CPA CHARTERED PROFESSIONAL ACCOUNTANTS CANADA

VIEWPOINTS:

Applying Canadian Auditing Standards (CAS) in the Crypto-Asset Ecosystem

AUDITING CRYPTO-ASSETS: AUDITING FINANCIAL STATEMENTS OF ENTITIES THAT ENGAGE WITH A THIRD-PARTY SERVICE PROVIDER IN ORDER TO TRANSACT AND/OR HOLD CRYPTO-ASSETS

MARCH 2021

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 CAS when auditing in the crypto-asset ecosystem.

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

Entities that hold crypto-assets may engage with a variety of third parties in the crypto-asset ecosystem (or sector) to perform various services, including:

- executing crypto-asset transactions on their behalf
- holding a crypto-asset balance on their behalf[1]
- providing wallet services to the entity

1 Where crypto-assets are held only as collateral, certain risks and example controls discussed in this paper may not apply.

The third parties performing these services might be trading platforms, custodians or wallet providers.

It is important for the user entity and the auditor to understand that, given the nature of the technology, the services performed may not be as simple as those performed by a traditional third-party service provider such as a payroll service provider or traditional asset custodian. Further, the third-party service providers may not be as sophisticated; their control environments may be less mature, including the design of appropriate controls.

To inform their risk assessment and plan further audit procedures, the auditor needs to obtain a sufficient understanding of the entity's internal controls over financial reporting, and this includes understanding how the entity uses a third party's services in their operations. These third parties may or may not be considered a service organization to the user entity being audited – it depends on how the entity interacts with them. The auditor will apply judgment to determine first whether the third party is a service organization and second, where applicable, what procedures are necessary to understand which controls at the service organization are relevant to the audit.

When designing and performing audit procedures, the auditor considers the relevance and reliability of information to be used as audit evidence, including information from third parties that are service organizations. Given the stages of maturity of the service organizations in this ecosystem, a System and Organization Controls (SOC) report may not be available. Even when a SOC report is available:

- It may not address all the controls determined to be relevant to the audit.
- It may not sufficiently cover the period under audit.
- The user auditor may not be satisfied as to the service auditor's professional competence.

In such circumstances, as the auditor you would need to determine whether you could perform other audit procedures to obtain audit evidence to address the assessed risks of material misstatement. If not, you would need to modify your opinion.

Scope

This guidance is intended to:

- assist auditors of financial statements that contain material crypto-asset balances and/or transactions and whose entity ("user entity") engages with a third party (e.g., a trading platform, custodian or wallet provider) to transact and/or hold their crypto-assets
- focus on the user auditor considerations. There may be additional business risks that the user entity should consider before they engage a third party, but these considerations are beyond the scope of this guidance.

It is not intended to:

- provide a comprehensive list of relevant controls related to the illustrative control objectives

- address the relevance and reliability of information obtained from a public blockchain to be used as audit evidence[2]
- address all of the requirements in CAS 402;[3] instead, we focus on those aspects that may have unique considerations in a crypto-asset ecosystem.

For the purposes of this paper, we use the term "crypto-assets" to mean only the specific subset of crypto-assets that are bought, sold or transferred using a trading platform or held for investment purposes. There may be other audit risks associated with utility tokens and smart contracts, which are not contemplated in this paper.

The crypto-assets focused on in this paper are without physical substance and generally not linked to any currency or backed by any government, central bank, legal entity, underlying asset or commodity. Holdings of crypto-assets allow individuals and businesses to transact directly with each other without an intermediary such as a bank or other financial institution.

This paper does not discuss matters such as auditing the following:

- financial statements of a crypto-asset trading platform, custodian or wallet provider[4]
- financial statements of entities (see footnote 4) that:
  - validate crypto-asset transactions on a blockchain (i.e., miners)
  - issue initial coin offerings (ICO) or initial token offerings (ITO)
  - engage in smart contracts
- conclusions on the basis of accounting for crypto-assets.

Issue

When addressing the assessed risks of material misstatement over crypto-asset transactions and balances recorded in a user entity's financial statements, several questions emerge:

- What are the audit considerations when a third party holds crypto-assets on behalf of the entity, when transactions occur on a third-party trading platform or when a third party provides wallet services to the entity?
- What are some of the unique considerations related to crypto-assets that the auditor might consider when obtaining an understanding of the nature and significance of the services provided by the third party and their effect on the user entity's internal control?
- What controls may be relevant to the audit at the third-party custodian, trading platform or wallet provider, and how might audit evidence be obtained?

2 For further guidance, please refer to CPA Canada's *Relevance and reliability of information from a blockchain*

3 CAS 402, *Audit Considerations Relating to an Entity Using a Service Organization*

4 Except to the extent that this type of entity uses a third party to perform one of the services addressed in this paper.

This paper addresses each of the following matters:

PART 1

1. Understanding the crypto-asset ecosystem
2. Understanding the nature of the third-party services provided, including assessing whether a third party is a service organization
3. Approaches to obtaining an understanding of and evaluating the relevant controls at a service organization

PART 2

1. Identifying risks and relevant controls at a service organization

PART 1

Understanding the crypto-asset ecosystem

The crypto-asset ecosystem has evolved to include several types of third parties. The following are examples of such entities and the services they provide:

- *Trading platforms* – These businesses enable users to buy, sell, hold and exchange crypto-assets and traditional "fiat" currencies. They generate and manage the cryptographic keys that are needed to use, sell or transfer the crypto-assets on the blockchains they support. You will find further background information on trading platforms below.[5]
- *Custodians* – Similar to custodians for equity securities, these businesses hold crypto-assets on behalf of users such as hedge funds, asset managers and other entities.
- *Wallet providers* – These organizations specialize in designing and operating cryptographic key management solutions to help protect highly sensitive private keys associated with public blockchain addresses from theft or destruction.

