Comments on Consultation Paper 21-402:
Proposed Framework for Crypto-Asset Trading Platforms

TO: Canadian Securities Administrators/Investment Industry Regulatory Organization of Canada
FROM: PARADISO VENTURES INC. O/A Balance
Date: May 15th, 2019

Dear Sir/Madam,

As a federally incorporated fintech business focused on crypto-assets, PARADISO VENTURES INC. O/A Balance ("**Balance**") respectfully wishes to make the following observations and comments in reply to *Consultation Paper 21-402: Proposed Framework for Crypto-Asset Trading Platforms* jointly published by the *Canadian Securities Administrators* (the "**CSA**") and the *Investment Industry Regulatory Organization of Canada* ("**IIROC**") on March 14th, 2019. Allowing room for innovation while ensuring the fair and efficient functioning of our capital markets is a tough balancing act. We hope our contribution will help towards building a tailored framework that will not only bring much needed clarity to ecosystem participants, but also ensure that Canada maintains its reputation on the international stage as a financial markets leader and innovator in this new digital economy.

We address some of the consultation questions below.

1. *Question 1: Are there additional factors not mentioned in the paper that should be considered in making the determination of whether or not a security or derivative might be involved in the trading performed on Platforms?*

We believe the factors enumerated are sufficient in helping make a determination, however further clarification is needed around the criteria of what counts as delivery of crypto assets. To provide some context before explaining our view, we would like to highlight the distinctions between possession, ownership, and control. If a participant generates the private cryptographic key used to access the crypto-asset themselves, they have possession, ownership, as well as control of the asset. If a Platform generates it on their behalf:

- directly: the participant lost both possession, as well as control;
- indirectly (e.g. through a custodial key management system): the participant lost possession, but retains partial or full control.

The matter of ownership comes down to whether or not the Platform passes the full legal title to the client, or whether the right in the bundle get split and held by both the participant as well as the Platform (specified typically in a Platform User Agreement or equivalent document).

As such, if a participant purchases a crypto-asset from a Platform, we expect the following criteria to be met for delivery to have occurred:

- the crypto-asset was delivered to a participant approved digital wallet that they have partial or full control of (i.e. participant controls the asset);
- the participant has first rights and full legal title to the crypto-asset (i.e. participant owns the asset);

- delivery needs to occur within a reasonable time frame as evidenced by an independently verifiable cryptographic proof (confirmed blockchain transaction or signed transaction in a state channel or sidechain that could be closed and broadcast to the blockchain by the participant at any time).

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

   We suggest the following best practices for mitigating some of the risks highlighted:
   - *Investors' crypto-assets may not be adequately safeguarded*: With over 1B dollars worth of crypto-assets lost or stolen from Platforms globally last year, we would see this risk mitigated by Platforms through:
     - full-segregation of digital wallets for each client as evidenced by regular third-party audits (i.e. no more pooled wallets where the entire Platform treasury can be lost in one incident);
     - offline (i.e. air-gapped) generation of private keys controlling the wallets, as well as offline management of the key for its entire lifetime (i.e. transactions signing must also be performed offline);
     - adequate disaster recovery and succession planning protocol that are tested and meet the business purpose as well as specified service level agreements, as evidenced by regular third-party audits.

   Whether Platforms self-custody or choose to work with a third-party custodian, we see a *SOC 2 Type I (Security)* report as a core minimum competency that should be met by any ecosystem participant providing custodial services.

   - *Processes, policies, and procedures may be inadequate*: This risk could be partially mitigated by Platforms requiring personnel have any form of access to Platform's or participants' crypto-assets to pass and be subject to ongoing background and criminal checks. The existence, suitability, and application of processes for ensuring business continuity, and addressing key personnel and regulatory compliance risks can be demonstrated through a qualified opinion provided by a third-party, typically in the form of a SOC report.

   - *Investors' assets may be at risk in the event of a Platform's bankruptcy or insolvency*: fully mitigated by Platforms that pass the full legal title to the participant and do not keep the participants' assets on their balance sheet. For Platforms that include participants' assets on their balance sheets for rehypothecation, existing risk mitigation strategies in the applicable regulation should be sufficient.

   - *Investors may not have important information about the crypto assets that are available for trading on the Platform*: could be partially mitigated by requiring Platforms to publicly disclose their selection criteria through the form of a Digital Asset Selection Framework or equivalent document, as well as their policy for managing hard and soft forks, as well as airdrops in a Fork Policy or equivalent document.

   - *Investors may not have important information about the Platform's operations*: could be partially mitigated by requiring Platforms to publicly disclose the ownership, possession, and control parameters around the participant's crypto-assets (as per the definitions in the answer to Question 1 above) in their User Agreement or an equivalent document.

   - *Conflicts of interest may not be appropriately managed:* partially mitigated through requiring Platforms that act as market markers or trade as principal to publicly disclose so in their User Agreement or an equivalent document.

- *Investors may purchase products that are not suitable for them*: partially mitigated by Platforms that keep any information displayed to participants as general, historical, and impersonal in nature. For Platforms that offer financial and investment advice, existing risk mitigation strategies in the applicable regulation should be sufficient.

