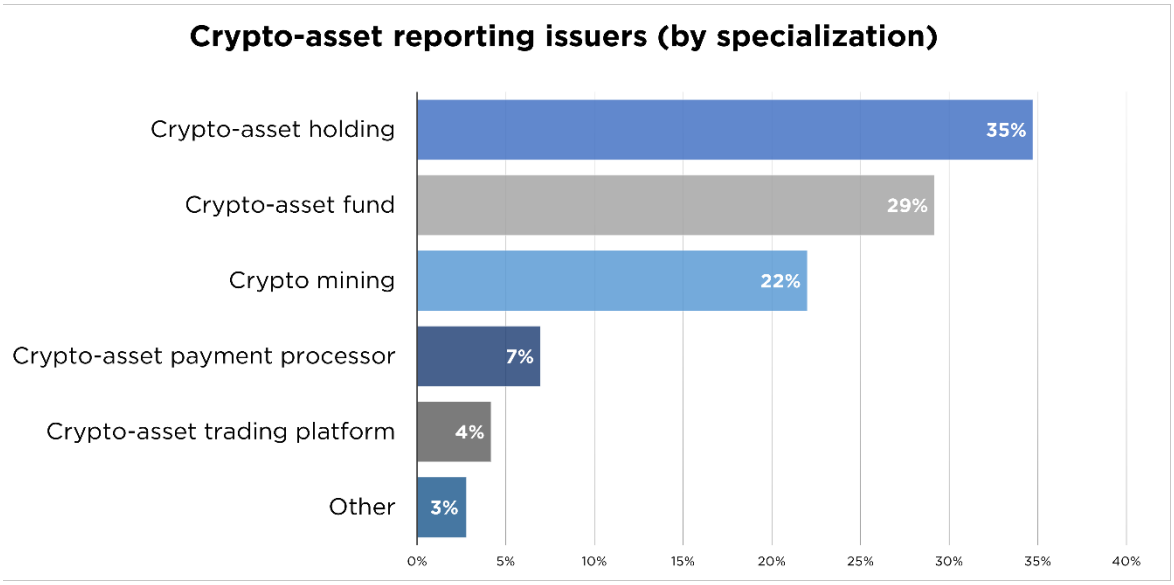
cpab exchange

Crypto assets inspections insights

The landscape for reporting issuers with crypto-asset[1] activities continues to evolve. The Canadian Public Accountability Board (CPAB) recognizes that this evolving landscape creates challenges for both reporting issuers and audit firms in the sector. This publication provides insights and illustrative examples into common inspection findings for auditors of crypto-asset reporting issuers, outlines good practices observed in audit files without findings and highlights some emerging risks.

As of February 2024, there were 72 Canadian reporting issuers in the crypto-asset industry audited by 26 public accounting firms registered with CPAB. The chart below indicates the primary area of specialization in which these reporting issuers operate.



What our inspections reveal

Between 2020 to 2023, CPAB inspected 33 audit files of reporting issuers with crypto-asset activities and identified significant findings[2] in 23 of those files. Although we have seen improvements to the procedures performed by auditors of reporting issuers in this industry, and we have seen the rate of findings trending downward—in 2020 all files inspected had significant findings compared to 50 per cent in 2023—the types of inspection findings and the rate of findings remain unacceptably high.

[1] The term crypto asset generally refers to digital assets such as cryptocurrencies, tokens etc. that use cryptography and distributed ledger technology to create, verify and secure transactions.

[2] A significant inspection finding is defined as a deficiency in the application of generally accepted auditing standards related to a material financial balance or transaction stream where the audit firm must perform additional audit work to support the audit opinion and/or is required to make significant changes to its audit approach.

This publication includes some emerging risks in the crypto-asset industry. The issues and risks included in this publication should not be considered an exhaustive list. It is the auditor's responsibility to determine the appropriate audit procedures, in accordance with applicable auditing standards, based on the specific facts and circumstances of the reporting issuer.

Common significant inspection findings

No identification or consideration of the specific risks associated with crypto assets, including fraud risks.

In eight of the 23 files with significant inspection findings, the auditor had an insufficient understanding of the specific operational and business risks associated with the crypto-asset reporting issuers. This level of inspection findings indicates that auditors need to do more to ensure they obtain an understanding of the entity and have the specialized industry knowledge that will allow them to effectively identify and assess the risks of material misstatement.

