitcoin: at exchange, at bitcoin ATM, person to person or in exchange of goods or services.

It's vulnerable:
Online wallet companies and exchanges are susceptible to cybersecurity threats and hacking, putting your deposits at risk.

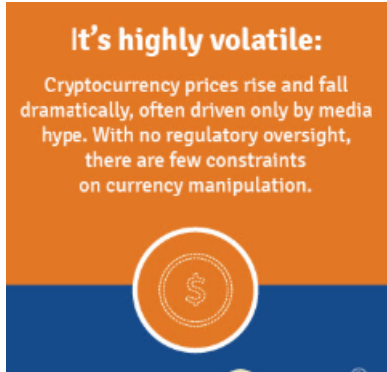


Any secured website or application in the digital realm is susceptible to hacking. This is not exclusive to online wallets. Credit cards, smartphones, clouds, connected devices, secured websites are all subject to hacking. Facebook⁷⁹, Amex⁸⁰ and Equifax⁸¹ are all recent public examples of hacking of consumer's personal data. If the regulators' mission is one of education (and not of fear), mentioning there are different ways to custody crypto-assets (where some are more secured than others), would better inform the audience. Alternatives have pros and cons, but do exist.

⁷⁹ <https://www.theguardian.com/technology/2018/sep/28/facebook-50-million-user-accounts-security-berach> (04/23/19)

⁸⁰ https://thenextweb.com/in/2018/11/07/amex-blunder-left-thousands-of-indian-customers-personal-info-unsecured/?utm_source=TNW&utm_campaign=3fdf8a3b9b-EMAIL_CAMPAIGN_2018_06_07_01_28_COPY_01&utm_medium=email&utm_term=0_32f70ba9aa-3fdf8a3b9b-12941949&mc_cid=3fdf8a3b9b&mc_eid=d643670b08 (04/23/19)

⁸¹ <https://techcrunch.com/2018/12/10/equifax-breach-preventable-house-oversight-report/> (04/25/19)



This next statement leads to believe there is currency manipulation. Is data available to support or is it a speculative statement?

Can there be price spreads between various trading places? Yes. Were there opportunities in traditional markets to arbitrage the price differential of an individual stock listed on two different exchanges? Yes. Did technological improvements and increased competition reduce the arbitrage opportunity with time? Yes. Was this available from the start? No. Can regulation force tight spreads or rule out price discrepancies? No. The market will, if it can.

It would be a mistake to think that regulated markets are completely exempt from price manipulation. Traditional regulated markets have had their fair share of price manipulation: Libor fixing scandal⁸², Foreign exchange rates manipulation⁸³, metals markets⁸⁴. Convicted banks paid fines and continued operating.

For those interested in the "fake volume" aspects of crypto assets trading, Bitwise Asset management presented an extensive document⁸⁵ to the U.S. S.E.C.

For those interested in how "artificial volume" is generated in traditional regulated markets and for what reason it is seen as beneficial, these articles^{86 87} provide great examples and broader perspective.

⁸² https://en.wikipedia.org/wiki/Libor_scandal (04/25/19)

⁸³ <https://www.reuters.com/article/us-banks-forex-settlement/global-banks-admit-guilt-in-forex-probe-fined-nearly-6-billion-idUSKBN0050CQ20150520> (04/25/19)

⁸⁴ <https://www.forbes.com/sites/traceygreenstein/2011/03/25/j-p-morgan-chase-and-hsbc-may-have-gained-billions-from-influencing-the-price-of-silver-2/#3d8843313a89> (04/25/19)

⁸⁵ <https://www.sec.gov/comments/sr-nysearca-2019-01/srnysearca201901-5164833-183434.pdf> (04/26/19)

⁸⁶ <https://www.bloomberg.com/graphics/2019-etf-tax-dodge-lets-investors-save-big/> (04/26/19)

⁸⁷ <https://www.bloomberg.com/graphics/2019-vanguard-mutual-fund-tax-dodge/> (05/05/19)



The data behind the statistical claim **“often driven only by”** would be interesting to obtain and to consult as it talks about a global, fragmented, multi-media, 24/7 market.

But first and foremost, this completely fails to account that Bitcoin is not a company. There is no publicity paid by bitcoin, there is no marketing department or PR agency.

So, are the securities regulators after bitcoin or after media outlets in this claim? Media is paid by publicity and assessed in clicks and views. Their coverage is spontaneous and they are incentivized to talk about what people wish to hear.

When securities regulators pay publicity or actively campaign in the media against the category, aren't they also part of that media hype? Are the securities regulators contributing to this price volatility? Has the impact of all global regulators been accounted for in this claim?

In 3.4, we saw securities regulators say the value of a cryptocurrency (...) is based strictly on supply and demand. But here we read “often only driven by media hype”.

Are securities regulators accusing the media of manipulating their audience? Are the securities regulators trying to regulate speech and media content? Imagine if Bitcoin was THE company (or event) everyone wanted to hear about. How can “it” be held responsible for the spontaneous, unpaid and earned media coverage?

Have the securities regulators envisioned that perhaps some bitcoin market participants do not care, value, listen or form their opinion by mainstream media coverage?

There are risks involved in bitcoin. Bitcoin is a technological experiment with a successful ten-year track record. As in any journey, it should be understood that there is no guarantee of success. But ignoring may be just as hazardous. Decentralization, security and scalability are technological risks not regulatory risks. Education is the best investment one can make and is probably a better advice than “don't get involved” when you don't understand. To the contrary, do get involved. People should be invited to be curious, to question, to invest the time needed to understand, to form their own opinion, to develop critical thinking. ‘Do not get involved’ is a similar message to ‘stay ignorant’. This is not a productive recommendation when the objective is public protection.

Education and knowledge don't happen by osmosis. It requires hard work and time. For many this investment of hard work and time is their skin in the game and everyone should be encouraged to educate themselves. In the era we live in, information is abundant, free and easily accessible to every human being with access to Internet. Do your own research. Don't trust, verify.

3.6 Double standard (2) – Accountability

As seen in 3.5 volatility is a pretty big deal for regulators because volatility is a measure of risk. Then, what if adding a small % of bitcoin in a portfolio was the right thing to do? What if because of its low correlation to traditional assets, a clients' portfolio's risk/return profile would be improved by an allocation to bitcoin?

Presenting the potential risk without also presenting potential reward draws is an incomplete picture. The picture is as incomplete if you only present returns. Both risk and return are important.

Retail investors who deal with IIROC / CSA investment advisors do not have access to risk measures. Examples of risk measures include: variance, standard deviation, maximum drawdown, peak-to-trough. None of these metrics are available to retail end investors.

If volatility is so important to securities regulators, then why no such measures are offered to end investors about their overall investment's portfolio performance?

Institutional investors have several reports and measures to demonstrate if they generated alpha (value added) and where their performance ranked versus their peers. Why is there no such statistics available to Canadian retail investors?

Let me illustrate with Bob's investments. Bob filled the risk assessment questionnaire and was categorized as a balanced (medium) risk investor. After a certain period of time, Bob might want to know: So, were my advisor's recommendations good or not? Said differently, versus all the other retail investors with a balanced risk profile in Canada, where do I stand? How far away am I from the pack? Is it excellent, fair or mediocre?

The answer does not exist because it is not calculated by the industry. Volatility (risk) is not measured⁸⁸ nor compared, nor accessible at the individual investor's account level.

Back to my initial question, what if adding a small allocation of bitcoin to the client's portfolio was the right thing to do? Where would this show? What if advisors making that allocation end up delivering a better risk-adjusted portfolio returns than their peers? How can investors verify? How can investment professionals demonstrate their investment management skills, if they have no quantitative means to compare their performance with their peers?

The double standard is that on one hand only returns are presented, but when it comes to bitcoin, only risk is put forward by securities regulators.

The chart below contains the returns of 33 different markets⁸⁹ in the decade that followed the regulated market financial crisis. Data is from March 9th 2009 to March 9th 2019.

⁸⁸ IIROC dealers may state that they look at risk metrics such as standard deviation. Those who do, use monthly data. Daily data are needed for statistical significance. The monthly data risk statistics is not shared with clients.

⁸⁹ <https://www.rcmalternatives.com/2019/03/heres-how-33-markets-performed-since-the-2009-low/> (04/17/2019)

MARKET	NOW	THEN	% CHANGE
Bitcoin	3,900	0.025	390,000.00%
Fed Funds	2.40%	0.20%	1,100.00%
Nasdaq 100	7015.69	1043.87	572.08%
RUSSELL 2000	1521.629	343.26	343.29%
S&P 500	2743.07	676.53	305.46%
German Dax	11457.84	3692.03	210.34%
MSCI World Index	2051.12	684.07	199.84%
US 2yr Yield	2.45%	0.96%	155.21%
Cotton	0.6899	0.3593	92.01%
Copper	2.894	1.630	77.60%
Live Cattle	128	81.72	56.63%
Gold	1298.17	922.78	40.68%
China Shanghai Composite	2970.24	2118.75	40.19%
Case-Shiller US Home Prices	205.35	146.52	40.15%
Crude Oil	56.12	47.07	19.23%
Silver	15.323	13.013	17.76%
Aussie Dollar	0.7045	0.6316	11.55%
Wheat	466.5	452.5	3.09%
Soybeans	840.5	860.5	-2.32%
Candian Dollar	0.7450	0.7715	-3.43%
Corn	356.25	371.50	-4.10%
British Pound	1.3012	1.3816	-5.82%
US 10yr Yield	2.62%	2.89%	-9.34%
Sugar	12.18	13.5	-9.78%
Euro Currency	1.123	1.264	-11.15%
Japanese Yen	0.8995	1.0124	-11.15%
Cocoa	2244	2592	-13.43%
Coffee	124.28	145.28	-14.45%
Lean Hogs	0.5170	0.6100	-15.25%
US 30yr Yield	3.00%	3.59%	-16.43%
Natural Gas	2.865	3.870	-25.97%
VIX	16.05	40.8	-60.66%
German 10yr Yield	0.06%	3.02%	-98.01%

Sources: Commodity markets = barcharts.com 'cash' contract, Stock indices = Yahoo Finance, Bond yields, Home prices = FRED, Bitcoin = coinbase.com

In all fairness, very few knew about bitcoin in March 2009 and it is unlikely that investment professionals could have been able to make such recommendation. Many market observers became aware of bitcoin during its most recent bull run (December 2017) and subsequent drawdown. But how many observed higher lows and higher highs in its history.

What if some investment professionals regulated by IROC and/or the CSA read bitcoin as a computing revolution (and not just a financial one)? What if they see bitcoin as a resilient computing system? What if they believe bitcoin is a worthy hedge against disruption in the business model of securities (such as AWS, Google, Facebook, Visa,) they own in the client's portfolio they manage? What if they assess bitcoin as a global hedge⁹⁰? Why would such tool not be available to them?

Past returns are certainly not an indication of future returns, but if bitcoin succeeds, now that pretty much everyone knows it exists, advisors' clients may ask why a small allocation of their portfolio was not invested in it. They may also question why crypto funds^{91 92} were available to accredited investors⁹³ and not to the mass market investors. They may question why and how inserting bitcoin in a securities format transformed it into a product available to just a few (already rich people)? If 1% of Bob's portfolio can benefit from it, why can't a 1% also be available to Alice?

Who is accountable for the risk-adjusted returns delivered to clients? Who is responsible to look at the peer-to-peer statistics? Who is responsible for the fairness of opportunities? The securities regulators, the investment dealers or the investment advisors?

⁹⁰ <https://www.cnbc.com/2019/05/13/bitcoin-emerges-as-a-global-hedge-while-stocks-tumble-in-us-china-trade-war.html> (05/13/19)

⁹¹ <https://rivemont.ca/en/rivemont-crypto-fund/> (04/25/19)

⁹² <https://3iq.ca/3iq-global-cryptoasset-fund/> (04/25/19)

⁹³ <http://accreditedcapitalcorp.com/cadosc45.php> (04/25/19)

4. The crux of the issue

4.1 Problem: Custodial exchanges & the misuse of funds

21-402 tries to cast a very wide net when it is really trying to address one fundamental challenge: audit and custody. The problematic situation recently highlighted in Canada with QuadrigaCX is not a new situation or an isolated event. In fact, there has been over USD\$1,3 billion worth of cryptocurrency stolen at exchanges since 2009⁹⁴. The problem exists but casting as wide as 21-402 is trying to may create the risk that securities regulators may step out of their jurisdiction, create unnecessary delays and costs while failing to accomplish what matters most: consumer protection.

The problematic situation primarily arises from platforms who offer both transactional and safe keeping (custodial) services. But not all exchanges or applications are custodial. Platforms offering custodial services have safekeeping responsibilities and are exposed to several risks such as: internal/external hacks and frauds, key personnel risk and critical errors.

Despite the adage, *not your keys, not your coins*, many end up leaving their crypto assets on exchange platforms. Some do it because they want to trade, while others may lack the know-how to self-custody or have other reasons to use a third party. This custodial relationship is what places the platform in a position to potentially misuse the client's funds and to run a fractional reserve system.

The crux of the issue is proving the solvency of the exchange. Do they have on-hand all the crypto they say they have and should have? They may be transforming a custodial service into a bank-like mechanism. In the traditional banking system, all depositors cannot withdraw their cash at once because their money has been lent by the bank. This is partially how money is created and permits borrowers to access lending products such as mortgages and personal loans. When they are not outright frauds, custodial exchanges operating a bank-like fractional reserve system, should disclose their solvency ratio and unless they have the in-house expertise, may run into several problems such as regulatory, cash management, treasury management. This is a consumer's right protection issue. Proving reserves and solvency will demonstrate there is no misuse of funds.

Similar challenge (proof-of-reserves) can also occur in the gold market. Could the gold audit for investment trusts, *technically* be cheated? Yes. The trust is on the audit process to demonstrate that there is, *at all times*, sufficient gold bullions to back funds held in the investment structure.

Similar challenge (*proof-of-reserve*) can also occur with traditional financial institutions. Could a bank misuse client cash? Yes. This 2016 example⁹⁵ from Merrill Lynch shows it happened.

This is not a problem which is unique to the crypto-asset industry. However, bitcoin could offer a level of transparency and real-time auditability that no other assets have been able to provide up to now. Bitcoin reserves can be verified at no cost, with little effort and with mathematical precision using public key cryptography⁹⁶.

⁹⁴ <https://www.aon.com/unitedkingdom/insights/keeping-cryptocurrency-secure.jsp> (05/14/19)

⁹⁵ <https://www.sec.gov/news/pressrelease/2016-128.html> (04/26/19)

⁹⁶ To avoid any confusion, this cryptographic proof is not a de facto feature in all crypto-assets (ex: stablecoins).

4.2 Solution: Vires in Numeris

As explained in this research piece from Blockstream⁹⁷, it is technically possible to standardize a solution to bitcoin's proof-of-reserves challenge while offering a more uniform way to understand and compare various exchanges. There is still work to be done, but this is an example of a solution that solves for both provability of reserves without revealing themselves.

Another great article by Nic Carter, a partner at Castle Island Ventures⁹⁸ explains this custodial challenge and how it can be tackled without compromising privacy.

It must be understood, that this is not a regulatory problem; this is a technological problem and Bitcoin has the means to offer a level of audit proofs not possible in traditional markets. This is an opportunity for the bitcoin industry to step up, develop solutions and purge out bad actors by establishing high standards. This is an opportunity for the crypto-currency industry to self-regulate itself, to educate clients and to set rigorous standards. Unwillingness to provide proof-of-reserves by custodial platforms would be seen as suspicious and business should migrate towards strongest propositions.

This is also an opportunity for securities regulators to influence the development of the industry in Canada without stepping outside of their jurisdiction, without stifling innovation all while allowing a home-grown talent pool to flourish.

There are investment funds who want to offer bitcoin exposure in mass-market investment format (such as an ETF). A regulated investment structure investing in physical bitcoin, just like a physical gold investment would occur, is a way for less tech savvy investors and for finance professionals to participate. Securities regulators have the opportunity to influence the exchange platforms and crypto custodians who target non-securities crypto-assets investment funds. This is where securities regulators can be the most effective and achieve the desired outcome of protecting the end investors without having to attempt at regulating all platforms and all crypto-assets all at once.

Securities regulators could take into account the questions gold and real estate have already trailed blazed and provide the investment funds with a list of outcome requirements that are missing for bitcoin. Regulators could express what their objectives are rather than forcing instructions on how to achieve it. This will incentivize platforms and custodian to develop solutions that meet the regulatory desired outcome, should they wish to service investment funds.

As covered in section 2.2, there are non-traditional assets like gold and real estate who have answered several preoccupations of the securities regulators. This leaves much fewer open-ended questions than presented in 21-402. The focus should revolve around custody and be concerned with; wallet architecture, key security, physical protection, cybersecurity program and operational controls.

Lastly, it is important that securities regulators be mindful of not creating unintended consequences with the framework they propose and outcome requirements they may express.

⁹⁷ <https://blockstream.com/2019/02/04/en-standardizing-bitcoin-proof-of-reserves/> (05/05/19)

⁹⁸ https://medium.com/@nic_carter/how-to-scale-bitcoin-without-changing-a-thing-bc4750dd16c7 (05/05/19)

4.3 Unintended consequences

Contrary to gold or cash, bitcoin is much more portable as illustrated in the picture below. Theft prevention has a very different meaning and it is important that well-intended regulators do not introduce risks and vulnerabilities in their requirements when there is a cross-over with this industry.



Source Reddit

Creating vulnerabilities

Privacy is a major concern as revealing too much information publicly weakens the safety of the exchange and of the custodian. Imposing the disclosure of certain elements pertaining to the preservation of the private keys or security process can be the actual security breach. Funds, custodial exchanges and custodians are honey pots. Not only is it undesirable to publicly disclose the size of the bounty, it is easy to understand that employees with access to the map of the treasure's location are subject to being compromised.

This transparency must be achieved in a way that does not breach privacy which would lead to identifying the pot-of-bitcoin size. Understanding the need for mixing coins will be important. For example, one doesn't need to know how much gold Kitco custodies, it just needs to know that they have the amount they claim to have (zero knowledge proof). From a game theory perspective, crime and specie insurance providers are best positioned to assess security procedures of the assets they insure. They have vested interest in not creating vulnerabilities in the risks they insure. The market for this type of insurance is developing and so is institutional grade custody solutions

Privacy is also a major concern for individual clients. Money Service Businesses with AML/KYC requirements (such as Kitco or crypto-exchanges) have the dual responsibility to both comply with regulatory requirement and preserving with the highest possible standards the identification of the clients. They are also the custodian of personal and sensitive information. This ID custody is a regulatory requirement. How can one ensure that this regulatory requirement doesn't become another honey pot for bad actors?

Even though this is not a 2019 problem, and unlikely a securities regulator's consideration, we nevertheless may, in the future, face a disadvantageous situation for humans versus machines. A decentralized digitally native payment system can service the economic relationship needs of non-biological users like software and connected devices. What if in time, my connected-refrigerator needs to transact directly with a retailer to replenish supplies? What if my personal artificial intelligence assistant needs to buy more RAM with crypto. Point is some forward-looking situations will arise outside the scope of securities regulation. It is important to leave room for innovation to breathe as we don't know the future holds.

Conclusion

Regulators in general, not just securities regulators, are placed in a difficult situation when confronted to change. This is best illustrated by a quote from Elon Musk's biography⁹⁹:

"There is a fundamental problem with regulators. If a regulator agrees to change a rule and something bad happens, they could easily lose their career. Whereas if they change a rule and something good happens, they don't get a reward. So, it's very asymmetric. It's then very easy to understand why regulators resist changing the rules. It's because there is a big punishment on one side and no reward on the other. How would any rational person behave in such a scenario?"

Crypto-assets are mind-bending and they force various regulatory agencies to think differently. Traditionally, financial regulation was split in distinct buckets such as commodities, securities and money. Crypto-assets are blurring these lines. What lies ahead of us is the potential for global, open and interoperable exchange of value just like data. Amongst other things, this has an impact on notions of ownership, storage and custody that were traditionally serviced by securities dealers. This is a solid paradigm shift.

Canadian securities regulators are not the only one struggling with this challenge. However, individuals like SEC Commissioner Hester M. Peirce are expressing concerns shared by the industry participants. These quotes are taken from her most recent allocution (four days ago)¹⁰⁰:

I worried that, by contrast, a regulatory sandbox, something the SEC had been urged to establish, would tempt the Commission to "grab hold of the shovels and buckets" and meddle in the building of sandcastles. It is not the regulator's job to get involved in the creative process, and, in any case, creativity is not the regulator's strong suit.

(...)

It is not the SEC's overzealous action that has stifled the crypto industry, but its unwillingness to take meaningful action at all.

Forbearance on the part of a regulator is often appropriate, especially in the interest of allowing market forces, rather than knee-jerk regulatory impulses, to shape a developing industry. The problem is that the securities laws do not cease to operate as a new industry develops. Consequently, individuals and companies in the industry must comply with our securities laws or risk becoming the subject of an enforcement action. It is therefore our duty as a regulator to provide the public with clear guidance as to how people can comply with our law. We have not yet fulfilled this duty.

⁹⁹ Elon Musk by Ashlee Vance (page 242)

¹⁰⁰ <https://www.sec.gov/news/speech/peirce-how-we-howey-050919> (05/13/19)

I invite Canadian securities regulators to clearly state, in plain English, what is a crypto-assets security. Then, businesses, entrepreneurs, investors and clients will know if they are concerned or not with 21-402. Failure to do so, may create costs, delays and move projects and businesses who want to do things right in a jurisdiction that offers greater clarity.

Some platforms and service providers may want to service only non-securities crypto like bitcoin and their endeavors may be stalled by lack of clarity. It would be quite unfair to them to be stalled by a securities regulator, when they are not dealing in securities.

While securities regulators are trying to regulate very broadly with 21-402, they may miss the low hanging fruit and the opportunity to directly influence the development of the industry by allowing the inclusion of bitcoin in a regulated securities format. They risk imposing regulatory standards that are disproportionate in comparison to previously approved structured containing different, but comparable risks.

I also invite Canadian securities regulators to not paint the entire industry with the same brush and to be mindful of the stigmatization they can create on legitimate entrepreneurs who are trying to build a business to service Canadians. Good actors in this ecosystem have a vested interest in protecting the public against charlatans.

Bitcoin is not a security, therefore not a securities regulator's matter.

Thank you

Elisabeth Préfontaine
MBA, CFA, CAIA
Founder

www.octonomics.com

<https://twitter.com/eprefon>

<https://www.linkedin.com/in/elisabethprefontaine/>



OCTONOMICS



Hello IIROC and CSA team,

My name is Vakeesan Mahalingam, CFA.

I would like to provide some comments/feedback on the 'Joint CSA/IIROC Consultation Paper 21-402 Proposed Framework for CryptoAsset Trading Platforms', I have worked formerly as a short term rates trader at one of the largest independent asset managers in Canada for 5+ years. Most recently, I've spent about 6 months as Portfolio Manager, Head Trader, and Strategist of Kintaro Capital (MFSA Licensed and Regulated), managing a hybrid Equity and Crypto Fund (Digital Innovation Fund).

To your proposed questions:

Are there factors in addition to those noted above that we should consider?

- You need to consider the insurance policies of platforms. Centralized Exchanges that hold and control assets over XX million, should have an insurance policy against theft to make sure clients and exchange users are made whole, in case of exchange hacks or other misuse of user funds.
- Delivery of cryptoassets to cold and hot wallets from and into exchanges occur within seconds, if not minutes, depending on the cryptoasset. The user can decide to leave assets on exchange, thus transferring ownership to the platform, or can choose to withdraw funds from the platform to their own hot or cold wallet, where delivery of assets is made to one's personal control and wallet.
- Crypto custody has been one of the large looming question for mass institutional adoption. Those seeking to develop custody solutions (Xapo, Fidelity, etc.) need to be insured against theft or loss of assets. The main concern is around how and where will custody solutions that ARE developed manage or control the crypto assets. The main solutions seems to be twofold; that crypto custody would need to involve a combination of cold wallets (offline crypto hardware wallets) that require multi-signature and are held in a secure location like a bank safe. Then some form of hot wallets (online/web based wallets). What I mean by this is that to unlock the assets held on cold storage, it would involve multiple parties with a majority signature required to unlock crypto assets (e.g let's say there is 5 member board, you would need the keys from 3/5 members to unlock assets). This is a where a bulk, 60-70%, of assets should be held. The remaining should be left on exchange in pure form for liquidity needs.
- A formal Crypto Classification System (CCS) needs to be developed and distributed to the financial industry and other economic participants. This will need to be periodically updated every 6 months as the space is changing at a rapid pace.
- Crypto platforms that have their own token (Huobi, Binance, etc.) are more susceptible to misconduct. The reason being their own exchange-based token value is solely based on the trading activity that comes from the platform in question. This incentivizes the platform to increase platform based trading activity at all costs, and serves the grounds for exchange

abuse, wash trades, fake trading volume, and other trade related misconduct as exchange tokens are also generated in finite supply.

Are there challenges associated with a Platform being structured so as to make actual delivery of crypto assets to a participant's wallet? What are the benefits to participants, if any, of Platforms holding or storing crypto assets on their behalf?

- There are no challenges to moving assets to a different crypto wallet. It usually takes between 10-20 confirmation on the blockchain, but after that, assets are transferred almost immediately from crypto exchange to personal private wallet.
- The benefit for participants is the timing and convenience. For example, imagine you had your money sitting in your RBC or TD bank account. You hear some news (in crypto space new comes quick and investors react quick) and you want to take advantage of a trading opportunity or you want to reposition yourself before a major event occurs, like traditional equity trading platforms, there is a delay in transfer time from a bank to a trading platform like Questrade, that will make it difficult to react on instant news or rumours. The same applies to the crypto world, except the worst case scenario transfer time to move money from a personal wallet to exchange is seconds to minutes. Having money on a crypto exchange already is thought of as having your money in cash on your Questrade or Interactive Broker account. Most reputable crypto exchanges backup customer funding

What factors should be considered in determining a fair price for crypto assets?

Are there reliable pricing sources that could be used by Platforms to determine a fair price, and for regulators to assess whether Platforms have complied with fair pricing requirements? What factors should be used to determine whether a pricing source is reliable?

