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

AND:
The Secretary Ontario Securities Commission
20 Queen Street West
22ndFloor, 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

Introduction:

The purpose of this submission is to give several Canadian Bitcoin users the opportunity to comment of this public consultation without the need to disclose their identifying information or go through the process of submitting a letter to a regulator as an individual. This can be intimidating for some, which can discourage full participation. The hope is that this submission will encourage more participation and feedback directly from Canadian cryptocurrency users and inform the regulator(s) of the views held by those on the front lines of this new frontier.

Within this submission is the collective community feedback by some reddit users who are pseudonymously identified by their reddit username (example: “User One: Regulator”). Some of these reddit users have elected to remain anonymous and therefore their reddit username is omitted in this submission (example: “User Two: Anonymous”).

Background:

Reddit.com is an online community platform where anyone can participate and register an account with an email address. Users are identified by a handpicked username and can comment and create public or private discussions. A user can vote on other users’ comments and discussions. Voting can help to promote a discussion or comment so that it is more widely viewed by the reddit community. Furthermore, users can create communities, called subreddits. Users can subscribe to these subreddits, much like one can subscribe to a mailing list or RSS feed with your email address.

There are several popular subreddits for Bitcoin and cryptocurrency, some of which have more than a million reddit subscribers. There is a subreddit for Canadian Bitcoin discussion specifically called r/BitcoinCA. This subreddit has more than 11200 subscribers, many of who are Canadian cryptocurrency enthusiasts. The responses below are a collection of comments made by these subscribers in response to Consultation Paper 21-402 *Proposed Framework for Crypto-Asset Trading Platforms.*

We trust that the regulator(s) will consider this feedback with the same respect they give other submissions from Canadian constituents. Thank you for conducting this consolation and accepting this feedback from Canadians.

Fiach_Dubh

For more details, see:

www.reddit.com/r/BitcoinCA/comments/b3d9f0/a_crowdsourced_rbitcoinca_response_to_the/

General Comments By r/BitcoinCA Constituents on Regulation of Crypto-Asset Trading Platforms:

(User One: MrRGnome)

If I could communicate one idea and one idea alone to regulators with crystal clarity it would be this: The role of regulators should be largely educational and standards setting. Establish well informed access and control standards for private keys and multisignature wallets for Canadian Bitcoin businesses. Establish best practices for public and private auditing of Bitcoin reserves. Educate users and businesses on how to protect themselves in this new global economic environment. These are the exact same tools you would use for any peer to peer activity resistant to regulation or enforcement, the tools that allow people to protect themselves.

It worked for the internet, another regulatory resistant environment, where warning families of the dangers of the internet and providing business guidance on security has proven a winning formula. Using the tools from the securities toolbox which belong in an environment where enforcement is possible is backwards thinking.

It creates costs of regulatory burden with immensely diminished regulatory benefit compared to centralized industries, if any benefit at all. The good news is Bitcoin offers new techniques and open source technologies to protect users and enable regulatory and public real time audits which address the majority of regulatory concerns. One such tool is Blockstream's proof of reserves tool, which uses the public nature of the blockchain to demonstrate an entity has access to a set of Bitcoin addresses representing their reserves: (https://github.com/ElementsProject/reserves).

Tools like reserves enable public and independent audits of a company's Bitcoin holdings. It is my opinion Canadian Bitcoin companies acting as custodians should have to prove their custodial holdings either through tools like reserves or public Bitcoin addresses and signed messages. This coupled with user education and your department establishing and auditing access/control procedures for private keys would eliminate nearly all the forms of corporate fraud possible in this space. Educating users is the last piece of the puzzle in reducing fraud for the average Canadian in this space.

Therefore, I am only in favor of 3 regulations ever and in total.

1. Disclaimers describing how, if at all, they hold the keys of their users and the risks of allowing the company to hold and manage keys. If they are a trading platform, disclosure of trading they do on their own platform.
2. Instructions and encouragement to users on how to hold their own keys.
3. Auditing of key storage and access/control procedures and use of public auditing tools like; https://github.com/ElementsProject/reserves.

Now on to my thoughts about this document. 100% of the proposed regulations are harmful, and 0% of the proposed regulations address private key handling and storage. None of these proposals would have stopped the Quadriga fraud or the current ezbtc fraud or other similar mismanagement instances in the space. To answer the completely off-base questions and misapplied securities regulations, cont.

