**Chartered Professional Accountants of Canada**
277 Wellington Street West Toronto ON CANADA M5V 3H2
T. 416 977.3222 F. 416 977.8585
www.cpacanada.ca

**Comptables professionnels agréés du Canada**
277, rue Wellington Ouest Toronto (ON) CANADA M5V 3H2
T. 416 204.3222 Téléc. 416 977.8585
www.cpacanada.ca

May 15, 2019

The Secretary
Ontario Securities
Commission 20 Queen
Street West
22nd Floor, 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

Investment Industry Regulatory Organization of Canada
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

Dear Sirs/Mesdames:

**Subject: Joint CSA/IIROC Consultation Paper 21-402 Proposed Framework for Crypto-Asset Trading Platforms**

Chartered Professional Accountants of Canada (CPA Canada) appreciates the opportunity to comment on the Joint Canadian Securities Administrators (CSA) / Investment Industry Regulatory Organization of Canada (IIROC) Consultation Paper 21-402 *Proposed Framework for Crypto-Asset Trading Platforms* (Consultation Paper) which seeks feedback on how requirements may be tailored to establish a framework that provides regulatory clarity to platforms that facilitate the buying and selling or transferring of crypto assets (Platforms).

We support the joint CSA/IIROC initiative to provide greater regulatory certainty and appropriately regulate Platforms in a market that continues to evolve, while endeavoring to facilitate innovation that benefits investors and our capital markets.

CPA Canada is one of the largest national accounting bodies in the world representing more than 210,000 members. CPA Canada conducts research into current and emerging business issues and supports the setting of accounting, auditing and assurance standards for business, not-for-profit organizations and government. CPA Canada also issues guidance and thought leadership on a variety of technical matters, publishes professional literature and develops education and professional certification programs.

In formulating our response on specific aspects of the Proposed Platform Framework referred to in the Consultation Paper, we have drawn on our knowledge of audit and assurance practices and unique challenges related to auditing crypto assets. We also solicited input from our extensive network of volunteers representing members from accounting firms with expertise in the areas of crypto assets, blockchain, and system and organization controls (SOC) reporting.

## Overall Comments

We see continued interest in blockchain technology and foresee a future filled with digital asset transactions. From this perspective, this consultation is extremely important, and the issues raised in the Consultation Paper are critical for investor protection.

Emerging financial technology is a key area of focus for CPA Canada. We believe transparent and auditable crypto asset trading and custodial services are critical, and that the accounting profession plays a vital role in building public confidence in these areas.

CPA Canada is committed to supporting our members and other stakeholders in the blockchain and crypto asset ecosystem by working with industry experts, the CSA, academia, and accounting and auditing and assurance standards setters through our various committees and working groups. Some

of our recent educational initiatives include publications on blockchain technology[1], accounting for cryptocurrencies[2] and auditing cryptocurrencies[3].

We also wish to highlight a recently formed Crypto-Asset Auditing Working Group, facilitated by CPA Canada and Auditing and Assurance Standards Board (AASB) staff, which includes representatives from the Canadian Public Accountability Board (CPAB), CPA provincial practice inspection, and the auditing firms. The purpose of this working group is to discuss issues related to the application of Canadian Auditing Standards (CASs) in the crypto asset industry and develop relevant non-authoritative guidance for audit practitioners.

## Responses to Consultation Questions

After reviewing the specific questions in the Consultation Paper, we have elected to provide a response to question 5 only:

***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?***

### Background Information

In Canada, SOC 2 reports are issued based on engagements performed under Canadian Standard on Assurance Engagements (CSAE) 3000, *Attestation Engagements Other Than Audits or Reviews of Historical Financial Information* and with use of the AICPA's Trust Services Criteria (TSC) for Security, Availability, Processing Integrity, Confidentiality, and Privacy. SOC 1 reports are issued in Canada based on engagements performed under CSAE 3416, *Reporting on Controls at a Service Organization* as well as CSAE 3000. These standards are included in the "Other Canadian Standards" section of the *CPA Canada Handbook - Assurance*. Herein, we will refer to SOC 1 and SOC 2 reports for simplicity.

### The Importance of Establishing Relevant Controls

Before determining the assurance approach, it is vital to first identify the controls required at a Platform to mitigate the risks related to Platforms (i.e., those identified in Part 3 of your Consultation Paper and any additional risks identified through consultation). It is important that you establish expectations regarding the scope and/or a baseline set of high-level control objectives (i.e., control objectives are opined upon in a SOC 1 report) or system requirements (i.e., system requirements are opined upon in

[1] https://www.cpacanada.ca/en/business-and-accounting-resources/audit-and-assurance/canadian-auditing-standards-cas/publications/impact-of-blockchain-on-audit
[2] https://www.cpacanada.ca/en/business-and-accounting-resources/financial-and-non-financial-reporting/international-financial-reporting-standards-ifrs/publications/accounting-for-cryptocurrencies-under-ifrs
[3] https://www.cpacanada.ca/en/business-and-accounting-resources/audit-and-assurance/canadian-auditing-standards-cas/publications/cryptocurrency-audit-considerations

a SOC 2 report) that may be relevant in a controls assurance engagement for a Platform. The baseline control objectives/system requirements (herein referred to as 'controls') expected may include, among others, those that would be intended to manage and mitigate the custodial risks, including safeguarding of private keys and ensuring that investors' crypto assets exist, are appropriately segregated and protected, and that transactions with respect to those assets are verifiable.

In addition to traditional custodial risks, there are unique risks that need to be addressed for Platforms such as client authentication, address verification, transaction approvals and multi-signature implementation, key management, asset verification, currency due diligence, and fork management. Another important consideration is whether there are controls in place that address completeness of balances and transactions, and more specifically the risk of "off-chain" transactions not being recorded by the Platform.

The SEC's Custody Rule is one example of how you may specify what is appropriate from a control scoping standpoint without being too prescriptive. Custody is only one aspect of the Platform's services that may need to be expanded upon to include critical control requirements that may be relevant depending on what services are being offered by the particular Platform.

Once you have established the scope and/or baseline of controls expected, options to provide assurance over the design and operating effectiveness of those controls can be explored. We would appreciate the opportunity to provide input on alternatives once that baseline has been established. CPA Canada's Crypto-Asset Auditing Working Group is currently exploring which risks and controls at a custodian (i.e., service organization) of crypto assets are relevant to the user-entity's[4] financial reporting. Although the scope of controls at a custodian relevant to audits of user-entity financial statements may differ from the scope of controls expected by you as the regulator, our research could inform the development of your Platform Framework and we would be happy to share our findings when they are ready.

The Consultation Paper notes that Platforms seeking registration as an investment dealer and IIROC membership that plan to provide custody of crypto assets will not only need to satisfy existing custody requirements but will also be expected to meet other yet-to-be determined requirements specific to the custody of crypto assets. We agree that requirements specific to the relevant risks should be established. It will be important to understand the unique risks and address them appropriately to balance the protection of the public interest and the ability for organizations to innovate in Canada.

**Contemplation of SOC Reports**

The Consultation Paper notes that you are contemplating requiring SOC 2, Type I and II Reports for a Platform's custody system, and if they use third-party custodians, to ensure that the third-party custodians have SOC 2, Type I and II Reports. While we agree that one way to provide assurance on such controls may be through the issuance of SOC 2 reports, not all SOC 2 reports have the same scope of controls. If the SOC 2 report does not cover the scope of controls you expect, then it will not

[4] A user-entity is an entity that uses a service organization and whose financial statements are being audited.

provide the assurance you are seeking.

For example, a minimum scope SOC 2 report may cover only those controls required to meet the Security category of the TSC and would exclude the additional criteria and controls for system Availability, Processing Integrity, Confidentiality, and Privacy. While it seems unlikely that the securities and investment industry regulators would require a SOC report on confidentiality and privacy controls (which is not an independent assurance reporting requirement for traditional asset exchanges), it is possible you may expect SOC 2 reports for some or all Platforms to address relevant aspects of security, processing integrity and possibly availability. If this is the case, it may be appropriate that the SOC 2 report for a Platform cover the criteria for Security, Processing Integrity, and possibly Availability.

In addition, you may wish to require specific regulatory controls for such Platforms (see the 2018 SOC 2 Description Criteria[5] and 2017 Trust Services Criteria[6] for details) to help ensure the controls covered in the SOC 2 report meet your expectations. For example, there may be specific control requirements related to client acceptance, transaction processing, and custody that may not be covered by the generic Processing Integrity criteria from the TSC.

As an alternative to SOC 2 reporting, you may consider if a SOC 1 report, with the appropriate scope and control objectives, may be sufficient in addressing regulatory expectations for controls assurance. SOC 1 reports are often used to provide controls assurance for traditional custody and exchange services, so it is unclear why they may not also be suitable for Platforms, provided the appropriate scope and control objectives are covered.

It may be possible to develop a set of regulatory requirements for Platforms that could be used as either System Requirements for SOC 2 reporting, or Control Objectives for SOC 1 reporting, and allow the exchange to decide whether to obtain a SOC 1 or SOC 2 report.

**Platform Readiness**

Regardless of whether a SOC 1 or SOC 2 report is provided, it is not possible to provide an unqualified opinion in a Type II report (e.g., SOC 1 Type II or SOC 2 Type II) until the Platform has been in operation for a reasonable period of time (e.g., 6 months). Consideration should be given when a Type I report may be accepted initially, and what the maximum period of time is that the Platform can operate until a Type II report is required; or if some scope limitations in the service auditor's opinion may be acceptable for an initial Type II report on a new Platform.

It is also important to consider if effective controls were in place from the commencement of crypto-asset activities, not just the audit year- or period-end. For example, if a wallet was created without appropriate safeguards over the private key, it may be difficult for an auditor to conclude whether all

[5] https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/dc-200.pdf

[6] https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/trust-services-criteria.pdf

relevant controls were designed, implemented and operating effectively.

**Alternative Assurance Options**

CSAE 3000

An alternative way in which auditors or other parties could provide assurance over a Platform's controls (other than SOC 1 and SOC 2 reporting) may be by performing an engagement under CSAE 3000, which could potentially provide assurance on a wide variety of relevant subject matter that may include but not necessarily be limited to controls, transactions, balances, regulations, etc. as long as suitable reporting criteria can be defined.

CSAE 3000 engagements may include, for example, an audit of a service organization's description of its controls and the suitability of design and operating effectiveness of those controls. This type of engagement is currently accepted for entities providing traditional exchange or custodial services, however we are aware of scrutiny in the market with this type of report since the scope can vary significantly. The viability of this option depends on the availability of appropriate criteria and controls to promote consistency and quality in reporting.

Another factor to consider is that CSAE 3000 engagements can provide reasonable assurance (i.e., the level of assurance obtained by an audit) or limited assurance (i.e., the level of assurance obtained by a review), as defined in CSAE 3000. You may consider what level of assurance you require (reasonable assurance, limited assurance or possibly no assurance through an Agreed-Upon Procedures engagement – see below) prior to finalizing your Proposed Platform Framework.

Agreed-Upon Procedures (AUP) Engagement[7]

While Question 5 in this Consultation Paper asks for alternative ways in which auditors or other parties can provide assurance, you may also wish to consider AUP engagements. AUP engagements do not provide assurance but may still be a viable option depending on the objectives of the Proposed Platform Framework. As an example, this is the type of engagement performed in Japan with respect to customer asset segregation for virtual currency exchange (VCE) service providers. With the enactment of the amended Payments Services Act in April 2017 in Japan, VCE service providers are now subject to financial statement audits and segregation of funds audits, with the segregation of funds audits being performed using the Segregation of Funds AUP Guidance[8].

[7] In Canada, AUP engagements are currently performed under one of the following standards: Section 9100, *Reports on the Results of Applying Specified Auditing Procedures to Financial Information Other than Financial Statements* or Section 9110, *Agreed-Upon Procedures Regarding Internal Control Over Financial Reporting*

[8] https://kmra-cpa.com/en/financial-statement-audits-of-virtual-currency-traders-2/

**********

We appreciate the opportunity to participate in this consultation and would be happy to meet to discuss our comments further. Please do not hesitate to contact Taryn Abate, Director, Research, Guidance and Support (tabate@cpacanada.ca) or myself.

Yours truly,

Gordon Beal, CPA, CA, M. Ed
Vice-President, Research, Guidance & Support
Chartered Professional Accountants of Canada