- Crypto 'Fair Price' is different than a reliable exchange based compilation of current market price, so it depends on what you are looking for exactly
- For 'Fair Price; or intrinsic value for a crypto asset is a based on a lot of things that go into crypto valuation frameworks, none of which, has won as the global standard for valuation. There are a multitude of different valuation frameworks that all provide insight into the intrinsic value of cryptoassets. NVT/NVTS, metcalfe's law are two of the prominent that stand out in the community .For metcalfes laws, there are over 50 variations using different formulas and functions. Different valuation methods apply to different cryptoassets based on their use case, functionality, network activity, consumer demand. A reliable price source commonly used is a coinmarketcap, or a combination of price aggregation from various top exchanges and coinmarketcap as a baseline comparison.
- To determine whether a price source is reliable the most important aspect to consider is exchange trading volume and token trading volume on specific exchanges. Spikes in trading volume and the tons of research already done to try and isolate fake trading activity is

critical to the correct pricing of assets. Companies like **Chainalysis** should be relied on in these instances to provide good information as they are already working with various law enforcement and anti-criminal organizations in the U.S. to help fight fraudulent activity.

Is there disclosure specific to trades between a Platform and its participants that Platforms should make to their participants?

- Platforms should make it obvious to which tokens are involved in an IEO (Initial Exchange Offering). These are tokens that are launching publicly for the first time on a specific exchange (Think of a firm conducting an IPO but restricted only to the NASDAQ for example)
- Platforms should make it clear to users whether storage of exchange assets is held in custody, a cold wallet, or hot wallet and what provisions are in place to protect users against theft or loss of exchange held cryptoassets as a result of a hack or cyberattack.

What type of insurance coverage (e.g. theft, hot-wallet, cold-wallet) should a Platform be required to obtain? Please explain.

Are there specific difficulties with obtaining insurance coverage? Please explain.

Are there alternative measures that address investor protection that could be considered equivalent to insurance coverage?

- A centralized crypto exchange platform should be obligated to insure against a loss of assets. That means they should have protection against at least 90% of assets held on exchange, based on a median or average over a period of time. This includes coverage against theft, cyber attack, hot and cold wallet theft and hack, and any other situation where the exchange is taking control of the cryptoassets (these are situations where the user has left their assets on the exchange). Any cryptoasset transferred off an exchange to a personal or user controlled wallet, is the responsibility of the user.
- Insurance coverage is very hard to obtain as there are not many prominent or dominant crypto insurers in the game. Most insurers are non-reputable and new in the space so the default rate of the insurer is hard to determine as well.
- Alternative measures usually involve the centralized exchange taking responsibility for any attack that results in the loss of users assets. A recent example is the Binance hack, where CZ, the CEO, makes all users who lost assets 'whole' from a fund he has created just for this purpose of unforeseen malicious attacks. In essence, a model for platforms would be that a portion of profits be contributed to a 'Emergency Fund' or Loss Fund, where assets accrue and are used in unforeseen circumstances to make users whole in the case of an attack or company-led loss of funds.

What, if any, significant differences in risks exist between the traditional model of clearing and settlement and the decentralized model? Please explain how these different risks may be mitigated.

- The biggest significant difference is that the traditional securities model of clearing involves a clearinghouse, settlement agencies and teams, and typically takes 1-3 days depending on the asset class. The decentralized crypto exchange model involves no intermediaries, no clearinghouse, no settlement delays. An instant transfer of funds peer-to-peer that is fully trustless and ensures 100% accuracy and compliance through the use of technology, in this case, what we call atomic swaps in the crypto world
- The biggest issue with decentralized exchanges is liquidity. Most decentralized exchanges actually see centralizing liquidity by creating pools as a convenient solution, but that in turn means that these end up as hybrid exchanges and not actual decentralized exchanges. Until decentralized exchanges (DEX) can solve the liquidity issue that each has on its own exchange, if it were to receive a massive influx of new users, DEX do not remain a prominent trading platform for the time being. Centralized crypto exchanges currently, can barely handle a huge influx of trading volume or an addition of 10-100K new users in a day or week, so decentralized exchanges are that much smaller in the game. Decentralized exchanges face a huge liquidity risk that currently can only be mitigated by pooling assets or relying on other exchange platforms for hidden liquidity.

I've also attached a crypto classification system I've started on creating a few months ago that may be of use.

If you would like further feedback or consulting, I'd be happy to work with the CSA, IIROC, or the OSC on such matters, having been a subject matter expert for quite a while.

Thank you!

INCLUDES COMMENT LETTERS

CBA Submission on CSA/IIROC Consultation Paper 21-402 *Proposed Framework for Crypto-Asset Trading Platforms*

05/15/2019



Submission to the Canadian
Securities Administrators and
Investment Industry Regulatory
Organization of Canada

Delivered via email

The Secretary
Ontario Securities Commission
20 Queen Street West
22nd Floor
comments@osc.gov.on.ca

Me Anne-Marie Beaudoin
Corporate Secretary Autorité des marchés financiers
800, square Victoria, 22e étage
C.P. 246, tour de la Bourse
Montréal (Québec) H4Z 1G3
Consultation-en-cours@lautorite.qc.ca

IIROC
Victoria Pinnington Senior Vice President, Market Regulation
Investment Industry Regulatory Organization of Canada
Suite 2000, 121 King Street West
Toronto, Ontario M5H 3T9
vpinnington@iiroc.ca

Introduction

The Canadian Bankers Association (**CBA**)¹ appreciates the opportunity to comment on the Canadian Securities Administrators' (CSA) and the Investment Industry Regulatory Organization of Canada (IIROC) published consultation paper (**the Consultation Paper**) *21-402 on the Proposed Framework for Crypto-Asset Trading Platforms*.

Banks are strong proponents of innovation and competition in the financial sector as innovation often leads to better products and services to customers. In the case of a framework for crypto asset trading platforms (**Platforms**), the CBA is supportive of greater regulatory clarity with respect to this market space that both contributes to the integrity of the financial services ecosystem and protects investors while fostering innovation. As the Consultation Paper recognizes, crypto assets may demonstrate characteristics of a currency, security or commodity, and these characteristics can change depending on the context in which a crypto asset is used. In addition, the number of Platforms that facilitate buying or trading these assets continues to grow with minimal or no regulatory oversight across the globe. Understanding that the emergence of new Platforms and the exchange of crypto assets is a relatively nascent market, providing regulatory clarity, while continuing to support innovation, would be beneficial for all industry stakeholders.

¹ The CBA is the voice of more than 60 domestic and foreign banks that help drive Canada's economic growth and prosperity. The CBA advocates for public policies that contribute to a sound, thriving banking system to ensure Canadians can succeed in their financial goals. www.cba.ca.

The need for regulatory clarity is clear, and we commend the CSA and IIROC for launching this consultation. However, determining the appropriate level and scope of regulation will require a deep understanding of a complex and rapidly-evolving industry. Therefore, we strongly recommend that CSA and IIROC continue to collaborate with other industry stakeholders in developing a regulatory framework for crypto assets, with the objective of sharing technical expertise.

We have chosen to focus our comments on certain important issues raised by the Consultation Paper with respect to regulatory clarity around Platforms, ensuring greater market integrity and facilitating innovation, rather than addressing each question in isolation. As such, our comments will focus on three underlying principles that should support the regulatory framework for Platforms, namely ensuring that:

- all participants in the financial services ecosystem are subject to effective regulation and meaningful oversight necessary for safety and soundness, investor protection, and the facilitation of innovation;
- the regulatory framework mitigates the potential for negative unintended consequences; and
- a regulatory framework that is consistent with the treatment of other financial products and market participants, and is aligned to developments globally

As the Platforms continue to evolve and mature, we would appreciate the opportunity going forward to continue the dialogue on the important issues raised by the Consultation Paper. We have set out below more detailed commentary on the principles noted above.

Ensure Stability, Investor Protection and Ongoing Innovation

Flexible and principles-based approach to regulatory clarity and oversight

A principles-based approach strikes a balance between the goals of effective oversight and fostering of innovation. As the Consultation Paper notes, crypto assets are not easily defined, are not necessarily amenable to specific categorization, and may change in nature depending on the context in which they are used. In addition, technology in the crypto asset sector continues to develop and change rapidly. Given these factors, we recommend a regulatory framework that is flexible and technologically neutral, that mirrors where appropriate existing regulatory frameworks, and that balances potential risks with the development of the crypto asset sector.

Further, we believe that this approach would be effective in minimizing the potential for avoidance schemes (e.g. the use of techniques to avoid the application of the regulatory framework to a particular technological representation of a crypto asset). We also believe it would avoid overly prescriptive requirements that may quickly become obsolete.

Investor Protection

As the Consultation Paper highlights “global incidents point to crypto assets having heightened risks related to loss and theft compared to other assets” with evidence of these risks seen in Canada as well. As such, we believe that one of the key objectives in establishing a new framework for Platforms is that the framework should facilitate the evolution of the Platforms in a way that remains safe and reliable for all parties. Given the wide variety of crypto assets characteristics, and their associated risks, there is an increased level of uncertainty for investors wishing to participate in these Platforms, particularly in relation to issues such as investor protection in the event of insolvency of the crypto asset-issuing firm. Investors have come to expect a level of comfort when dealing with investment firms, in particular knowing that the investor’s funds are safe in the event of an insolvency, as a result of the coverage provided by programs and institutions like the Canadian Investor Protection Fund (CIPF). We encourage regulators to clarify whether membership in self-regulatory organizations extends the protections offered to investors, via programs such as the CIPF, to crypto asset investments. Further, enhancing transparency of the Platforms for all participants will be essential to investor protection, as will developing robust custody requirements for and financial literacy around crypto assets generally. In each case, regulators will have important roles to play with respect to accomplishing these objectives.

Comparable Regulations to Promote Consistency and a Global Outlook

Consistency

A consistent set of rules and regulations helps to foster innovation and competition in financial services and is essential to avoiding market fragmentation and facilitating a level playing field among market participants. Platform operators that are performing functions analogous to the functions performed by entities in the traditional capital markets should be subject to the same regulations. Where a crypto asset falls within an existing regulated asset-class (i.e. a currency, commodity, equity, etc...), the classification of such crypto asset should be clearly defined and consistently applied. Alternatively, where regulation does not exist in respect of a certain class of crypto asset, regulators should consider creating a working group to collaborate with industry stakeholders to provide clear guidance on which crypto assets will become subject to regulation, including which of those are subject to oversight by securities regulators.

Where a new approach is necessary, regulators should begin by working with existing market infrastructure participants to determine how current capabilities and regulatory controls can be adjusted to address certain crypto assets. This would ensure that new and existing market participants would be subject to the same expectations and requirements and would also avoid the inconsistency that would result from providing case-by-case exemptions. Most importantly, it would provide clarity to the market, increasing the likelihood of compliance and meaningful regulatory oversight.

In addition, we believe that the obligations and standards outlined by IIROC, such as anti-money laundering (AML) and know your client requirements, should equally apply to all participants. The application of such requirements would work towards eliminating gaps that could be exploited and ensure consistency for the financial sector. Overall, regulation should strike the appropriate balance between promoting innovation and ensuring financial stability and investor protection without creating inconsistencies amongst existing infrastructure and mitigating the potential for negative unintended consequences.

Global Outlook

As the crypto asset market continues to mature, with different platforms in different jurisdictions becoming accessible to investors, we suggest a global outlook would be appropriate. We caution against regulation that is not aligned that in comparable jurisdictions, given that the nature of crypto assets allows individuals to transfer those assets outside of Canada at very low cost and largely without restrictions. Without domestic access, Canadian investors may increase their use of foreign-operated Platforms. Even if those Platforms are regulated and overseen by foreign authorities, those authorities may not share the objectives of the Canadian securities regulators. That could then result in heightened risks to Canadians transacting on those Platforms.

Some jurisdictions are taking steps to regulate Platforms. For example, since 2017 the Financial Services Authority in Japan has mandated that all crypto exchanges in the country obtain a license and, currently, there are 19 registered crypto exchanges in Japan.² As another example, the New York Department of Financial Services has required licensing of virtual currency business activities since 2013.³ As the Consultation Paper notes, a regulatory framework is welcomed by Platforms and there may be benefits to reviewing approaches taken by other jurisdictions such as New York or Japan, including potentially consulting with regulators in those jurisdictions to highlight best practices and explore streamlined approaches to regulation.

Additional Commentary

Set out below is our commentary responding to additional considerations raised in the Consultation Paper.

Pricing Considerations

Pricing issues relating to crypto assets can pose challenges. For example, recent evidence supplied to the U.S. Securities and Exchange Commission indicated that many exchanges potentially contain

² Japan to require crypto exchanges to bolster internal oversight: source. <https://www.reuters.com/article/us-japan-cryptocurrency-idUSKCN1RS0YO>

³ New York State Department of Financial Services. https://www.dfs.ny.gov/apps_and_licensing/virtual_currency_businesses

fraudulent or misleading trading activity.⁴ An approach that simply aggregates pricing across all exchanges may not provide the diversification benefits that such an approach may typically be expected to provide.

To address this concern, regulators may want to consider creating a working group that could collaborate with industry stakeholders to identify “reference” platforms or exchanges through which reliable data could be obtained for the purposes determining fair pricing. As part of this approach, the working group could assess the possible development of standards against which prospective platforms or exchanges would be assessed before including pricing data as reference points from those platforms or exchanges.

Risks Associated with Clearing and Settlement Models

We believe that care will need to be taken with respect to the treatment of clearing and settlement functions in relation to crypto assets. Clearing houses and agents are critical components of Canada’s resilient capital market infrastructure. These intermediaries have developed over time to reduce settlement and counterparty risks in transactions. One technique used by these intermediaries is Delivery Versus Payment (DVP), which effectively prohibits the same entity from performing both clearing and custody functions.

Concerns could arise if the regulatory framework were to allow Platforms to perform both clearing and custody functions (i.e. DVP would be impossible to achieve). If Platforms were to be permitted to engage in both activities, the result could be either the introduction of counterparty risk with associated risk-mitigating measures (e.g. the imposition of a requirement for participants to pre-fund trading accounts on the Platform with fiat currency prior to completing a trade on the Platform) or credit risk (i.e. by permitting participants to trade on margin, with settlement after).

To address these potential concerns, regulators may want to consider forming a working group to investigate creating market infrastructure, such as a clearing house, to facilitate DVP settlement of certain crypto assets, such as bitcoin, using technological innovations that include but are not limited to multi-signature wallets. Creating this infrastructure would enable agents of investors, acting as brokers and custodians (other than those controlled by the Platform), to participate in transactions on behalf of investors. This type of approach would increase innovation, competition, and growth in the overall marketplace while reducing the potential for systemic risk arising in the ecosystem.

Conclusion

Canada’s financial services sector, including the crypto asset market, is undergoing significant transformation. In order to protect and enhance the integrity of Canada’s financial markets, it is critical to establish an effective regulatory framework that balances the objective of the safety and soundness of the

⁴ <https://www.investor.gov/additional-resources/news-alerts/investor-alerts/investor-alert-watch-out-fraudulent-digital-asset>

system with the objective of fostering innovation and growth through a regulatory model that adapts quickly to changes in the market. This will lead to more robust and competitive system and build on the strengths of existing framework, while maintaining investor protection. We appreciate having the opportunity to contribute to this consultation process and look forward to continuing to engage on this issue with the Canadian Securities Administrators and the Investment Industry Regulatory Organization of Canada.

[IIROC Consultation Paper](#)

1. Are there factors in addition to those noted in Part 2 that we should consider?
 1. 1. Whether the platforms are structured for short selling of crypto assets,
 1. 2. Whether a platform play roles as a clearinghouse or just a middleman between the token buyer and seller,
 1. 3. How the platforms are structured to handle the liquidity issues,
 1. 4. How centralized and decentralized exchanges of the cryptocurrencies work and interact,
 1. 5. How off-chain order book and on-chain settlements connect with the platforms,
 1. 6. Whether all platforms are structured to be functioned as a broker, custodian and trading venue at the same time.
 1. 7. Does the concept oof the sec lending exist with crypto
 1. 8. Should it
 1. 9. Can we have a viable shorting capability without it
2. What best practices exist for Platforms to mitigate the risks outlined in Part 3? Are there any other significant risks which we have not identified?
 2. 1. The best practices are to set up appropriate regulations and force internal control policies and procedures to mitigate the risks outlined.
 2. 2. Significant risks that have not identified and clearly stated in part 3 include:
 - a. There are no rules to detect and monitor fraud and AML activities within and across platforms/exchanges.
 - b. It is not clear whether initial coin offering (“ICOs”) should be considered securities subject to the same rules and regulations as equity market offerings.
 2. 3. Regulators should immediately conduct on-site field reviews of existing market participants (exchanges, custodians) and bring in third parties.
 - a. These third parties would include accounting/auditing firms to provide guidance leading to the equilavent of GAAP but for crypto. The lawyers representing these market participants would learn from the process thereby allowing them to advise their existing client (who was just reviewed) as well as others. The deficiency letters for each particular visit can be aggregated. The accumulation of findings will lead to a list of problems.
 - b. In collaboration with those auditors and lawyers who were part of this discovery process, a series of solutions could be formulated. Take this list into another CSA/IIROC public dissemination and get feedback and you are then closer to a generally accepted set of policies and procedures. The regulators do with existing crypto custodians/exchanges like they do with those in the existing securities industry.
3. Are there any global approaches to regulating Platforms that are appropriate to be considered in Canada?

3. 1. There is a strong recommendation globally that apply the Anti-Money Laundry and Anti-Terrorism Financing or Count-Terrorism Financing (AML/ATF or CTF) regulation framework to the cryptocurrency platforms.
 3. 2. [ASIFMA Best Practices for Digital Asset Exchanges](#) may be considered as a reference when developing appropriate regulations in Canada.
 3. 3. I would strongly suggest that CSA/IIROC do not investigate or incorporate any efforts outside of Canada, at least not for now.
 3. 4. Go through the process mentioned above for section 2 as a start and once you have the list of problems, THEN explore how others outside Canada are looking to solve these. Suggesting here to define the problem first before thinking about solutions. This direct regulatory review will be healthy for all (regulators, participants, investors) to learn and possibly identify and remove bad actors.
4. What standards should a Platform adopt to mitigate the risks related to safeguarding investors' assets? Please explain and provide examples both for Platforms that have their own custody systems and for Platforms that use third-party custodians to safeguard their participants' assets.
4. 1. [The U.S. National Institute of Standards and Technology \('NIST'\) Cybersecurity Framework](#) could be adopted.
 4. 2. Certain internal control procedures should be established to safekeeping, record, monitor, report status of the digital assets and fiat currencies and associated transactions.
 4. 3. For platforms that use third-party custodians, a reconciliation process should be implemented to confirm its internal accounts and those of any third-party custody assets.
5. Other than the issuance of Type I and Type II SOC 2 Reports, are there alternative ways in which auditors or other parties can provide assurance to regulators that a Platform has controls in place to ensure that investors' crypto-assets exist and are appropriately segregated and protected and that transactions with respect to those assets are verifiable?
5. 1. Auditors should also consider Type I and II SOC 3 reports. In addition, testing and monitoring results on the internal controls performed by the first and second lines of defence would provide alternative support on the design (Type I) and operating (Type II) effectiveness of the internal controls.
6. Are there challenges associated with a Platform being structured so as to make actual delivery of crypto assets to a participant's wallet? What are the benefits to participants, if any, of the Platforms holding or storing crypto assets on their behalf?
6. 1. Actual or physical delivery of crypto assets to a participant's wallet for each transaction would result in significant challenges of operational processes and cost with a platform as well as the risk of losing passwords of private wallets.
 6. 2. The benefits to participants of the platforms holding or storing crypto assets like custodians in the traditional financial system would minimize the risk of individual participants losing their funds to bad actors and transaction cost and operational efficiency with the platforms. But there are other concerns on the security measures needed by the platforms or third-party custodians to keep the funds safe.

7. What factors should be considered in determining a fair price for crypto assets?

The following factors would be considered in determining the fair value of a crypto asset:

- Supply and demand
- Mining cost/difficulty
- Crypto unit reward per block
- Loss factor (estimated volume of lost crypto asset units due to private keys loss)

8. Are there reliable pricing sources that could be used by Platforms to determine a fair price, and for regulators to assess whether Platforms have complied with fair pricing requirements? What factors should be used to determine whether a pricing source is reliable?

CoinMarketCap API is a commonly used source that provides prices, volume and market capitalization of various cryptocurrencies.

9. Is it appropriate for Platforms to set rules and monitor trading activities on their own marketplace? If so, under which circumstances should this be permitted?

9. 1. Given the nature of the cryptocurrency platforms, platforms should set rules, policies, procedure, and risk appetite/thresholds/limits to regularly monitor trading activities on their own marketplaces and perform the day-to-day risk management.
9. 2. The Platforms should further investigate any suspicious transactions, price spikes, non-compliance with the Exchange's legal and regulatory obligations, alerts of frauds, etc.

10. Which market integrity requirements should apply to trading on Platforms? Please provide specific examples.

The following market integrity requirements would be considered to be applied to crypto asset trading on Platforms.

10. 1. [Universal Market Integrity Rules](#) ("UMIR") by IIROC, including
 - a. Short selling
 - b. Frontrunning
 - c. Manipulative and deceptive activities
10. 2. Systems and business continuity planning
10. 3. Effective monitoring and supervision
10. 4. Cybersecurity

11. Are there best practices or effective surveillance tools for conducting crypto asset market surveillance? Specifically, are there any skills, tools or special regulatory powers needed to effectively conduct surveillance of crypto asset trading?

There are a number of markets surveillance vendors that provide solutions for conducting crypto asset market surveillance.

12. Are there other risks specific to trading of crypto assets that require different forms of surveillance than those used for marketplaces trading traditional securities?

ICOs may require different forms of surveillance.

13. Under which circumstances should an exemption from the requirement to provide an ISR by the Platform be appropriate? What services should be included/excluded from the scope of the ISR? Please explain.

CSA has recently proposed amendments to National Instrument NI 21-101 – Marketplace Operations. The amendments address cyber resilience controls, expand obligation to report material “security incidents” to regulators, mandatory annual security vulnerability testing, annual independent system review (ISR) by “qualified external auditor”.

The following circumstances could be granted temporary exemptions from an annual ISR requirement:

- Regular and independent self-assessment of internal controls (from both design and operating effectiveness of the controls) conducted by platforms
- Comprehensive monitoring reports provided by platforms and no significant issues identified
- Exposure is limited

The scope of ISR should include

- Design and operating effectiveness of various controls over the platform;
- Performance evaluation including the future capacity requirements to handle changing market conditions
- Robustness of business continuity planning and disaster recovery planning
- Effectiveness of incident reporting/escalation, notification, follow-up actions, and remediation

The following services may be excluded from the scope of ISR for a platform.

- Third-party service providers or system vendors

14. Is there disclosure specific to trades between a Platform and its participants that Platforms should make to their participants?

- Trade incidents and system failures

15. Are there particular conflicts of interest that Platforms may not be able to manage appropriately given current business models? If so, how can business models be changed to manage such conflicts appropriately?

16. What type of insurance coverage (e.g. theft, hot-wallet, cold-wallet) should a Platform be required to obtain? Please explain.

The types of insurance coverage would include

- Cyber (hacks) & Privacy Insurance:
- Insurance for loss or theft of private keys (old and hot wallets):
- Errors & Omissions (“E&O”) Insurance: Having E&O coverage helps the Platforms avoid substantial claims of inadequate work, negligent actions, or defective products/services;

- Directors & Officers (“D&O”) Insurance: It is considered as a crucial form of protection for all businesses including crypto exchanges, before investors and board members risk their professional assets.
- Corporate crime insurance: It protects the platforms from losses that are a direct result of an employee or third-party dishonesty.

17. Are there specific difficulties with obtaining insurance coverage? Please explain.

The following factors are examples of specific difficulties in obtaining insurance coverage:

- Lack of historical and actuarial data in crypto markets to determine appropriate insurance premiums
- No comprehensive risk management framework for the crypto markets to provide principles in identification, measurement, mitigation/control, and reporting of the underlying risks in the crypto markets
- Insufficient insurers, supply and expertise in the market to meet the demand for insurance coverage and unique products
- Lack of proper underwriting processes for this unique market
- Lack of regulations and guidelines

18. Are there alternative measures that address investor protection that could be considered that are equivalent to insurance coverage?

Develop and implement robust internal governance and controls over the information technology and cybersecurity, trading supervision and surveillance, business continuity plan, disaster recovery plans could be considered as alternatives to insurance and reduce risks and investor protection.

19. Are there other models of clearing and settling crypto assets that are traded on Platforms? What risks are introduced as a result of these models?

20. What, if any, significant differences in risks exist between the traditional model of clearing and settlement and the decentralized model? Please explain how these different risks could be mitigated.

21. What other risks could be associated with clearing and settlement models that are not identified here?

Except for operational, custody, liquidity, investment and credit risks identified here, clearing and settlement models also exposure to reputational and regulatory risks.

22. What regulatory requirements (summarized at Appendices B, C, and D), both at the CSA and IIROC level, should apply to Platforms or should be modified for Platforms? Please provide specific examples and the rationale.

The following requirements may need to be modified for Platform

- Appendix C #4 – Financial condition and requirement capital: It is subject to a modification of the methods for regulatory capital calculation, including the mapping of asset classes by crypto assets and risk weights.

INCLUDES COMMENT LETTERS

Additional Questions/Comments:



Deanna Dobrowsky
Vice President, Regulatory
TMX Group
100 Adelaide Street West, Suite 300
Toronto, Ontario M5H 1S3
T (416) 365-8130
deanna.dobrowsky@tmx.com

May 16, 2019

VIA EMAIL

The Secretary
Ontario Securities Commission
20 Queen Street West
22nd Floor, Box 55
Toronto, Ontario M5H 3S8
Email: comments@osc.gov.on.ca

M^e Anne-Marie Beaudoin
Corporate Secretary
Autorité des marchés financiers
800, square Victoria, 22^e etage
C.P. 246, tour de la Bourse
Montréal, QC H4Z 1G3
Email: consultation-en-cours@lautorite.qc.ca

Victoria Pinnington
Senior Vice President, Market Regulation
Investment Industry Regulatory Organization of Canada
Suite 2000, 121 King Street West
Toronto, Ontario M5H 3T9
Email: vpinnington@iiroc.ca

Dear Sirs/Mesdames,

Re: Joint Canadian Securities Administrators/Investment Industry Regulatory Organization of Canada Consultation Paper 21-402 – *Proposed Framework for Crypto-Asset Trading Platforms* (the “Consultation Paper”)

TMX Group Limited (“**TMX Group**” or “**we**”) welcomes the opportunity to comment on the proposed regulatory framework for certain crypto asset trading platforms, as set out in more detail

in the Consultation Paper. Capitalized terms used in this letter and not otherwise defined have the meaning given to them in the Consultation Paper.