(User Two: TheAlexGalaxy)

Don't try to regulate exchange platforms. It will only create a false sense of security. Platforms have a vested interest to be secure and prove to their customers that they are secure and solvent. Let them compete and evolve.

(User Three: Anonymous)

I would like to know the owners of exchanges. Proof of reserves would also be ideal. A minimum of three people should be in control of the exchange's private keys through multisignature technology, but more would be ideal. I don't believe it's ideal if someone that wants to make an exchange must jump through a ton of regulatory hoops, the regulatory barriers to entry should be low.

(User Four: Gcotton135)

For context, I have worked at one of these crypto exchanges as a developer. I have also traded on the exchange, and then was arbitrarily blocked for "winning" too much. I am also a seasoned options trader.

(User Five: Anonymous#2)

Guidelines and best practices are welcome and needed in this wild west. However, hardline regulations with consequences are already enshrined in several pieces of legislation. I would encourage the regulators to use current legislation to promote and enforce any forthcoming guidelines.

One huge concern I have is privacy. How cryptocurrency exchanges and services collect, store and secure the personal information of Canadians. Things like credit card numbers, date of birth, full name, address, phone number, pictures of driver's licenses, health cards, passports, and bank statements are all commonly given to these unregulated companies by users, because they are asked for them in order to comply with KYC/AML policies. In one case a Canadian cryptocurrency exchange is even asking users to voluntarily hand over their Social Insurance Number.

Users have no way of knowing how this information is used or secured (if at all) after it is submitted to these non-regulated quasi-financial asset dealers. In fact, there have even been allegations that user data from these exchanges has leaked onto the internet or been stolen in some cases. This further increases the chances for identity theft of Canadians. I hope that the regulators will consider this angle of inquiry and investigate how these companies store user information and secure it against data theft. I also trust that future regulation will focus on this aspect of data security and privacy for Canadians.

Furthermore, it would be appreciated by the Canadian Bitcoin community if the regulators could somehow recognize exchanges that follow your eventual guidelines so Canadian consumers know which platforms are safe to use. Right now, there are several Canadian cryptocurrency platforms in operation, most of which have a good reputation. But some, like EZBTC.ca , owned and operated by David Smillie, have a reputation for making off with customer money and not honoring customer withdrawals. The EZBTC platform is still in operation to this very day despite multiple apparent lawsuits and complaints to the BBB. There

appears to be few consequences for the bad actors in this ecosystem thus far. Which is why I recommend you consider extending whistleblowing protection to former or current platform employees who report malfeasance to regulators. Hopefully this consultation is a step in the direction of a safer cryptocurrency ecosystem for Canadians. Thank you for your consideration.

Questions asked by the OSC, And r/BitcoinCA constituent answers:

1. **Are there factors in addition to those noted in Part 2 that we should consider?**

(User One: MrRGnome)

You should dump the existing language in "Part 2" in its entirety and adopt instead crypto-specific policies like the three I list above (Disclaimers, education and onchain real time audits of reserves/key management). Trying to misapply securities regulation is a recipe for stifling industry growth and not protecting users.

(User Four: Gcotton135)

There is no exchange in Canada that can prove its volume to a 3rd party auditor - zero! This includes the one (unnamed) that is trying to get regulated in almost every single interview, and again and again internally. Don't throw your reputation as an Ontario regulator into the dirt by giving the unjustified regulatory approval, as if these things were banks, and as if these were stocks... to a company that can't prove every single trade going back at least 2 full years.
Also, if these things are truly to be "exchanges" for futures, options, or equities, their owners and internal staff shouldn't be able to arbitrarily disable accounts for "winning". The very premise of an exchange is to provide liquidity. Users "winning" too much only matters if you're a casino.
Also, there needs to a be a whistleblower hotline setup for internal staff and clients of the exchanges that wish to take part in regulation.

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?**

(User One: MrRGnome)

All of the concerns stated in "Part 3" can be addressed with simple public auditing tools and auditable access and control procedures. Use tools like: https://github.com/ElementsProject/reserves enabling the public to audit in real time and reducing the regulatory burden for all parties.

(User Four: Gcotton135)

Regulators and auditors should be able to perform a full audit of all assets claimed to be under management within 24-hours of giving notice. Since all assets are digital and supposed to be backed in organized wallets (either hot or cold), this should be a trivial exercise unless there is something amiss.