Examples encountered in our inspections include:

- The auditor did not appropriately identify or assess a significant risk related to the existence and ownership of the crypto assets.
- The auditor did not obtain an understanding of the business rationale for a crypto-asset transaction.
- The auditor did not consider fraud risks associated with specific crypto-asset transactions that involved related parties.

Auditors must ensure that they understand the specific risks of the reporting issuer's business operations, their related party relationships and transactions, and management's overall integrity and competence.[3] Auditors should consider whether there is limited or a lack of governance at the crypto-asset reporting issuer and the impact that this may have on the overall risk assessment.[4] Finally, auditors should also understand the legal and regulatory environment for crypto assets, including considering the specific requirements across different jurisdictions.[5]

Fraud risk for all crypto-asset transactions is elevated due to the nature of the operations and pseudo-anonymity of the parties involved. Examples of fraud risks for auditors of crypto-asset reporting issuers to consider include:

- Private keys used to access the crypto assets are not appropriately safeguarded to prevent them from being stolen or corrupted.
- Protecting the ownership rights of crypto assets from being intercepted or claimed by unauthorized individuals requires sophisticated technology and strong cyber security protocols. If these are not in place, crypto assets can be fraudulently accessed, used or transferred to cyber criminals.
- Unusual or complex transactions involving crypto assets without a clear business rationale may indicate an alternative purpose for the transaction, especially when between related parties.

[3] CAS 315, para. 19(a).
[4] CAS 315, para. 19(a)(i).
[5] CAS 315, para. 19(a)(ii).

The scenarios presented throughout this publication are representative of the types of issues identified in our inspections. Facts have been modified and/or excluded to safeguard the identities of the reporting issuers.

Example: Purchase of equipment from a related party using crypto assets

Background:

A crypto-asset entity purchased equipment from a related party. The entity paid for the equipment using crypto assets that were transferred to the related party through a trading platform that was managed by the same related party.

Audit approach:

The engagement team did not identify a significant risk or fraud risk arising from this transaction. The engagement team concluded that substantive procedures would provide sufficient and appropriate audit evidence to address the existence, ownership and valuation of the equipment. The engagement team reviewed invoices prepared by the related party to support the purchase of the equipment. They also agreed the payment/transfer of crypto assets by confirming the amounts paid (i.e., crypto assets) to a transaction activity report from the crypto trading platform.

Findings:

The engagement team did not evaluate if there was a reasonable business rationale for the transaction or consider if it had been entered into to engage in fraudulent financial reporting and/or to conceal a misappropriation of assets.[6] The risk assessment was not adequately performed as the engagement team did not identify a risk of material misstatement that may exist when purchasing assets from a related party. The specific assertion-level risks relating to the existence, ownership and valuation of the assets were not appropriately assessed. For example, the engagement team did not consider whether the amount paid for the equipment acquired and crypto assets transferred was reflective of the transaction's fair value. As a result, the audit evidence obtained was not sufficient to address the risks of material misstatement associated with the transaction.

In March 2024, CPAB published Identifying and assessing the risks of material misstatement: Strengthening audit quality which provides additional insights relating to the identification and assessment of risks of material misstatement.

[6] CAS 240, para. 33(c).

Insufficient understanding of the entity's system of internal controls and inappropriate response to assessed risks.

The digital environment in which crypto assets are held and transacted is highly dependent on the entity's information technology (IT) systems and applications. In 15 of the 23 files with significant inspection findings, we observed a lack of understanding of processes and often no evaluation of the entity's system of internal controls. This resulted in significant findings as there was no evidence that the auditor determined whether substantive procedures alone could provide sufficient audit evidence for the risks of material misstatement at the assertion level.[7]

Examples encountered in our inspections include:

- The auditor designed a substantive audit approach for a crypto-asset reporting issuer where the audit support relied on data and reports (i.e., detailed records of the reporting issuer's crypto-asset transactions) from an internally-developed IT system. However, no audit procedures were performed to support the completeness and accuracy of the information contained in the internally-developed IT system.

- The substantive procedures performed by the auditor were dependent on the internal controls over the safeguarding of private keys being designed and implemented effectively. However, no audit procedures were performed over the internal controls to verify this.

