CHARTERED
PROFESSIONAL
ACCOUNTANTS
CANADA

VIEWPOINTS:

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

AUDITING CRYPTO-ASSETS: RELEVANCE AND RELIABILITY OF THE INFORMATION OBTAINED FROM A BLOCKCHAIN TO BE USED AS AUDIT EVIDENCE

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.

Disclaimer: The views expressed in this series are non-authoritative and have not been formally endorsed by CPA Canada, the AASB, the audit regulators or the firms represented by the working group members. Members may have differing views on how the guidance suggested in this *Viewpoints* should be implemented.

CPA Canada and the authors do not accept any responsibility or liability that might occur directly or indirectly as a consequence of the use or application of or reliance on this material.

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

Canadian Auditing Standard (CAS) 330[1] requires the auditor to design and perform further audit procedures whose nature, timing and extent are based on and responsive to the assessed risks of material misstatement at the assertion level.

[1] CAS 330, *The Auditor's Responses to Assessed Risks.*

Because crypto-assets are not physical assets and, by nature, only "exist" in digital form on a blockchain, the audit procedures typically involve using information obtained (or derived) from a public blockchain. For example, when testing the occurrence of an entity's crypto-asset transactions and the existence of the crypto-asset balance at year end, an auditor may use an IT application (often called a "block explorer") to display information recorded on a blockchain to be used as audit evidence. However, as further explained below, in such a case, the reliability of the information obtained likely depends on the reliability of the blockchain itself and of the block explorer used.

This paper addresses only one of the numerous issues that arise when applying CASs in the crypto-asset sector. There are several challenges to consider when applying auditing and ethical standards, including those related to independence, 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

When addressing the assessed risks of material misstatement of crypto-asset transactions and balances recorded in an entity's financial statements, what are the factors to consider concerning the relevance and reliability of the information obtained from a public blockchain to be used as audit evidence?

Scope

This *Viewpoints* focuses on information obtained from a public blockchain to be used as audit evidence. It focuses on the information obtained from the blockchain itself and not on the other additional audit evidence that may be needed. This *Viewpoints* does not discuss implications of smart contracts that may or may not be subject to the same protocol as the related blockchain.

When the entity's crypto-assets are held by a third party (e.g., a custodian), some information to be used as audit evidence may originate from that third party, not from a public blockchain. Audit evidence obtained from such a third party is outside the scope of this *Viewpoints*.

Viewpoints

When designing and performing audit procedures, CAS 500[2] requires the auditor to consider the relevance and reliability of the information to be used as audit evidence, including information obtained from an external information source.

[2] CAS 500, *Audit Evidence.*

The relevance of information deals with the logical connection with, or bearing upon, the purpose of the audit procedure and, where appropriate, the assertion under consideration. For example, the blockchain typically provides relevant information regarding the occurrence of a crypto-asset transaction. On the other hand, information obtained from a blockchain will likely not be relevant when testing the valuation of a crypto-asset or when testing for possible off-chain transactions.[3]

The reliability of information to be used as audit evidence, and therefore the reliability of the audit evidence itself, is influenced by the information's source and nature as well as the circumstances under which it is obtained. The reliability of information obtained from a blockchain to be used as audit evidence may depend on the:

- source of the information itself (i.e., the blockchain)
- appropriateness of technological resources, including IT applications, used by the auditor to directly obtain the information (e.g., a block explorer)

When the auditor does not have a sufficient basis with which to consider the reliability of information obtained from a blockchain, the auditor may have a limitation on scope if sufficient appropriate audit evidence cannot be obtained through alternative procedures. For example, currently the use of more privacy-preserving cryptography, such as zero-knowledge proofs or ring signatures, in a blockchain may result in the inability of the auditor to obtain appropriate audit evidence. CAS 705[4] contains reporting requirements for the auditor when dealing with the consequence of an imposed limitation in the scope of the audit.