- *Manipulative and deceptive trading may occur*: mitigated through the implementation of existing monitoring requirements in the applicable regulation, and regular reporting to a regulation services provider.

- *There may not be transparency of order and trade information*: mitigation strategies in the existing regulation should be sufficient, for the Platforms where this is applicable.

- *System resiliency, integrity and security controls may be inadequate*: although we are aware there currently are challenges in obtaining such reports, we believe the correct way to mitigate these risks is through requiring platforms to demonstrate the existence of appropriate controls by obtaining a qualified opinion (e.g. SOC for Cybersecurity) from a third-party auditor or cybersecurity firm.

At the time of this writing we do not identity any other substantial risks that would require mitigation, other than the ones already highlighted in the paper.

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

Proving and tracking ownership of a digital file through a cryptographically linked series of transactions recorded in a ledger secured via a proof of work consensus mechanism is a fundamental computer science breakthrough. When such digital file is a cryptographic key controlling a scarce resource with a finite supply and mathematically encoded emission schedule (e.g. Bitcoin), that resource can be best classified as a digital commodity, thus in our view the approach taken by the Securities Commission in Malaysia is not appropriate. The question of whether or not a Platform is dealing in digital commodities or securities such as a derivative comes down to a test of delivery (see the answer to Question 1). The CFTC's approach in the United States to the proposed interpretation of the term "actual delivery" is something the Canadian provincial regulators could mirror.

4. *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.*

We hope to see the following standards adopted by Platforms or any ecosystem participant involved
in the act of doing crypto-asset custody:

- one or more sets of fully segregated wallets are maintained for each participant;
- participant's assets are potentially split multiple digital wallets to prevent very large amounts being controlled by one individual cryptographic key;
- the cryptographic keys controlling the digital wallets should be generated offline and managed offlined for the lifetime of the key, on dedicated hardware (e.g. Hardware Security Modules) that have achieved a rating of FIPS 140-2 Level 3 or higher;
- access to the digital wallets by employees should be restricted based on role, following the principle of least-privilege;
- the cryptographic keys should be stored in bank grade vaults that are access controlled, monitored, and guarded 24/7;

- access to the digital wallets should be regulated using a per-wallet encryption scheme and one-time passwords for access to signing transactions;
- transactions should require the coordinated actions of multiple employees of both the participant, as well as multiple employees;
- access to funds as well as other relevant operations should be recorded on immutable, tamper-proof logs residing outside of the organization, and made available to the participant for auditing purposes;
- adequate disaster recovery and succession planning protocol that are tested and meet the business purpose are in place, as evidenced by SOC2 report done by an auditing firm;
- their corporate headquarters should not store or contain crypto-assets of material value;
- employees should pass and be subject to ongoing criminal and credit background checks.

Unfortunately Canada currently lacks a dedicated solution that meets the above criteria, and as such most Platforms are forced to work with foreign custodians (e.g. BitGo, Gemini Custody, Kingdom Trust, Coinbase Custody). Our aim at Balance is to bring such a solution to the Canadian market in the near future.

5. *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?*

Although we would like the case to be otherwise, after spending close to two years building a custody solution, we've come to regard a SOC2 report as a requirement in demonstrating the core competencies needed to provide crypto-asset custodial services. Most approaches we've seen attempted in the space around providing cryptographic proof of funds are either immature or can be easily spoofed.

6. *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?*

Actual delivery of crypto-assets is a challenge due primarily to the operational complexity involved in maintaining fully-segregated wallets for each participant. However, we do not see any benefits to participants in Platforms holding crypto-assets on their behalf, rather we regard this as a historical artifact. As the space gained momentum, some of the early solutions and processes had to be unfortunately stretched past their limit and kept in operation to this day. We hope this to change as more infrastructure pieces get built and brought to market, such as dedicated custodian and wallet management platforms.

7. *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.*

Given the risk and extremely sensitive nature of the business, we believe the custodial aspect of Platforms should be included in the scope of an independent systems review.

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

We believe Platforms that act as market markers or trade as principal should publicly disclose it to their participants in their User Agreement or an equivalent document.

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

We would expect Platforms to obtain insurance at least for their hot or warm wallets. Insurance for the assets kept offline in cold wallets is debatable, if the appropriate controls and policies are put in place to protect against external threats, human error, and misuse of insider access, as evidenced by a SOC 2 report.

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

While there is interest from both Platforms and brokers to put insurance policies in place, most underwriters lack the appropriate models for quantifying risk. As such most Platforms end up insuring just the hot or warm wallets, as insurance for the cold wallets is either impossible or prohibitively expensive to get.

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

While there are other measures that can be put in place to address investor protection and mitigate risk (e.g. split large amounts of crypto-assets across multiple digital wallets controlled together as a logical unit by the participant), they cannot unfortunately be considered equivalent to insurance coverage.

The management team at Balance hopes you found our comments and feedback insightful. We're grateful to be part of the process and have the opportunity to have our views considered, and are available to provide any further clarifications on our comments. Please do not hesitate to contact us.

With respect,

George Bordianu
Co-founder & CEO
PARADISO VENTURES INC. O/A Balance