TMX Group is an integrated, multi-asset class exchange group. TMX Group's key subsidiaries operate cash and derivatives markets for multiple asset classes, including equities and fixed income, and provide clearing facilities, data driven solutions and other services to domestic and global financial and energy markets. Toronto Stock Exchange, TSX Venture Exchange, TSX Alpha Exchange, The Canadian Depository for Securities, Montreal Exchange, Canadian Derivatives Clearing Corporation, Shorcan Brokers Limited and other TMX Group companies provide listing markets, trading markets, clearing facilities, data products and other services to the global financial community and play a central role in Canadian capital and financial markets.

It is vital to our clients and to all investors that the Canadian capital markets remain fair, efficient and competitive. Our businesses rely on our customers' continued confidence and participation in the Canadian capital markets. Therefore, we support regulatory efforts to facilitate innovation that benefits investors and our capital markets, while ensuring that regulators have the appropriate tools and understanding to keep pace with evolving markets.

Principles Applicable to the Regulation of Platforms

We believe the following three principles apply to the regulation of Platforms, which, as the Consultation Paper outlines, can have features that are analogous to marketplaces, clearing agencies and/or dealers. These principles underpin the regulatory regime for marketplaces, clearing agencies and dealers, and must similarly underpin the tailored regulatory regime for Platforms:

- *Public interest:* The public interest is informed by the Canadian Securities Administrators' ("**CSA**") mission to give Canada a harmonized securities regulatory system that (i) provides protection to investors from unfair, improper or fraudulent practices, (ii) fosters fair and efficient capital markets, and (iii) reduces risks to market integrity and to investor confidence in the markets, while retaining the regional flexibility and innovation that characterize Canada's system of provincial and territorial regulation.¹
- *Level playing field:* The CSA has developed a vision for a competitive Canadian marketplace environment that promotes fairness, transparency, market integrity, price discovery and liquidity. For example, in 2001, the CSA implemented the rules and policies creating this framework for marketplaces, National Instrument 21-101 *Marketplace Operation* ("**NI 21-101**") and National Instrument 23-101 *Trading Rules*. The principles underlying NI 21-101 indicate that having strong and competitive Canadian marketplaces is important to the CSA. It is fundamentally important that competition among capital market participants operating in Canada is rooted in a level playing field. All competitors, regardless of the particular technology they use or the

¹ See the CSA Business Plan 2016-2019, online: www.securities-administrators.ca/uploadedFiles/General/pdfs/CSA_Business_Plan_2016-2019.pdf.

particular types of securities with which they transact, must play by the same rules when they engage the same public interest concerns related to investor protection, fair and efficient capital markets and market integrity. This approach will ensure a truly fair, open and competitive environment for all participants in the Canadian capital markets.

- *Reducing undue regulatory burden:* We recognize that the regulatory framework applicable to Platforms must balance public interest concerns regarding investor protection and fostering fair and efficient capital markets with the cost to Platforms of complying with regulatory requirements. The CSA has prioritized the identification of opportunities to reduce regulatory burden while maintaining appropriate investor protections.² However, in developing a tailored framework for Platforms, the CSA and IROC must consider the parity of regulatory burden borne by all capital market participants, whether they are categorized as Platforms or traditional marketplaces, clearing agencies or dealers. The Canadian capital markets will not be truly competitive if different capital market participants face unequal levels of regulatory burden and compliance costs simply due to whether they transact in novel securities such as crypto assets or derivatives based thereon, versus traditional securities and derivatives.

Given the principles discussed above, TMX Group acknowledges that it is in the interest of all stakeholders of the Canadian capital market that Platforms are regulated in a manner that is consistent with the public interest, while at the same time accommodates the ability of Platforms to be innovative. However, it is fundamentally important that the Canadian regulatory regime applicable to Platforms does not provide Platforms with a regulatory advantage over traditional financial infrastructure providers and intermediaries. We believe this is particularly the case because Platforms, while transacting in non-traditional securities and derivatives, give rise to the same investor protection and market integrity concerns that underpin the securities regulatory regime applicable to traditional marketplaces, dealers and clearing agencies. Regulation among all capital market participants operating in Canada must be rooted in a level regulatory playing field to ensure that public interest objectives related to investor protection, fair and efficient capital markets and market integrity are maintained. Therefore, we support the premise in the Consultation Paper that Platforms should be subject to a tailored regulatory regime that addresses the specific features and risks of Platforms, but that is based on existing regulatory principles and requirements applicable to traditional marketplaces, dealers and clearing agencies. The operational model of, and the risks related to, a particular Platform must dictate the regulatory regime applicable to it.

Conclusion

It is in the interest of all stakeholders of the Canadian capital markets to have Platforms that are regulated in a manner that is consistent with the public interest, while at the same time accommodates the ability of Platforms to be innovative and competitive. However, a Canadian regulatory regime that provides Platforms with a regulatory advantage over traditional financial infrastructure providers and intermediaries does not benefit any participant of the Canadian

² *Ibid.*

capital markets because the public interest concerns arising from the operational models and risks related to Platforms are the same as those arising from traditional financial infrastructure providers and intermediaries. Therefore, we support the CSA's efforts to create a tailored regulatory regime for Platforms that is based on the existing regulatory regime for marketplaces, clearing agencies and dealers. The regulatory framework the CSA applies to Platforms must be consistent with the public interest, ensure a truly level playing field that fosters competition among all Canadian market participants and avoid undue regulatory burden on any Canadian market participant.

Thank you for the opportunity to comment. We would be pleased to discuss any aspect of these matters at your convenience.

Sincerely,

"Deanna Dobrowsky"

Deanna Dobrowsky
Vice President, Regulatory

**Submission to the Joint Canadian Securities
Administrators / Investment Industry Regulatory
Organization of Canada on Consultation Paper 21-402:
Proposed Framework for Crypto-Asset Trading Platforms**

May 16, 2019



About the Canadian Digital Asset Coalition

The Canadian Digital Asset Coalition (CDAC) is an informal industry working group of people and organizations participating in the crypto-asset industry across Canada. CDAC includes crypto-asset platforms and dealers, industry associations, service providers (legal, compliance, audit), blockchain and fintech companies, crypto-asset investors, and software developers. Participants in CDAC share a common desire to kickstart industry dialogue, identify common priorities, concerns, and recommendations, and provide regulators with a feedback on this important consultation.

This submission has been prepared by the CDAC Steering Committee – a team of professionals with policy, industry, compliance, and legal expertise.¹ The submission represents broad stakeholder feedback on the Consultation Paper which was provided through a Canada-wide industry roundtable discussion, an online consultation feedback form, and conversations with crypto-asset industry participants.

¹ The Steering Committee for CDAC is made up of Magdalena Gronowska (MetaMesh Group), Amber Scott (Outlier Solutions), Evan Thomas (Lawyer) and Tanya Woods (Chamber of Digital Commerce). In this process, Steering Committee members served as objective coordinators for collecting industry views, and the views expressed in this Paper reflect the views of the various organizations and individuals participating in the consultation.

Contents

About the Canadian Digital Asset Coalition	2
Introduction	4
Part I: Recommendations on the Development of Canada’s Crypto-asset Policy & Regulatory Framework	5
Overarching Recommendations:	5
Recommendation 1: Acknowledge crypto-asset types, the different functions, and different intermediaries.	5
Recommendation 2: Develop a regulatory framework that is responsive to rapid technology advancements.	6
Recommendation 3: Collaborate with industry experts to develop an appropriate policy and regulatory framework for crypto-assets in Canada.....	7
Recommendation 4: Establish a government + industry Task Force with working groups on specific policy and regulatory areas in the crypto-asset space.	7
Recommendation 5: Improve coordination across provinces, territories and the federal government. ..	8
Part II: Industry Feedback on the Consultation Paper Questions	9
Crypto-asset Platform Specific Recommendations	9
Risks Related to Platforms	10
Global Approaches	13
Custody and Verification of Assets	14
Insurance.....	16
Other Comments.....	17
In Conclusion	18
Appendix 1: Consultation Participants	19

Introduction

Digital- and crypto-assets and their underlying technologies have the transformative potential to generate enormous benefits for business, government, and consumers. Fundamentally, these technologies are reshaping how we transfer value, data and ownership, how we trust and interact with each other, how we structure our society and business models, and how we participate in global financial markets. Their broad potential for impact and accelerating pace of innovation have given rise to one of the most rapidly evolving sectors globally – and have equally have sparked tremendous activity in the global regulatory landscape.

Canada is increasingly competing globally in the innovation-based economy – this sector offers tremendous opportunity for Canada to capitalize on digitally-enabled and innovation-based economic growth and industry welcomes the opportunity to partner with government to further innovation, business and job growth, export potential, and economic diversification.

CDAC has prepared this response with the expectation that there will be ongoing and collaborative dialogue with industry as Canada works to chart a path forward on crypto-assets. This response is organized into two parts:

- Part 1: Overarching policy and regulatory development recommendations; and
- Part 2: Specific feedback in response to the Consultation Paper's twenty-two questions.

CDAC supports the views expressed in the response provided by the Chamber of Digital Commerce Canada. The following feedback offers additional insight collected through the discussions described above.

Part I: Recommendations on the Development of Canada's Crypto-asset Policy & Regulatory Framework

Overarching Recommendations:

Recommendation 1: Acknowledge crypto-asset types, the different functions, and different intermediaries.

Recommendation 2: Develop a regulatory framework that is responsive to rapid technology advancements.

Recommendation 3: Collaborate with industry experts to develop an appropriate policy and regulatory framework for crypto-assets in Canada.

Recommendation 4: Establish a government + industry Task Force with working groups on specific policy and regulatory areas in the crypto-asset space.

Recommendation 5: Improve coordination across provinces, territories and the federal government.

Recommendation 1: Acknowledge crypto-asset types, the different functions, and different intermediaries.

Definitional clarity in regulation allows companies to operate in a compliant, open and transparent manner, and provides businesses the certainty they need in order to operate, conduct long-term business planning, and make capital investments. Similarly, regulatory certainty helps to de-risk the sector, paving the way for businesses to be able to develop banking relationships or better access banking services, or to secure insurance coverage or audit/assurance services.

There is significant diversity across digital asset types and their use-cases, which continue to evolve as regulators know. As the Chamber of Digital Commerce Canada has clearly stated, Canada's industry needs policymakers to acknowledge digital token differentiation and work with industry to establish a supportive framework around crypto-assets, and their related activities and intermediaries.

It was also stakeholders observed that the Consultation Paper does not consider that many crypto-assets do not "fit" with securities laws. They shared concerns that fitting crypto-assets into the existing regime may overlooks many crypto-asset specific issues and risks. There was general disappointment that the creation of a separate regulatory regime for crypto-assets was not an option presented and that industry was not engaged to assist with this.

Industry raised a number of concerns regarding the scope and approach of the regulation proposed by the consultation paper. Stakeholders noted that the consultation paper does not address an important use case where crypto-assets are purchased or converted and used as a payment or means of exchange –

further consultation is needed around payments and Money Service Business (MSB) activities and how the two regulatory regimes (MSB and securities) will intersect.

A number of stakeholders also shared concerns that regulators intend to capture a broad set of crypto-assets and related activities under a regulatory framework for securities in order to protect users. Not only could this be costly, burdensome, and harm Canada's Fintech and blockchain ecosystem, some stakeholders believe that addressing custody of crypto-assets solely in the context of securities regulation may not provide sufficient consumer protection, nor have the ability to mitigate systemic impacts across the industry. Some industry experts suggest that custody and asset verification may need to be applied to all crypto-assets more broadly – however, the approach proposed around custody in this consultation paper has many challenges (refer to the custody discussion of this submission as well as those in the Chamber of Digital Commerce Canada's submission) and significant collaboration with industry is needed to work through an appropriate approach.

Canadian regulatory authorities must work to strike an appropriate balance between consumer protection and creating a space that allows for innovation. The implementation of complementary enabling initiatives and burden reduction strategies alongside regulations are important pillars in formulating a more strategic policy response – one that can better support this nascent industry sector and foster innovation and business growth in Canada.

Recommendation 2: Develop a regulatory framework that is responsive to rapid technology advancements.

Without a sufficient foundational assessment of the legal, regulatory, and economic landscape, Canadian regulators could introduce significant risk to Canada's growing blockchain ecosystem. Canada's crypto-asset market is small, both in terms of population size and daily global market volumes. Some stakeholders have voiced concerns that the proposed regulatory approach is onerous and will cause foreign exchanges to stop providing services to Canadians (e.g., by banning IP addresses) – in light of the risk that Canadian platforms may be locked out of their ability to source liquidity from global markets, consideration of systemic impacts is also needed. At the same time, there is a balance that needs to be struck between providing exemptive relief for foreign platforms and ensuring Canadian businesses are not at a competitive disadvantage due to high costs of domestic compliance they could face.

Some market participants are concerned about the high costs of compliance with the proposed framework (in particular around IIROC membership, insurance, and Type I and Type II SOC 2 Reports, and employee proficiency requirements) that may automatically remove smaller businesses from participating in the market, compromising competition and consumer choice.

As rapidly evolving crypto-asset technologies expand, it is important that regulatory approaches are mindful not to be too prescriptive and risk quickly becoming ineffective, obsolete, or unintentionally harmful to Canada's competitiveness. Flexible and function-based policy approaches are generally more responsive to evolving risks (e.g., cybersecurity threats), technology changes, and the changing nature and scope of crypto-asset companies. Some industry stakeholders suggest working with, or at minimum examining the practices of, industry leaders (like the world's top exchanges) to develop and adopt best practices or standards in the interim, and taking time to work through a more comprehensive regulatory framework in Canada.

The development of industry standards and/or guidelines is an alternative approach to the regulatory framework proposed – and it is prudent that regulators examine opportunities to apply standards to certain activities or operating procedures, such as platform custody and cybersecurity, and that they work with appropriate bodies like the Canadian Standards Association or the Canadian Center for Cybersecurity.

It is important to note that there is disagreement regarding timing across the industry – while some stakeholders advocate for taking a wait-and-see approach to overall regulation, others would prefer some clarity and regulatory certainty from government, particularly around less contentious areas (to be further determined by industry). Regardless of the pace, businesses will need sufficient lead time to be able to transition to a new framework, and there is an overall preference that the framework be coordinated with regulation constructed at a federal level (including around securities) to limit regulatory burden and confusion.

Recommendation 3: Collaborate with industry experts to develop an appropriate policy and regulatory framework for crypto-assets in Canada.

Canada's crypto-asset stakeholders are strongly aligned in the view that policy makers and regulators need to work closely with industry experts and market participants. Dialogue, information sharing and collaboration between industry and government is essential to building a regulatory framework in Canada that balances innovation and ecosystem growth with protecting users and preserving market integrity.

Our industry has had only a limited opportunity to consider the Consultation Paper, consult with one another, and formulate responses to the twenty-two detailed questions set out in the Consultation Paper. In light of the brief 60-day consultation period and the complexity of the issues addressed in the Consultation Paper, CDAC encourages the CSA and IIROC to meaningfully consult with industry participants before enacting any regulatory framework applicable to crypto-asset platforms.

To appropriately support and regulate Canada's rapidly growing digital asset ecosystem, it is critical that policy makers and regulators thoroughly understand blockchain and distributed ledger technologies, their broad applications and use cases, opportunities and risks, and unique characteristics as well as potential regulatory challenges. We encourage dialogue with Canadian technical, policy and legal experts, as well the Chamber of Digital Commerce Canada, as they can assist with navigation around this rapidly evolving technology and regulatory space.

Recommendation 4: Establish a government + industry Task Force with working groups on specific policy and regulatory areas in the crypto-asset space.

Globally, many regulators have set up internal teams, collaborative Working Groups or Task Forces to assess emerging crypto-asset-related activities, and are also working with industry to develop their economic strategies and regulatory frameworks. Our industry discussions support establishing expert working groups with policy makers and regulators to fully examine distinct topic areas relating to digital assets and crypto-asset platforms and markets. Specific topic areas of interest identified through roundtable consultations include custody, payments, securities, markets (integrity, infrastructure, and fairness), as well as enabling

policies to support businesses. Additional dialogue with industry experts is recommended to land on the appropriate Task Force areas of focus.

Recommendation 5: Improve coordination across provinces, territories and the federal government.

There is industry support for a strategic approach to policy and regulatory development and one that minimizes regulatory burden, duplication or conflicting requirements. Given that crypto-assets may have multiple policy and regulatory touch points, it is recommended that governments better coordinate and collaborate on the development of regulations and standards.

In developing a governance structure, it is critical that appropriate Ministries (i.e., those overseeing finance, economic development, innovation, consumer protection, and privacy policy areas), policy leads, regulators (securities administrators, FINTRAC, IIROC, CRA, etc.) and trade associations (Chamber of Digital Commerce Canada, CPA, etc.) are brought to the table. Within Canada, the Chamber of Digital Commerce Canada can provide or facilitate the establishment of an intergovernmental forum for further discussion regarding digital assets.

Lastly, while beyond the scope of this consultation, it is worth noting that the international nature of crypto-assets necessitates collaboration and alignment across regulators and standard-setting bodies to mitigate potential regulatory conflicts and allow for coordination and sharing of information and best practices. A recent study by the University of Cambridge found that the absence of consensus over terminology, definitions, and classification of digital assets may hamper regulatory harmonisation across jurisdictions.² The study cautions that a lack of harmonised and coordinated regulatory responses allows crypto-asset market participants to exploit regulatory loopholes and circumvent stringent regulations. The International Organization of Securities Commissions (IOSCO), the Financial Stability Board (FSB), and the Organisation for Economic Co-operation and Development (OECD) have been identified as potential venues where Canada can collaborate on standards and guidance at an international level.

² <https://www.jbs.cam.ac.uk/faculty-research/centres/alternative-finance/publications/cryptoasset-regulation/#.XN3vFshKhPa>

Part II: Industry Feedback on the Consultation Paper Questions

This section of this submission highlights specific feedback in response to the Consultation Paper's twenty-two questions, including a summary of recommendations for consideration. Please note that the submission only addresses the subset of the questions where the Steering Committee received sufficient input to formulate a response and recommendation that could be of assistance to CSA and IIROC.

In light of the relatively brief 60-day consultation period and the complexity of the issues addressed in the Consultation Paper, CDAC encourages CSA and IIROC to continue to consult with industry participants before enacting any regulatory framework applicable to crypto-asset platforms.

Crypto-asset Platform Specific Recommendations

1. CSA/IIROC should consider the confidentiality and privacy implications of regulations applicable to trading platforms that transact on public blockchains/ledgers. For example, requiring platforms to hold participants' crypto-assets in individually segregated wallets or to settle trades through delivery to participants could publicly reveal confidential and/or private information about individual participants' asset holdings, trades and counter-parties.
2. To the extent that securities legislation applies to crypto-asset trading platforms, of the various operational risks of crypto-asset trading platforms identified by CSA/IIROC, CSA/IIROC should prioritize addressing risks relating to the safeguarding of crypto-assets held or stored by platforms on behalf of participants.
3. To the extent that securities legislation applies to crypto-asset trading platforms, CSA/IIROC should align Canadian requirements applicable to crypto-asset trading platforms with requirements set by other jurisdictions to minimize the cost of compliance for platforms that operate transnationally and the likelihood of forum shopping to countries other than Canada.
4. CSA/IIROC should consult further regarding crypto-asset industry standards and best practices, and the ability and willingness of traditional assurance services providers to serve the crypto-asset industry before mandating any standards or practices for mitigating the risks relating to safeguarding crypto-assets or otherwise providing assurance to regulators.
5. CSA/IIROC should consider that there are potentially significant cost, security, risk management and privacy benefits to participants for platforms to hold or store crypto-assets on behalf of participants.
6. To the extent that securities legislation applies to crypto-asset trading platforms, CSA/IIROC should not mandate any insurance requirements for crypto-asset trading platforms unless and until insurance coverage is generally available at commercially reasonable cost.

7. To the extent that securities legislation applies to crypto-asset trading platforms, CSA/IIROC should conduct further analysis and consultation on the prevalence and significance of short-selling and margin trading on Canadian crypto-asset platforms before prohibiting these activities, even on a temporary basis.

Risks Related to Platforms

1. Are there factors in addition to [the following] that we should consider [when evaluating whether or not a security or derivative may be involved in trading on a Platform]?

- *whether the Platform is structured so that there is intended to be and is delivery of crypto assets to investors,*
- *if there is delivery, when that occurs, and whether it is to an investor's wallet over which the Platform does not have control or custody,*
- *whether investors' crypto assets are pooled together with those of other investors and with the assets of the Platform,*
- *whether the Platform or a related party holds or controls the investors' assets, 6*
- *if the Platform holds or stores assets for its participants, how the Platform makes use of those assets,*
- *whether the investor can trade, or rollover positions held by the Platform, and*
- *having regard to the legal arrangements between the Platform and its participants, the actual functions of the Platform and the manner in which transactions occur on it*
 - *who has control or custody of crypto assets,*
 - *who the legal owner of such crypto assets is, and*
 - *what rights investors will have in the event of the Platform's insolvency*

Multiple respondents cautioned that if platforms are considered to be trading in securities or derivatives because of the manner in which their operations are structured (even if structured for valid technological, security or other reasons), platforms may exit, or choose not to enter, the Canadian market. This would tend to increase consumer costs, reduce consumer choice, and potentially reduce the availability of desirable services for Canadians. It may also drive Canadian consumers towards trading in crypto-assets through underground or foreign marketplaces, thereby reducing, rather than enhancing, the protection of Canadian crypto-asset users.

A number of respondents familiar with the operations of custodial trading platforms provided general comments based on today's technological understanding regarding the factors referenced in Part 2:³

- Many platforms complete the sale of crypto-assets by updating their internal records of which customers own what amounts of the crypto-assets in the platform's custody, not by transferring crypto-assets between wallets using an "on-chain" transaction.

³ Custody of crypto-assets cannot be viewed through the same lens as custody of traditional assets or traditional securities, as the means of control and the ability to transfer crypto-assets is different. The term "custody" is used here to describe the holding of customer crypto-assets at addresses/accounts/wallets for which the platform, not the customer, has control of the private keys.

- Taking custody of customers' crypto-assets can be a source of risk for trading platforms but they do so for a variety of business reasons, including that taking custody mitigates the risk that a customer selling crypto-assets will fail to complete a sale (i.e., entering into a trade but failing to send the crypto-asset to the buyer) and that some customers prefer to keep their crypto-assets in the platform's custody.
- Platforms can provide customers with the ability to transfer their crypto-assets to a wallet under their sole control and many customers do transfer their crypto-assets shortly after purchase.
- Some trading platforms pool customer crypto-assets in their custody, which has a number of advantages compared to maintaining segregated wallets for each customer:
 - Pooling allows trading platforms to hold the bulk (often over 90%) of crypto-assets in cold wallets, which are accessed infrequently. This reduces the risk of loss due to security breaches or technical/human error. Managing private keys for individual segregated wallets would be complex and increases risk for the platform and its customers.
 - Completing a sale of crypto-assets using an "on-chain" transaction to a wallet for each customer would increase transaction costs, which would be passed on to the customer.
 - When customer crypto-assets are pooled together, holdings and transactions on the platforms are recorded "off-chain" in a private database controlled by the platform. If transactions occur on the public blockchain/ledger, private/confidential information about each customer's assets, trades and counter-parties could be publicly available.
- Many platforms provide the custody function themselves. Using a third party's services for custody would increase costs for the platform and its customers and create counterparty risks.
- Consistent with holding the bulk of customer crypto-assets in cold wallets, there are a number of platforms do not make use of customer assets but hold all such assets on a 1:1 basis.
- Many platforms consider customer crypto-assets in the platform's custody to belong to their customers, not the platform.
- The structure of many platforms, whereby the platform operates as a custodian or bailee, does not give rise to a security or derivative interest. The crypto-assets in these cases are legally owned by the customer and not the platform. This means, critically, that the customer's interest is not derived from the underlying asset – it is the underlying asset. The application of a securities law framework, accordingly, is inappropriate to this structure.

3. What best practices exist for Platforms to mitigate the risks outlined in Part 3? Are there any other significant risks which we have not identified? Do you believe that these accurately describe the current risk environment? Is there anything that should not be included here, or that is missing? Please explain.

CDAC surveyed respondents regarding their perception of what best practices exist to mitigate risks identified by CSA/IIROC in Part 3 of the Consultation Paper. Respondents identified the following as some of the current best practices, noting that they are evolving and improving as the technology also evolves and improves:

- The use of cold wallets and multi-signature wallets;
- KYC collection and user identification;

- The implementation of formal anti-money laundering (AML) compliance programs;
- Transparent and accurate trade information and trade monitoring;
- Sanctions and terrorist list related screening;
- Segregation of user funds/assets from operating funds/assets held by the platform operator;
- Formalized security processes;
- Disaster recovery and business continuity planning;
- Compliance and security audits.

Platforms collect and retain large volumes of sensitive personal information about participants, including financial information about participants' bank accounts and crypto-asset transactions, which exposes participants to the risk of loss, theft or misuse of their information in the custody of platforms. This risk may be greater compared to the privacy risks applicable to marketplaces and dealers because loss, theft or misuse of personal information may have privacy consequences beyond transactions on the platform due to the public nature of most crypto-asset blockchains/ledgers.

Recommendation #1: CSA/IIROC should consider the confidentiality and privacy implications of regulations applicable to trading platforms that transact on public blockchains/ledgers. For example, requiring platforms to hold participants' crypto-assets in individually segregated wallets or to settle trades through delivery to participants could publicly reveal confidential and/or private information about individual participants' asset holdings, trades and counter-parties.

CDAC also surveyed respondents regarding their perception of the relative importance of the risks identified by CSA/IIROC in Part 3 of the Consultation Paper. Respondents identified the following risks as the most significant risks:

- Investors' crypto-assets may not be adequately safeguarded;
- Investors' crypto-assets may be at risk in the event of a bankruptcy or insolvency;
- Investors may not have important information about a platform's operations;
- System resiliency, integrity, and security controls may be inadequate;
- Processes, policies and procedures may be inadequate.