CAS 200[5] requires the auditor to plan and perform an audit with professional skepticism and to recognize that circumstances may exist that cause the financial statements to be materially misstated. Professional skepticism is necessary to the critical assessment of audit evidence, including information obtained from a blockchain. This includes questioning contradictory and inconsistent audit evidence as well as the reliability of information.

CAS 500 requires the auditor to determine what modifications or additions to audit procedures are necessary to resolve inconsistency in, or doubt over the reliability of, audit evidence. One example is audit evidence obtained from one source that is inconsistent with that obtained from another, such as inconsistency in the information from two different block explorers. Another example is doubts about the reliability of the blockchain itself, as further discussed below. CAS 230[6] includes a requirement that if the auditor identified information inconsistent with the auditor's conclusion regarding a significant matter, the auditor must document how they addressed the inconsistency.

[3] An off-chain transaction may be described as a transaction outside the blockchain. While an on-chain transaction modifies the blockchain and depends on the blockchain to determine its validity, an off-chain transaction relies on other methods to record and validate the transaction.

[4] CAS 705, *Modifications to the Opinion in the Independent Auditor's Report.*

[5] CAS 200, *Overall Objectives of the Independent Auditor and the Conduct of an Audit in Accordance with Canadian Auditing Standards.*

[6] CAS 230, *Audit Documentation.*

Blockchain

When designing procedures related to a blockchain from which information will be obtained, the auditor may consider the:

- characteristics of the blockchain (as discussed below)
- assessed risks of material misstatement for the assertions to which the use of the information is relevant
- entity's controls over the reliability of information the entity has obtained from a blockchain
- degree to which the use of that information contributes to reducing audit risk to an acceptably low level for an assertion (e.g., whether the information is the primary source of audit evidence or supplements other evidence obtained)

Even though information to be used as audit evidence is often more reliable when obtained from an external source (which may be the case with a public blockchain), circumstances may still exist that could affect its reliability (e.g., a blockchain may not be operating as it is generally thought to be operating). Generalizations about the characteristics of blockchain technology (e.g., that transactions recorded cannot be modified) may be subject to important exceptions (i.e., the generalization may not be appropriate to a specific blockchain). The auditor may consider the potential sources of inaccurate or incomplete information by asking "what could go wrong?" (WCGW) within a given blockchain, and the characteristics of the blockchain affecting such WCGW. The WCGWs and characteristics noted below can provide a helpful frame of reference when considering reliability. However, these are only examples; they may be expressed in more detail and others may exist.

WCGW

- Invalid transactions are recorded on the blockchain.
- Data is not agreed upon by the network (break in consensus).
- Valid transactions are not accurately recorded on the blockchain.

Characteristics

- **Cryptography protocol or algorithm:** Use of a robust cryptographic protocol (based on the current state of technology) is important. A poor protocol or algorithm can cause weaknesses in the blockchain.
- **Consensus model (e.g., "proof of work" or "proof of stake"):** The consensus reached by the network represents the "truth" in a blockchain (from a probabilistic finality[7] perspective). The mechanism by which the consensus protocol resolves splits and forks that arise routinely as part of the mining process is important.

[7] In the blockchain setting, finality is the affirmation that all valid blocks will not be revoked once committed to the blockchain. Probabilistic finality refers to the type of finality provided by chain-based protocols, in which the probability that a transaction will be reverted decreases as the block which contains that transaction sinks deeper into the chain.

Certain other WCGWs may have a less direct effect on the reliability of information recorded in a blockchain. For example, a "consensus attack" (often called at 51% attack) on a blockchain may represent a business risk in that such an attack can result in the misappropriation of an entity's crypto-assets by a third party. An understanding of the business risks facing the entity increases the likelihood of identifying risks of material misstatement, since business risks may eventually have financial consequences and, therefore, an effect on the financial statements. Certain characteristics of the blockchain may be more relevant in addressing business risks than risks regarding the reliability of information on the blockchain (e.g., a higher hash power / rate reducing the possibility of a consensus attack).