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

(User One: MrRGnome)

The only successful approaches are global. It's a global protocol that Canada cannot control or influence. To start with, every thought about regulating securities needs to be thrown out the window and every proposed regulatory thought needs to revolve around private keys. Use open source tools such as those mentioned to enable public audits and set a global standard for how to offer consumer protections specific to and enabled by bitcoins unique technology.

(User Four: Gcotton135)

Proof of keys is a worldwide phenomenon, but the single exchange left standing can't provide this because of internal issues, supposedly. If these exchanges wish to be operating like real stock or options markets, then they need to be treated as such. Don't buy the baloney about how it's a new technology so the old rules don't apply - you're not a foolish venture capitalist, you're here to protect the public! If for whatever reason they can't provide the same basic checks and balances, such as compliance on each user, audit trail of each and every trade (i.e. confirming that there is no fake volume), etc. then there is no real market. It's just a black-market and needs to be thought of as such.

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.**

(User One: MrRGnome)

The answer to all these questions is the same. Use public auditing tools like reserves and a standardized set of access and control procedures.

(User Four: Gcotton135)

A third-party custodian needs to safeguard a certain reserve ratio. This may be the Bank of Canada, or a third party like KPMG, RBC, Deloitte, or some well-respected financial firm. Trust me... these guys cannot be trusted to be their own custodians. Do a full audit and you'll see for yourself.

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?**

(User One: MrRGnome)

Use reserves or other public auditing tools.

(User Four: Gcotton135)

You need to provide both a financial and technical audit that goes beyond what you are currently doing. Frankly, the technical audit needs to be even more thorough than the financial audit due to the nature of this ecosystem. Both need to be done simultaneously, and yearly without any notice, just like the CRA can audit a business without much notice. See above and google "proof of keys".

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?**

(User One: MrRGnome)

Different users have different needs. Some will want custodial solutions, some will want semi custodial solutions that imply delivery, some will want strictly non-custodial solutions. All have unique challenges; all of those challenges can be solved by requiring proof of reserves as stated over and over in this response. It is not necessary to discriminate against any of these various service providers.

(User Four: Gcotton135)

Holding onto crypto assets for the customers behalf is what the exchanges like to do (acting as custodians). The problem with that is they can exit or disappear without warning, like QuadrigaCX did. Users are often charged high fees to withdraw these crypto assets or fiat funds from exchanges, so many users are dissuaded from doing this. At least with a federally recognized stable coin, you should not be penalized for offboarding from any exchange as a user.

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

(User One: MrRGnome)

You (the regulators) should have no role in that. The fair price of a speculative asset in its infancy with potential to change trust as we know it is not something within your purview to dictate. It's worth whatever it's paid for, and any assertion that the Canadian market has enough volume to be suspect of manipulation is lunacy.

(User Four: Gcotton135)

The market itself. Nothing else matters.

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?**

(User One: MrRGnome)

No. Stop trying to create a fair price. Derivatives products requiring a "fair price" are best suited following successful parties like BitMex's "fair price" mechanics and it needs not be regulated. Bad implementations of "fair price" are avoided.

(User Four: Gcotton135)

Any platform that misprices with respect to another by too much is by definition "incorrect" relative to the fair price. This can be either too high or too low. QuadrigaCX was well known for having very high prices. Coinsquare is known to sometimes have lower prices than the rest of the market, while at other times, pricing too high. There are so many much more reliable markets in the world that you should use weighted average of the major exchanges (Coinbase, Bitfinex, Binance, etc.) to determine what the "fair" or realistic price.

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?**

(User One: MrRGnome)

No.

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

(User One: MrRGnome)

None.

(User Four: Gcotton135)

Settlement, conversions, book balances must all be taken care of within the same time frames as real markets.

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?**

(User One: MrRGnome)

Stop trying to surveil crypto assets trading. If you do it will push the activity into peer to peer examples of how impossible it is to force these requirements without driving population to obfuscated peer to peer activity. These proposed regulations, this questionnaire, betray a complete misunderstanding of the possible role of regulation in the bitcoin economy.

