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_IIROC_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 vie 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