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 hold 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 incentives 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 compliation 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 were 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 in liquidity. Most decentralized exchange 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!