Respondents were less concerned about the following risks, compared to those identified above (note, this does not mean that should not be considered, just that they are perceived to be lower priority):

- Investors may purchase crypto-assets that are not suitable for them;
- Investors may not have important information about the crypto-assets that are available for trading on the platform;
- Conflicts of interest may not be appropriately managed;
- Manipulative and deceptive trading may occur;
- There may not be transparency of order and trade information.

These responses tended to show that respondents were more concerned about the safeguarding of crypto-assets held or stored on platforms than they were about risks arising from crypto-asset transactions on platforms. Investment risk regarding suitability and information gaps for crypto-assets (not digitized traditional securities) may be better addressed through education rather than regulatory enforcement. As described in the submission by the Chamber of Digital Commerce Canada, there is a broad benefit to developing objective investor and consumer education tools to help inform the public.

Recommendation #2: To the extent that securities legislation applies to crypto-asset trading platforms, of the various operational risks of crypto-asset trading platforms identified by CSA/IIROC, CSA/IIROC should prioritize addressing risks relating to the safeguarding of crypto-assets held or stored by platforms on behalf of participants.

Global Approaches

3. Are there any global approaches to regulating Platforms that are appropriate to be considered in Canada?

Respondents identified approaches taken in Bermuda, Malta, Mauritius, Switzerland, Gibraltar, Wyoming, Japan, Singapore, and France as potentially appropriate for consideration in Canada. The in-depth jurisdictional scan of the global crypto-asset regulatory landscape by the Cambridge Centre for Alternative Finance, released in April 2019, is a good resource for regulators and policy makers to refer to as it includes overviews of the regulatory space across various jurisdictions.⁴ Key points relating to each of these jurisdictions are also described in the submission presented by the Chamber of Digital Commerce Canada (for expedience, these will not be repeated here).

A number of respondents emphasized that the largest global trading platforms operate from outside Canada, and may exclude Canadian participants if the cost of compliance with Canadian regulatory requirements is out of proportion to the size of the Canadian market. They noted that exclusion of Canadians by major global trading platforms could result in higher costs and other inferior outcomes for Canadians.

Access to banking services is a significant challenge facing crypto-asset companies worldwide and banking challenges contributed to liquidity and solvency issues at QuadrigaCX. With banks refusing to operate or outright closing accounts of Canadian companies due to regulatory barriers and risk aversion, businesses are leaving for more favourable international jurisdictions, like Liechtenstein, Malta, Bermuda and France which have amended their laws to help crypto-asset companies access banking services. Banking restrictions present a competitive disadvantage and an impediment to economic growth – a number of industry participants have voiced that Canada should also consider implementing enabling and complementary policies, such as those related to banking.

Respondents commented that restrictions on access to banking for crypto-asset trading platforms create risks for Canadian consumers using those platforms. Lack of access to banking may require platforms to use unregulated payment processors for accepting and making fiat currency payments, which may delay transactions with customers and increase the risk of loss.

⁴ <https://www.jbs.cam.ac.uk/faculty-research/centres/alternative-finance/publications/cryptoasset-regulation/#.XNrHBY5KhPY>

Certain platform operators noted that they would prefer to be registered with FINTRAC because they expect it could improve banking relationships and consumer confidence, but they are currently unable to register because pending amendments and regulations under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act are not yet in force. They suggested that bringing these requirements into force would reduce risks for crypto-asset trading platform users. There are also a few stakeholders that believe that Bitcoin should be considered money (as it is in Japan) and thus subject to foreign exchange rules and regulation under upcoming FINTRAC amendments – they further argue that Bitcoin, unlike the majority of digital assets, should not be covered under securities laws.

Recommendation #3: To the extent that securities legislation applies to crypto-asset trading platforms, CSA/IROC should align Canadian requirements applicable to crypto-asset trading platforms with requirements imposed by other jurisdictions to minimize the cost of compliance for platforms that operate transnationally and reduce the risk of Canadian companies being disadvantaged in the international market.

Custody and Verification of Assets

4. What standards should a Platform adopt to mitigate the risks related to safeguarding investors' assets? Please explain and provide examples both for Platforms that have their own custody systems and for Platforms that use third-party custodians to safeguard their participants' assets.

Respondents identified various practices for mitigating risks related to safeguarding crypto-assets:

- Use of multi-signature wallets and other key management practices;
- Limits for hot wallet balances;
- Screening process (criminal background checks, etc.) for individuals (e.g., staff, officers, directors, and all beneficial owners) with crypto wallet handling responsibilities;
- Segregated addresses for different participants.

A number of respondents highlighted the Crypto Currency Security Standard (CCSS) published by the Crypto Currency Certification Consortium (C4).⁵ According to C4, CCSS is designed to complement existing information security standards (i.e. ISO 27001:2013) by introducing guidance for security best practices with respect to cryptocurrencies.

Some respondents noted that Mauritius has taken one of the best approaches globally to custodial regulation, by working with industry experts to develop a regulatory framework for custodial services.⁶

Some respondents also noted that platforms could self insure by maintaining a reserve for customer losses using a portion of trading fees.

5. Other than the issuance of Type I and Type II SOC 2 Reports, are there alternative ways in which auditors or other parties can provide assurance to regulators that a platform has controls in place to ensure that investors'

⁵ <https://cryptoconsortium.org/standards/CCSS>

⁶ https://www.fscmauritius.org/media/67493/consultation-paper-custody-of-digital-assets_final.pdf

crypto-assets exist and are appropriately segregated and protected, and that transactions with respect to those assets are verifiable?

Certain respondents noted that due to the public nature of most blockchains, the amount of crypto-assets held by a trading platform could in theory be verified by anyone with knowledge of the platforms' hot and cold wallet addresses. It was also noted, however, that disclosure of platform wallet addresses, particularly cold wallet addresses, may affect customer privacy, increase security risks, and be competitively harmful for platforms.

Respondents identified various methods for trading platforms to provide cryptographic "proof of reserves" without necessarily disclosing hot and cold wallet addresses:

- Blockstream's "Proof of Reserves Tool"⁷;
- Coinfloor's "Provable Solvency Report"⁸;
- Kraken's "Proof-of-Reserves Audit Process"⁹;
- Bitbuy's "Proof of Reserve and Security Audit"¹⁰.

One respondent noted that the participation of CPA Canada is required to ensure SOC 2 Reports are "practically obtainable in Canada" for crypto-asset trading platforms.

Another respondent commented that considerations should be made for fewer requirements / reporting obligations for public blockchains, whose transactions are fully audited and available via the blockchain for any private entity's operations and consumers' transactions. In order to support innovative products on the blockchain, regulators are encouraged to explore low cost ways start-ups could become exempt market dealers or licensed broker dealers (with appropriate oversight).

Recommendation #4: CSA/IIROC should consult further regarding crypto-asset industry standards and best practices, and the ability and willingness of traditional assurance services providers to serve the crypto-asset industry before mandating any standards or practices for mitigating the risks relating to safeguarding crypto-assets or otherwise providing assurance to regulators.

6. Are there challenges associated with a Platform being structured so as to make actual delivery of crypto assets to a participant's wallet? What are the benefits to participants, if any, of platforms holding or storing crypto assets on their behalf?

Respondents noted that platforms could be structured to deliver crypto-assets to a participant's wallet (and certain platforms use this model of operation), but some respondents observed that confirming every trade to the blockchain or other public ledger to deliver crypto-assets to a customer's wallet can be complex and expensive, particularly where there is frequent trading. As it is less costly to record crypto-asset transactions "off-chain" (i.e., in a separate database maintained by the platform), these cost savings accrue

⁷ <https://blockstream.com/2019/02/04/en-standardizing-bitcoin-proof-of-reserves/>

⁸ <https://blog.coinfloor.co.uk/post/184391946481/provable-solvency-report-61-april-2019>

⁹ <https://www.kraken.com/proof-of-reserves-audit>

¹⁰ <https://bitbuy.ca/assets/documents/Bitbuy%20Proof%20of%20Reserve%20and%20Security%20Audit%20Report.pdf>

to the benefit of participants. Additionally, some prefer the platforms to hold or store the crypto-assets on their behalf for the reasons set out below.

Respondents identified certain other benefits to participants of platforms holding or storing crypto-assets on their behalf:

- Participants have a means of recovering their crypto-assets in the event of a lost or forgotten password. Participants who hold crypto-assets in their own wallets risk permanent loss in the event of lost or forgotten private keys. One respondent noted: “One benefit of holding assets on the behalf of investors is that many people find it challenging to manage their own keys. I feel very secure that I won’t lose my [on exchange] crypto-assets because I don’t control the private keys.”
- Participants can sell crypto-assets quickly in response to market developments (for example, by setting stop-loss orders), better allowing them to manage market risk.
- Platforms may take better security measures than participants, who may be more likely to store all of their crypto-assets in hot wallets (e.g., on mobile devices), increasing their exposure to theft.
- As records of platform participants’ ownership and trades are maintained “off-chain”, there may be greater protection against the disclosure of personal information about participants’ crypto-asset holdings, trades and counter-parties.

The platforms that perform on-chain transactions and do not store crypto-assets on behalf of users want to ensure that regulations will not require the storage of crypto-assets on behalf of users as this activity could increase the platform’s risk of losing customers’ assets (e.g., by theft, hack).

Recommendation #5: CSA/IIROC should consider that there are potentially significant cost, security, risk management and privacy benefits to participants for platforms to hold or store crypto-assets on behalf of participants.

Insurance

16. What type of insurance coverage (e.g. theft, hot-wallet, cold-wallet) should a platform be required to obtain? Please explain.

There were differing views expressed by respondents regarding insurance requirements:

- One commenter suggested that “insurance should be optional [and] platforms should use it as a competitive advantage”. Another commenter suggested that insurance should be mandatory in order to exclude marginal platforms that “cannot afford or would not obtain such insurance”, leaving “legitimate platforms that have the means to be insured”.
- Two commenters contended that both hot and cold wallet insurance against theft or loss was optimal because of the significant consequences in the event of theft or loss with respect to cold wallets.

- One commenter suggested insurance for technological errors and omissions. The commenter cited the example of a reported software bug that allegedly resulted in the loss of millions of dollars worth of Ethereum by the now-bankrupt QuadrigaCX trading platform.¹¹

17. Are there specific difficulties with obtaining insurance coverage? Please explain.

Respondents stated:

- There are very few insurers willing to underwrite crypto-related policies. There are only two underwriters globally.
- Where policies are available, premiums are very high (e.g., 1-2% annualized on the insurable asset).
- Technology errors and omissions coverage is prohibitively expensive for all but the largest organizations.
- There are limitations to insurance and how it's structured – notably, cold wallets are not insured by all insurers.
- Insurer knowledge of the business/asset class is insufficient to ensure appropriate coverage.

One commenter noted that the banking challenges for market participants contribute to the inability of platforms to obtain insurance coverage, noting “[f]inancial inclusion for the industry is a necessity”.

Another commenter noted that industry standards are welcome as they can help de-risk the sector and help companies access insurance. However, the insurance industry needs to be made a stakeholder in this conversation going forward, to ensure that any required insurance is practically obtainable in Canada.

Another commenter noted that the CSA should not restrict Canadian domiciled actors from competing internationally through the imposition of onerous capital reserve requirements.

Recommendation #6: To the extent that securities legislation applies to crypto-asset trading platforms, CSA/IIROC should not mandate any insurance requirements for crypto-asset trading platforms unless and until insurance coverage is generally available at commercially reasonable cost.

Other Comments

A number of respondents commented on the Consultation Paper’s statement that “[t]o reduce the risks of potentially manipulative or deceptive activities, in the near term, we propose that Platforms not permit dark trading or short selling activities, or extend margin to their participants.” Comments included:

- “It is our belief that margin trading and short-selling are important activities that help crypto-assets become legitimate assets in the mainstream financial markets.”
- “[Margin and short-selling] also provide means of stability and risk mitigation in the market.”

¹¹ https://www.reddit.com/r/ethereum/comments/6ettq5/statement_on_quadrigacx_ether_contract_error/

- “Banning short-selling prevents true price discovery in a healthy market (as it eliminates the downward price pressure), and effectively prevents market forces from operating to regulate the market itself.”
- “Additionally, as the asset is truly a global border-less asset, banning such activities on Canadian platforms will simply push such activities to other jurisdictions. We have the opportunity to draw participants to come into a regulated environment, but in banning such activities, participants will simply go jurisdiction shopping, thus pushing participants back to an unregulated space.”
- “Banning short-selling or margin trading in Canada will not stop such activity from occurring in the global crypto-asset market, and will simply incentivize clients to seek alternatives outside Canada.”

Recommendation #7: To the extent that securities legislation applies to crypto-asset trading platforms, CSA/IIROC should conduct further analysis and consultation on the prevalence and significance of short-selling and margin trading on Canadian crypto-asset platforms before prohibiting these activities, even on a temporary basis.

In Conclusion

Through consultation with a broad diversity of entrepreneurs and community members, it is clear that while there is not consensus on all matters, there is a willingness to engage in a meaningful dialogue with regulators. We urge the readers of this submission to carefully consider the points raised here, in addition to the points raised by other industry participants in their submissions and the Chamber of Digital Commerce Canada. We urge the CSA and IIROC to establish an ongoing dialogue with the industry, in order to ensure effective outcomes for all stakeholders.

Appendix 1: Consultation Participants ¹²



Eric Kryski, CEO & Co-Founder



Cryptocurrency Exchange. Pamela Draper, President & CEO



Canadian Bitcoins – Cryptocurrency Brokerage. James Grant, Owner



Centigram International Ltd. Sameem Monzaviyan, Founder and President



CryptoChicks – Blockchain Educational Hub. Nataliya Hearn, Co-Founder



GraafOne – Non-Custodial Bitcoin Services. Pavel Dolzhenko, Founder



Grayblock Power. Chris Ciaravino, Founder & CEO



iComply Investor Services. Matthew Unger, CEO



Ledn – Credit & Savings Products for Bitcoin. Adam Reeds, Co-Founder & CEO; Mauricio Di Bartolomeo, Co-Founder & CSO



Metamesh Group. Magdalena Gronowska, Consultant



Outlier – AML Consulting Services & Strategies. Amber Scott, Founder



Shyft Network International Inc. Joseph Weinberg, Co-Founder; Chris Forrester, CTO



Toda Network. Toufi Saliba, CEO



Unitralis, Joseph Iuso, Advisor

¹² Note, CDAC consulted with a number of companies and individuals. The following companies have consented to being identified.

INCLUDES COMMENT LETTERS



Canadian Digital Asset Coalition

MDC Response to IIROC' consultation paper on Crypto Assets and Trading Platforms



Written by

Managing Principal Innovation Practice Leader

Alexander Izak Levesque

Market Data Company

77 King Street West

Suite 1179

Toronto, Ontario

M5K 1P2

Email: Alex.Izak@marketdatacompany.com

Phone : 438 - 937 - 7777

Consultation Link

https://osc.gov.on.ca/documents/en/Securities-Category2/csa_20190314_21-402_crypto-asset-trading-platforms.pdf

APPENDIX A

Consultation Questions

1.

Are there factors in addition to those noted in Part 2 that we should consider?

MDC Believers Factors that should be brought up for consideration include:

- Exchanges and custodians might reduce their liability by using multisig wallets shared either between other reputable third parties or the client themselves. Multisig wallets are shared wallets or joint funds that can only be moved if all the required parties sign the transaction. This greatly reduces risk of insolvency and theft because the client is required to move the money in addition to the platform. Not all coins support multisignature wallets.
 - (a) Who has control of a joint or multisig wallet and which parties should be included to approve the transaction ?

- (b) Who is responsible for funds shared between the platform and the client ?
 - (c) Should multisig be enforced to protect users funds and reduce the liability of exchanges ?
- Consideration should be given to the specific obligations of token holders and custodians to mine, vest or destroy certain coins and how might they be rewarded or diluted if they do not. This applies most to a proof of stake coins where the token holders ability to mine or forge new coins is based on their existing balance. For example a popular proof of stake coin “Tezos” requires holders of coins to participate in the mining process and if they do not their stake is diluted.
 - (a) What should a custodians responsibility be for these coin specific obligations given that some of these tasks such as mining a proof of stake coin come with inherent costs ?
 - (b) Can a custodian mine on behalf of a client, can a custodian keep a part of the mining revenue in such a scenario ?
 - (c) What should a custodian's responsibility to disclose information about a token holders obligations and possible consequences or benefits of meeting those obligations or not to clients ?
- Consideration should be given to a custodian's responsibility in the case of a fork. This could be a fork of the distribution meaning that for every coin a person holds they can claim an equivalent amount of a different coin or a network fork where either miners or in some cases coin holders can choose between two competing visions of the same coin and the one that gets the most votes or in the case of mining the most hashpower becomes the official coin. It is important to note that not all forks are created equally, some can come with different security implications, economic implications and unsupported or new wallets that may also introduce security vulnerabilities to the wider platform. It follows that if custodians were forced to support specific forks they might also be introducing security vulnerabilities onto their platform. Additionally, if custodians that act as

exchanges are forced to allow trading of any forked coins it might allow people to force reputable exchanges to support poor quality coins simply because they were forked off the distribution of a more reputable one. This would give these poor quality coins lots of exposure and liquidity and might give investors the false perception that these coins are more widely supported and traded than they actually would be on their own merit.

(a) What responsibility do custodians have to clients to make available forked coins ?

(b) How much decision power should custodians have in the scenario of choosing between two competing forks ?

(c) What responsibility do custodians have to make these forked coins available for trading on their platform ?

- Consideration should be given to the responsibility of custodians that hold coins that give them the ability to vote on issues relating to the coin or its community. Some coins give holders the right to vote on issues in that community based on stake.

(a) Should custodians be able to vote using the wallet balance they control on behalf of their clients ?

(b) Should custodians make voting with coins they hold available to their clients ?

(c) What responsibility do custodians have to disclose information about ongoing votes to clients holding relevant coins ?

2.1

What best practices exist for Platforms to mitigate the risks outlined in Part 3 ?

- The best way to mitigate the risk of poorly safeguarded coins is to introduce trusted third parties that share control over multisignature wallets. This could be multiple trusted custodians, a designated organization or the client themselves. The use of multisig wallets can also increase transparency by allowing clients direct access and oversight over wallets they share control of.

- Another way to safeguard coins is to enforce DLT specific security standards such as the CryptoCurrency Security Standard (CCSS) by the The CryptoCurrency Certification Consortium (C4) as well as having some members of the team managing the platform complete a certification such as the Certified Bitcoin Expert (CBX) by the same organization or a similar one.
(see <https://cryptoconsortium.org/>)
- Custodians should work with third party market data providers or crypto rating agencies to mitigate the risk that investors are not getting adequate information about the assets they are buying, the associated risks and obligations. In much the same way Moodys rates bonds and provides information to investors an analogue should exist in the world of crypto and DLTs. This approach would also reduce the risks of a conflict of interest if this reporting was left to the platform itself.
- Independent third party ratings of the exchange platforms themselves could mitigate the risk that investors do not have enough information about the operations and security in place at a given exchange. The independent ratings should also provide metrics and ratings for the transparency of order and trade information. These ratings will mitigate the risk of deceptive or manipulative trading and allow for better price discovery.

2.2 Are there any other significant risks which we have not identified?

- There is a major problem with exchanges creating fake volume or inflating volume.
- There is a real risk to business continuity and trading if third parties such as banks cease working with an exchange suddenly. Exchanges and Investors

should be made aware in advance of such changes and a procedure should be put in place to transition to new third parties. It is possible that banks might be able to use such sudden closures or withholding of funds as a punitive measure against groups they see as competition. By providing a clear regulatory framework and ratings financial institutions can better trust exchanges and this mitigates the risk for third parties so they can better serve exchanges.

- Risk to the exchanges posed by forks. It is important to note that not all forks are created equally, some can come with different security implications, economic implications and unsupported or new wallets that may also introduce security vulnerabilities to the wider platform. It follows that if custodians were forced to support specific forks they might also be introducing security vulnerabilities onto their platform. Additionally, if custodians that act as exchanges are forced to allow trading of any forked coins it might allow people to force reputable exchanges to support poor quality coins simply because they were forked off the distribution of a more reputable one. This would give these poor quality coins lots of exposure and liquidity and might give investors the false perception that these coins are more widely supported and traded than they are because users associate it with the coin it's forked from. For example Bitcoin Cash was forked off the Bitcoin distribution and its caused some confusion, the creators of Bitcoin cash even owned Bitcoin.com and promoted the Bitcoin cash variant through the site which had previously been used as an information source for Bitcoin. These coins are not the same except for the initial distribution of Bitcoin cash was froked off of (came from) Bitcoin so anyone who held a Bitcoin could claim the same amount of Bitcoin cash.
- Many assets are supported by their own miner network and proof of work, while this does pose the risk of a 51% attack whereby a group of miners gain majority control over the network the fundamental economic design of these assets makes it more costly to do so the more valuable they become. In this way the network security scales with the miners and

increase in market cap. Many miners are also highly disincentivized to coordinate such an attack as it could easily wipe out their main source of profit. One possible risk is that a nation state could force an attack using the largest mining pools to coordinate such an attack if too much of the mining is done in one country as is the case with Bitcoin mining being concentrated in China and with a few large mining pools.

- Assets that use delegated proof of stake and proof of stake are at risk of even greater manipulation. Delegated proof of stake means a few centralized groups are delegated to mine the network, this allows that group to take unilateral decisions that include moving users funds or reversing transactions without their approval. Projects such as EOS and other delegated proof of stake (DPOS) projects therefore pose an enormous risk to users funds. Understanding that no one nation, group or individual should have such unilateral control of users funds globally is one of DLT greatest features however delegated proof of stake and proof of stake projects compromise on decentralization, security and immutability in order to get more transactions and faster transactions.
- Proof of stake coins also are at risk of the “nothing at stake problem”. The Ethereum Wiki describes the nothing at stake problem for proof of stake algorithms “this algorithm has one important flaw: there is "nothing at stake". In the event of a fork, whether the fork is accidental or a malicious attempt to rewrite history and reverse a transaction, the optimal strategy for any miner is to mine on every chain, so that the miner gets their reward no matter which fork wins. Thus, assuming a large number of economically interested miners, an attacker may be able to send a transaction in exchange for some digital good (usually another cryptocurrency), receive the good, then start a fork of the blockchain from one block behind the transaction and send the money to themselves instead, and even with 1% of the total stake the attacker's fork would win because everyone else is mining on both.” <https://github.com/ethereum/wiki/wiki/Problems>

In a normal proof of work coin there is a cost associated with mining multiple forks of the same coin. One's hashpower (miners) can only be directed at one of the chains at a time forcing miners to choose between chains. In Proof of Stake economic protocol, there's nothing actually at risk when making consensus decisions so optimal behavior from an individual's perspective is to participate in as many forks as possible which could lead to rapid dilution of value through inflation and manipulation of the transactions.

3.

Are there any global approaches to regulating Platforms that are appropriate to be considered in Canada ?

- Gibraltar is one of a number of island nations looking to establish themselves as a big player in cryptocurrency industry. Banks that work with regulated exchanges such as those in New York have been very open to businesses regulated under the GFSC license. The Gibraltar Financial Services Commission (GFSC) have made quick progress in implementing regulations for all companies using distributed ledger (blockchain) technology. From the 1st January 2018, any company wanting to “store or transmit value belonging to others” using blockchain technology, including cryptocurrency exchanges, are required to become licensed by the GFSC. Not unlike the new York “Bitlicense” except the implementation of Gibraltar regulations has been much less criticized than New York's “Bitlicense”. The regulations outlined by the GFSC allude to a number of obligations of DLPs (Distributed Ledger Providers) to have adequate infrastructure in place for AML and CFT, solvency, corporate governance and cybersecurity. <http://gibraltarlaws.gov.gi/articles/2017s204.pdf>
- Due to the complex and evolving nature of digital assets a regulatory sandbox should be used in Canada much like the Hong Kong Securities and Futures Commissions (HKSF's) Regulatory Sandbox. It will help regulators understand new projects with unique qualities and economic models as well as promoting much needed innovation in the space.

4.

What standards should a Platform adopt to mitigate the risks related to safeguarding investors' assets? Please explain and provide examples Both for Platforms that have their own custody systems and for Platforms that use third party custodians to safeguard their participants' assets.

For platforms that safeguard their investors assets.

- First and foremost the use of multisig wallets by exchanges to share custody over wallets with third parties or the clients themselves reduces their liability and the risk that any one party could unilaterally move coins without the consent of another. It reduces the chances coins are lost forever if a team member dies or that any one person or group could steal the coins.
- The CryptoCurrency Security Standard (CCSS) by the The CryptoCurrency Certification Consortium (C4) outlines a great checklist of security measures exchanges could take to protect the assets they manage. CCSS covers a list of 10 security aspects of an information system that stores, transacts with, or accepts cryptocurrencies.
(see <https://cryptoconsortium.github.io/CCSS/Matrix/>)

For platforms that use third parties

- The third party should be insured for theft
- The third party should have regular external security audits
- Users should verify their funds are actually held with the third party by using view keys or moving funds temporarily to show they are actually under the users control.

5.

Other than issuance of Type I and Type II SOC 2 Reports, are there alternative ways in which auditors or other parties can provide assurance to regulators that a Platform has controls in place to ensure that investors' crypto assets exist and are appropriately segregated and protected, and that transactions with respect to those assets are verifiable?

- The platforms can provide a view only key to regulators and auditors that gives them full visibility over the coins in the wallet. It is verifiable and does not allow anyone holding the view key to actually spend the coins in the wallet greatly reducing chances of theft should the actual private spend key get passed around many parties which would otherwise create new security vulnerabilities with each group that gains access to the coins.

6.

Are there challenges associated with a Platform being structured so as to make actual delivery of crypto assets to a participant's wallet? What are the benefits to participants, if any, of the Platforms holding or storing crypto assets on their behalf?

- Ideally crypto exchanges would never have to fully hold users funds and many efforts are being made by the industry to roll out decentralized exchanges where users are fully in control of their funds, no third party holds them. When an exchange holds too many coins it becomes a larger target for hackers, the safest places to store coins therefore become at higher risk of theft as more people place funds with those institutions. Therefore there needs to be greater diversity and number of custodians to limit the risk of a few large custodians holding a large number of coins. The benefit of holding funds on behalf of users is that it makes the process of settling transactions faster and more streamlined. The centralized nature of holding coins allows an exchange to better manage the settlements internally and apply its own key management schemes. There are tradeoffs for users as well, some might not have the skill required to safely store their

own currency or might want to place that risk onto a reputable exchange and its insurers.

