CANADIAN PUBLIC ACCOUNTABILITY BOARD
CONSEIL CANADIEN SUR LA REDDITION DE COMPTES

Auditing in the Crypto-Asset Sector

Inspections Insights

NOVEMBER 2019

What we found

There are currently 48 Canadian reporting issuers with activities in the crypto-asset sector. Those activities include a variety of crypto-asset trading strategies and crypto-asset mining.

The Canadian Public Accountability Board (CPAB) found significant findings (deficiencies in the application of generally accepted auditing standards that could result in a restatement of the company's financials) in seven of eight audit files inspected to date. Remediation remains in progress for some of those audits.

Five most common deficiencies

1. Auditors did not have an adequate understanding of audit risks when they designed their audit approaches.
2. Auditors relied on information obtained from crypto-exchanges and custodians without evaluating the reliability of that information.
3. For entities that hold self-custodied crypto-assets, auditors did not obtain sufficient evidence to support the entities' ownership claims to those assets.
4. Auditors did not evaluate the reliability of information obtained from blockchains.
5. For entities engaged in crypto-asset mining activities, auditors that limited their audit work to vouching crypto-assets received to the blockchain did not obtain sufficient audit evidence.

1. Risk assessment during audit planning

Several auditors did not obtain an adequate understanding of the audit risks of the entities under audit.

For example, for entities that hold a wide variety of crypto-assets, some auditors failed to identify the unique risks applicable to each material class of crypto-assets including whether information obtained from each applicable blockchain can be relied on as audit evidence in their audits.

A root cause of many of our inspection findings is the lack of involvement of blockchain and cryptography experts during the audit planning phase to help auditors identify audit risks and design an appropriate audit approach.

2. Reliability of information from crypto-exchanges and custodians

When an entity (user entity) uses a crypto-exchange or custodian, it is often relying on the effective operation of the underlying infrastructure of these service organizations to safeguard its assets and to maintain adequate records of its crypto-asset balances and transactions.

Several user entity auditors (user auditors) did not obtain an adequate understanding of the nature and significance of the services provided by service organizations to user entities and their relevance to their audits. Those auditors inappropriately relied on information obtained from these service organizations as audit evidence, including crypto-asset transactional data and custodial records, without additional testing.

Canadian Auditing Standard (CAS) 402, *Auditing Considerations Relating to an Entity Using a Service Organization*, deals with the responsibility of a user auditor to obtain sufficient appropriate audit evidence when a user entity uses the services of one or more service organizations. CAS 402 expands on how the user auditor applies CAS 315, *Identifying and Assessing the Risks of Material Misstatement through Understanding the Entity and Its Environment*, and CAS 330, *The Auditor's Responses to Assessed Risks*.

When the user auditor's risk assessment includes an expectation that internal controls at a service organization are operating effectively to address risks relevant to the user entity's audit, the user auditor is required to test the operating effectiveness of those controls directly or rely on related testing performed by other auditors (i.e., service auditors' reports, etc.).

3. Ownership of crypto-assets

The pseudonymity of blockchains poses a unique challenge for auditors; it is difficult to associate the real-world identity of the owner of a crypto-asset to the string of alphanumeric characters that represents the owner's pseudonymous identity on the blockchain.

A fundamental audit risk is that the rightful owner of a crypto-asset could share its private key with others. Multiple parties with access to the private key could then assert an ownership claim over the related crypto-assets.

We found deficiencies in the audit work intended to test that crypto-assets held in self-custody by entities were in fact their assets. Auditors appropriately verified that each entity had access to the private keys that controlled the related crypto-assets. However, because access does not necessarily imply ownership, those auditors failed to obtain sufficient audit evidence to support the entity's ownership claim.

In most cases auditors will also need to test the design and operating effectiveness of those internal controls put in place by management that help to establish the entity's ownership claim to their crypto-assets.

4. Reliability of the blockchain record

Blockchain protocols are intended to make blockchains resilient to tampering. However, it is not appropriate for auditors to assume that all protocols are effective and that the information recorded on the blockchains of all 3,050 crypto-assets currently in circulation (refer to CoinMarketCap for more current information) can be relied on.

Auditors should identify those risks related to the reliability of the information obtained from the blockchain including, for instance, that invalid transactions are added to a blockchain ledger and validated transactions on the blockchain are subsequently modified. Auditors should then test the attributes of a blockchain's protocol that address those risks. Significant inspection findings were identified where auditors failed to perform this work and information obtained from blockchains was used as a primary source of evidence to support the existence/occurrence of material crypto-asset balances/transactions.

We expect auditors to engage blockchain and cryptography specialists to assist them in designing and executing an appropriate audit approach.

5. Crypto-asset mining revenue

Entities that engage in transaction verification services for blockchain networks (commonly termed crypto-asset mining) receive crypto-assets (and recognize these assets as revenue) on the completion and addition of a block to the blockchain.

Auditors that limited their work when auditing revenue recognition to vouching the crypto-assets received by entities to the blockchain failed to address the risk that the revenue could be materially misstated due to error or fraud.

An appropriate audit approach includes obtaining an understanding of how the entity performs its mining activities and testing the computing capacity of the entity's mining equipment, electricity consumption patterns associated with mining activities, mining pool arrangements (when applicable) and other factors relevant to supporting the auditor's conclusion that crypto-assets received are attributable to the entity (i.e., ownership assertion) and presented fairly for the reporting period.

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