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.html

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 then 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.