- The auditor identified control deficiencies relating to the processing and recording of crypto-asset transactions but did not consider the impact of those control deficiencies on the design and execution of further audit procedures. Furthermore, the auditor did not appropriately communicate the control deficiencies to those charged with governance.

Even if the auditor does not plan to rely on internal controls as part of their audit approach, the auditor needs to obtain an understanding of the relevant control environment relevant to the preparation of the financial statements, which may include information technology general controls and other IT controls.[8] Auditors may find it useful to obtain this understanding as part of the client acceptance and continuance process.

[7] CAS 315, para. 33.

[8] CAS 315, para. 21.

Example: Revenue recognition by a crypto-asset payment processor

Background:

A reporting issuer that specializes in crypto-asset payment processing facilitates transactions between merchants selling goods and customers using crypto assets as the method of payment. The merchants receive their proceeds in an underlying fiat currency (i.e., cash). The reporting issuer charges a service fee based on a percentage of the crypto-asset transaction. The crypto-asset payment processing system is highly automated and facilitates a large volume of transactions daily with little or no manual intervention.

Audit approach:

The engagement team took a substantive approach to test the accuracy and occurrence of revenue earned. The primary audit evidence obtained included cross-referencing cash receipts paid to the merchants with a report generated by the system that supports the amount of revenue recognized.

Findings:

The engagement team did not obtain sufficient appropriate audit evidence to address the risks of material misstatement, relating to the completeness, accuracy and occurrence of revenue. There was no evaluation of the design and implementation of the internal controls (including IT controls) relevant to the payment processing system and therefore no consideration as to whether substantive procedures alone were sufficient to address the risks of material misstatement. The audit procedures placed an implicit reliance on the controls of the payment processing system, including a reliance on the calculation of the fees earned and the conversion of crypto assets to cash.

Crypto-asset staking

Certain reporting issuers have engaged in staking to earn a return on their crypto assets. Due to speed and energy-efficiencies, the proof-of-stake model is emerging as the preferred mechanism to validate and secure transactions on a blockchain. For staked crypto assets, the risks relating to the validation process can differ depending on whether the validation is performed by the reporting issuer (validator) or if the reporting issuer outsources validation to a third party (delegator).

When the reporting issuer is the validator[9], auditors may need to consider the relevant internal controls over the entity's IT systems that are used to validate transactions and determine whether these should be tested for operating effectiveness. When the reporting issuer is a delegator[10], auditors should consider the reliability of the information received from the service organization that is responsible for validating the transactions (including the considerations identified in the section below). In some cases, staked crypto assets may be locked in for a set period of time. This restriction should be considered as part of the auditor's assessment of the valuation of the staked crypto assets. Auditors should also consider what procedures are required to address the risks related to recognising rewards from staked assets, including the presumed risk of fraud in revenue recognition.

[9] A validator is a blockchain participant that verifies transactions on a proof-of-stake blockchain as part of its consensus mechanism. Validators operate a node to sign blockchain transactions as valid.
[10] A delegator is an individual or entity that stakes its crypto assets with a trusted validator instead of operating a node and validating the blockchain transactions itself.

No assessment of the reliability of information provided by third parties.

In 13 of the 23 files with significant findings, CPAB found that auditors did not assess the reliability of information obtained from third parties or third-party tools that were used to obtain audit evidence.[11]

Examples encountered in our inspections include:

- The auditor did not obtain sufficient appropriate audit evidence to support the relevance and reliability of information provided by third parties (e.g., crypto-asset custodians and exchanges) to corroborate the existence and/or ownership of crypto assets held with those third parties. In instances where a service organization control report was available, the auditor did not consider the reliability of that report and the relevant complementary user entity controls required to rely on the service organization.[12] When a service organization control report was not available, the auditor did not consider if it was relevant to obtain an understanding of the control environment or evaluate the design and implementation and operating effectiveness of the relevant controls at the third parties holding the crypto assets.[13]

- The auditor relied on the use of third-party tools, such as public blockchain explorers, to obtain information that was recorded on distributed ledgers, without validating the reliability and appropriateness of the tool.

