Joint Canadian Securities Administrators/Investment Industry Regulatory Organization of Canada

Consultation Paper 21- 402 – KNØX INDUSTRIES Response

PART 2 - Nature of crypto assets and application of securities legislation

Question 1: Are there factors in addition to those noted above that we should consider?

Ans:

In some cases, the responsible entity or trustee may elect to provide self-custody, but must be able to demonstrate that the assets are held separately from its own assets and meet capital requirements. Benefits of appointing a custodian include:

- Ensuring assets are properly segregated from the assets of other trusts
- Safeguarding asset portfolios to protect investors
- Enabling the responsible entity/trustee and trust manager to concentrate on managing the fund
- Assisting with the marketing of the fund to investors by increasing investors' confidence
- Demonstrating corporate governance
- Protecting investors' assets in the event of an insolvency event of the responsible entity/trustee
- Utilizing the custodian's scale to minimize transaction costs and operational efficiency

In addition to traditional custodian services, depicted above, modern custodians of digital assets provide security and safekeeping of assets, which requires additional controls.

In today's market place, the following factors need to be considered:

a) The design and orchestration of the technology involved in digital asset safekeeping is a highly specialized endeavour.

b) Organizations engaging in a number of activities are simultaneously undertaking digital asset safekeeping.

Given the current environment and understanding of digital assets, specialized organizations which understand and can demonstrate adequate implementation of requisite controls can be relied on to provide modern custodial services. Just the same, if self-custody is implemented, it should be expected to meet the same level of stringent controls. Due to the specialized nature of the activity and the advantages of appointing a specialized custodian, the industry should be encouraged to segregate custodial services from others.

PART 3 - Risks related to platforms

Question 2: What best practices exist for Platforms to mitigate these risks? Are there any other substantial risks which we have not identified?

Ans:
Risks are best mitigated by ensuring implementation and practice of identified controls, which are monitored, reported on, and audited by a third party. The best way to assert controls are designed and operating effectively is by obtaining an insurance policy via regulated insurance companies.

The act of obtaining an insurance policy mitigates risks in two very important ways:

1. It allows for the issuance of insurance claims in the event of losses, making customers whole.

2. Insurance companies are currently the most knowledgeable third parties regarding the design and implementation of a rigorous set of controls. This is no surprise considering they are accepting the transfer of the underlying risk.

Insurance providers must on a periodic basis assure themselves that all operational controls are in order, including internal and/or external controls; both qualitative and/or quantitative. Thus, the act of obtaining insurance is a higher marker for safety than any other controls (i.e. SOC2, COSO, ITIL, etc) and provides a degree of security to those whose assets are insured under custody. By enforcing insurance coverage on custodial services, regulators will enable effective and tested controls which in turn provide lower overall risk to the customer's digital assets under custody.

The safe-keeping of customer funds by entities that have not undergone the rigorous process of obtaining an insurance policy is a substantial unidentified risk.

PART 4 - Regulatory approaches in other jurisdictions

Question 3: Are there any global approaches to regulating Platforms that would be appropriate to be considered in Canada?

Ans: There are many other global approaches with arising regulatory frameworks in the space of digital custody and fintech. One of the ones that we have looked into is Autorité des Marchés Financiers (AMF) in France. As of April 11th, 2019, AMF has adopted the PACTE draft Bill (action plan for business growth and transformation). This law will establish a framework for fundraising via the issuance of virtual tokens (ICOs) and digital assets services providers (DASP). Under this bill, there are two focus areas: 1) optional visa regime for ICOs and 2) optional license for digital assets services providers.

PART 5 - The Proposed Platform Framework

5.2.1 Custody and verification of assets

Question 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.

Ans:
As indicated in previous answers, it is highly recommended that regulators discourage self-custody until organizations develop the knowledge and technology required to be able to provide insured custodial services.

In most cases, the best route for any Platform will be to appoint a third party custodian that is adequately insured.

Question 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?

Ans:
In our experience, working extensively with both the insurance industry and consulting firms in the current climate, the issuance of SOC 2 Type I and Type II reports is not an adequate marker of safety.

As indicated above, at the current moment, based on our experience, entities from the insurance industry are the third parties best fit to assess the design and implementation of a set of controls in digital asset custody.

In addition to the advantages stated above, insurers have shown themselves capable of learning and adapting to the level of controls expected at a faster pace than any other third parties. They can thus be expected to steadily increase the safety of the industry as a whole.

Many organizations are generating SOC2 reports by using smaller third party consulting practices not recognizable on the market while the big 4 consulting firms are still establishing benchmarks for SOC2 controls that will apply to digital custody services. Should SOC2 reports mature to the point that they are useful markers of safety, their issuance may be recommended. At the moment, however, we do not believe that obtaining such a report is indicative of a sound operation.