7.

What factors should be considered in determining a fair price for crypto assets?

Important factors to be taken into consideration when pricing any digital token

- Some ICO tokens are securities, the tokens act as a debt or equity and are exchanged for money the token creators use to fund an underlying business model and delivery of some form of dividend or technology. There is an important role to be played by ratings agencies that can help investors make sense of these complex liabilities. In the same way rating agencies rate a bond a role exists for new specialized ratings bodies that rate securities tokens and their ability to meet investors expectations and financial obligations.
- Issuance: How many tokens have been issued, how many tokens will be issued, at what rate of inflation will new coins be issued, how fair or decentralized is issuance and does a small group award themselves or control a large portion of the issued tokens (arguably a form of price manipulation). If someone creates a token but issues 99% of the tokens to themselves they can control the price and investors should be aware of how that coin is issued.
- Tokens can be built on a pre-existing Blockchain such as Ethereum. These tokens are referred to as colored coins and could affect the economics of the host chain and the host chain can affect the security and economics of the colored coins. Understanding how a token is designed and which projects directly affect its economic model is critical to better pricing a token.
- A token can be forked from an existing distribution so every person holding one Bitcoin can claim a Bitcoin Cash or some other fork of the distribution

such as Bitcoin Gold. The stated coin cap for the fork is the same as the coin it forked from. So if there are 21 million Bitcoin and every Bitcoin holder can claim one bitcoin cash there are technically 21 million Bitcoin cash. The problem is its very safe to assume that not all Bitcoin holders will claim or be capable of claiming their Bitcoin cash and those that do will take time. This leads to situations where the actual supply of coins is significantly lower than what is reported to investors. It can affect the perceived market cap because if only 100 investors claim their Bitcoin cash and Bitcoin cash applies that price to a supply of 21 million coins instead of the active supply of claimed coins people are being misled. This can be seen in the way Bitcoin cash actually reached a billion dollar market cap in the first few days it was traded.

- Lost Tokens: How many tokens are lost and therefore cannot be traded.
- Locked coins: How many coins are locked up in a smart contract, hack or ICO and therefore cannot be traded.
- Volume: There is a major problem with exchanges creating fake volume or inflating volume. In the case of the cited article the author looked at the percentage change between the observed mid-spread price and the lowest price the author had to consent to to sell the asset and found many exchanges blatantly faking volume with *"OKex, #1 exchange rated by volume, the main offender with up to 93% of its volume being nonexistent"* <https://medium.com/@sylvainartplayribes/chasing-fake-volume-a-crypto-plague-ea1a3c1e0b5e>

There needs to be independent pricing sources, market data tools as well as independent rating agencies which help investors determine the quality of exchanges order books and factor for fake volume.

- Sourcing: Many investors get information about price and volume from third party sources like coinmarketcap.com the most visited such source which can and has manipulated the price by simply adding or removing

data from specific exchanges. The third party pricing source can manipulate and front run coins prices by listing them or delisting them, listing exchanges with fraudulent data or blocking exchanges suddenly for their fraudulent data. What is required is a trustworthy rating of the quality of information from each orderbook so investors can decide for themselves how to account for fake volume.

8.

Are there reliable pricing sources that could be used by Platforms to determine a fair price, and for regulators to assess whether Platforms have complied with fair pricing requirements?

- Third party sources can be used but the best way right now would be to use information pulled directly from exchanges order books using their APIs. Our firm plans to release a reliable pricing source as well as ratings for each exchange and the quality of information in its orderbook with a focus on identifying fake volume.

What factors should be used to determine whether a pricing source is reliable?

Key signs of unreliable volume data include

- Too much Slippage indicates fake volume
- Number of users VS Volume: Increasing Volume without increasing number of users.
- Trading patterns : Consistent uniform Volume that does not conform with what we expect to see on an exchange. Does the volume look organic or faked.

9.

Is it appropriate for Platforms to set rules and monitor trading activities on their own marketplace? If so, under which circumstances should this be permitted ?

- While exchange platforms should be expected to monitor their platforms trading activities for fraudulent behaviors, critical errors on the order books and manipulative trading as a security precaution it is important that this monitoring is not exclusively done by the exchange alone. An external monitor is needed to assure the integrity of the reporting. Exchanges have been known to hide losses, manipulate order books and in some cases thefts of tokens can be an inside job. Exchanges cannot be trusted to monitor trading alone. Given the complex nature of crypto assets new approaches will be necessary for the bodies that monitor traded assets to better understand unforeseen risks. Whether that group is IIROC monitoring exchanges trading security tokens or an RSP, the monitors will need to take into consideration the programmable nature of each token, what that enables and its limits. Each token type has a unique economic model, features and limitations and monitors will have to understand each one in order to properly surveil exchanges. New Market data tools will need to be employed by IIROC and RSPs to get this information regularly and reliably. The potential risk of most exchanges using a single regulator or RSP is if some aspect of market surveillance is missed by the monitor due to the unique technology behind a token that aspect might be exploited across multiple exchanges.

10.

Which market integrity requirements should apply to trading on Platforms ?

- Based on how a token is classified, as equity, as a debt as is the case with many ICOs or if it is a self contained commodity/currency the same relevant market integrity requirements should apply as any other equity, debt or currency exchange. The market integrity requirements should apply in the same way but might require a new market trade reporting system that includes and integrates with transaction data on the distributed ledgers themselves.

There are risks to market integrity that are unique to these markets and should be taken into consideration.

- If definitions for a security are too broad tokens that are not designed as such might not be able to compete because they do not raise money and therefore cannot cover the costs associated with regulation of a security. These projects are open source where there is no equity, no raise, no employees and work is done by volunteers. These projects include Bitcoin, the effect of wrongly classifying assets could have devastating effects for the market and liquidity as a whole.
- If regulations affect the distribution of the coin such as say a regulation that forced a change in the number of coins minted in Bitcoin or the supply cap of Ethereum it could cause a total loss of confidence in the agreed upon economic models and a collapse in price. Most people buy into coins like Bitcoin or a given token distribution because there is a set distribution that is baked into the system and can be known years in advance. If any regulation affected that distribution it could threaten market integrity.
- For institutions buying on behalf of clients there might be an edge over retail investors. There is very low liquidity in many of these markets so changes such as the delisting of Bitcoin futures from the CME have a large effect on the market. These kind of institutional decisions can move the price up or down and could pose a risk to market integrity.

11.

Are there best practices or effective surveillance tools for conducting crypto asset market surveillance? Specifically, are there any skills, tools or special regulatory powers needed to effectively conduct surveillance of crypto asset trading?

- The best way to conduct crypto asset market surveillance is through existing blockchain explorers which allow one to verify which wallets contain which coins without introducing any risks and with a high degree of certainty. One benefit of DLTs is the ease and certainty with which well trained persons can verify the existence of coins and their location.

- Individuals should be trained in how to understand various crypto currency and how to monitor their transactions, verify multisignature addresses and audit crypto currency balances.

12.

Are there other risks specific to trading of crypto assets that require different forms of surveillance than those used for marketplaces trading traditional securities?

- The main difference between surveillance of securities and digital assets would be integrating the information on transactions from the blockchain itself. It should not require a unique approach to surveillance outside of the information used directly from the blockchain. For example a security issued on the Ethereum blockchain could be monitored at the exchange level and that reporting could be backed up by monitoring of the transactions on the blockchain itself. This could be as simple as verifying the trades using an Ethereum Block Explorer run by a reputable market data provider running an full node (with its own full copy of the blockchain data not a third party).
- Under which circumstances should an exemption from the requirement to provide an ISR by the Platform be appropriate?
- If an exchange is designed so that the tokens or keys being traded are never fully in their custody often referred to as decentralized exchanges, they should be exempt because they do not pose the same risk to investors.

What services should be included/excluded from the scope of the ISR?

Please explain.

- When an exchange or platform offers custodian services they should be included in the scope of the ISR

- When an exchange does not hold users funds or shares custody with users in a joint or multisig account they should be exempt from the scope of the ISR

14.

Is there disclosure specific to trades between a Platform and its participants that Platforms should make to their participants?

- Platforms should disclose if they are trading against their clients.
- Platforms that are given free coins or paid directly to list specific cryptocurrencies should disclose the payment to clients.
- Platforms should disclose support for a specific fork of a coin. Otherwise they can use investors funds in some cases to influence the development of crypto projects.
- Platforms should disclose if they own coins traded on their platform through other exchanges. Platforms could trade on foreign or third party exchanges rather than their own while using the listing or delisting of a token to affects it price and profit off of clients.

15.

Are there particular conflicts of interest that Platforms may not be able to manage appropriately given current business models? If so, how can business models be changed to manage such conflicts appropriately?

- They might not disclose payment in exchange for listing specific coins. This in turn brings liquidity to the new coins and can increase an assets price significantly. Sometimes they are paid with the coin they are listing or invest in it themselves. That information should be available to potential customers.

- Exchanges should disclose when they trade against clients.
- Certain exchanges create plenty of fake volume, investors should have access to that information through new market data tools.
- They might not disclose information about the assets to clients. The solution is for independent ratings agencies and market data tools to provide investors with the information they need in way that is easily understandable. Many DLT projects are small and new so we are just beginning to see the development of new market data tools to understand them. In much the same way bonds are rated by Moodys so to should crypto assets be rated by specialized ratings agencies. Whether a firm is looking to use Blockchain technology to power an internal settlement mechanism, investing directly into a cryptocurrency or tokenized security, relevant regulations or simply looking into the infrastructure needed to securely receive and manage new forms of digital assets our team breaks down the information investment managers need into an understandable Crypto Rating.

16. What type of insurance coverage (e.g. theft, hot-wallet, cold-wallet) should a Platform be required to obtain? Please explain.

- If tokens are held in multisig wallets by multiple parties possibly including the client or multiple trusted exchanges they should be allowed to share liability and insurance policies and in the case of decentralized exchanges or clients sharing the keys with the exchange insurance might not be necessary.
- Ideally if available insurance should be acquired for all wallets hot and cold for loss or theft for exchanges or custodians holding large amounts of tokens on behalf of their customers.

- Not all cold wallets or hot wallets are equally secure. One could have a cold wallet in a secure swiss bank vault or one could keep it in an unsecured location and the procedures for accessing that cold wallet vary enormously. Similarly, a hot wallet might use a hardware configuration with known security vulnerabilities or it might be a well tested and audited hardware configuration. Some companies even produce special hardware wallets for securely moving coins such as the Ledger or the Trezor and each comes with a different level of security and security audits. What is needed are market data tools that provide ratings of the different hardware and procedures used to create, use and store hot and cold wallets for each custodian. These ratings will inform the insurance industry as well as clients of their potential exposure working with a given custodian. The ratings will help insurance companies form a standard that determines the risk involved and cost of insurance.
- There is less risk when each user holds their own private keys over a single centralized custodian that acts as a large point of failure and target for hackers. Therefore users or groups who hold their own coins will need insurance and again the insurance industry should use information about the procedures and hardware groups use to secure their coins to determine their exposure and cost of the insurance policy.
- There is a lack information on how much fraud is actually happening. Insurers need to first know what proportion of transactions are fraudulent and understand the risks before they can offer good policies.

17.

Are there specific difficulties with obtaining insurance coverage? Please explain.

- It may not be possible for smaller startups or exchanges to get insurance. Insurance should only be required when an exchange holds a substantially large amount of money in order to give smaller exchanges time to grow.

- It should also be noted that insurance markets for crypto exchanges are extremely new and therefore there is limited data available for insurers to understand the tokens, the regulations and the exchanges security procedures. There is a short history of hacks, thefts and losses for insurers to calculate the risks to their business. We believe that independent market data and ratings platforms will play an important role in informing the insurance industry of the risks so better policies can be provided with less risk and cost to all involved. Ideally if available insurance would be provided for all wallets hot and cold for loss or theft.

18.

Are there alternative measures that address investor protection that could be considered that are equivalent to insurance coverage?

- If investors hold their keys and the exchange is fully decentralized and does not act as a custodian then the decentralized exchange should bear no liability for customers funds and no insurance should be required.
- It is quite complicated and we are not advising to adopt this measure but further study could be made into Bitfinex an exchange which was robbed of about \$73 million in 2016. Exchange customers, even those whose accounts had not been broken into, had their account balance reduced by 36% and received BFX tokens in proportion to their losses. All exchange customers were repaid eight months after the hack. There is currently ongoing investigations into Bitfinex how it handled the hack. The New York AG's office has also filed a lawsuit under New York's Martin Act (the NY laws regulating securities and commodities fraud) against the Bitfinex and Tether companies alleging that they may have defrauded Bitfinex customers and tether owners.

19.

Are there other models of clearing and settling crypto assets that are traded on Platforms? What risks are introduced as a result of these models?

- Swaps: New technology is being developed that allow holders of one cryptocurrency to swap or trade with another user on chain without any third party. This reduces the risk of a third party losing funds but there are always risks that the technology could be flawed and funds are lost through a technical error. Sufficient testing should be done before on chain swaps are widely adopted. As the swaps reduce the role of dealers, custodians and exchanges they should come with fewer risks and less need for regulation.
- DEX: Decentralized exchanges match users with each other to trade but do not hold users funds at any point of the transaction.

20.

What, if any, significant differences in risks exist between the traditional model of clearing and settlement and the decentralized model? Please explain how these different risks could be mitigated.

- The main significant difference is a decentralized model does not hold users funds and therefore there exists less friction and centralized cybersecurity risk than if the funds were held by a custodian or exchange. Decentralized models should come with fewer cyber security restrictions although it should be clear that an exchange that holds users private keys cannot claim to be decentralized.
- We have seen so called DEX exchanges where users are holding a proxy token for an actual token held by a custodian. An example would be ETHBTC which allows you to trade between Ethereum tokens and Bitcoins on Ethereum based decentralized exchanges but only allows you to trade Bitcoin in the form of an Ethereum token backed by a Bitcoin token held with a custodian. These types of projects are not really decentralized even

though they claim to be. The nuance comes down to who holds the private keys for the asset you are trading.

21. What other risks could be associated with clearing and settlement models that are not identified here?

- There exist complex risks in using platforms such as Ripple or Ethereum to settle interbank transactions. DLT is being rolled out in many institutions and most do not understand the potential risks associated to this model of inter organization settlement. Ratings Agencies should provide information in the form of ratings and market data about private blockchain applications and associated risks.

22.

What regulatory requirements, both at the CSA and IIROC level, should apply to Platforms or should be modified for Platforms? Please provide specific examples and the rationale.

- Market Integrity requirements should apply specifically to exchanges that are trading in tokens that qualify as securities. Exchanges trading in securities should follow existing NI 23 - 103 and UMIR requirements. New requirements might include using raw transaction data to verify the records and reporting being done by exchanges. Exchanges should have in place robust infrastructure and network firewalls to keep their exchanges online in the face of Denial-of-service attacks and attempted hacks which could have an affect on market integrity over time.
- Transparency of operations: In addition to existing transparency requirements exchanges should disclose what procedures they have in place to audit and safeguard users funds. Transparency when it comes to security is critical to insurers and clients understanding the risk of loss or theft of their funds. Exchanges could make available ways for a user to

audit the exchanges funds themselves by making available transaction data or wallet balances to clients or third party auditors.

- Transparency of orders and trades: Information processors should verify the volume and orders using raw transaction data or view keys before publishing the order books. This would lead to less false reporting and market manipulation.
- Outsourcing: In addition to keeping access to the books and records a marketplace that outsources key services or systems to a service provider should have policies in place and procedures relating specifically to cryptocurrency transactions and holdings as well as more stringent cryptocurrency security standards and that data should in some way be available to securities regulatory authorities. For example, if an crypto exchange outsources a key service to a third party that third party should keep records as well as verifiable transaction to back up the records.
- Confidential treatment of trading information: The public design of many blockchain tokens makes it very difficult for exchanges to assure the confidentiality of users trades as anyone has access to the full history of transactions not only regulators and can from that information learn users deposits, withdrawals, trading strategy and even if they spend that money at a Doctors office. For example if I know Mr.X has a substantial fund holding tokens in a given wallet and those funds are deposited to an exchange I can presume that those coins are being sold on the exchange and even trade before the funds have time to confirm. While privacy tokens have their own regulatory challenges they shouldn't be written off as they solve key problems in maintaining users trading strategies private while allowing users to still disclose wallet balance to regulators. There exists a place for innovations in confidential technologies and blockchains that are necessary to maintain privacy necessary for market integrity and any negotiation. Additionally if anyone can see a users funds it poses a danger to their safety, they can be targeted based on their wealth by anyone with

access to transaction data from the blockchain unless a confidential technology such as ring-ct or zero knowledge proofs is used.

- Systems and business continuity planning: This should include a multisignature scheme to recover funds if any member of a team falls ill or dies. Regulators should know who the key holders with access to the funds are. This means redundant keys assigned for recovery purposes (i.e. 2of3, 3of5, etc.) No two keys belonging to the same wallet should be present on any one device. Key/seed backup should be stored in a separate location from primary key/seed. Keys should be distributed across multiple organizational entities. Keys should be distributed across multiple separate locations. A written checklist/procedure document exists that outlines procedures for each actor to carry out in order to remove the risk of compromise. Regular training is provided to keyholders to ensure they are prepared to invoke the protocol when required.
- Clearing and settlement: There is a lack of appropriately regulated clearing houses capable or equipped to handle and understand the clearing and settlement of digital token securities and therefore there needs to be an education push as well as clearly defined crypto specific regulations for existing and new clearing entities to begin servicing the DLT industry.
- Proficiency: Firms should hire ultimate designated persons or experts in crypto with relevant experience or training in using blockchain technology. Firms trading in Blockchain tokens should also do their best to understand the structure, governance, technology and economic model for each crypto currency or security token they list. Some can be very complex so there needs to be coordination among ratings agencies, regulators, exchanges and educational or financial training institutions to form standards and understand the information and risks associated to each token.

- Books and records: What is great about blockchain is it is itself a very well kept record of transactions and can serve itself to verify the recordkeeping of exchanges or their balances.
- Compliance system: The sole difference in the compliance is that the UDP and CCO will have to be well versed in crypto specific regulations, risks, obligations and technologies. The compliance system would have to account for digital transactions through internal blockchain monitoring and procedures.
- Know your product requirement: In order to understand the products or tokens they are selling we suggest that independent ratings and market data providers be engaged to inform exchanges, their clients and insurers of the risks and obligations they face as well as the technological risks and limitations involved in each cryptocurrency or tokenized security.

23. FEEDBACK

The Market Data Company innovation practice is working to create the tools insurers, exchanges, custodians, clearing houses, investors and regulators need to better understand crypto currencies and tokenized securities. We are creating a rating standard for blockchains, crypto currencies and tokenized securities so that investors and insurers can easily understand the risks associated to each token along with their obligations both legal and technical. We are also rating exchanges, custodians and hardware wallets based on the security standards, procedures and insurance each have in place. We also aim to help investors and insurers understand what proportion of transactions are fraudulent in addition to verifying and rating the integrity of existing exchanges order books for fake volume. Our goal is to meet the needs of this growing industry with a new generation of crypto specific market data tools and consulting. If anything we have covered requires further elaboration or if IIROC would like to explore further our innovation practice and what we are creating for this industry please feel free to open a dialogue with the Market Data Company Innovation Practice. We are

very excited to see how the regulatory ecosystem changes in the space and we thank IIROC for this opportunity to share our insights.

End



Blockchain Technology
COALITION OF CANADA

Blockchain Technology Coalition of Canada

Canada Not-for-profit Corporation
1081587-0

**Response to Joint Canadian Securities Administrators/Investment Industry Regulatory
Organization of Canada: Consultation Paper 21-402: Proposed Framework for Crypto-
Asset Trading Platforms**



Blockchain Technology

COALITION OF CANADA

To the Investment Industry Regulatory Organization of Canada, and the members of the Canadian Securities Association:

British Columbia Securities Commission;
Alberta Securities Commission;
Financial and Consumer Affairs Authority of Saskatchewan;
Manitoba Securities Commission;
Ontario Securities Commission;
Autorité des marchés financiers;
Financial and Consumer Services Commission (New Brunswick);
Superintendent of Securities, Department of Justice and Public Safety, Prince Edward Island;
Nova Scotia Securities Commission;
Securities Commission of Newfoundland and Labrador;
Superintendent of Securities, Northwest Territories;
Superintendent of Securities, Yukon;
Superintendent of Securities, Nunavut;

We are the Blockchain Technology Coalition of Canada. We're a coalition of Canadian blockchain companies working for smart standards and public policy that protects consumers, supports innovation and keeps jobs in Canada.

We would like to thank you for taking the initiative on this consultation. Please find our answers below to the questions posed in your joint statement.

Our recommendations can be summarized as follows: all suggestions and consultations for regulation requirements should be made only after there is consensus, standardization, and clarification of the terms and concepts surrounding in crypto assets.

Let us be specific. The CSA Staff Notice 46-307 lists the following characteristics of the ICO/ITO market as evidence that they are securities:

- Soliciting a broad base of investors, including retail investors;
- Using the internet, including public websites and discussion boards, to reach a large number of potential investors;
- Attending public events, including conferences and meetups, to actively advertise the sale of the coins/tokens; and
- Raising a significant amount of capital from a large number of investors.

It is our view that these standards can apply to consumer packaged goods just as much as they do to ICOs/ITOs, if “investor” is replaced with the word “customer”.



For example, consider the marketing campaign of Red Bull energy drinks, which involves not only internet (and TV and radio) advertising, but also driving around to different public events and private functions, to actively advertise their product, and to reach a large number of potential consumers. And they've raised a significant amount of capital from a large number of customers.

Obviously Red Bull is not a security. Advertising activities and "significant" fundraising are neither necessary nor sufficient conditions of a securities. Thus, these cannot be standards to judge whether a crypto asset is a security.

There are already legal standards for identifying securities. As per the Ontario Securities Act, there are 16 separate *sufficient conditions* for something to be considered a security. Not one of them is in regards to fundraising or advertising. The other 9 provinces have extremely similar language on the definition of securities as well.

It is our estimation that *none* of the 16 separate sufficient conditions for identifying a security, as outlined in any of the Securities Acts of any province in Canada, apply to crypto assets.

To make an example of one particular case: consider definition (c) from section 1 of the Ontario Securities Act: "title to or interest in the capital, assets, property, profits, earnings, or royalties of any person or company."

However, while it may be possible to design a crypto asset to be consistent with that definition, crypto assets per se do not *necessarily* entitle their holders to the capital, assets, property, profits, earnings, or royalties of any person or company.

Moving on, we do not believe crypto assets are *commodities*, either. The government of Ontario defines a commodity under the *Commodities Futures Act*, as "any agricultural product, forest product, product of the sea, mineral, metal, hydrocarbon fuel, currency or precious stone or other gem, and any goods, article, service, right or interest, or class thereof, designated as a commodity under the regulations." Crypto assets are not any of the listed things.

A *currency* is a *medium of exchange* that is *current*. A *medium of exchange* is any object or service that is bought or sold not because of its value as an object or service (also known as its *use value* or *intrinsic value*), but because other people will exchange objects or services for it. Common media of exchange include metallic coins, bullion or bars of gold, or legal tender paper notes. But any good or service could be a medium of exchange. *Money* is the most commonly accepted medium of exchange.

To be *current* is an accounting term that means capable of being sold (or, synonymously, exchanged) within a short period of time, typically one year. An effective currency, however, is typically saleable much faster than that.



The *Currency Act* of Canada uses the words “currency” and “monetary unit” interchangeably. The Act defines the currency of Canada as a dollar, further specifying that a dollar can be offered for payment only if it is a coin minted by the Royal Canadian Mint or a note printed by the Bank of Canada. The only other legal tender of payment, according to the Currency Act, is using the currencies of other countries.

Neither decentralized ledger technologies, nor crypto assets, are countries. It is also not a currency.

So while crypto assets share many functional similarities with ordinary securities, they differ in a crucial way: they do not *necessarily* represent any claim, or title, or interest, or agreement, or indebtedness, or a subscription to any capital, assets, property, profits, earnings, or royalties; nor are they any commodity or derivative thereof.

Thus, crypto assets are not necessarily securities. And as such, we find the use of the word “investors” in the questions below to be inappropriate and confusing, as opposed to clarifying.

So again, we repeat our request: we ask that you adopt a unified, clear, precise definitional framework for crypto assets. Without clear definitions, we risk not only talking past each other, but also misregulating an entire industry.

We would like to thank you for taking the issue seriously, and for seeking comments from the public. We are available for any further discussions if you so require.

Sincerely,

Ash Navabi
Senior Economist and Director of Policy

Blockchain Technologies Coalition of Canada
129 Spadina Avenue
Suite 200
M5V 2L3
<http://joinbtcc.org>



Blockchain Technology
COALITION OF CANADA



1. Are there factors in addition to those noted above that we should consider?

The most important factor to consider is whether the crypto assets in question are, pursuant to the definition of a security in section 1 (1) of the Securities Act, indeed “*titles to or interest in the capital, assets, property, profits, earnings or royalties of any person or company.*”

There are potentially several tests for this. First, is the proposed “Howey Test” as suggested by the United States Securities and Exchange Commission. The Howey Test has three components: (i) that an investment have been made (ii) in a common enterprise (iii) with the expectation of profit *solely* from the work of a promoter or other third-party. No case involving crypto assets has yet been tried under this standard.

A second, potentially much simpler, test could be whether simply if, under any circumstances, the owner of the crypto asset is entitled to any of the *capital, assets, property, profits, earnings or royalties* in an enterprise. Under this standard, we believe very few ICOs would classify. But it is possible that some would indeed classify as securities even under this standard.

This is why we are proposing a comprehensive nomenclature and taxonomy for all things crypto, in order to better understand what needs oversight and what does not.



2. What best practices exist for Platforms to mitigate these risks? Are there any other substantial risks which we have not identified?

In terms of best practices against insolvency, the [recent situation](#) with Binance is a useful case study. It was revealed that Binance has an emergency fund in case of such situations, which it used to recoup the losses from the hack. In world where crypto assets are not under a shroud of regulatory regime uncertainty, we can expect the existence of insurance companies to provide these services for such platforms.



3. Are there any global approaches to regulating Platforms that would be appropriate to be considered in Canada?

Globally, crypto asset regulations continue to be a quagmire of confusion. Companies operate in a perceived gray area of the law, and so attracting funding, as well as talent, is a challenge. Canada has an opportunity to lead in this regard. And it must begin by being explicitly clear about the terms surrounding crypto assets.

