IIROC Consultation Paper

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

1. 1. Whether the platforms are structured for short selling of crypto assets,
1. 2. Whether a platform play roles as a clearinghouse or just a middleman between the token buyer and seller,
1. 3. How the platforms are structured to handle the liquidity issues,
1. 4. How centralized and decentralized exchanges of the cryptocurrencies work and interact,
1. 5. How off-chain order book and on-chain settlements connect with the platforms,
1. 6. Whether all platforms are structured to be functioned as a broker, custodian and trading venue at the same time.

1. 7. Does the concept oof the sec lending exist with crypto

1. 8. Should it

1. 9. Can we have a viable shorting capability without it

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?

2. 1. The best practices are to set up appropriate regulations and force internal control policies and procedures to mitigate the risks outlined.
2. 2. Significant risks that have not identified and clearly stated in part 3 include:
    a. There are no rules to detect and monitor fraud and AML activities within and across platforms/exchanges.
    b. It is not clear whether initial coin offering ("ICOs") should be considered securities subject to the same rules and regulations as equity market offerings.

2. 3. Regulators should immediately conduct on-site field reviews of existing market participants (exchanges, custodians) and bring in third parties.

    a. These third parties would include accounting/auditing firms to provide guidance leading to the equilavent of GAAP but for crypto. The lawyers representing these market participants would learn from the process thereby allowing them to advise their existing client (who was just reviewed) as well as others. The deficiency letters for each particular visit can be aggregated. The accumulation of findings will lead to a list of problems.

    b. In collaboration with those auditors and lawyers who were part of this discovery process, a series of solutions could be formulated. Take this list into another CSA/IIROC public dissemination and get feedback and you are then closer to a generally accepted set of policies and procedures. The regulators do with existing crypto custodians/exchanges like they do with those in the existing securities industry.

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

3. 1. There is a strong recommendation globally that apply the Anti-Money Laundry and Anti-Terrorism Financing or Count-Terrorism Financing (AML/ATF or CTF) regulation framework to the cryptocurrency platforms.
3. 2. ASIFMA Best Practices for Digital Asset Exchanges may be considered as a reference when developing appropriate regulations in Canada.

3. 3. I would strongly suggest that CSA/IIROC do not investigate or incorporate any efforts outside of Canada, at least not for now.

3. 4. Go through the process mentioned above for section 2 as a start and once you have the list of problems, THEN explore how others outside Canada are looking to solve these. Suggesting here to define the problem first before thinking about solutions. This direct regulatory review will be healthy for all (regulators, participants, investors) to learn and possibly identify and remove bad actors.

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.

4. 1. The U.S. National Institute of Standards and Technology ('**NIST**') Cybersecurity Framework could be adopted.
4. 2. Certain internal control procedures should be established to safekeeping, record, monitor, report status of the digital assets and fiat currencies and associated transactions.
4. 3. For platforms that use third-party custodians, a reconciliation process should be implemented to confirm its internal accounts and those of any third-party custody assets.

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?

5. 1. Auditors should also consider Type I and II SOC 3 reports. In addition, testing and monitoring results on the internal controls performed by the first and second lines of defence would provide alternative support on the design (Type I) and operating (Type II) effectiveness of the internal controls.

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?

6. 1. Actual or physical delivery of crypto assets to a participant's wallet for each transaction would result in significant challenges of operational processes and cost with a platform as well as the risk of losing passwords of private wallets.
6. 2. The benefits to participants of the platforms holding or storing crypto assets like custodians in the traditional financial system would minimize the risk of individual participants losing their funds to bad actors and transaction cost and operational efficiency with the platforms. But there are other concerns on the security measures needed by the platforms or third-party custodians to keep the funds safe.

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

The following factors would be considered in determining the fair value of a crypto asset:

- Supply and demand
- Mining cost/difficulty
- Crypto unit reward per block
- Loss factor (estimated volume of lost crypto asset units due to private keys loss)

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?

CoinMarketCap API is a commonly used source that provides prices, volume and market capitalization of various cryptocurrencies.

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?

9. 1. Given the nature of the cryptocurrency platforms, platforms should set rules, policies, procedure, and risk appetite/thresholds/limits to regularly monitor trading activities on their own marketplaces and perform the day-to-day risk management.
9. 2. The Platforms should further investigate any suspicious transactions, price spikes, non-compliance with the Exchange's legal and regulatory obligations, alerts of frauds, etc.

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

The following market integrity requirements would be considered to be applied to crypto asset trading on Platforms.

10. 1. Universal Market Integrity Rules ("UMIR") by IIROC, including
    a. Short selling
    b. Frontrunning
    c. Manipulative and deceptive activities
10. 2. Systems and business continuity planning
10. 3. Effective monitoring and supervision
10. 4. Cybersecurity

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?

There are a number of markets surveillance vendors that provide solutions for conducting crypto asset market surveillance.

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?

ICOs may require different forms of surveillance.

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.

CSA has recently proposed amendments to National Instrument NI 21-101 – Marketplace Operations. The amendments address cyber resilience controls, expend obligation to report material "security incidents" to regulators, mandatory annual security vulnerability testing, annual independent system review (ISR) by "qualified external auditor".

The following circumstances could be granted temporary exemptions from an annual ISR requirement:

- Regular and independent self-assessment of internal controls (from both design and operating effectiveness of the controls) conducted by platforms
- Comprehensive monitoring reports provided by platforms and no significant issues identified
- Exposure is limited

The scope of ISR should include

- Design and operating effectiveness of various controls over the platform;
- Performance evaluation including the future capacity requirements to handle changing market conditions
- Robustness of business continuity planning and disaster recovery planning
- Effectiveness of incident reporting/escalation, notification, follow-up actions, and remediation

The following services may be excluded from the scope of ISR for a platform.

- Third-party service providers or system vendors

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

- Trade incidents and system failures

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?

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

The types of insurance coverage would include

- Cyber (hacks) & Privacy Insurance:
- Insurance for loss or theft of private keys (old and hot wallets):
- Errors & Omissions ("E&O") Insurance: Having E&O coverage helps the Platforms avoid substantial claims of inadequate work, negligent actions, or defective products/services;

- Directors & Officers ("D&O") Insurance: It is considered as a crucial form of protection for all businesses including crypto exchanges, before investors and board members risk their professional assets.
- Corporate crime insurance: It protects the platforms from losses that are a direct result of an employee or third-party dishonesty.

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

The following factors are examples of specific difficulties in obtaining insurance coverage:

- Lack of historical and actuarial data in crypto markets to determine appropriate insurance premiums
- No comprehensive risk management framework for the crypto markets to provide principles in identification, measurement, mitigation/control, and reporting of the underlying risks in the crypto markets
- Insufficient insurers, supply and expertise in the market to meet the demand for insurance coverage and unique products
- Lack of proper underwriting processes for this unique market
- Lack of regulations and guidelines

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

Develop and implement robust internal governance and controls over the information technology and cybersecurity, trading supervision and surveillance, business continuity plan, disaster recovery plans could be considered as alternatives to insurance and reduce risks and investor protection.

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?

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.

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

Except for operational, custody, liquidity, investment and credit risks identified here, clearing and settlement models also exposure to reputational and regulatory risks.

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.

The following requirements may need to be modified for Platform

- Appendix C #4 – Financial condition and requirement capital: It is subject to a modification of the methods for regulatory capital calculation, including the mapping of asset classes by crypto assets and risk weights.

Additional Questions/Comments: