cpab exchange

Auditing in the crypto-asset sector

Existence of crypto-assets held by third parties

The Canadian Public Accountability Board (CPAB) is concerned about the quality of evidence that some auditors are obtaining when auditing the existence of crypto-assets held in custody by third parties. This report describes things that auditors should be considering when auditing the financial statements of reporting issuers that use custodians to safeguard their crypto-assets.

Introduction

The nature of crypto-assets makes them more vulnerable than traditional assets to theft or loss[1]. Reporting issuers with business models that involve holding material crypto-assets are often outsourcing custody of their crypto-assets to third parties that specialize in offering crypto-asset custodial services (collectively "custodians"). Custodians include crypto-asset trading platforms (i.e., where crypto-assets can be bought, sold and custodied) and other third-party custodians.

About CPAB

CPAB is Canada's independent, public company audit regulator. Charged with overseeing audits of financial statements of reporting issuers performed by registered public accounting firms, CPAB contributes to public confidence in the integrity of financial reporting and is committed to protecting Canada's investing public.

We are concerned about the quality of audit evidence that some auditors are obtaining when auditing the existence of crypto-assets held by custodians. A recurring theme in many of our significant inspection findings is that auditors did not obtain a sufficient understanding of the risks associated with the reporting issuers' crypto-asset custody outsourcing arrangements. That led those auditors to perform audit procedures that were not sufficiently responsive to the risks. For example, CPAB identified significant inspection findings where auditors relied on information produced by custodians (e.g., audit confirmations and client account statements) as their only source of audit evidence that crypto-assets held by custodians existed at the reporting issuers' balance sheet dates.

It is important for auditors to recognize that outsourcing custody of crypto-assets to custodians does not necessarily mean those assets will be safe. Relying on representations from custodians as the only source of audit evidence is not an adequate response by auditors to elevated risks associated with the existence assertion. Appropriate audit responses will often include evaluating and testing the custodians' relevant controls. Those include controls associated with how the custodians are safeguarding customers' crypto-assets and ensuring that records of customers' balances and transactions are complete and accurate.

[1] Due to the susceptibility of crypto-asset private keys to being lost or stolen, whether held directly or with a third party.

The existence assertion

When management records crypto-assets held by custodians on the reporting issuer's balance sheet, management is asserting that the reporting issuer owns the assets and that the assets exist (i.e., they haven't been lost or stolen while in the custody of the custodian) at the balance sheet date. The existence assertion is fundamentally a claim that those assets stand ready to be transferred out (i.e., withdrawn) of wallets maintained by custodians without delay at the reporting issuer's balance sheet date.

This report focuses on the existence assertion when reporting issuers retain ownership of the crypto-assets they've transferred to custodians for safekeeping (Exhibit 1).

Exhibit 1

Impact on ownership rights when custody of crypto-assets is outsourced

Outsourcing custody of crypto-assets to custodians gives rise to a complex accounting question: do the crypto-assets continue to belong to the reporting issuer or have the ownership rights passed to the custodian?

The answer depends on a consideration of concepts of "control" and "benefits" to determine which party, the reporting issuer or the custodian, is subject to substantial risks and rewards incidental to ownership. Canada's Accounting Standards Board's (AcSB) **IFRS Discussion Group** published guidance on factors to consider, from the vantage point of the custodian, when determining whether the custodian owns the crypto-assets they are tasked with safeguarding. Auditors may find that the guidance is also useful when evaluating the ownership determination from the reporting issuer's perspective.

Required work effort for user auditors

Canadian Auditing Standard (CAS) 402 describes the audit requirements for audits of financial statements of user entities that obtain services from service organizations. We describe in this report some of the requirements in CAS 402 that are relevant to auditors (user auditors) in audits of the financial statements of reporting issuers that use the services of custodians to safeguard their crypto-assets.

User auditors are required to perform the following, among other things, for each material custodial-services arrangement:

- **Identify and assess risks ->** Obtain an understanding of the nature and significance of the custodial services provided by each custodian that holds material crypto-assets to inform the identification and assessment of the risks of material misstatement.
- **Respond to assessed risks ->** Design and perform audit procedures responsive to those risks.

This report is not intended to describe all the considerations or procedures that auditors should perform in their audits. User auditors should understand the requirements in CAS 402 and consult with internal or external experts when those requirements are unclear.

Identify and assess risks

It is critically important for user auditors to obtain an understanding of the material custodial arrangements to inform their identification and assessment of risks of material misstatement related to the existence assertion for crypto-assets held at custodians.