The [United State Library of Congress](#) has a collection of nearly 110 countries that have taken public positions on distributed ledger technologies. However, a cursory analysis reveals that most countries have simply sent a press release warning consumers to be cautious. Many others have confused, inconsistent legislation.

In terms of examples of good legislation, we like this hodgepodge mix:

1. From Latvia, crypto assets are explicitly recognized as not being currency: “The position of the Bank of Latvia and the State Revenue Service is that cryptocurrency is a contractual, not statutory, means of payment that can be used in transactions of exchange. Cryptocurrency cannot be considered as official currency or legal tender because the issuance and use of these instruments remains unregulated and they are not linked to any national currency”;
2. Barbados has promised to not regulate utility tokens (or protocol tokens) as securities;
3. The United States has adopted the “Howey Test” to distinguish between securities and non-securities.

Barbados also has a comprehensive legislation that aims at regulating the security of crypto asset exchanges.

It should be noted that although Canada is a small market from a global perspective, Toronto is quickly becoming an important hub for innovation and investment in DLTs. This is why having the correct approach to regulation in this space is crucial—if regulation is too heavy handed, too burdensome, too anti-business and anti-innovation, firms will simply pack up and leave.

Hence, Canadian regulators need to be writing policy with the utmost attention to detail, specifically having precise and accurate terms. To achieve this requires close collaboration between policy makers and technologists.

Canada’s opportunity to lead can come from a laissez-faire approach to crypto assets, by recognizing that they are nothing new under the sun: insofar as a crypto asset is tied to a title to or interest in another person or entity, it is already a security. This opportunity comes from the fact that currently no other country or jurisdiction has the correct approach to DLTs. No is taking



Blockchain Technology

COALITION OF CANADA

the lead to recognize that DLTs are here to stay, and that they should be a welcome experiment in the financial services industry.

Only this kind of attitude towards policy will engender the climate of entrepreneurship and innovation that can enable many different businesses to succeed at meeting market demand. Hence, Canada must take advantage of this opportunity now.



4. What standards should a Platform adopt to mitigate the risks related to safeguarding investors' assets? Please explain and provide examples both for Platforms that have their own custody systems and for Platforms that use third-party custodians to safeguard their participants' assets.

The first step would be to clarify who is an investor. Is a person who cannot profit *directly* from the earnings of another entity an “investor”? Can a direct analogy be made to persons who give money to online “crowdfunding” campaigns (like for new toys, comic books, music albums, etc.), even though they are not gaining title to the entity they are contributing funds to?

Following clarification on that, security standards for protecting the relationship between Platforms and their partners should not be a matter of centralized regulation. There must be freedom to experiment with different security practices and procedures. Especially in these early days of the technology, forcing a standardization—however broad it may *appear* to be at first—may be a death knell for innovation at best, and (given the infant-like nature of industry in terms of experiences, in the likely event that the adopted standard is later found to be seriously flawed) may invite widespread security vulnerabilities at worst.



5. Other than the issuance of Type I and Type II SOC 2 Reports, are there alternative ways in which auditors or other parties can provide assurance to regulators that a Platform has controls in place to ensure that investors' crypto-assets exist and are appropriately segregated and protected, and that transactions with respect to those assets are verifiable?

The industry is still too new and too experimental to be subjected to a uniform standard of auditing. Experimentation must continue to take place, even in auditing standards. Platform customers will then have incentive to assess the safety features of each Platform. As this is a costly and difficult assessment to make for any retail customer, we anticipate the emergence of a variety of auditing methods and auditors vying and competing for the trust of the retail public, including even a “Yelp”-style user-submitted audit based on ethical hacking principles—if regulators clarify that experimentation in auditing standards are allowed.

This experimentation process would, over time, lead to an emergent standard as customer preferences are revealed after trial and error. But this result is still years away. However, while it took centuries for modern accounting practices to become general for ordinary securities, we expect that with the globalization of information, auditing standards for crypto assets will standardize within five to seven years.

It is also worth noting that there are already *voluntary* disclosure programs being created within the industry. As just one example, messari.io is one such instance of an independent research and information registry.



6. Are there challenges associated with a Platform being structured so as to make actual delivery of crypto assets to a participant's wallet? What are the benefits to participants, if any, of Platforms holding or storing crypto assets on their behalf?

There are many challenges for Platforms in this regard, but the number one reason that a participant would want to keep their crypto assets with the Platform is ease of trading with other crypto assets.



7. What factors should be considered in determining a fair price for crypto assets?

Because it is possible to exchange crypto assets in multiple Platforms, using a variety of methods; and because markets for many crypto assets are very thin (meaning that they have low transaction volumes, enabling high price volatility) by traditional standards, fair prices are more nebulous to determine for crypto assets. The only objective “fair price” standard is the price which a seller agrees to accept from a buyer, and vice versa.

Just like with exchanges for ordinary securities or currencies, a DLT Platform could act as a market maker. That is, a Platform could be an intermediary for transactions. (Note well that it is not necessary for a Platform to be involved in a transaction.) This is consistent with how fair prices are determined in ordinary exchanges.

Regulators should refrain from legislating fair price requirements for Platforms. Platforms face economic incentives to report truthfully the bid and ask spreads, especially if Platforms are subject to competition. If Platform X, acting as a market maker, is misrepresenting bid and ask spreads in a predatory manner, then Platform Y can attract buyers and/or sellers from Platform X by offering more truthful information about spreads.

There is also the possibility that a Platform that exercises unfair market making practices will be exposed by its own participants. As it's currently possible for the same individual to have multiple anonymous stores of crypto assets, the same person can participate as both buyer and seller of the same crypto asset within the Platform, and judge the posted bids and asks with their own bids and asks.

Indeed, as crypto asset markets mature, specialized auditing firms can arise that grade the honesty of Platforms in this very manner. In the meantime, however, the dedication of decentralized yet vigilant crypto asset market participants has been working to keep Platforms fair and honest.

Notwithstanding these and related effects, regulatory fair price requirements could potentially amount to implicit price controls—which could cause a market shortage (in the case of a price maximum), or a market surplus (in the case of a price minimum). In both cases, this creates an incentive for Platform participants to seek to make exchanges elsewhere, in perhaps riskier environments offering less liquidity than a Platform.

To be precise, all 3 of the following factors must be considered for determining a fair price:

1. Did the rightful owner of crypto asset make the decision to sell (to any party) on their own free will and accord;



2. Did the rightful buyer of the crypto asset make the decision to buy (from any party) on their own free will and accord; and
3. If the Platform was acting as market maker, did it truthfully represent the bid and ask to the participants?



8. Are there reliable pricing sources that could be used by Platforms to determine a fair price, and for regulators to assess whether Platforms have complied with fair pricing requirements? What factors should be used to determine whether a pricing source is reliable?

The only reliable pricing sources for a Platform are the bids and asks posted by the buyers and sellers on the Platform in question. Given the thin markets that currently dominate crypto asset exchanges, reliable pricing sources for many crypto assets may be sparse. As well, the anonymous nature of the ownership and distribution of crypto assets makes conventional regulation difficult.

As such, at the current time, we cannot recommend a prima facie rule to determine fair pricing— notwithstanding evidence of coercion against the buyers and sellers, or willful misrepresentation on behalf of the market making Platform.



9. Is it appropriate for Platforms to set rules and monitor trading activities on their own marketplace? If so, under which circumstances should this be permitted?

It is appropriate for Platforms to set rules and monitor trading activities on their own marketplace. Exchanges have already started doing this themselves. Indeed, [Nasdaq reports](#) that seven crypto exchanges are currently using their proprietary monitoring software.



10. Which market integrity requirements should apply to trading on Platforms? Please provide specific examples.



11. Are there best practices or effective surveillance tools for conducting crypto asset market surveillance? Specifically, are there any skills, tools or special regulatory powers needed to effectively conduct surveillance of crypto asset trading?



12. Are there other risks specific to trading of crypto assets that require different forms of surveillance than those used for marketplaces trading traditional securities?



13. Under which circumstances should an exemption from the requirement to provide an ISR by the Platform be considered? What services should be included/excluded from the scope of an ISR? Please explain.

Section 12.2 (1) of the [National Instrument 21-101](#) requires an independent systems review to report “report in accordance with established audit standards”. However, audit standards are still being established for crypto asset Platforms. Determining optimal organization for custody of crypto assets for Platforms, and determining best practices for cyber security and other efficient technologies is still very much a work in progress.

As a result, we recommend a very broad approach to regulating this area. There are various competing standards and protocols in place to prevent and identify cyber security threats; many technologies are possible for organizing and constructing a marketplace; and disaster recovery can be approached from multiple angles, and is also open to experimentation.

That said, a good marketplace will be proactively conducting ISRs on its own accord. Thus, we recommend that marketplaces voluntarily submit ISRs for the next five years, until which time patterns can be observed and perhaps a generalized approach can better be conceived.



14. Is there disclosure specific to trades between a Platform and its participants that Platforms should make to their participants?

Yes. Platforms should be forthright that the so-called “hot wallets” used for trading on the Platform are significantly less secure than the “cold wallets” outside of the Platforms. This security discrepancy is poorly understood by the general public, and it would be a best practice for Platforms to be proactive about educating customers in this way.

Platforms should also disclose what kinds of insurance they have *and don't have* that will affect customer crypto assets. For example, they should be to what extent customer accounts are protected from theft, technical malfunctions, and other disasters.



15. Are there particular conflicts of interest that Platforms may not be able to manage appropriately given current business models? If so, how can business models be changed to manage such conflicts appropriately?

Insofar as Platforms are acting as market makers or dealer-restricted person, they ought to be liable to complying with the same ethics and protocols for those roles in ordinary securities legislation.

Determining and conceiving of the best business models should be the sole prerogative of the entrepreneur. It is, in fact, the entrepreneur who senses Any directives regarding business models would be a recipe for stultification, homogenization, and stagnation of innovation and value creation.



16. What type of insurance coverage (e.g. theft, hot-wallet, cold-wallet) should a Platform be required to obtain? Please explain.

No Platform should be required, by law, to obtain any insurance. Such a requirement is at best unnecessary (as any legitimate and sophisticated platform will be acting in its own and its customers' best interests by knowing what kind of insurance to get, and it would optimally advertise such insurance as a marketing strategy to attract more customers), and at worst a subsidy to rich incumbents while simultaneously a deterrent against new entrants.

Platforms without insurance not only save operations costs, but they also provide more consumer choice. This can allow an uninsured start-up Platform with to compete with larger yet insured incumbents by offering cheaper services. Consumers can then judge for themselves whether the cost savings from the new Platform are worth the increased security risk.



17. Are there specific difficulties with obtaining insurance coverage? Please explain.

Yes. In our experience, insurance companies of *all* types are wary and hesitant to work with any decentralized ledger technologies business. The most common reason is concerns over compliance with anti-money laundering (AML) regulations. Hence, our recommendation is clarity from regulators on how DLT businesses can be compliant with AML regulations.



18. Are there alternative measures that address investor protection that could be considered equivalent to insurance coverage?

Yes. Following the recent example from Binance, the Platform itself can set aside some of its profits (in either fiat currency or crypto assets) in a different, sequestered or partitioned account. Binance calls it the “[Secure Asset Fund for Users](#)”, or SAFU. This could be its emergency re-capitalization fund, which it could deploy to recoup customer losses in the event of a hack.

It’s worth noting that this innovation was developed independently by Binance, without any government mandate or oversight. [And it worked](#). Our belief is that as long as Platforms are allowed to innovate without permission, we will continue to see innovations like this on behalf of customer-centric Platforms.



19. Are there other models of clearing and settling crypto assets that are traded on Platforms? What risks are introduced as a result of these models?

Like many other functions in this space, clearing houses are a particular business model. As in other sections of this response, we worry that setting a national standard for a business model would be a recipe for stultification, homogenization, and stagnation of innovation and value creation



20. What, if any, significant differences in risks exist between the traditional model of clearing and settlement and the decentralized model? Please explain how these different risks may be mitigated.

If Bank X owes \$10,000 to Bank Y, and Bank Y owes \$10,000 to Bank Z, and Bank Z owes \$10,000 to Bank X, then there are two ways the banks can settle their debts with each other. First, each bank can choose to remain quiet with respect to the debts of the whole system, and that money has to change hands several times. This method has several features. First, it requires that each bank have enough cash to cover all of its debt by the end of the day. Second, it requires limited coordination between the banks.

The alternative method to settle these daily debts is for the banks to communicate with each other, and figure out that, on net, no one owes anyone anything. This also has two interesting features. First, the banks now longer have to carry as much cash as they might possibly need to settle their immediate debts with other banks. And second, this requires quite a lot of coordinated communication.

The economic incentives—particularly that of having to carry less cash—greatly favored the second method. Hence, some enterprising men started specializing in this interbank communication and debt clearing. As more and more banks embraced the second option, the interbank communication institutions became known by a new name: *clearinghouses*.

So these clearinghouses developed step by step, as opposed to all at once. They have their roots in New York and London and Edinburgh. They developed organically and through market mechanisms.¹

But then the clearinghouses started consolidating. And soon enough, they were intertwined with the regulatory state. By the 1890s, there was already the New York City Clearinghouse Association (NYCHA). And these centralized information hubs had a problematic downside: they incentivized individual banks to lend out more than they could cover with their deposits, than if the banks were not able to coordinate their lending decisions in concert.

This issue of credit in excess of reserves has a name. It is called *fiduciary media*. And according to some economists, including Ludwig von Mises and the Nobel laureate Friedrich Hayek, the issue of fiduciary media is what enables the business cycle (that is, the cyclical pattern of economic ups and downs). Here is the theory in brief:²

¹ Selgin, George A. (1988). *The theory of free banking: Money supply under competitive note issue*. Rowman & Littlefield pub Inc, pp. 26-29.

² Ebeling, Richard M. (1983). *The Austrian Theory of the Trade Cycle and Other Essays*. Ludwig von Mises Institute.



First, banks issue new fiduciary media. As these media are given out as loans, they in effect lower interest rates. This has two conflicting effects: one, investors who get this new fiduciary media get to use this money to start (long-term) investment projects. And two, the lower interest rates induce savers and consumers to save less and spend more money in the present. As this state of affairs represents both an increase in consumption *and* production, this is seen as boom times for the economy.

Unfortunately, this activity creates an intertemporal discoordination: the investors are making goods for the long term, but the consumers are spending all their money in the short term. Sooner or later, this mismatch between what investors are making and what producers are spending their income on, makes it difficult for investors to sell their inventory. They must liquidate: halt production, fire employees. The beginning of a bust.

This centralization of credit—aided and abetted by clearing houses—creates an increased risk of systemic failure.

Hence, by decentralizing the clearinghouse settlement model, crypto asset Platforms are limiting the issue of new credit. By limiting the issue of new credit, the booms will be smaller, as will the busts. The risks of systemic failure are reduced.



21. What other risks are associated with clearing and settlement models that are not identified here?

The existence of a powerful regulatory body enables what economists call “regulatory capture”. That is, the rise of a cozy, “revolving door” relationship between the regulator and the regulated. In the case of the New York clearinghouses, despite laws against over-issuing credit, because of the regulator’s cozy relationship with the clearinghouse association that the law was openly flaunted.

By setting strict, yet convoluted standards that *require* industry expertise, the regulator is effectively asking to be “captured” by the special interests.³

The only remedy against this is by strictly limiting the regulatory powers to begin with, by limiting the scope and scale of what can be regulated.

³ McSherry, Bernard and Berry K. Wilson. "Overcertification and the NYCHA's Clamor for a NYSE Clearinghouse." *The Quarterly Journal of Austrian Economics* 16, No. 1 (Spring 2013): 13–26. <https://mises.org/library/overcertification-and-nychas-clamor-nyse-clearinghouse>



22. What regulatory requirements, both at the CSA and IIROC level, should apply to Platforms or should be modified for Platforms? Please provide specific examples and the rationale.

The only requirements should be ethical: maintaining fiduciary duties, revealing material information, etc., as outlined above.

The CSA and IIROC should avoid any and all regulations of business plans, cybersecurity strategies, and other operational and capital expenditures. These are highly sensitive areas that determine the growth and international competitiveness of Canada's crypto asset Platforms. We recommend as light a touch as possible, in order to allow innovation without permission.

Otherwise, we risk irreversibly damaging our burgeoning high tech industry, and dooming it to the stultification, homogenization, and stagnation of innovation and value creation.

National Digital Asset Exchange Inc.
 #200, 815- 8th Ave. SW, Calgary, AB T2P 3P2
 Toll Free: 1-800-727-NDAX (6329)

May 30, 2019

SENT BY ELECTRONIC MAIL

Alberta Securities Commission Financial and Consumer Affairs
 Autorite des marches financiers
 Authority of Saskatchewan
 British Columbia Securities Commission
 Financial and Consumer Services Commission (New Brunswick)
 Manitoba Securities Commission
 Nova Scotia Securities Commission
 Ontario Securities Commission
 Securities Commission of Newfoundland and Labrador
 Superintendent of Securities, Department of Justice and Public Safety, Prince Edward Island
 Superintendent of Securities, Northwest Territories
 Superintendent of Securities, Nunavut
 Superintendent of Securities, Yukon

c/o The Secretary Ontario
 Securities Commission
 20 Queen Street West
 22nd Floor, Box 55
 Toronto, Ontario M5H 3S8

Fax: 416.593.2318

via: comments@osc.gov.on.ca

Me Anne Marie Beaudoin
 Corporate Secretary
 Autorite des marches financiers
 800, square Victoria 22e etage
 C.P. 246, tour de la Bourse
 Montreal, Quebec H4Z 1G3

Fax: 514.864.6381

via: consultation-en-
 cours@lautorite.qc.ca

IIROC
 Victoria Pinnington
 Senior Vice President, Market
 Regulation
 Investment Industry Regulatory
 Organization of Canada
 Suite 2000, 121 King Street W.
 Toronto, Ontario M5H 3T9
 via: vpinnington@iroc.ca

RE: Consultation Paper 21-402 Proposed Framework for Crypto-Asset Trading Platforms (the “Consultation Paper”)

National Digital Asset Exchange Inc. (“NDAX”) would like to thank the Canadian Securities Administrators and the Investment Industry Regulatory Organization of Canada (collectively the “Regulators”) for the opportunity to participate and provide feedback to the Consultation Paper. We look forward to collaborating with the Regulators to bring forward this new paradigm in the financial industry. For simplicity and clarity, we seek to include all crypto assets under the scope of our comments to the Consultation Paper. From day one, NDAX’s mission has been to bring more traditional financial frameworks to the crypto asset industry for the benefit and security of investors. NDAX has led the way in being the first Platform to establish a strong Canadian banking relationship; offering a frictionless experience for getting clients’ money in and out of crypto assets. Advanced trading tools, institutional-grade custody, and 24/7 live customer service are key

factors that set NDAX apart from its competitors. We take pride in our exceptional client service, data protection and security of assets.

Please find to follow our comments to the Consultation Paper.

1. *Are there factors in addition to those noted above we should consider?*
 - a. Whether investors' fiat currencies are pooled together with those of other investors and with the assets of the Platform.
 - b. How cold storage is protected? Who has access to cold storage? How many signatures are required to access it? Can one individual access it in the case of an emergency?
 - c. If the Platform has insurance on its hot wallet.
 - d. The resiliency of Business Continuity Plan, how often it is updated, and how extensively possible are issues covered.
 - e. How is the hiring, selection and screening of new employees done? Do they all go through a police check and other available verification processes, to prevent the possibility of internal fraud?
 - f. At this point, the majority of crypto asset trading is speculative. We encourage the Regulators to enforce rules across the board to keep a level playing field.
 - g. Rule enforcement and prosecution in accordance with applicable law, to deter bad players from entering the market and violating the rules.

2. *What best practices exist for Platforms to mitigate these risks? Are there any other substantial risks which we have not identified?*
 - a. There should be no abusive trading of any kind on Platforms. Such practices (i.e. "wash trading") have been used by many crypto asset trading platforms to enhance their Platform's popularity by creating artificial volumes.
 - b. Registered exchanges should be held to a higher standard of diligence, including insurance and audits.
 - c. Custody of crypto assets on Platforms has been a major issue of concern. With new developments in the space, it is now one of the major topics up for discussion. Protection and segregation of investors' crypto assets can be addressed through custodial services. NDAX was able to resolve this issue with the implementation of a secure storage system provided by world-renowned third-party service provider Ledger Vault. Ledger Vault provides multi-signature access and is deemed one of the most reliable solutions for crypto asset storage and safekeeping. Strong internal controls for custody need to be into place and clearly outlined in a Platform's Policies and Procedures manual (the "P&P").
 - d. Processes, policies and procedures – strong internal controls need to be established with clear segregation of duties between departments. All processes must be clearly outlined in the P&P and regularly updated to reflect any changes in regulations or internal business structure.
 - e. A Business Continuity Plan must be established, covering all issues that may arise and providing a clear and precise action plan in the case of an emergency. Unforeseen circumstances such as natural disasters should be outlined in detail, including an indication of an alternative workplace, call tree established, with roles and responsibilities assigned.
 - f. All employees of the firm need to go through extensive background checks through a reliable third-party service provider.

- g. Investors' assets may be at risk in the event of a Platform's bankruptcy or insolvency – an issue that can be mitigated through full segregation of the Platform's operating capital and investors' assets. This can be addressed through the proper custody of crypto assets as well as a segregation of the Platform's and investors' fiat accounts.
- h. Investors may not have important information about the crypto assets that are available for trading on the Platform – Platforms should be responsible for providing “full, true and plain disclosure” about the assets that are trading on the platform, as well as trading volume and historical data.
- i. Investors may not have important information about the Platform's operations – all of the functions should be clearly outlined on the Platform's website. All fees should be disclosed to investors prior to the use of the Platform and should be fully disclosed when placing a trade.
- j. Investors may purchase products based on their independent research as no additional recommendations are provided by the trading platform – full risk disclosure should be provided to clients prior to executing a trade on the Platform. Risk disclosures should be published on the website, and the client should read and acknowledge it at the account opening stage. Service provided to the clients through crypto asset trading platforms is equivalent to the service currently provided by discount brokerages, where no assurance of suitability of the assets purchased is provided.
- k. Conflicts of interest may not be appropriately managed – strong internal policies and procedures to manage conflict of interest should be established. If the Platform acts as a principal to the trade fulfilling their market-making responsibility, such information should be disclosed at the account opening stage.
- l. Manipulative and deceptive trading may occur – proper internal controls should be put into place for monitoring trading activities regardless of the source. Automated brakers should be put in place to prevent manipulative and deceptive trading. All such functions must be regularly tested and monitored to ensure the adequacy and efficiency of the systems.
- m. There may not be transparency of order and trade information – the Platform should show the most up to date order book for every trading pair available for purchase and sale. An order book must show the current price and the quantity offered at that price. Additional statistics should be shown on the trading platform, such as the last price, 24H change, 24H volume, 24H high, 24H low and buy and sell volume.
- n. System resiliency, integrity and security controls may be inadequate - resiliency of the trading platform must be frequently tested. A dedicated technical team should be testing the trading platform regularly for the adequacy of security controls and vulnerabilities. Cybersecurity risks must be taken very seriously and fully understood by the technical team behind the platform. Strong safeguards against risks are of utmost importance.
- o. To prevent unauthorized access and protect participants' confidential information, access to such information should be limited internally and given only to employees required to have such access to adequately perform their duties. Two-factor identification (2FA) should also be enabled in all programs, used in day to day operations where that program permits. Additionally, it is important to select third-party service providers with careful due diligence, ensuring their cybersecurity policies and procedures are in line with that company's standards.
- p. Above all, any Platform dealing in crypto assets, cryptocurrencies or crypto tokens of any kind should be subject to the same or similar requirements as existing regulated securities dealers and marketplaces. This allows for certainty to both investors and businesses.

3. *Are there any global approaches to regulating Platforms that would be appropriate to be considered in Canada?*

The proposed regulations in the United States and guidance that were issued by the US Securities and Exchange Commission are most relevant to the way the Canadian market operates and could be used as guidance for new regulations in Canada.

In the new and rapidly changing environment of crypto assets, crypto asset trading Platforms are becoming a very popular and easy way for investors to buy and sell crypto assets. Investors prefer to utilize Platforms over crypto ATMs as they provide greater transparency, convenience, and lower fees. Regardless of one's location, a participant can visit multiple marketplaces, compare trading options, pricing and volumes available to make decisions suitable for them. With no regulatory guidance in place, however, Canadians can easily be taken advantage of. Several fraudulent exchanges operate in the space and, with hundreds of millions of dollars lost in the last few years, it's time for crypto asset regulation that will not stifle innovation.

With people around the world utilizing crypto assets for buying and selling goods online, transferring money to relatives overseas, or simply for general investing purposes, it is evident cryptocurrency is here to stay. As numerous companies have begun to choose Initial Coin Offerings (ICOs) over more traditional ways of fundraising, there is a burgeoning market for crypto assets, and new regulations are needed.

Crypto asset trading platforms provide a marketplace for listing, buying and selling crypto assets. This may lead to listing ICOs and helping new companies enter the market. Crypto asset trading platforms register their clients and perform their due diligence through the client onboarding process, fulfilling the role of a dealer. Platforms normally do not perform suitability assessments, as they operate in the same way as a discount brokerage and not a full-service brokerage. Also, the majority of Platforms provide crypto asset storage solutions to their clients, acting as a custodian for crypto assets. Based on the hybrid functions that crypto asset trading platforms perform, they likely fall into more than one category such as Alternative Trading System (ATS), Exchange, Discount Brokerage, and in some cases, Custodian.

You can also refer to the sandbox implemented in Switzerland referenced in the following links

<https://www.news.admin.ch/newsd/message/attachments/55153.pdf>

<https://www.finma.ch/en/authorisation/fintech/>

<https://switzerlandblog.ey.com/2019/03/15/updates-on-the-swiss-fintech-license-and-sandbox/>

4. *What standards should a Platform adopt to mitigate the risks related to safeguarding investors' assets? Please explain and provide examples both for Platforms that have their custody systems and for Platforms that use third-party custodians to safeguard their participants' assets.*

All clients trading on a crypto asset trading platform should have Direct Electronic Access to such Platform. Before receiving such access, all clients should read and acknowledge the terms of the Platform's User Agreement, Privacy Policy, Risk Disclosure and provide essential information to satisfy KYC requirements.

