CPA CHARTERED PROFESSIONAL ACCOUNTANTS CANADA

VIEWPOINTS:

Applying Canadian Auditing Standards (CASs) in the Crypto-Asset Sector

AUDITING CRYPTO-ASSETS: DO YOU NEED TO TEST CONTROLS WHEN OBTAINING AUDIT EVIDENCE TO SUPPORT THE RIGHTS (OWNERSHIP) ASSERTION?

JANUARY 2020

Crypto-Asset Auditing Working Group

The rapid rise and volatility of crypto-assets have led to increased global interest and scrutiny by organizations, investors, regulators, governments and others. An entity's financial statements may include material crypto-asset balances and transactions; auditors need to be aware of the challenges when auditing these balances and transactions. The Chartered Professional Accountants of Canada (CPA Canada) and the Auditing and Assurance Standards Board (AASB) created the Crypto-Asset Auditing Working Group with representatives from audit firms and audit regulators in Canada to share views on the application of the CASs when auditing in the crypto-asset sector.

The technologies supporting crypto-assets can be complex; the content of this *Viewpoints* reflects this reality. For reasons of brevity, explanations are not provided for all technical concepts mentioned. Expertise in blockchain technology and related fields, such as cryptography, is often needed when auditing crypto-assets. It is therefore typical for the auditor to use the work of an auditor's expert when auditing crypto-assets.

Background

One of the key features of crypto-asset transactions is that they have "pseudo-anonymity" (i.e., blockchain ledgers represent the identity of transacting parties as public addresses using a string of alphanumeric characters). Ownership rights (herein referred to as "ownership") of a crypto-asset are not readily apparent from a public blockchain because of the pseudo-anonymity of the transacting parties. Consequently, because there is no legal title recording the identity of the actual owner of the crypto-asset, it is challenging to verify the rightful owner of those assets.

In evaluating an entity's ownership of crypto-assets, auditors are required to design an audit approach to obtain sufficient appropriate audit evidence that the entity owns the crypto-assets associated with its public address(es).

Paragraph A24 of CAS 330, *The Auditor's Responses to Assessed Risks*, contemplates that, in certain situations, the auditor may find it impossible to design effective substantive procedures that by themselves provide sufficient appropriate audit evidence at the assertion level. In such a situation, it will be necessary for the auditor to design and perform tests of the operating effectiveness of controls to obtain sufficient appropriate audit evidence to support the ownership assertion.

This *Viewpoints* explores the factors an auditor may consider when determining how to obtain sufficient appropriate audit evidence to support the ownership assertion for financial statements that contain material crypto-asset balances. In exploring this emerging and complex topic with firm representatives and experts on the CPA Canada Crypto-Asset Auditing Working Group, it became clear that each circumstance is unique and requires expertise to determine an appropriate audit approach.

This paper addresses only one of the numerous issues that arise when applying CASs in the crypto-asset sector. For an introduction to the topic of auditing crypto-assets and some of the other challenges an auditor may encounter, please read CPA Canada's ***Audit Considerations Related to Cryptocurrency Assets and Transactions***.

Issue

Are tests of the operating effectiveness of controls necessary to obtain sufficient appropriate audit evidence regarding the ownership of a crypto-asset? Are there specific facts and circumstances that allow an auditor to determine the possibility of obtaining sufficient appropriate audit evidence without testing the operating effectiveness of controls?

Scope

This *Viewpoints* specifically addresses the ownership assertion for self-custodied crypto-assets (i.e., not held by a third party). If an entity's crypto-assets are held by a third party, the auditor may need to assess (among other things) the need to obtain audit evidence regarding the operating effectiveness of relevant controls at the custodian.

This *Viewpoints* only covers the audit of crypto-assets recorded in a public blockchain where all transactions recorded on the blockchain are observable to the general public; therefore, it excludes the audit of crypto-assets recorded in private blockchains.

Furthermore, this *Viewpoints* does not address how to test the design and implementation of controls or the operating effectiveness of controls if the auditor concludes that tests of the operating effectiveness of controls are necessary.

Canadian Standard on Quality Control 1 (CSQC 1) requires the establishment of policies and procedures for the acceptance of client relationships and specific engagements. This *Viewpoints* assumes the firm has undertaken this process and has concluded the audit engagement can be accepted. In such policies, the firm may include the need to obtain an understanding of the overall control environment and, more specifically, the controls regarding ownership as part of its client and engagement acceptance process.