(User Four: Gcotton135)

You will need skilled software developers and engineers to be a part of the OSC. This should be paid for entirely by the regulatory fees that these exchanges pay to the OSC.
As well, I should add that any conflicts of interest need to be disclosed immediately (i.e. I used to or plan to work for QuadrigaCX or Coinsquare in the past or future) and failure to do so must be punishable to the fullest extent of the law. This is a nascent industry and there is no room for corruption or greed if we as a society are to put our faith in cryptocurrencies.

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?**

(User One: MrRGnome)

Stop.

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.**

(User One: MrRGnome)

If the regulations are published as currently written everyone deserves an exemption.

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

(User One: MrRGnome)

Platforms should have to disclose when they are trading against their users as a 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?**

(User One: MrRGnome)

Yes. Businesses wants to control users' keys. Bitcoin is made to enable users to control their own keys. Regulators must force companies to disclose and educate users to encourage them to hold their own keys as I describe in the 3 simple steps I propose in my initial general comment.

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

(User One: MrRGnome)

No insurance will possibly be provided unless it is by the state. It would be madness for an insurance provider to insure one of these exchanges' entire holdings. The correct solution is the auditability tools previously stated and insurance against employee mistakes.

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

(User One: MrRGnome)

See my response to question 16. Yes, it is impossible. No insurer will cover deposits, ever, just like no insurer will cover 100% of bank deposits.

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

(User One: MrRGnome)

Proof of reserves: https://github.com/ElementsProject/reserves

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?**

(User One: MrRGnome)

Yes. Users will move to p2p services if you enact these proposals. The risk is you as a regulator will be blind to their existence and operation. There is nothing that can be done about this, Bitcoin is by design censorship resistant. The solution is to not push users into the p2p market in the first place with pointless, onerous regulations.

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.**

(User One: MrRGnome)

There are many risks. The decentralized model does not abide to regulatory pressure. Unlike every other model you have experienced, your regulations WILL be avoided by anyone inclined to avoid them. The biggest risk is damaging the legitimate and transparent cryptocurrency industry with regulations that would do nothing to stop the kind of fraud recently at QuadrigaCX and currently active at ezbtc.ca. This will force more users outside the purview of any regulation. Moreover, decentralized environments have tools to enable users to regulate themselves. Use and enable them. Not using these tools risks imposing regulation ill fit for the goals desired by the regulator.

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

(User One: MrRGnome)

Management fraud, like that of Quadriga and ezbtc, is entirely unaddressed by the proposed regulations. What happens when management decides to walk off with the coins? Until there are proper access and control procedures ensuring management cannot walk off with coins, and proof of reserve tools in use that users and regulators can assure that the keys/coins exist and are accessible, these frauds will continue.

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.**

(User One: MrRGnome)

As previously stated, I am only in favor of three regulations no more no less. 1) Disclaimers describing how if at all they hold the keys of their users and the risks of allowing the company to hold and manage keys 2) Instructions and encouragement to users on how to hold their own keys and 3) Auditing of key storage and access/control procedures and use of public auditing tools like proof of reserves: https://github.com/ElementsProject/reserves

Appendix A: List of r/BitcoinCA constituents

User One: MrRGnome
User Two: TheAlexGalaxy
User Three: Anonymous
User Four: Gcotton135
User Five: Anonymous#2

Appendix B: Reserves in Brief

https://github.com/ElementsProject/reserves

Reserves

Reserves is a tool for generating and verifying proof-of-reserves for funds in the Bitcoin network.

It currently has the following features:

- use of a single "proof file" that can include several separate proofs to ease the use of distinct wallets
- add a proof challenge to prevent proofs to be reused or exchanged
- two-step procedure to ease use with hardware wallet or HSMs: first collecting UTXOs to be bundled, then signing the proof
- proofs are made at a specific block number and can be verified even if the funds moved after the point of proving
- relying on existing standards: Final proofs are unspendable, but valid Bitcoin transactions and in-progress proofs are kept in PSBT format to ease integration with hardware wallets.

How it works

For every proof-of-reserves, a Bitcoin transaction will be generated. This transaction will be invalidated so that it cannot be broadcast to the Bitcoin network. This is done by adding an input that refers to a non-existing UTXO.

The remainder of the transaction consists of UTXOs owned by the proving party and a single output with the sum of the values of all the UTXOs in the inputs. The prover signs this transaction to prove that it can spend the UTXOs.

Since the transaction contains a non-existing input, the provers inputs cannot be spent, but the signatures on the inputs can be verified as if the transaction did not contain the non-existing input to verify the proof.