It is critical that Platforms have strict internal controls and automated braker systems, as the trading is done on a twenty-four hours a day, seven days a week basis; requiring robust automated system monitoring.

The industry is still evolving, and major industry players are collaborating to determine the most secure practices to safeguard investors' assets. The digital nature of assets makes them susceptible to cybersecurity threats. NDAX recommends at least 95% to 98% of crypto assets stored in cold wallets that are air-gapped and have multi-signature authority. Best practices for managing hot wallets governed by agreed-upon policies and procedures should be uniquely tailored to crypto assets under a broker-dealer license.

5. *Other than the issuance of Type I and Type II SOC 2 Reports, are there alternative ways in which auditors or other parties can assure regulators that a Platform has controls in place to ensure that investors' crypto-assets exist and are appropriately segregated and protected and that transactions with to those assets are verifiable?*

Independent third-party audits could be sufficient to ensure that investors' crypto assets exist and are appropriately segregated and protected. Another approach would be to provide periodic proof-of-reserve.

6. *Are there challenges associated with a Platform being structured to make actual delivery of crypto assets to a participant's wallet? What are the benefits to participants, if any, of the Platforms, holding or storing crypto assets on their behalf?*

There are no direct challenges associated with a Platform making actual delivery of crypto assets to a participant's wallet. Centralized platforms need to act as a custodian to participants' funds briefly to ensure the execution of the trade. Another reason for a Platform to temporarily hold customer funds is to comply with FINTRAC's regulatory framework and monitor for money laundering, terrorist activity financing and fraud prevention. Once these conditions are met, a Platform can deliver assets quickly to participants' wallets. Benefits to participants keeping assets on a Platform include easily accessible crypto assets for trading, no requirement to pay withdrawal or mining fees upon delivery to a private wallet, the convenience of not having to worry about custody of their assets, and the challenges associated with misplacing private wallet keys, theft, etc.

7. *What factors should be considered in determining a fair price for crypto assets?*

Generally, the free market will determine fair pricing for crypto assets. However, the market cannot be hindered by manipulation to do so. Some Platforms have invested in security and systems, creating appropriate liquidity to mimic current regulatory standards as near possible and, therefore, should be looked upon with more favourable regulatory standards.

8. *Are there reliable pricing sources that could be used by Platforms to determine a fair price, and for regulators to assess whether Platforms have complied with fair pricing requirements? What factors should be used to determine whether a pricing source is reliable?*

Major financial data feeds such as Bloomberg, NASDAQ and others have been utilizing the services of financial services providers to disseminate information on crypto assets. These indices may be a good place to start. As the industry evolves and liquidity increases, we expect the markets and its participants will dictate fair pricing.

9. *Is it appropriate for Platforms to set rules and monitor trading activities on their marketplace? If so, under which circumstances should this be permitted?*

Until such time that appropriate marketplace surveillance is available, Platforms will need to be trusted to monitor their activities and should employ well-trained and highly qualified compliance and operations personnel to assist in doing so.

10. *Which market integrity requirements should apply to trade on Platforms? Please provide specific examples.*

Platforms should abide by integrity requirements set similar to traditional markets. Platforms should have policies and procedures towards abusive trading, short selling, best execution, trading in the marketplace, and others based on each Platform's offering.

11. *Are there best practices or effective surveillance tools for conducting crypto asset market surveillance? Specifically, are there any skills, tools or special regulatory powers needed to effectively conduct surveillance of crypto asset trading?*

We believe that there are no crypto asset market surveillance tools currently developed that can adequately perform market surveillance, supervision and oversight. The industry is changing rapidly, and several widely used equity marketplace surveillance providers may expand their offerings to the crypto space.

12. *Are there other risks specific to trading of crypto assets that require different forms of surveillance than those used for marketplaces trading traditional securities?*

Most surveillance tools currently used for traditional marketplaces are tailored to securities trading and contain the core functionalities that should be sufficient to monitor the crypto assets industry. Additionally, Platforms should be mandated to adopt blockchain forensic tools to monitor for money laundering, terrorist financing, and other criminal activities.

13. *Under which circumstances should an exemption from the requirement to provide an ISR by the Platform be appropriate? What services should be included/excluded from the scope of the ISR? Please explain.*

All platforms should be subject to an ISR, with some exemptions. The crypto market is relatively new, and so are the Platforms. The Platforms will require a transitional period to work with regulators, auditors, and their technology to meet the ISR standards.

14. *Is there disclosure specific to trades between a Platform and its participants that Platforms should make to their participants?*

Disclosure specific to trades between a platform and its participants should be made during the account opening process and not on a trade by trade basis. The Canadian market has extremely low liquidity, and platform acting partially as a counterparty to the trade is almost always granted. The combination of being a market dealer registrant, complying with the fair pricing model, and providing full disclosure during the account opening stage should be considered satisfactory.

15. *Are there particular conflicts of interest that Platforms may not be able to manage appropriately given current business models? If so, how can business models be changed to manage such conflicts appropriately?*

Yes, promoting certain coins above others and being both a broker-dealer and a marketplace would be viewed as a conflict of interest as measured by traditional standards. Such conflicts can be easily managed by full segregation of departments and responsibilities, effectively creating a “Chinese Wall” where required.

16. *What type of insurance coverage (e.g. theft, hot-wallet, cold-wallet) should a Platform be required to obtain? Please explain.*

Insurance coverage for loss of crypto assets through theft, fraud, and hot wallets threats should be governed by the business limited insurance policy. Having strong internal governance will dictate the Platform’s ability to manage risk and determine the level of insurance coverage. Mandating cold storage solutions to have a minimum of 95% of the total assets, third-party audit reports and strict access policy should allow for lower insurance requirements.

17. *Are there specific difficulties with obtaining insurance coverage? Please explain.*

Yes, there are a lot of challenges surrounding insurance coverage for crypto assets. The crypto marketplace is still evolving and there is a limited number of insurance providers who are willing to provide insurance coverage to crypto asset trading platforms. These insurance providers can dictate

higher premiums, which prevent most of the Platforms to obtain coverage. We urge regulators to work with platforms to create a framework that reduces risks and protects the client's and Platforms' assets.

18. *Are there alternative measures that address investor protection that could be considered that are equivalent to insurance coverage?*

The Canadian Investor Protection Fund (CIPF) would apply if a Platform became registered with IIROC. As an alternative, the platform could adopt the Binance platform model by using a percentage of trading fees towards a self-insurance policy, which proved to be successful in their latest cyber attack.

19. *Are there other models of clearing and settling crypto assets that are traded on Platforms? What risks are introduced as a result of these models?*

There are currently no models of clearing and settling crypto assets traded on Platforms. Crypto asset platforms are unique in such a way that Platforms generally act as both the facilitator between counterparties and the custodian for their funds. Platforms typically maintain an internal ledger that audits and maintains a record of all transactions that occur between parties, while the Blockchain acts as an open distributed ledger that can be used to audit transactions in & out of the Platform. NDAX understands the risks associated with Platforms maintaining internal ledgers and therefore propose that Platforms be required to register as a broker-dealer with designated securities regulators where they are obligated to produce audited policies and procedures to accurately handle clearing and settlement of the Platform's internal ledger. The Blockchain will then act as the public validator by providing the records of deposits and withdrawals.

20. *What, if any, significant differences in risks exist between the traditional model of clearing and settlement and the decentralized model? Please explain how these different risks could be mitigated.*

Having a hybrid model where the Blockchain, along with the Platform's policies and procedures maintain their internal ledger, should be sufficient to address the risk associated with not having third-party clearing and settlement house. Additionally, please see the response to Q19.

21. *What other risks could be associated with clearing and settlement models that are not identified here?*

Ultimately, there are no designated regulatory body monitoring transactions. Please see responses to Q19 and Q20.

22. *What regulatory requirements (summarized at Appendices B, C, and D), both at the CSA and IIROC level, should apply to Platforms or should be modified for Platforms? Please provide specific examples and the rationale.*

1. Exemption for clearing and settlement house as justified in the response above – Q19 and Q20
2. Exemption from third-party custody
3. Broker-dealer license with exemption to the listing and issuance of securities requirements

We appreciate the opportunity to provide feedback to the Canadian Regulators and look forward to hearing recommendations from the industry. Investor protection, security and certainty are of utmost importance to the NDAX team. Should you have any questions or require further feedback, please do not hesitate to contact us for additional information.

Date: 31 May 2019

**Canadian Securities Administrators/Investment Industry Regulatory Organization of Canada
Joint Consultation Paper 21-402: Proposed Framework for Crypto-Asset Trading Platforms**

Comments from the National Crowdfunding & Fintech Association of Canada (NCFA)

Introduction

The NCFA welcomes this consultation. We are in favour of the regulation of crypto asset platforms as long regulation is:

- principles based and outcomes focused,
- proportionate,
- risk based,
- not unduly limiting of innovation and competition,
- consistent with global regulation and international best practices,
- fully harmonized across Canada, and
- technology neutral to the extent reasonably possible.

Whether Platforms are trading securities or not, they should be covered by KYC/AML/CFT legislation. Apart from that, regulators should be nimble yet cautious as global approaches remain unclear and the landscape remains unsettled. We also know that overly prescriptive regulation can severely limit innovation and competition. At this stage, less is more.

Questions:

1. Are there factors in addition to those noted in Part 2 that we should consider?

- We have nothing to add to the remarks of other commenters.

2. What best practices exist for Platforms to mitigate the risks outlined in Part 3? Are there any other significant risks which we have not identified?

- ASIFMA Best Practices for Digital Asset Exchanges June 2018

(<https://www.lw.com/thoughtLeadership/ASIFMA-best-practices-digital-asset-exchanges>)

- Cryptocurrency security standard (<https://cryptoconsortium.github.io/CCSS/Details/>)

- <https://www.bitcoinmarketjournal.com/ico-investment-best-practices/>

- ISDA CDM on representing derivatives trade events and processes

(<https://www.isda.org/2019/03/20/isda-publishes-cdm-2-0-for-deployment-and-opens-access-to-entire-market/>)

The risks have been highlighted in the CP, but we think that regulators should give equal status to the opportunities (as well as the threats) – for example: democratisation of investment opportunities, the advantages that come from dis-intermediation, more product/services innovation and efficiencies, access to wider sources of capital, more liquidity, and so on.

3. Are there any global approaches to regulating Platforms that are appropriate to be considered in Canada?

- We prefer the less restrictive and prescriptive (and more supportive and collaborative) approaches in

the United Kingdom and Germany, which are clearly working.

4. What standards should a Platform adopt to mitigate the risks related to safeguarding investors' assets? Please explain and provide examples both for Platforms that have their own custody systems and for Platforms that use third-party custodians to safeguard their participants' assets.

- Market participants have responded to this question. Standards should vary depending on the size, functions, risks, etc of each Platform. Each platform should have a duty to protect the digital assets, security of its users, and their data; however following regulatory standards through on-boarding should remain the responsibility of the custodian(s) of capital.

- We note that for permissioned/centralized issues, there is lower custody risk as the issuer can freeze when potential threats occur, burn and reissue if the threat is confirmed.

5. Other than issuance of Type I and Type II SOC 2 Reports, are there alternative ways in which auditors or other parties can provide assurance to regulators that a Platform has controls in place to ensure that investors' crypto-assets exist and are appropriately segregated and protected, and that transactions with respect to those assets are verifiable?

- For a period of time, finding enough competent internal and external auditors or other sources of assurance may be tough. We assume that CSA is collaborating with the relevant accounting and auditing bodies in Canada and internationally on education and standards. It may be that auditors will need to retain the support of skilled persons to provide them with the necessary confidence to sign off on the Reports, or should perhaps be able to rely on an ISR. The comments of the CPA in this consultation are helpful. Auditors may also collect a list of "best practices" to understand what common virtual checklists may include throughout the vetting/assurance of a Platform.

- Having said that, we understand that some auditors are today offering these services in Canada and are competent to do so.

6. Are there challenges associated with a Platform being structured so as to make actual delivery of crypto assets to a participant's wallet? What are the benefits to participants, if any, of the Platforms holding or storing crypto assets on their behalf?

- These questions are better answered by market participants, but one obvious benefit is that holding or storing crypto (safely) should reduce the costs (and risks) of moving the assets on and off the Platform.

7. What factors should be considered in determining a fair price for crypto assets?

- We suggest that regulators should usually leave this question to the market, subject to full disclosure and regulatory and audit oversight.

8. Are there reliable pricing sources that could be used by Platforms to determine a fair price, and for regulators to assess whether Platforms have complied with fair pricing requirements? What factors should be used to determine whether a pricing source is reliable?

- Market participants have responded to this question in this consultation.

9. Is it appropriate for Platforms to set rules and monitor trading activities on their own

marketplace? If so, under which circumstances should this be permitted?

- Yes, subject to regulatory access and oversight, where the activities are relatively straightforward, and the Platforms are relatively small and low risk. As the risks increase, so will the regulatory requirements and oversight. Platforms that have a built in trust systems (eg, smart contracts) or hashes of transactions, or any other type of verifiable audit trail will require less oversight as their process will be more transparent.

10. Which market integrity requirements should apply to trading on Platforms? Please provide specific examples.

- This question is best answered by market participants.

11. Are there best practices or effective surveillance tools for conducting crypto asset market surveillance? Specifically, are there any skills, tools or special regulatory powers needed to effectively conduct surveillance of crypto asset trading?

- This question is best answered by market participants.

12. Are there other risks specific to trading of crypto assets that require different forms of surveillance than those used for marketplaces trading traditional securities?

- Yes (dis-intermediation, global reach, speed, highly technical nature of the business, security issues, anonymity of wallets – FATF guidance on a risk-based approach for the regulation of virtual asset service providers is coming, and FinCEN is here – <https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf>. Recent FINTRAC Guidance on the Interpretation of Money Services Business is also broadly helpful.

13. Under which circumstances should an exemption from the requirement to provide an ISR by the Platform be appropriate? What services should be included/excluded from the scope of the ISR? Please explain.

- Once again, it depends on the risks to the regulatory objectives. Each situation must be evaluated on its own facts.

14. Is there disclosure specific to trades between a Platform and its participants that Platforms should make to their participants?

- As above, question 13.

15. Are there particular conflicts of interest that Platforms may not be able to manage appropriately given current business models? If so, how can business models be changed to manage such conflicts appropriately?

- None that we are aware of.

16. What type of insurance coverage (e.g. theft, hot-wallet, cold-wallet) should a Platform be required to obtain? Please explain.

- Platforms should obtain insurance that is adequate/ appropriate. The appropriate nature and extent of the insurance will vary with the circumstances, taking into account the nature of the risks, other forms of risk transfer and risk mitigation mechanisms used, whether an insured custodian is involved, etc.

17. Are there specific difficulties with obtaining insurance coverage? Please explain.

- Yes. Most insurers and brokers have inadequate experience with crypto assets, cyber security, DLT, etc, so insurance cover (if available at all) is unlikely to be wholly adequate at this time and may cost too much. CSA guidance might be helpful here, drawing on global sources. (We note the more positive comments in the submission of the Wall Street Blockchain Alliance.)

- One option is to start with eg D&O insurance and add to that as the insurers become more confident.

18. Are there alternative measures that address investor protection that could be considered that are equivalent to insurance coverage?

- Yes. EG, security bonds, guarantees, letters of credit, catastrophe bonds (being used in an ever widening variety of situations), ring-fenced capital, investor's own insurance, an industry fund.

19. Are there other models of clearing and settling crypto assets that are traded on Platforms? What risks are introduced as a result of these models?

- We agree with what CSA/IIROC propose in this section.

- We understand that in a permissioned/centralized Platform, which will be standard for all regulated securities exchanges, clearing and settlement will be instant, enabled by initial security token programming (assuming that the AML/KYC requirements are met by both the seller and the buyer).

20. What, if any, significant differences in risks exist between the traditional model of clearing and settlement and the decentralized model? Please explain how these different risks could be mitigated.

- There are increased risks in a decentralized model, but it appears that these can be mitigated. It is crucial that the programming of the securities ensures that CFT/AML/KYC requirements will be met.

21. What other risks could be associated with clearing and settlement models that are not identified here?

- Best answered by market participants.

22. What regulatory requirements (summarized at Appendices B, C, and D), both at the CSA and IIROC level, should apply to Platforms or should be modified for Platforms? Please provide specific examples and the rationale.

- This would be an enormous (but valuable) exercise which the NCFE is not resourced to perform. We support calls for a collaborative ongoing discussion about this (and regulation generally) among regulators and market participants.

Sincerely

Craig Asano, CEO
On behalf of NCFE

About NCFA

The **National Crowdfunding & Fintech Association** (NCFA Canada) is a financial innovation ecosystem that provides education, market intelligence, industry stewardship, networking and funding opportunities and services to thousands of community members and works closely with industry, government, partners, and affiliates to create a vibrant and innovative fintech and funding industry in Canada. For more information, please visit: ncfacanada.org

May 31, 2019

Via Email

Alberta Securities Commission
British Columbia Securities Commission
Financial and Consumer Affairs Authority of Saskatchewan
Manitoba Securities Commission
Ontario Securities Commission
Autorité des marchés financiers
Financial and Consumer Services Commission (New Brunswick)
Superintendent of Securities, Department of Justice and Public Safety, Prince Edward Island
Nova Scotia Securities Commission
Securities Commission of Newfoundland and Labrador
Superintendent of Securities, Northwest Territories
Superintendent of Securities, Yukon
Superintendent of Securities, Nunavut
Investment Industry Regulatory Organization of Canada

Re: Bitvo Global Inc. Comments on Consultation Paper 21-402

In response to the joint Canadian Securities Administrators (“CSA”) and Investment Industry Regulatory Organization of Canada (“IIROC”) Consultation Paper 21-402 – *Proposed Framework for Crypto-Asset Trading Platforms* (“CP 21-402”), please find the commentary of Bitvo Global Inc. (“Bitvo”) below.

Background

Thank you for providing us the opportunity to comment on CP 21-402 and the proposed regulatory framework for the regulation of cryptocurrencies by the CSA and IIROC (the “Framework”).

Bitvo operates a cryptocurrency exchange platform to facilitate the purchase, sale and trading of cryptocurrencies for fiat currencies and cryptocurrencies for other cryptocurrencies. Bitvo is committed to ensuring that its exchange platform operates in a fair and orderly manner and the security of its customers and their funds are a top priority.

We are in favour of regulation that thoughtfully addresses the unique risks and characteristics of cryptocurrencies, including security and custody. There is considerable uncertainty under securities laws in Canada as to when or whether a certain cryptocurrency may or may not be considered a “security” under such laws. Traditional securities law analysis was not developed with consideration of the unique characteristics of various types of cryptocurrencies, which has led to uncertainty in Canada, in the United States and internationally as it relates to the application of securities laws to a given cryptocurrency. Without a clear analytical framework to determine whether a cryptocurrency is a security under applicable securities laws in Canada, the Framework seeks to solve the question “how should certain cryptocurrencies be regulated?” without first defining which cryptocurrencies ought to be the subject of the regulation.

The nature of cryptocurrency is diverse. A crypto-asset could be a digitized traditional security, a cryptocurrency used for payment purposes, a utility token, a stablecoin, or another novel use of a digital asset utilizing cryptography protocols to solve a particular problem. There may be different risks inherent in a crypto-asset, or the dealing with a crypto-asset, depending on the nature of the cryptocurrency itself.

The risks inherent in a crypto-asset that is a digitized traditional security will be substantially similar if not the same as those surrounding traditional securities. The application of securities laws to such cryptocurrencies is consistent with the purpose of, and intent behind, such laws. The application of securities laws to a cryptocurrency used for payment purposes may quickly render such payment method unusable. Regulation that does not appropriately contemplate the unique and varied nature of cryptocurrencies may restrict Canadian individuals and companies from participating in global innovation as it relates to the prolific utility, in payments and otherwise, that can be made available through cryptocurrency technology.

As a result, while Bitvo is in favour of a regulatory framework that is implemented with a view to mitigate risk and promote innovation, the Framework as proposed in CP 21-402 does not appropriately achieve that balance for cryptocurrencies that are not digitized traditional securities. The government should consider a standalone regulatory regime developed specifically for platforms dealing exclusively with cryptocurrencies that fall outside of the spectrum of traditional securities (including those that would not be considered securities under the current securities law analysis, which may not be governed under the Framework as proposed). It may be appropriate for this regulatory regime to be administered and overseen by a separate federal regulatory body with a cryptocurrency specific mandate.

Please find our view on certain of the consultation questions posed in CP 21-402 below. For cryptocurrencies that operate as digitized traditional securities, which by their nature and characteristics reflect a traditional security except in the sense that they have been digitized through the use of blockchain and cryptography, the current securities laws in place are appropriate and currently apply, as they have been developed to address the risks associated with such securities. The responses below relate to cryptocurrencies that would not properly be considered digitized traditional securities.

Consultation Paper Questions

1. Are there factors in addition to those noted in Part 2 that we should consider?

A key factor that is missing from Part 2 is the consideration of the cryptocurrencies offered by the platform or broker. The nature of such cryptocurrencies will vary the risk profile of such assets, which, in turn, might require that regulation applies differently to cryptocurrencies with different risk profiles. As discussed above, cryptocurrency that is a digitized traditional security, for example, would be unlikely to require significant (if any) changes from the current securities law regime. The current securities law regime may be unworkable to apply to a cryptocurrency that is a utility token or cryptocurrency used for payments and the application of such laws would render the utility token or payment-based cryptocurrency unusable by Canadians and Canadian businesses.

2. What best practices exist for Platforms to mitigate the risks outlined in Part 3? Are there any other significant risks which we have not identified?

In order to effectively safeguard customers' funds, Platforms should operate on a full reserve basis with segregated accounts, meaning that customers' funds are held separately from the Platform's funds and must at all times be equal to the sum total of the aggregate amount in all customers' accounts. This

should be true for the total value of all funds as well as the value of each asset class (i.e. Canadian dollars, Bitcoin, etc.).

To further safeguard crypto assets held on customers' behalf, Platforms should hold the majority of these assets in "Cold Storage" (offline, not connected to the Internet). Only amounts required to facilitate daily trading liquidity on the Platform and withdrawal requests made by customers should be held in "Hot Storage" (online, connected to the Internet). Access to both Hot and Cold Storage should be restricted to a small group of trusted individuals.

Best practice Cold Storage procedures include locating Cold Storage offsite at a secure third-party location, requiring multiple signatures of a group of trusted individuals to access and implementing secure backup and disaster recovery protocols.

Appropriate information disclosure can also help mitigate risks facing participants when they are looking for a Platform on which to trade. Platforms should publicly disclose information about the Platform that allows participants to educate themselves and effectively choose Platforms they would like to transact with. Platforms should also provide information about the crypto-assets they list, including reference to the assets' websites, whitepapers, etc. as applicable. All fees charged by a Platform should be transparent, easy to understand and easy to locate on a Platform's website.

Prior to launching to the public, a third-party security and threat assessment should be conducted on the Platform's website and associated infrastructure. Any identified deficiencies should be addressed prior to offering services to the public and the Platform should be vigilant in ensuring the ongoing safety of its infrastructure and of crypto-assets in its storage.

3. Are there any global approaches to regulating Platforms that are appropriate to be considered in Canada?
--

Bermuda implemented a *Digital Asset Business Act* (the "DABA") to govern a digital asset business. The definition of a "digital asset business" under the DABA includes a business that issues, sells or redeems cryptocurrencies, a business that operates a payment service provider business that utilizes cryptocurrencies, a business that operates an exchange platform, a business that provides custodial wallet services and a business that operates as a cryptocurrency service vendor.

The DABA is a standalone, comprehensive regulatory regime drafted with the particularities of cryptocurrencies in mind, which includes provisions pertaining to anti-money laundering, custody and security, information disclosure, crisis management and regulatory oversight. This approach creates certainty for businesses looking to provide digital asset services, as such services are clearly defined and the regulatory requirements applicable to such businesses are clearly defined and have been drafted with regard to specific risks to which the different types of cryptocurrency related business models are exposed. This approach provides the sought-after benefits of regulatory certainty and consumer protection without sacrificing innovation and the ability of businesses to succeed on a global scale.

If Canada's approach is inconsistent with regulatory approaches in other countries, it may result in decreased ability for Canadian companies to innovate or succeed internationally, it may drive Canadian users of cryptocurrencies to non-Canadian companies over which Canadian regulators have no oversight and it may limit Canada's access and contribution to a new technology that is making waves on a global scale.

4. What standards should a Platform adopt to mitigate the risks related to safeguarding investors' assets? Please explain and provide examples both for Platforms that have their own custody systems and for Platforms that use third-party custodians to safeguard their participants' assets.

The standards that should be adopted by a Platform to mitigate the risks related to safeguarding investors' assets are, for the most part, outlined in our response to question 2.

Key considerations include segregating customer assets and operating on a full reserve basis to ensure funds are always available.

With respect to storing customer assets, fiat assets should be stored in a regulated financial institution that is located in a trusted jurisdiction. Digital assets held in Hot Storage should be minimized to only the amount required to facilitate trading on the Platform and allow for customer withdrawals. The majority of customer assets should be held in Cold Storage.

Best practice Cold Storage procedures are outlined in our response to question 2. Platforms utilizing their own custody solution should abide by these best practices and Platforms utilizing a third-party custody solution need to ensure they are working with a trusted entity that abides by these best practices. Bitvo would be pleased to discuss with the CSA and IROC specific practices for the safeguarding of crypto-assets.

5. Other than issuance of Type I and Type II SOC 2 Reports, are there alternative ways in which auditors or other parties can provide assurance to regulators that a Platform has controls in place to ensure that investors' crypto-assets exist and are appropriately segregated and protected, and that transactions with respect to those assets are verifiable?

We would encourage the CSA and IROC to consider input from accounting firms and accounting industry groups to determine what type of regulatory approach would enable such firms to be comfortable providing audit and similar services to cryptocurrency businesses, including audit of internal controls and verifiability of cryptocurrency transactions.

6. Are there challenges associated with a Platform being structured so as to make actual delivery of crypto assets to a participant's wallet? What are the benefits to participants, if any, of the Platforms holding or storing crypto assets on their behalf?

From an operational perspective, each Platform should have a mechanism in place allowing a participant to instruct actual delivery of cryptocurrencies to such participant's wallet outside of the Platform, most often through a withdrawal procedure. By requiring actual delivery of crypto assets on completion of each trade without the off-chain option, this would create logistical challenges, timing delays and increased costs as it relates to cryptocurrency-to-cryptocurrency trades as there may be discrepancies in timing of verification on the respective distributed ledger protocol underlying such transfer and the settlement of such transaction.