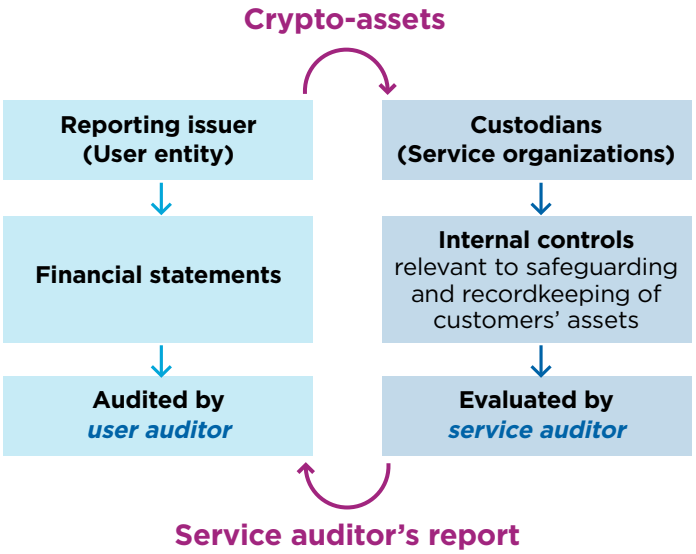
Obtain and review the custody service contract

User auditors should obtain and review the contract (i.e., service-level agreement) between the custodian and reporting issuer to understand the following:

- Are the reporting issuer's crypto-assets held by the custodian in a segregated account (i.e., segregated from other customers' crypto-assets and with a unique address on the blockchain) or commingled with crypto-assets of other customers (referred to as an omnibus account)? Custodians often commingle their customers' crypto-assets in an omnibus account with a single address on the blockchain. It simplifies key management for custodians and is a more cost-effective way for custodians to manage their customers' crypto-assets. Omnibus accounts do, however, give rise to new risks. For example, customers lose the ability to monitor movements of their crypto-assets when they are commingled in omnibus accounts and customers have to rely on commitments by the custodian that the custodian will act in an agreed-upon manner (e.g., to not use customers' crypto-assets for the custodian's own investment purposes, etc.).
- Does the custodian have the right to use customers' crypto-assets (e.g., pledge, repledge, hypothecate, rehypothecate, sell, lend, stake, arrange for staking, etc.) for its own investment purposes? This could create a mismatch between the duration of the custodian's assets (i.e., investments) and the custodian's liabilities (i.e., customer deposits) that leads to an inability by the custodian to honour withdrawal requests by the reporting issuer in a timely manner.
- Has the custodian outsourced the responsibility to safeguard its customers' crypto-assets to another custodian (sub-custodian)? When that responsibility has been outsourced to sub-custodians, the user auditor also needs to understand the sub-custodial service arrangements, risks that emerge from the use of each sub-custodian (including understanding the relevant controls of the sub-custodian) and respond to those risks.
- Is there an indemnification clause in the contract that specifies remedies for the reporting issuer in the event its crypto-assets are lost or stolen while in the care of the custodian?
- How much insurance coverage does the custodian have to indemnify customers in the event of loss or theft of its customers' crypto-assets?
- Does the user auditor have rights of access to the custodian's accounting records related to the reporting issuer (i.e., account details, transaction history and related controls)?
- Does the contract allow for direct communication between the user auditor and the custodian's auditor (service auditor)?

Obtain and review the service auditor's report

User auditors are also required to obtain an understanding of relevant controls[2] in place at each custodian tasked with safeguarding a material amount of the reporting issuer's assets (e.g., crypto-assets) to inform user auditors' assessments of control risk[3]. Relevant controls are those that address significant risks and risks that cannot be mitigated with substantive procedures alone. Relevant controls that relate specifically to the existence assertion will generally fall into one of two categories:



- Controls over safeguarding of customers' crypto-assets (i.e., loss or theft). For example, the custodian will typically have controls related to cryptographic key management for "hot" and "cold" wallets.[4]
- Controls over record keeping of customer balances (i.e., crypto-asset balances). For example, the custodian may perform periodic reconciliations of blockchain data to the custodian's internal books and records related to customer crypto-assets held in omnibus accounts.