- Third-party confirmations were obtained as the primary source of audit evidence that the reporting issuer had rightful claims to the crypto assets held by the third parties. However, no assessment of the reliability of the information included in the response to the confirmation request was performed.[14] In doing so, the auditor implicitly relied on the operating effectiveness of the internal controls at the third party without any further evaluation or testing.

For additional insights related to service organizations, please refer to CPAB's publication on audit considerations relating to an entity using service organizations.

[11] CAS 500, para. 7; CAS 402, para. A26.
[12] CAS 402, para. 17.
[13] CAS 402, para. 16(b).
[14] CAS 402, para. A26(c).

Example: Crypto assets held with a third party

Background:

A reporting issuer holds and transacts with crypto assets. They use a third-party custodian to secure their crypto assets.

Audit approach:

The engagement team obtained an understanding of the services provided by the third-party custodian through inquiry with management. The primary source of audit evidence was a confirmation from the third-party custodian that provided the transaction history during the reporting period, and the crypto-asset holdings at the reporting issuer's year end.

Findings:

The procedures performed were insufficient as the auditor's understanding was limited to inquiry and the engagement team did not appropriately assess the reliability of information provided in the confirmation received by the third-party custodian. There were no procedures performed to further understand the services provided by the third-party custodian. The engagement team did not assess if they were a service organization, nor did they understand the risks associated with using the information provided by the third-party custodian. For example, the auditor did not consider whether the crypto assets held by the third party were commingled or if there were appropriate and effective controls over the safeguarding of the crypto assets held at the third party.

Use and reliance on smart contracts

Smart contracts within decentralized finance platforms are self-executing contracts with the terms of the agreement between the parties directly written into the code. Smart contracts can be subject to coding errors and if not properly coded, vulnerable to exploitation. This is due to the immutability of the blockchain once the smart contract is deployed. Transactions that rely on smart contracts can be vulnerable to code discrepancies and hacking.

Management may provide a smart contract audit[15] to the auditors as a form of audit evidence. Smart contract audits commonly examine the functioning and code of a smart contract and can assist in detecting vulnerabilities in the code or deployment of the contract through code review, penetration testing and functional testing. They can be used by management to demonstrate that the smart contract is operating as intended.

It is important to note that while a smart contract audit may be labelled as an 'audit', it may not be prepared in accordance with assurance standards[16] and auditors should be aware of this limitation if they are using it as audit evidence. Similar to 'proof of reserve' reports issued by some crypto trading platforms or exchanges, smart contract audits do not always provide the information needed by auditors to support their audit opinion. For example, they are generally point-in-time engagements that do not address internal controls. Auditors may consider involving a smart contract expert to review the code deployed on the blockchain to ensure execution is consistent with the contract terms agreed between parties.

[15] The term "audit" is commonly associated with audits of historical financial statements, however here it is being used to describe an "other form of assurance". These audits are not performed in accordance with Canadian Auditing Standards (CAS).
[16] Such as the Canadian Standards on Assurance Engagements (CSAE).

Insufficient audit work performed to evaluate complex crypto-asset transactions and events.

The evolving use of crypto assets frequently results in new, unusual and complex transactions that require a significant amount of professional judgement. Auditors must ensure that sufficient appropriate audit evidence is obtained[17] to support the accounting of transactions and balances as well as disclosures relating to business models, operations and performance. In six of the 23 files with significant inspection findings, CPAB observed a lack of audit evidence to support the auditor's conclusions on management's accounting for complex transactions and events.

Examples encountered in our inspections include:

- The auditor did not have a sufficient understanding of the business rationale or economic substance of the crypto-asset transaction. For example, when evaluating the performance obligations[18], limited or no audit evidence was obtained to assess the implied and explicit promises between a crypto-asset reporting issuer and the customer. This resulted in both inappropriate and unsupported accounting for the transaction.

- The interrelationships between all parties involved in the crypto-asset transaction were not examined, therefore certain related party relationships were not identified or appropriately disclosed in the financial statements.[19]

- The auditor did not appropriately consider contradictory evidence or apply an appropriate level of professional skepticism to challenge the accounting position taken by management.[20] For example, management assessed the sale of a digital token to be a point-in-time product sale. The auditor concurred with management's accounting treatment without further consideration of other evidence they obtained signaling that the digital tokens were sold as a licencing agreement. As a result, the auditor did not sufficiently challenge the timing of revenue recognition despite conflicting evidence.