The best way of assuring regulators that a Platform has an adequate level of controls is by way of obtaining an insurance policy that transfers the most critical risks. In such a way, regulated third parties who are willing to expose capital to these risks are vetting the safety of any Platform.

Question 6: Are there challenges associated with a Platform being structured so as to make actual delivery of crypto assets to a participant's wallet? What are the benefits to participants, if any, of Platforms holding or storing crypto assets on their behalf?

Ans:
In many cases, a Platform's operation requires holding or storing assets on a participant's behalf. In cases where this is not required, it is recommended that participants be given the right to hold the assets on their own terms.

However, in the many cases where a Platform's operation requires that it hold or store assets on a participant's behalf, regulators should be assured that the assets are safely stored. The recommendation for most cases is for the Platform to appoint an insured third party custodian that meets the stringent levels of safety expected.

5.2.2 Price determination

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

Ans:
In our opinion, the best demonstrated pricing of digital assets has been shown in the pricing of futures contracts traded on the CME and CBOE. For example, the CME CF Bitcoin Real Time Index (BRTI) and and the the CME CF Bitcoin Reference Rate (BRR).

The methods used are in alignment with SEC requirements, and the generation of agreeable reference rates for other products should be welcomed by the industry.

Question 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?

Ans:
See Question 7.

5.2.3 Surveillance of trading activities

Ans:
We believe that Questions 9 through 12 are important to address. However, we do not presently engage in trading activities and we wish to leave treatment of this area to others.

Question 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?

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

Question 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? ?

Question 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?

5.2.4 Systems and business continuity planning

Technology and cyber security are key risks for Platforms. For these reasons they will also be required to comply with the systems and business continuity planning requirements applicable to existing marketplaces in Regulation 21-101.

Question 13: Under which circumstances should an exemption from the requirement to provide an ISR by the Platform be considered? What services should be included/excluded from the scope of an ISR? Please explain. ISR = independent system review.

Ans: Third party assessments are recommended and should continue to be a requirement. Independent system reviews are already a part of insurance market efforts. Insurance policies are priced partly on the basis of such reviews. It is highly recommended that the scope of services be defined by insurance markets in the interim, with others such as consulting services set to follow.

5.2.5 Conflicts of interest

Question 14: Is there disclosure specific to trades between a Platform and its participants that Platforms should make to their participants?
We do not presently engage in trading activities and we wish to leave treatment of this area to others.

Question 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?

Ans:
Beyond the worries surrounding safe-keeping, entities engaging in self-custody may produce conflicts of interest that need to be carefully considered. As such, the appointment of a third party custodian is the best recommended practice at the moment, until such time as the full set of conflicts of interest are understood and appropriately accounted for in entities wishing to engage in self-custody of digital assets.

5.2.6 Insurance

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

Ans:
As indicated above, we believe that obtaining an insurance policy is one of the best ways to both safeguard participants and assure regulators that a Platform has implemented an adequate set of controls.

The risks transferred should include, at a minimum, theft and loss of assets, including internal collusion within the entity safekeeping digital assets. Obtaining such insurance ensures the client that operational and security controls have been tested and continue to be monitored by the insurance provider. In most cases, companies obtaining insurance policies are obtaining either inadequate levels of insurance, inadequate range of coverage, or both.

Question 17. Are there specific difficulties with obtaining insurance coverage? Please explain.
Ans:
Exceedingly few firms have designed and implemented the rigorous set of controls necessary to safely store digital assets. Most of these firms, including those capable of obtaining SOC Type I or Type II reports, would fail to secure an insurance policy due to the stringency of controls expected. It is for this reason that the capability to obtain and renew an insurance policy remains the best assurance of underlying safety to regulators and participants.

Custodians with adequate controls should have no problem obtaining insurance.

Question 18. Are there alternative measures that address investor protection that could be considered equivalent to insurance coverage?
Ans:
Alternatives may include practices such as the establishment of a reserve fund of cryptocurrencies or digital assets whose prices correlate with those of the digital assets exposed to theft and loss risk. Such reserves should themselves be held in an insured custody arrangement.

5.2.7 Clearing and settlement

Ans: Questions 19-21 are not within the scope of KNØX's operations.

Question 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?

Question 20: What, if any, significant differences in risks exist between the traditional model of clearing and settlement and the decentralized model? Please explain how these different risks may be mitigated.

Question 21: What other risks are associated with clearing and settlement models that are not identified here?

5.2.8 Applicable regulatory requirements

Question 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.
Ans: SOC2 requirements need to be modified for digital custodians before they are deemed fit to assess the safety of any firm engaging in custodial activities. Digital custodians need to mature for SOC2 requirements to be modified and/or updated thereby incorporating/understanding digital custody service needs.