Viewpoints

The following are factors that an auditor may evaluate in determining whether tests of the operating effectiveness of controls are necessary to obtain sufficient appropriate audit evidence regarding the ownership of crypto-assets. It should be noted that some of these factors are interrelated, and the factors are not comprehensive. These factors include:

- complexity of the entity's business processes and IT environment
- availability of evidence outside the blockchain
- volume of transactions
- other auditor risk assessment factors

It is important for the auditor to consider the facts and circumstances of both the entity and the audit to appropriately plan and execute the audit. Based on these specific facts and circumstances, the auditor may determine that substantive procedures alone will not provide sufficient appropriate audit evidence at the assertion level regarding ownership of the crypto-assets. In these circumstances, paragraph A24 of CAS 330 refers the auditor to the requirement in paragraph 8 of CAS 330 that the auditor test not only the design and implementation but also the operating effectiveness of the relevant controls to obtain sufficient appropriate audit evidence at the assertion level regarding the ownership of any crypto-assets.

There is, however, a narrow set of circumstances under which the auditor can obtain sufficient appropriate audit evidence regarding the ownership assertion using substantive procedures alone. To determine whether these specific facts and circumstances exist, the auditor may carefully evaluate the factors discussed in this *Viewpoints* using expertise and professional judgment.

It is important for the auditor to evaluate the quality and sufficiency of the evidence expected to be obtained and determine whether, based on the entity's facts and circumstances, this body of evidence will be sufficient to conclude that the entity has rightful ownership of the crypto-assets.

Complexity of Business Processes and IT Environment

The level of complexity of business processes is likely to have a significant effect on the approach taken by the auditor. For example, the crypto-asset-related business processes and IT environment may be less complex for a corporate client that does not use crypto-assets in its primary business but has some crypto-asset holdings in a buy-and-hold

investment portfolio. In this scenario, the auditor may be able to obtain sufficient appropriate audit evidence to support the ownership assertion without testing the operating effectiveness of controls. On the other hand, if the entity is a crypto-asset trading platform,[1] it likely operates in a highly automated environment with complex IT systems and generates little or no documentation of transactions other than through the IT system. In this case, the auditor may conclude that substantive procedures alone cannot provide sufficient appropriate audit evidence at the assertion level and that evidence as to the operating effectiveness of relevant controls is required.

Availability of Evidence Outside the Blockchain

The ability to obtain sufficient appropriate audit evidence will also be affected by the availability of audit evidence from outside the blockchain. For example, to the extent crypto-assets are acquired through cash transactions, bank statements and/or contracts may provide ownership evidence. In addition, the auditor considers the reliability of the evidence obtained from outside the blockchain. For example, the auditor may consider a statement of holdings from a crypto-asset trading platform less reliable than a bank statement when used as audit evidence. In some cases, there may be limited evidence outside the blockchain, such as when an entity acquires crypto-assets through non-cash transactions. Examples of non-cash transactions include selling goods and services in exchange for crypto-assets, acquiring crypto-assets in exchange for other crypto-assets, or crypto-asset mining in which crypto-assets are received in exchange for mining efforts. The pseudo-anonymity of such transactions may impact the availability of evidence outside the blockchain. In these situations, it may be more difficult for the auditor to obtain sufficient appropriate audit evidence without testing controls. The auditor considers the overarching reliability of the evidence and its source.

Volume of Transactions

When auditing an entity that reports a large number of transactions in crypto-assets, an auditor may conclude it is impossible to obtain sufficient appropriate audit evidence without testing the operating effectiveness of controls. On the other hand, the auditor may determine that, where the entity reports few transactions in crypto-assets, it is possible to obtain sufficient appropriate audit evidence without testing the operating effectiveness of controls. For example, for an entity with a buy-and-hold strategy, thus making limited purchases and sales of crypto-assets during the year, sufficient appropriate audit evidence may be obtained regarding ownership without testing the operating effectiveness of controls.