To understand the relevant controls, user auditors will typically obtain and review relevant service auditors' reports that describe the scope and related testing in System and Organization Controls (SOC) engagements for applicable custodians. SOC engagements are performed by auditors engaged directly by custodians (i.e., service auditors). There are several types of SOC[5] assurance engagements (i.e., SOC 1, SOC 2, SOC 3, etc.) and each is designed for a specific purpose and for different stakeholders. The type of SOC engagement that best[6] meets the needs of a user auditor is a SOC 1 engagement because it relates specifically to the service organization's controls applicable to the user entity's internal control over financial reporting. There are also two types of SOC 1 reports:

- A Type 1 report attests to whether controls have been designed effectively and implemented at a point in time.
- A Type 2 report attests to whether controls have been designed effectively, implemented and operating effectively throughout the period covered by the report. A Type 2 report is required by user auditors when they intend to rely on the custodians' controls in their audit approaches when testing the existence of crypto-assets held by custodians.

[2] CAS 315 (Revised), *Identifying and assessing the risks of material misstatement,* paragraph 26(a) and CAS 402, paragraph 10.

[3] CAS 315 (Revised), paragraph 34.

[4] Also refer to a Viewpoints article by the Crypto-Asset Auditing Discussion Group that describes controls that custodians may be expected to have to adequately safeguard their customers' assets. The Crypto-Asset Auditing Discussion Group was assembled CPA Canada and the Canadian Auditing and Assurance Standards Board (AASB) and also includes representatives from audit firms, academics and CPAB.

[5] There is a patchwork of standards under Canadian, U.S, and international standards that apply to SOC engagements. Refer to non-authoritative guidance by Canada's Auditing and Assurance Standards Board (AASB) that describes the applicable standards in each jurisdiction that apply to the various types of SOC engagements.

[6] CPAB recognizes there may also be controls that are tested by service auditors in SOC 2 engagements that may be relevant to user auditors in their audits of financial statements of reporting issuers.

Respond to assessed risks

There is a low degree of interaction[7] between the reporting issuer and custodian when it comes to the custodian's safeguarding activities of the reporting issuer's crypto-assets. Auditors evaluate the degree of interaction to understand the significance of the custodian's controls. A low degree of interaction refers to the limited ability of a reporting issuer to implement its own controls to mitigate risks associated with the custodian's safeguarding of the reporting issuer's assets. Accordingly, controls at the custodian become particularly significant as the reporting issuer is forced to rely entirely on the effectiveness of the custodian's safeguarding controls to protect its assets.

In most cases, it will not be practicable for user auditors to respond to elevated risks associated with the existence assertion (for crypto-assets held by custodians) by performing substantive procedures alone. User auditors will often need to rely on tests of the operating effectiveness of relevant controls at custodians performed by service auditors. When SOC 1, Type 2 reports are available for custodians that hold material amounts of the reporting issuer's crypto-assets, the user auditor should obtain them and evaluate whether the controls described in the reports adequately respond to the user auditor's assessed risks. When SOC 1, Type 2 reports are not available, the user auditor will need to perform tests of controls at the relevant custodians directly or engage another auditor to perform those tests on its behalf.

There may be situations where controls described in SOC 1, Type 2 reports do not adequately address elevated risks identified by the user auditor that cannot be adequately responded to by performing substantive procedures alone. For example, the user auditor may identify that the custodian has the contractual right to use (e.g., pledge, repledge, hypothecate, rehypothecate, sell, lend, stake, arrange for staking, etc.) customers' crypto-assets for its own investment purposes (e.g., to earn a yield) but there are no controls in the SOC 1 report related to the custodian's asset and liability management (ALM). ALM controls respond to the risk that the custodian will not be able to honour withdrawal requests by customers because the custodian's investments (i.e., investments made using customers' deposits) cannot be realized in the same timeframe (i.e., as withdrawal requests). To respond to that risk, the user auditor may need to engage the service auditor to perform specified procedures including, for example, evaluating the design and operating effectiveness of ALM controls if such controls exist.

Audit engagement acceptance or continuance

Before accepting or continuing an audit engagement, auditors should consider whether they will be able to complete the audit engagement when the reporting issuer has outsourced custody of material crypto-assets to custodians that have not yet had their internal controls scrutinized by service auditors (i.e., SOC 1, Type 2 reports are not available). Integrating discussions with management and the audit committee about the reporting issuer's outsourcing arrangements when considering whether to accept or continue an audit engagement allows firms to anticipate and respond to obstacles that could affect the timely completion of their audit engagements.

[7] CAS 402, paragraphs 9(c) and A7 deal with the auditor's understanding of the degree of interaction between the activities of the service organization and those of the user entity.

Learn More

Visit us at www.cpab-ccrc.ca and join our mailing list. Follow us on Twitter — @CPAB-CCRC

www.cpab-ccrc.ca / Email: info@cpab-ccrc.ca

cpab ccrc
Canadian Public Accountability Board
Conseil canadien sur la reddition de comptes