CANADIAN PUBLIC ACCOUNTABILITY BOARD

CONSEIL CANADIEN SUR LA REDDITION DE COMPTES

CPAB

CCRC

Auditing in the Crypto-Asset Sector

Introduction

Many of the reporting issuers in Canada's crypto-asset sector obtained material crypto-asset holdings or engaged in material crypto-mining activity during the most recent fiscal year under audit. Planning and execution of these audits have begun.

CPAB will publish communications that reflect our perspectives and expectations of auditors related to audits of reporting issuers in the crypto-asset sector.

This communication highlights our expectations in a number of challenging areas but should not be regarded as an audit program. Auditors should continue to refer to relevant auditing standards when planning and executing their audits.

Existence and ownership rights associated with crypto-asset holdings

Existence

When an entity uses a blockchain to support the occurrence/existence of crypto-asset transactions/balances recorded in its financial statements, auditors will need to evidence their understanding of how transactions are recorded on the applicable blockchain ledger.

The protocols and cryptography associated with blockchains are designed to make blockchain ledgers resilient to tampering. However, the effectiveness of these attributes varies by blockchain and it would be inappropriate for auditors to rely on blockchain ledgers without first evaluating the reliability of the blockchains that are relevant for the audit. We expect auditors to engage blockchain and cryptography specialists to assist in understanding and evaluating blockchains that support amounts recorded in an entity's books and records where there is a risk of material misstatement[1].

Auditors should identify and document their understanding of the relevant *risks* relating to the occurrence/existence of crypto-assets on the blockchain including (i) invalid transactions are recorded on the blockchain, (ii) validated transactions are not recorded on the blockchain, and

[1] CAS 620, *Using the Work of an Auditor's Expert*, para. 7

(iii) validated transactions are subsequently modified. Auditors should identify the relevant *attributes* of the blockchain (e.g., cryptography, blockchain validation algorithms and consensus mechanisms) that mitigate those risks and perform tests to determine whether they are operating as intended.

In testing occurrence of an entity's crypto-asset transactions and the existence of the crypto-asset balance at year end, auditors will typically use tools called block explorers to review the information recorded on blockchain ledgers. Auditors should perform procedures to ensure that these tools are designed and operating effectively to extract the relevant information from the blockchain.

Ownership rights

Crypto-asset transactions offer some degree of anonymity because blockchain ledgers represent the identity of entities that have transacted crypto-assets as a string of alphanumeric characters for each public address.

In evaluating an entity's ownership assertion, auditors will need to design an audit approach that seeks to obtain sufficient appropriate audit evidence that the entity owns the crypto-assets that are associated with a public address.

Auditors, for instance, may request management to transfer a specified amount of a crypto-asset balance between crypto wallets controlled by the entity and inspect the blockchain record for the occurrence of the transaction. Alternatively, auditors may ask management to sign arbitrary messages to prove they have access to the private key that controls a crypto-asset.

The procedures above may be useful to verify an entity's access to the private key and control over the related assets. However, an entity's access to a private key should not be interpreted by auditors to mean that the entity has ownership rights to the related crypto-asset. This is because there is a risk that an entity could share the alphanumeric sequence of a private key with others such that multiple entities or individuals could assert ownership rights over the same crypto-asset.

We expect that auditors will assess the potential for misrepresentation of ownership rights as a fraud risk in most of these types of audits and design procedures to mitigate that risk[2].

Designing substantive procedures that are limited to verifying that an entity has access to the private key which controls a crypto-asset will be necessary but not likely sufficient to mitigate the fraud risk.

We expect that effective internal controls will be essential for management to establish to its auditors that the entity has rightful and sole ownership of crypto-assets. It will be very challenging for auditors to mitigate the risk associated with ownership rights without understanding and testing the design and operating effectiveness of these internal controls.

[2] CAS 240, *The Auditor's Responsibilities Relating to Fraud in an Audit of Financial Statements*

Internal controls that should be in place at the entity and tested by auditors include:

- Entity executes key ceremonies[3]. The objective of a key ceremony control is to ensure that the keys are generated in a cryptographically secure manner, that no one could have made unauthorized copies, and that the entity is the rightful owner of the related crypto-assets. The sophistication of the key ceremony will depend on how significant crypto-asset transactions are to the entity.

- Entity has implemented multi-signature access controls requiring multiple levels of approval before a transaction is executed.

- Entity has implemented information technology general controls (ITGCs) to address the IT risks that apply to digital wallets.

Additional considerations where private keys are held by a third party custodian

Generally, crypto-exchanges execute trades on behalf of their clients by retaining custody of the private keys that control the assets. They act as brokers and custodians for their clients.

In contrast to custodians in the traditional securities industry, crypto custodians and exchanges are relatively immature entities that remain largely unregulated. To CPAB's knowledge, no service auditors' reports are available that attest to the effectiveness of internal controls in place at crypto-exchanges and custodians. The use of third party custodians creates additional audit risks the auditor will need to address.

When a service auditor's report on the effectiveness of relevant controls at an exchange or custodian is unavailable and the occurrence of transactions or existence of year-end balances represents a risk of material misstatement, the auditor will need to test internal controls at the exchange or custodian directly[4].