CAS 315[8] requires the auditor to obtain an understanding of the entity and its environment. This includes the entity's internal control, which provides a basis for designing and implementing responses to the assessed risks of material misstatement. When auditing crypto-assets, this understanding typically includes the characteristics of the underlying blockchain(s) that are relevant to the blockchain's reliability. This understanding may be obtained from various sources, for example:

- documents and source code published by developers of the blockchain
- technical or industry publications as well as publications from members of the community supporting the blockchain
- the auditor's own experience with operating a node of the blockchain, as further described in the "Source of information" section below
- discussions with experts in relevant subject matter, such as cryptography, computer science or game theory
- discussions with management or management's expert

The engagement team and any auditor's experts who are not part of the engagement team are collectively required to have the appropriate competence and capabilities to perform the audit engagement, which includes obtaining an understanding of the entity and its environment. When considering the competence and capabilities expected of the engagement team, technical expertise (including expertise with relevant information technology) as well as knowledge of relevant industries in which the client operates is important. An auditor's expert may be needed to assist the auditor in obtaining this understanding. CAS 620[9] discusses using the work of an auditor's expert.

An auditor (or firm or network) may decide to evaluate a blockchain outside the context of a specific engagement. Such an approach may be efficient and effective, especially for a widely used blockchain. However, it may be necessary to consider whether this evaluation is appropriate for the audit engagement, including the adequacy of the period covered by the evaluation and the time elapsed since the evaluation. A significant update to the code may indicate the need to update the evaluation, especially if the updated code is not backwards compatible.

[8] CAS 315, *Identifying and Assessing the Risks of Material Misstatement through Understanding the Entity and Its Environment.*

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

Source of information

An auditor can operate their own node (often a non-mining node) on a blockchain from which audit evidence will be obtained. Running a node enables the auditor to download every block and transaction and check them against the blockchain consensus rules. Running a node also allows the auditor to obtain audit evidence more directly. The auditor may also use an IT application to verify that transactions previously recorded on a blockchain (for a specific client or in general) are not changing over time. Matters discussed in "Technological Resources" below may be relevant when an IT application is used.

Technological Resources

As mentioned above, an example of a technological resource may be the use of a "block explorer" to browse and display information recorded on a blockchain. The following factors may affect the reliability of such an IT application. Such factors include whether the:

- IT application has been specifically developed for the auditor (or firm or network), has been obtained or purchased from a third-party provider or is available in the public domain; the competence and reputation of the provider of an IT application may be especially relevant
- IT application operates appropriately, including the risk of inaccurate reading and displaying of the information
- IT environment, including IT infrastructure and processes, supports the IT application
- necessary changes to the IT application are identified and implemented

The auditor may need training in the appropriate use of the IT application. Furthermore, for certain IT applications, specialized skills may be needed, such as those of an auditor's expert. In some cases, the auditor may consider using more than one IT application to obtain sufficient audit evidence, especially when using an IT application obtained or purchased from a third-party provider or available in the public domain. Obtaining more audit evidence, however, may not compensate for the lack of visibility into the quality of the IT application.

CAS 220[10] requires the engagement partner to take responsibility for the overall quality on each audit engagement to which that partner is assigned. The availability of sufficient and appropriate resources to perform the engagement, including technological resources, is a factor contributing to audit quality.

[10] CAS 220, *Quality Control for an Audit of Financial Statements.*

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 Raymond Chabot Grant Thornton 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: Do You Need to Test Controls When Obtaining Audit Evidence to Support the Rights (Ownership) Assertion?* www.cpacanada.ca/en/business-and-accounting-resources/audit-and-assurance/canadian-auditing-standards-cas/publications/viewpoints-crypto-assets-ownership-assertion
3. *CPA Canada Handbook*, CAS 315, CAS 330 and CAS 500

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