There are significant benefits to a participant when a Platform holds or stores cryptocurrencies for the participant due to greater ease of use and likely increased security and peace of mind.

Many participants find the current process of handling and managing their own external wallet to be cumbersome or confusing and may take a less intensive approach to the security of their cryptocurrencies than the Platform would. Such participants appreciate a third party, such as the trusted

Platform through which they acquired the cryptocurrency, taking care of that element of their cryptocurrency ownership. If a participant loses his or her private key to an external wallet, the cryptocurrencies may be lost forever. If such participant loses his or her password to the Platform, he or she would be able to recover the cryptocurrencies held on such Platform. Furthermore, by not settling every transaction on the applicable blockchain, the Platform and the participants are able to avoid mining verification costs and timing delays associated with the verification of such transactions on-chain. The transaction can occur in real-time and the participant can have the peace of mind that the trade occurred immediately exactly on the terms contemplated.

- 7. What factors should be considered in determining a fair price for crypto assets?**
- 8. Are there reliable pricing sources that could be used by Platforms to determine a fair price, and for regulators to assess whether Platforms have complied with fair pricing requirements? What factors should be used to determine whether a pricing source is reliable?**

The fair price of a crypto asset should be determined in the same manner as traditional financial assets, as set by the supply and demand of traders at a point in time. It is essentially the market clearing price of the most recent trade on a Platform as set by willing buyers and/or sellers. As the cryptocurrency market is a global market, there is stronger price discovery for cryptocurrencies than for most other asset classes.

Reliable pricing sources include large Platforms with significant trading liquidity as well as trusted websites such as coinmarketcap.com, which aggregate real-time pricing information of hundreds of Platforms globally. In determining whether a pricing source is reliable, the quoted price can be compared to other Platforms as well as trusted websites such as coinmarketcap.com. A pricing source can be determined to be reliable if the price is established based on the most recent legitimate transaction completed.

- 9. Is it appropriate for Platforms to set rules and monitor trading activities on their own marketplace? If so, under which circumstances should this be permitted?**
- 10. Which market integrity requirements should apply to trading on Platforms? Please provide specific examples.**

For an efficient marketplace to exist, the integrity of trading activity on the marketplace is critical. Every Platform ought to set rules and monitor trading activities on their own marketplace. Platforms should not be engaging in deceptive practices, such as false trading, front running and preferred trading.

Certain negative impacts of such deceptive practices may be inherently limited in the case of cryptocurrencies due to the 24/7 availability and global nature of cryptocurrency trading activities. For instance, as cryptocurrency platforms are typically open for trading 24/7, there is a reduced risk of certain market manipulation activities developed to take advantage of market open and/or close. In addition, the global nature of cryptocurrency trading transactions with global price information available in real-time creates barriers to market manipulation activity and tends to limit the impact of such activities.

11. Are there best practices or effective surveillance tools for conducting crypto asset market surveillance? Specifically, are there any skills, tools or special regulatory powers needed to effectively conduct surveillance of crypto asset trading?

The industry employs a wide variety of approaches and products to conduct market surveillance on trading activities. Given the unique nature of cryptocurrencies, to determine best practices for market surveillance, it is important to consider the risks that are intended to be mitigated. These risks may include market manipulation, false trading, fraud or other improper activities. To ensure a fair and efficient market, Platforms monitor market activity to identify and investigate anomalies in trading activity or unusual or suspicious transactions.

We respectfully submit that the comment from CSA and IIROC that short selling and/or margin trading should not be permitted does not appreciate the benefits of such activities for the market, including in preventing market manipulation. For example, if a market participant is acting to manipulate prices in an inflationary way on a Platform and the Platform allows other participants to take advantage of this through short selling, the market would be able counteract and limit the potential manipulation naturally. Market participants would be incentivised to do this to profit from the spread that existed between the manipulated Platform and other Platforms, which would result in the manipulated Platform's pricing coming back in line with that of other Platforms, creating a more consistent global price for digital assets.

12. Are there other risks specific to trading of crypto assets that require different forms of surveillance than those used for marketplaces trading traditional securities?

There are anti-money laundering and anti-terrorist financing considerations that are more specific to the trading of crypto assets than for marketplaces trading traditional securities. These are addressed under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* and the regulations promulgated thereunder, including the proposed amendments thereto. Surveillance of such risks typically falls under the jurisdiction of The Financial Transactions and Reports Analysis Centre of Canada (FINTRAC).

14. Is there disclosure specific to trades between a Platform and its participants that Platforms should make to their participants?

If a Platform is acting as the counterparty to the trade, the Platform ought to disclose that information to the participant. The terms of the trade, including pricing, ought to be consistent with the market at the time of the trade. If there is any discrepancy between the terms of the trade and the terms of the equivalent trade if made on the market, such discrepancy ought to be disclosed to the participant.

15. Are there particular conflicts of interest that Platforms may not be able to manage appropriately given current business models? If so, how can business models be changed to manage such conflicts appropriately?

Trading by employees of the Platform may create a conflict of interest, for example, where the employee has access to non-public information which might result in a material change in the market price of a cryptocurrency, such as the new listing of a cryptocurrency on a Platform. Bitvo manages these risks through policies and procedures prohibiting trading on the basis of information that gives employees and advantage over non-employee participants.

- | |
|---|
| <p>16. What type of insurance coverage (e.g. theft, hot-wallet, cold-wallet) should a Platform be required to obtain? Please explain.</p> |
| <p>17. Are there specific difficulties with obtaining insurance coverage? Please explain.</p> |
| <p>18. Are there alternative measures that address investor protection that could be considered that are equivalent to insurance coverage?</p> |

Only a small number of insurance providers have invested the time, resources and capital required to adequately understand the cryptocurrency industry and provide coverage. As a result, insurance coverage for the crypto industry is thin and prohibitively expensive such that only the largest Platforms can afford to have a small portion of their assets insured.

Insurance coverage is one way of managing the risk associated with the potential loss of participants' assets. Risk of loss can also be managed by adhering to robust practices, policies and procedures with respect to handling customer assets (as discussed in our responses to questions 2 and 4), combined with ensuring a Platform is adequately capitalized such that a loss of assets can be absorbed by the Platform. These factors should ensure that the risk of loss can be appropriately managed while the industry waits for adequate insurance coverage to become available at commercially reasonable rates.

Concluding Remarks

Cryptocurrencies are a global development. A key benefit of many cryptocurrencies is the fact that such assets are not limited to a geographic region and may be transferred internationally without delay and only nominal cost.

The intentions behind the Framework, being increased regulatory certainty and consumer protection, are laudable and regulation that achieves such goals in a meaningful and measured manner will be welcomed by the industry. The Framework looks to apply existing securities laws in a variety of manners, from marketplace rules to dealer and IIROC requirements, to cryptocurrencies that do not bear the characteristics of traditional securities (and which the Framework does not appear to define with clarity). Existing securities laws apply appropriately to digitized traditional securities, however a patchwork approach to regulating a new and diverse asset class, such as cryptocurrencies, may not achieve the desired goals. On the contrary, this approach may encourage Canadian companies to move offshore, provide a regulatory monopoly to Canadian crypto-asset companies that already wish to deal in traditional securities thereby stifling innovation and domestic competition and push Canadian consumers to use cryptocurrency platform services from non-Canadian entities (as Canadian entities would not compete internationally on the same footing).

If Canada follows the approach of other jurisdictions seeking to balance regulatory certainty and consumer protection through a standalone regulatory regime developed specifically for cryptocurrency, Canada would establish an environment that will enable companies in the industry to thrive while protecting the interests of Canadians. In doing so, Canada can position itself as a hub for innovation in this nascent sector. By developing a cryptocurrency specific regulatory regime, including appropriate considerations from applicable securities laws and anti-money laundering laws, this would enable a standalone framework to create regulatory certainty and address risks facing the industry head-on without having to shoehorn solutions from existing laws not developed with these risks in mind. This would enable the framework to protect and promote Canadians and Canadian businesses.

Thank you for the opportunity to comment on the Framework. Bitvo appreciates the approach by the CSA and IIROC to consult with industry to collaborate in establishing a regulatory framework governing cryptocurrency platforms that balances risk controls and consumer protection without stifling innovation or restricting normal course adoption of cryptocurrencies in everyday life.



May 31, 2019

DELIVERED VIA EMAIL

The Secretary of the Ontario Securities Commission
20 Queen Street West 22nd Floor, Box 55
Toronto, Ontario M5H 3S8
Fax: 416-593-2318
comments@osc.gov.on.ca

Me Anne-Marie Beaudoin, Corporate Secretary
Autorité des marchés financiers
800, square Victoria, 22e étage C.P. 246, tour de la Bourse
Montréal (Québec) H4Z 1G3
Fax : 514-864-6381
Consultation-en-cours@lautorite.qc.ca

Victoria Pinnington
Senior Vice President, Market Regulation
Investment Industry Regulatory Organization of Canada
Suite 2000, 121 King Street West
Toronto, Ontario M5H 3T9
vpinnington@iiroc.ca

RE: Consultation Paper 21-402 Proposed Framework for Crypto-Asset Trading Platforms

Introduction

We are responding to the Joint Canadian Securities Administrators/Investment Industry Regulatory Organization of Canada Consultation Paper 21-401 *Proposed Framework for Crypto-Asset Trading Platforms* (March 14, 2019) (RFC 21-401 or the Proposal)

This letter sets out our general comments, followed by our comments to the specific questions being asked in the Proposal. We have tried to be constructive in our comments and have provided recommendations where we agree and where we think alternative options should be considered. We acknowledge that there may be other options than what we have recommended.

We thank the CSA and IIROC for identifying the issues and seeking comment and input into the regulatory responses being considered.

The Proposal

The Proposal is considering what parts of the regulation relating to marketplaces and regulation of dealers should be applicable to the trading of crypto assets on electronic platforms (Platforms). The Proposal acknowledges that crypto assets often differ in their functions, structure, governance and rights. However, in taking the view that most of the offerings involve investment contracts or commodities, it proposes a combination of the current regulatory requirements that exist for marketplaces and dealers. The starting place for marketplaces is the bringing together of multiple buyers and sellers and the starting point for dealer regulation is the trading of securities.

The Proposal sets forth requirements based on current categories of regulated entities (marketplaces and dealers) rather than considering if the nature of the assets and goal of promoting innovation requires a different approach. We are concerned that this approach sets up barriers to new entrants with new business models because the requirements are not relevant and too costly. The regulatory approach should not cut off opportunities for investors and new business models because of possible risks but rather should focus on actual or probable risks that are likely to have a significant impact.

Application of Marketplace Requirements

The marketplace requirements set out in National Instrument 21-101 *Marketplace Operation* are based on the assumption that the securities being traded were securities listed on a stock exchange. Thus, the nature of the asset being bought and sold by the multiple buyers and sellers was an intrinsic part of the regulatory approach underlying those requirements. Whether or not they are investment contracts, crypto assets are very different from common shares or other types of equity securities that are based on companies with operations or derived from shares based on these types of investments. Financial information relating to the operations of a business are the underlying assumption for valuation and trading of these securities, which is not usually the case with many crypto currencies or even other crypto assets in the early stages of the offering(s) or trading. For this reason, starting with current marketplace regulation may not be the best starting point.

In addition, the Proposal does not take into consideration the impact of this level of regulation on innovation and the use of distributed ledger technology.

We suggest that a more open and less intrusive regime be used, at least in the short term, that addresses the actual (verses potential) risks that have been identified. If a Platform is used for exchanging crypto assets among participants (and not directly with the operator of the Platform), we are setting out below recommendations on which and how such risks should be addressed.

Recommendation for the determination of whether a security or derivative is involved: The concept of investment contract with some guidance (including clear exceptions) is sufficient. If the proposed list of factors is used, this would create jurisdiction over an excessively broad category of assets.

Recommendation that requirements for Platforms that are marketplaces should focus on actual and material risks:

- Risk of lack of clear and complete information to evaluate trading risks – transparency requirements regarding operations of the Platform, its operators, conflicts, trading information, and custodial information to enable investors to understand the risks of using the Platform;
- Risk of assets disappearing – segregation, custodian and insurance (if available) requirements to address the risks that the assets may not be where they are supposed to be; and
- Risks of operational failures – technology system requirements (security processes and disaster recovery) to address security risks such as theft.

A tiered approach should be used to establish the extent of the requirements and additional requirements can be applied as the risks increase and/or other requirements become more relevant (as size of market gets larger, bigger impact, or other risks become known or increase).

Application of Dealer Requirements

If the Platform is used for exchanging crypto assets with the Platform operator as the counterparty, the current requirements applicable to dealers are more than sufficient and should address the potential risks identified in the paper. A tiered or proportional approach should also be considered. A dealer should be allowed to operate using a discount broker model where it does not have to provide advice or recommendations and therefore is not responsible for suitability.

Responses to Specific Questions

1. Factors used to determine if a security or derivative is involved

The factors suggested in the RFC 21-401 to determine if a security is involved on the trading platform are based on the nature and type of delivery involved, who holds or controls the investors' assets, and rights of investors in case of bankruptcy. These kinds of factors can apply to any type of asset and could suggest that marketplaces that buy and sell any asset should be subject to securities laws. There is the potential for over-inclusiveness if all of these factors are considered.

RFC 21-401 notes that there are differences in functions, structures, governance and most importantly, rights. Due to the broad definition and range of characteristics, it is more difficult to provide the appropriate regulation related to the nature of the assets since different types of assets are and should be treated differently. If a broad definition is used, then a more principled approach to regulation would be less intrusive on innovation.

Recommendation for the determination of whether a security or derivative is involved: The concept of investment contract with some guidance (including clear exceptions) is sufficient. Including the proposed list of factors would create jurisdiction over an excessively broad category of assets and would not address the current regulatory uncertainty.

2. What best practices mitigate the identified risks and are there other risks?

We believe that the Proposal has identified the right risks; however, it has not indicated the likelihood of the risk or impact. The list seems to arise from the risks related to any marketplace trading more traditional securities rather than those specific to platforms trading crypto assets. The nature of the asset being traded is relevant and should be considered. If the likelihood or impact is small, then specific regulation may not be required but could be mitigated through an oversight regime that addresses risks as they occur. Based on information reported in the news and other analysis, it seems the current key risks are:

- Transparency (clear disclosure about the platform, its operators, conflicts, and operations including trading information);
- Custody and segregation issues (requirements that will confirm the assets exist and can properly be allocated to the rightful owners); and
- Security Issues (these are similar to the custody issues but focus on operational issues).

Previous research indicated that most of parties involved in trading are young people who are interested in the technology, so it is not clear that suitability needs to be addressed at this time, and would be covered if traded through a dealer. Over time, as trading and acquiring these assets grow, then additional requirements may be appropriate since the impact is greater. The CSA/IIROC should consider a tiered approach based on the size of the marketplace or whether all trades are done through dealers who would provide sufficient protection.

Best practices require finding the appropriate level of regulation that addresses the key risks while enabling innovation.

Recommendation regarding the best practices which should focus on actual and material risks:

- Transparency requirements regarding operations of the platform, its operators, conflicts, trading information, and custodial information to enable investors to understand risks of using the Platform;
- Segregation, custodian and insurance requirements to address the risks that the assets may not be where they are supposed to be (safeguarding of assets); and
- System requirements to address operational risks.

A tiered or proportional approach should be used to establish the extent of the requirement as well as whether additional requirements should be applied as the risks increase and/or other requirements become more relevant (i.e., as size of market gets larger, bigger impact, or other risks become known or increase).

3. Are there any global approaches to regulating platforms that are appropriate to be considered in Canada?

No comment.

4. What standards should a Platform adopt to mitigate the risks related to safeguarding investors' assets? Please explain and provide examples both for Platforms that have their own custody systems and for Platforms that use third party custodians to safeguard their participant assets.

When trading securities, custodian risk has usually been very limited and has often been addressed by type of institution and size of assets under control. A similar approach could be used for crypto assets.

However, these are new types of assets, so the suggestion in the Proposal of focusing on internal controls to address operational risks or risks of fraud by getting an appropriate independent audit report is a reasonable requirement. The same requirement can apply whether the Platform does its own custody, or it is done by a third party. Consideration should be given to a tiered approach based on the size of the Platform or custodian. Also there already may be technology solutions that can be identified as providing best practices regarding custody of these assets without requiring independent audit reports.

Recommendation regarding safeguarding investors' assets: Using independent audit reports and minimum size tests are reasonable requirements to address risks of safeguarding assets. Consideration should be given to the availability and cost of obtaining the report. This is also an area where the requirement should only apply to later stage or more developed Platforms (proportional requirements). Identifying specific technology solutions as best practices (rather than as a requirement) may achieve the same results in a more cost effective way.

5. Other than issuance of Type I and Type II SOC 2 Reports, are there alternative ways in which auditors' or other parties can provide assurance to regulators that a Platform has controls in place to ensure that investors' crypto-assets exist and are appropriately segregated and protected, and that transactions with respect to those assets are verifiable.

There are numerous companies that specialize in the understanding and application of distributed ledger technology to commercial products. If relevant qualifications concerning independence and expertise could be established, then allowing these qualified experts to provide an independent report might be as or more useful than using auditor reports. The topics that should be covered in the report could also be included in new requirements. This would be similar to how mining experts are used in the prospectus requirements for mining companies. However, any new approach should take into consideration creating overly burdensome costs that are disproportionate to the activities. A tiered and principled approach in terms of the contents of any report could be used to address this issue and therefore not act as a barrier.

Recommendation for use of alternative specialists to address risks regarding loss of assets: Requirements regarding expertise and content of reports of third parties should be established but the impact of the costs on the Platform should be considered, including whether a tiered approach is appropriate.

6. Are there challenges associated with a Platform being structured to make actual delivery of crypto assets to a participant's wallet? What are the benefits to participants, if any, of Platforms holding or storing crypto assets on their behalf?

No comment.

7. What factors should be considered in determining a fair price for crypto assets?

Fair pricing is generally determined by supply and demand as determined by market participants. It is assumed to occur in the public markets if there is order and trade transparency and no evidence of unfair trading practices. On the other hand, there are no requirements for the private markets and it is left to the participants to agree on a price. In both cases, the fundamental issue is whether the market participants have access to the information they need to make the appropriate investment decisions. Regulators should only be concerned about the risk of lack of appropriate information or unfair trading practices and not market risk.

Recommendation regarding determining a fair price to address risk of lack of information:

Requirements regarding transparency of trading information (orders and trades) and information regarding the asset should be established.

8. Are there reliable pricing sources that could be used by Platforms to determine a fair price, and for regulators to assess whether Platforms have complied with fair pricing requirements: What factors should be used to determine whether a pricing source is reliable?

Fair pricing depends upon the mechanisms of the trading platform and appropriate transparency. Difference in customers (institutional verses retail), market structure and nature of intermediation on the Platform can create differences in pricing and market data information which do not reflect reliability issues. The reliability of any pricing source depends on what market data it uses and/or how it produces the information. There are many market data sources in the public markets that exist today without any requirements or criteria regarding reliability. Market participants have been able to evaluate and determine their credibility without any regulation. It is not clear that additional requirements are required for alternative pricing sources for crypto assets. A Platform's pricing should be determined to be fair without reference to alternative sources; however, if third sources are used, any concerns could be addressed by full transparency regarding the source and processing of information by the third party, including any real or potential conflicts.

Recommendation regarding reliability of pricing sources to address risk of lack of a fair price:

No additional requirements should be put in place since the Platform should be responsible for establishing its own mechanisms for fair pricing.

9. Is it appropriate for Platforms to set rules and monitor trading activities on their own marketplace? If so, under which circumstances should this be permitted?

It is not clear what risk that the CSA and IIROC are trying to address by prohibiting the Platforms from setting requirements and monitoring compliance with the requirements. Platforms that enable any kind of matching or orders will, by necessity, have to set rules of order entry, allocation and matching priorities. In order to attract clients, they will also want to set other rules that will establish fair markets. If they set requirements, they should monitor compliance with the requirements and enforce any breaches. Regulators should encourage them to do this since this encourages investor protection and efficient capital markets.

Uniform requirements or the use of IIROC as a market regulator is not necessary at this time and is likely to act as a barrier to the development of these types of Platforms because it adds unnecessary complexity and costs.

Recommendations for Platform requirements and monitoring compliance: Platforms should set requirements and should monitor compliance with the requirements so that they can enforce any breaches and maintain fair markets.

10. Which market integrity requirements should apply to trading on Platforms? Please provide specific examples?

At this stage of the development of these types of Platforms, the only requirements should be clear and complete transparency regarding the rules and how non-compliance will be handled. The Platforms could deal with non-compliance issues by limiting or refusing access and/or reversing trades. At this time there is a higher risk of safeguarding assets than trading abuses.

Recommendations for Platform requirements to address unfair trading practices: At this time, it should be left to the Platforms since they have the incentive to prevent abuses in order to maintain the reputation of the Platform. Alternatively, the principle of fair and orderly markets could be used provided it is interpreted in the context of these Platforms and not the current rules that are in place for other types of securities marketplaces.

11. Are there best practices or effective surveillance tools for conducting crypto asset market surveillance? Specifically, are there any skills, tools or special regulatory powers needed to effectively conduct surveillance of crypto asset trading?

See response to Consultation Question 10.

12. Are there other risks specific to trading of crypto assets that require different forms of surveillance than those used for marketplaces trading traditional securities?

The specific risks relate more to custody than surveillance. See response to Consultation Question 9.

13. Under which circumstances should an exemption from the requirement to provide an Independent System Review (ISR) by the Platform be considered? What services should be included/excluded from the scope of an ISR? Please explain.

From the experience we have seen so far, the most common technology risks facing these types of Platforms have been in relation to cybersecurity issues rather than to capacity and resiliency. Also, the failure of an exchange trading public securities has a more significant impact. The ISR requirement is a significant cost which may not be justified in the early stages of these types of platforms. In addition, it should be confirmed whether the auditing firms are able and willing to provide these reports and opinions.

Recommendation for requirements to provide ISR to address technology system risk: Basic technology requirements should be applicable, but an ISR should only be applied when the Platform reaches a certain size (a tiered approach).

14. Is there disclosure specific to trades between a Platform and its participants that Platforms should make to their participants?

We agree that the Platforms should be required to identify and manage potential conflicts of interest and to disclose whether they trade against their participants. We do not think it is necessary for the Platforms to be IROC members to address the conflicts or other risks.

Recommendation for requirements to address conflicts of interest: There should be requirements to disclose and manage any conflicts.

15. Are there particular conflicts of interest that Platforms may not be able to manage appropriately given current business models? If so, how can business models be changed to manage such conflicts appropriately?

Since these business models are still evolving, the range of potential conflicts can best be handled by a principled approach which requires that they manage the conflicts and are transparent about them. Regulators should not try to design or limit business models but rather, should set the appropriate requirements.

Recommendation for requirements regarding conflicts arising out of business models: There should be a principled base approach to conflicts rather than prescriptive limitations on business models.

16. What type of insurance coverage (e.g. theft, hot-wallet, cold-wallet) should a Platform be required to obtain? Please explain.

We agree with requiring appropriate insurance (being insurance that is available, affordable, and addresses issues) because it provides a useful incentive for the operators of the Platform to try to prevent the risk so that a claim does not arise.

Recommendation for insurance requirements to address risk of loss of assets: Appropriate insurance requirements should be identified if available at an affordable cost.

17. Are there specific difficulties with obtaining insurance coverage? Please explain.

No comment.

18. Are there alternative measures that address investor protection that could be considered equivalent to insurance coverage?

Alternatives could include other evidence of funding (for example, bonds, letters of credit or sufficient working capital) to support the Platform being able to cover any liabilities.

19. Are there other models of clearing and settling crypto assets that are traded on Platforms? What risks are introduced as a result of these models?

Requiring the use of currently available clearing houses or establishing identical requirements for these new Platforms ignores the value and reasons for using distributed ledger. Technology and custodian requirements are sufficient to address the risks.

Recommendation regarding additional requirements to address settlement risk: Technology, segregation and custodian requirements are sufficient to address the risks.

20. What, if any, significant differences in risks exist between the traditional model of clearing and settlement and the decentralized model? Please explain how these different risks may be mitigated.

The traditional model of clearing and settlement has significant systemic risk due to the concentration of the risk in one entity and requires regulation to confirm that the clearing agent has addressed third party risk appropriately through its risk model and collateral requirements. Also, it involves the central bank in protecting against systemic risk. A decentralized model which emphasizes establishing the provenance of the assets in ways that cannot be fraudulently undermined mitigates and significantly reduces the systemic and counterparty risks. Less regulatory oversight and intervention is required because technology itself can mitigate, if not eliminate, the risks.

21. What other risks are associated with clearing and settlement models that are not identified here?

We are not aware of any additional risks regarding clearing and settlement.

22. What regulatory requirements, both at the CSA and IIROC level, should apply to Platforms or should be modified for Platforms? Please provide specific examples and the rationale.

When new services or products are introduced, it is not unusual for the regulators to start with their current categories and requirements as the basis and then eliminate requirements. This

approach places significant burdens on these new solutions, especially if they are attempting to disrupt current models at reduced prices for their solutions. It is also difficult for the businesspeople to understand why traditional requirements are applying to their business when their model attempts to avoid the risks that the traditional models face.

It might be more productive to start with the risks and then identify what are the relevant requirements. We have tried to do that in the recommendations we set forth at the beginning and throughout this letter.

Relevant topics (but not necessarily the detail of the requirements) set out in appendix B for Platforms that are marketplaces are:

- Transparency of operations (No. 2)
- Transparency of orders and trades (No. 3)
- Conflict of interest (No. 7)
- Confidential treatment of trading information (No. 9)
- Recordkeeping (No. 10)
- Systems and business (no. 11)

All of the requirements set out for dealers providing trading services in connection with crypto assets may be relevant with the exception of suitability if the dealer does not intend to provide advice or recommendations regarding the buying and selling of specific crypto assets.

We are happy to discuss any of our comments. Please contact Randee Pavalow at rpavalow@corpcounsel.ca for any questions.

Please do not hesitate to contact the undersigned with any questions.

Yours very truly,

CC Corporate Counsel Professional Corporation

/s/ Randee Pavalow

Randee Pavalow, Of Counsel on behalf of the Firm