Other Auditor Risk Assessment Factors

In performing the overall risk assessment, the auditor may identify other specific factors that affect the determination of whether tests of the operating effectiveness of controls are necessary to support the ownership. For example, if the auditor assesses there is a higher risk that related-party transactions will not be recorded, the auditor may also conclude that the pseudo-anonymity of the blockchain prevents substantive audit procedures alone from providing sufficient appropriate audit evidence. Similarly, the auditor may identify an elevated

1 Joint Canadian Securities Administrators / Investment Industry Regulatory Organization of Canada, Consultation Paper 21-402, *Proposed Framework for Crypto-Asset Trading Platforms*, March 2019 www.osc.gov.on.ca/documents/en/Securities-Category2/csa_20190314_21-402_crypto-asset-trading-platforms.pdf

risk that another entity (e.g., a related party) may also be claiming ownership of the same crypto-assets. This may indicate that substantive procedures alone are not sufficient and that the auditor needs to satisfy themselves that, for example, controls over access to the private key(s) were operating effectively. By carefully considering whether these or other risk factors are present, the auditor may determine that substantive procedures alone may not be sufficient to address the assessed risks.

An Auditor's Requirement Regardless of Approach

It is also important to note that, regardless of the approach taken, the auditor is always required to:

- evaluate the design and implementation of controls relevant to the audit[2]
- perform substantive procedures

Under paragraph 29 of CAS 315, *Identifying and Assessing the Risks of Material Misstatement through Understanding the Entity and its Environment*, if there is a significant risk, including fraud risk, associated with the ownership assertion, the auditor is required to obtain an understanding of the entity's controls, including its control activities, relevant to that risk. Such understanding includes evaluating the *design* of such controls and determining whether they have been implemented. A combination of relevant controls related to the ownership assertion *may* address the following, among other matters:

- initial generation of private key(s) in a secure manner
- ongoing safeguarding of private key(s) from being copied, lost, stolen or shared
- appropriate authorization and approval of crypto-asset transactions
- segregation of duties among those who have access to the private key(s), those responsible for accounting and those with operational responsibilities

Upon completion of procedures to obtain an understanding of the entity's controls, the auditor may determine that the design and implementation of controls are not adequate to prevent a material misstatement. In this case, if the auditor also concludes that performing substantive procedures alone will not provide sufficient appropriate audit evidence regarding the ownership assertion, then the auditor is required to determine whether it is necessary to modify the opinion in the auditor's report in accordance with CAS 705, *Modifications to the Opinion in the Independent Auditor's Report*. The auditor may also conclude that there is a significant deficiency in internal control.

Conclusion

The decision whether to take a substantive or controls-based audit approach becomes increasingly complex when emerging technologies and related issues are involved.

2 CAS 315, paragraphs 12 and 13.

For each scenario, it is important to consider various entity-specific factors including, but not limited to, those identified above. For entities with only a small number of crypto-asset transactions, less complex IT and business processes, additional evidence available from outside the blockchain, and no other specific risk factors relating to ownership, an auditor may be able to conclude that the body of evidence obtained from substantive audit procedures is sufficient to conclude the entity has rightful ownership of the crypto-assets. However, in many cases, such an approach may not be possible. Accordingly, auditors are reminded to carefully evaluate whether testing the operating effectiveness of controls is necessary in order to obtain sufficient appropriate audit evidence regarding the ownership of crypto-assets.

Acknowledgments

CPA Canada wishes to express its gratitude to the CPA Canada and Auditing and Assurance Standards Board's Crypto-Asset Auditing Working Group for its assistance in the authoring and review of this publication. The working group is composed of representatives from the Canadian Public Accountability Board, provincial practice inspection and volunteers from the following Canadian firms: BDO, Davidson & Company, Deloitte, EY, KPMG, MNP, PwC and Raymond Chabot Grant Thornton.

CPA Canada gratefully acknowledges EY for leading the authoring of this publication on behalf of the working group.

Additional Resources

1. CPA Canada. *Audit Considerations Related to Cryptocurrency Assets and Transactions.* www.cpacanada.ca/en/business-and-accounting-resources/audit-and-assurance/canadian-auditing-standards-cas/publications/cryptocurrency-audit-considerations
2. CPA Canada. *Auditing Crypto-Assets: Relevance and Reliability of the Information Obtained from a Blockchain to Be Used as Audit Evidence.* www.cpacanada.ca/en/business-and-accounting-resources/audit-and-assurance/canadian-auditing-standards-cas/publications/viewpoints-crypto-assets-blockchain-reliability
3. *CPA Canada Handbook*, CAS 315 and 330

Comments

Comments on this *Viewpoints* or suggestions for future *Viewpoints* should be sent to:

Kaylynn Pippo, CPA, CA
Principal, Audit & Assurance
Research, Guidance and Support
Chartered Professional Accountants of Canada
277 Wellington Street West
Toronto ON M5V 3H2
Email: kpippo@cpacanada.ca