We further note that several crypto-exchanges engage in the practice of commingling their clients' assets in exchange wallets. When crypto-assets are commingled, a crypto-exchange reflects transactions between buyers and sellers of the same crypto-asset in its records but not on the applicable blockchain ledger (i.e., off-chain transactions). This makes it impracticable for auditors to verify the occurrence of an entity's crypto-asset transactions by referring to the applicable blockchain record.

[3] Additional information on key ceremonies may be found in the AICPA's Statement on Auditing Standards No. 70, *Service Organizations*.
[4] CAS 402, *Audit Considerations Relating to an Entity Using a Service Organization*, para. 12

Revenue from crypto-asset mining

Blockchain miners receive rewards for creating blocks of validated transactions and including them in the blockchain. Many blockchain miners pool their computing power in mining pools with other miners. We understand these pools are managed using programmed protocols or are administered by third party companies or individuals. When the mining pool adds a block to a blockchain and earns the associated reward, each miner participant receives its share of the reward based on one of several allocation methods.

An auditor of a crypto-asset miner will need to develop an audit approach to test each of the major assertions relating to revenue recognition including occurrence, accuracy, and completeness. When an entity earns revenue through a mining pool, the auditor needs to understand the terms of the arrangement with the mining pool and the associated risks. The auditor's testing of revenue should include procedures to test the accuracy and completeness of the amounts allocated to the entity by the mining pool.

It will not be sufficient for auditors to limit their procedures for auditing revenue transactions to vouching remuneration received for validation activities to the blockchain ledger. The auditor must understand how revenue is earned and develop an audit approach responsive to the risks identified.

Other challenging areas

Impairment of mining assets

Several of the reporting issuers in Canada that carry out crypto-asset mining acquired mining equipment when crypto-asset prices were significantly higher than they are currently. For example, Bitcoin, Ripple and Ethereum have declined by approximately 70, 90, and 85 per cent, respectively, from January 2018 to early December 2018.

The significant decline in crypto-asset prices over the past year should be viewed as an indicator[5] that the carrying amounts of mining equipment may be impaired and that, accordingly, management should be estimating the recoverable amount of these assets. Auditors should be skeptical if management's estimates include unrealistic expectations about future crypto-asset prices and productivity of the mining equipment.

[5] IAS 36, *Impairment of Assets*, para. 12(b)

Related party transactions[6]

Public addresses on a blockchain consist of alphanumeric strings of characters that will be difficult to associate with the real world identities of the parties that have transacted crypto-assets during the year under audit. It will be challenging for auditors to evaluate whether management has appropriately identified and disclosed all crypto-asset transactions with related parties.

Auditors will likely assess this as a significant risk area. It will be difficult to obtain sufficient appropriate audit evidence when the entity does not have effective internal controls to identify related parties and related party crypto-asset transactions.

Auditors should continue to perform focused audit procedures around transactions with related parties, including assessing the business purpose of crypto-asset transactions and, when applicable, that the transactions were made on terms equivalent to those that prevail in arm's length transactions.

Valuation of crypto-assets[7]

For entities that measure crypto-assets at fair value, valuation will likely be assessed as a significant risk by auditors.

In evaluating the reasonability of an entity's crypto-asset valuations, auditors will consider whether an active market exists for the crypto-asset (i.e., whether a level 1 valuation can be performed). In some cases, there might be several markets for a particular crypto-asset that meet the definition of an active market, and each of those markets might have different prices at the measurement date. In these situations, the entity will need to determine the principal market (or, in the absence of a principal market, the most advantageous market) to value the asset.

Some entities use price quotations from data providers that aggregate prices from several crypto-exchanges to value crypto-assets that trade in active markets. Auditors will need to evaluate whether those prices are reasonable proxies for what an entity will be able to sell the crypto-asset in its principal market at the measurement date.

Many crypto-assets will not have an active market and the entity will need to use a valuation technique to value these assets. We expect that auditors will engage valuation specialists where the crypto-assets do not trade in active markets.

[6] CAS 550, *Related Parties*
[7] IFRS 13, *Fair Value Measurement*

Subsequent events[8]

Because of the significant risks associated with existence and ownership of crypto-assets, auditors should perform procedures designed to obtain sufficient appropriate audit evidence that the assets were not lost or compromised (therefore requiring disclosure in the financial statements) during the period between the year-end date and the date of the auditor's report. These procedures may include many of the same procedures applied to test the year-end crypto-asset balances.

Client acceptance considerations

We've highlighted that cryptocurrency transactions involve unique risks and auditors need to develop a comprehensive audit response. We've also highlighted areas where we think it would not be practicable to audit cryptocurrency-related assets and transactions without relying on the effective operation of relevant controls.

We expect audit firms to have a good understanding of the audit risks they will face, and the expertise they will bring to bear, in the audit before accepting these types of engagements[9]. It will not be satisfactory for audit firms that have already accepted clients to assert that the audit risks for reporting in this nascent industry are not yet well understood.

Further, we continue to expect to see thorough "know your client" procedures being performed by audit firms prior to acceptance of these engagements.

Concluding comments

We encourage a comprehensive approach by auditors in addressing the specific audit risks that are unique to the crypto-asset sector. We encourage the use of experts and consultation by auditors in developing their audit plan.

CPAB expects to issue further communications on this topic as we learn more and conduct inspections of the audits of reporting issuers in this sector.

[8] CAS 560, *Subsequent Events*
[9] Refer to CAS 220, *Quality Control for an Audit of Financial Statements,* para. 12, 13, A8-A10, for more information on quality control requirements related to client acceptance