Auditors should consider whether a formal consultation with subject matter experts[21], including crypto specialists, is necessary to ensure management's conclusions are reasonable and consistent with relevant accounting guidance.

[17] CAS 500, para. 6.
[18] IFRS 15, para. 24.
[19] CAS 550, para. 3-4.
[20] CAS 500, para. 11(a).
[21] CAS 330, para. A1.

Example: Acquisition of a blockchain technology company

Background:

A reporting issuer acquired a crypto-asset company. The crypto-asset company was developing a crypto-asset trading platform and proprietary crypto assets that could be used within their trading platform. The crypto assets were not recognized as identifiable assets included in the purchase price allocation (PPA) for the business combination. Revenue from the sale of the crypto assets that occurred prior to and after the acquisition date was recognized as revenue by the reporting issuer.

Audit approach:

The engagement team obtained management's assessment of the business combination and the valuation report from management's expert as the audit evidence over the acquisition. The engagement team included management's revenue recognition policy in its audit file to support the timing of recognition.

Findings:

The engagement team did not sufficiently assess the complexity of the transaction to ensure the accounting conclusions determined by management were appropriate. Specifically:

- The engagement team did not challenge management or appropriately evaluate management's conclusions as to why the crypto assets were not recognized as identifiable assets in the PPA for the business combination.
- The engagement team did not appropriately assess contradictory information relating to the sales of the crypto assets.
- Insufficient audit evidence was obtained to support the engagement team's conclusions over the appropriateness of management's revenue recognition policy.

Crypto-asset borrowing and lending

Borrowing and lending arrangements of crypto assets often involve specific and different complexities that require significant judgement and careful consideration of the facts and circumstances. Auditors should obtain a sufficient understanding of the terms and conditions of the borrowing or lending arrangement. The auditor may also consider obtaining a legal opinion to help ensure all elements of the contract have been adequately assessed.

Good practices observed in files with no findings

We have observed progress in the audit procedures designed and performed to address certain risks and assertions. Audit files without significant inspection findings ensure there is sufficient expertise and knowledge on the engagement team or involve subject matter specialists during the planning and execution stages of the audit.

Examples of audit procedures observed in inspections of auditors of crypto-asset reporting issuers with no significant findings include:

- The auditor performed specific risk assessment procedures to identify the specific risks of material misstatement. For example, there was a detailed assessment of related fraud risk factors and technological risks that were specific to the facts and circumstances of the underlying crypto-asset transactions and activities of the reporting issuer.

- The auditor documented detailed process narratives and performed walkthroughs for crypto-asset transaction flows that demonstrated their understanding and identification of the relevant internal controls and/or control deficiencies. Furthermore, the auditor evaluated the design and implementation of the relevant internal controls, including IT general and application controls and, where applicable, tested for operating effectiveness. When control deficiencies were identified, the auditors determined if compensating controls existed and were operating effectively or whether incremental audit procedures were required. Any control deficiencies identified were also appropriately communicated to those charged with governance.

- The auditor involved and consulted with, specialists during the risk assessment process and the design of audit procedures (e.g., IT and blockchain experts).

- The interaction between the third-party service organization and the reporting issuer, including the flow of information and degree of reliance on the service organization, was clearly understood and assessed by the auditor, to ensure appropriate audit procedures were designed and executed.

- The auditor assessed whether audit evidence obtained from third parties, such as crypto-asset custodians or exchanges, was sufficiently relevant and reliable, or whether further audit evidence was necessary.

- There was sufficient appropriate audit evidence to challenge management's accounting conclusions and consideration of both corroborative and contradictory audit evidence.

- The auditor assessed the legislative and regulatory environment in all jurisdictions in which the entity operates, including jurisdictions outside of Canada. The auditor involved an industry expert to assist in identifying instances of non-compliance and obtained an external legal opinion.

Learn more

CPAB continues to monitor emerging issues in the crypto-asset industry through our inspections and share our observations through various communications. For more information on CPAB's previous auditing insights in the crypto-asset industry refer to our website.

Visit us at https://cpab-ccrc.ca/home and join our mailing list. Follow us on LinkedIn.

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

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