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. Ones 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 Yorks "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 (HKSFC'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 crypto currency 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