Crypto-asset trading platforms enable users to purchase, sell or transfer crypto-assets. Some trading platforms also make it possible for users to store crypto-assets in a wallet on the platform. This draws an important distinction between two main types of crypto-asset trading platforms that you may encounter: *Custodial* and *noncustodial*.

- **Custodial trading platforms** enable users to store their crypto-assets within the platform, allowing them to access their funds and to trade and transact quickly. Custodial services include protection of the assets within their system.
- **Noncustodial trading platforms** do not take custody of a user's crypto-assets by maintaining an on-platform wallet for them; rather, users can use multiple different wallet technologies to personally (and digitally) sign transactions to authorize a sale or purchase.

5 Joint CSA/IIROC Consultation Paper 21-402, *Proposed Framework for Crypto-Asset Trading Platforms,* states that *trading platforms* facilitate the buying and selling or transferring of crypto-assets.

A second important distinction within these two types of crypto-asset trading platforms is whether the platform is *centralized* or *decentralized*.

Centralized trading platforms (CTP) enable users to use fiat currencies (such as Canadian dollars, U.S. dollars or Euros) to purchase crypto-assets. This type of platform earns transaction or platform fees when users use fiat currencies to purchase crypto-assets (or vice versa), use crypto-assets to buy other crypto-assets, or execute trades on the trading platform.

Another general feature of CTPs is that they facilitate trading that is "on-platform" but not on-chain. Thus, not all transactions that occur between users on the platform (independent trades), or between the platform and the user (deposits, withdrawals or transfers, including those where the platform is the counterparty to the transaction), are necessarily recorded on the respective blockchain network's distributed ledger.

This can be of critical importance if you are a financial statement auditor performing substantive testing. If the CTP cannot enable its user entities and their auditors to verify that these transactions – which are settled internally within the platform and outside the public blockchain – exist and are reported completely and accurately, this could result in a lack of sufficient audit evidence for the auditor. Some trading platforms store crypto-assets in individual wallets, while others store it in an omnibus account, which commingles or pools clients' assets together. Auditors should consider the implications of these circumstances when determining what additional audit procedures may be required.

In contrast, **decentralized trading platforms (DTP)** do not offer fiat gateways, but they do facilitate transactions between individuals in a peer-to-peer fashion. Although many DTPs take internal transaction fees from both buyers and sellers, users also may be required to pay external transaction fees to the blockchain network on which they are trading in order to process the transaction. A true DTP would likely not be considered a service organization, and thus DTPs are not considered in this paper.

As an auditor, it is important that you have a comprehensive understanding of the entity under audit and the third parties they interact with. While this is undoubtedly true for all audits, it is particularly important for user entities in the crypto-asset ecosystem given the complexities and different types of third parties involved in its ecosystem.

Understanding the Nature of the Third Party Services Provided, Including Assessing Whether a Third Party is a Service Organization

It is management's responsibility to establish appropriate controls over the services the third party provides. This may include establishing their processes and controls for selecting third-party service providers, ensuring that personnel with the relevant competencies review SOC reports, and implementing complementary user entity controls.

As with other asset classes such as equities and real estate, crypto-assets must be controlled. As the auditor, you need to consider the financial statement assertions related to the asset (accuracy, valuation and allocation; completeness; existence; cutoff; rights [and ownership]).

You are then required to obtain an understanding of internal controls relevant to the audit. You would use this understanding as a basis to identify and assess the risks of material misstatement at the assertion level for classes of transactions, account balances and the related disclosures, and to determine the nature, timing and extent of further audit procedures responsive to those risks. It is important to note that the controls relevant to the audit may encompass both those established by the entity and those placed in operation at the third party. Crypto-asset trading platforms, custodians and wallet providers often provide financially relevant services to user entities, and user auditors need to consider the relevant risks of material misstatement.

When obtaining an understanding of how the user entity uses the third party's services in their operations, as an auditor you are required to understand:

- the nature of the services the third party provides (i.e., trading, custodial or wallet services) and the significance of those services to the user entity, including their effect on the user entity's internal control
- the nature and materiality of the transactions processed, or the accounts or financial reporting processes on which the third party has an affect
- the degree of interaction (e.g., directing and monitoring versus autonomy) between the activities of the third party and those of the user entity
- the nature of the relationship between the user entity and the third party, including the relevant contractual terms for the activities the third party undertakes

Through obtaining the above understanding, you also need to determine whether the third party is in fact a service organization. In accordance with the CAS, the CAS defines a service organization as a third-party organization (or segment of a third-party organization) that provides services to the user entity that are part of that user entity's information systems relevant to financial reporting.

There are likely many controls at a service organization that will be part of the user entity's information system relevant to the preparation of the financial statements or related controls. For example, controls over the safeguarding of assets. A service organization's services are part of a user entity's information system if these services affect any of the following:

a. the way that information relating to significant classes of transactions, account balances and disclosures flows through the user entity's information system, whether manually or using technology, and whether it is obtained from within or outside the general ledger and subsidiary ledgers. This includes when the service organization's services affect:
    — how transactions of the user entity are initiated and how information about them is recorded, processed, corrected as necessary and incorporated in the general ledger and reported in the financial statements
    — how information about events or conditions, other than transactions, is captured, processed and disclosed by the user entity in the financial statements
b. the accounting records, specific accounts in the user entity's financial statements and other supporting records relating to the flows of information in paragraph a)

c. the financial reporting process used to prepare the user entity's financial statements from the records described in paragraph b), including as it relates to disclosures and accounting estimates relating to significant classes of transactions, account balances and disclosures; and

d. The entity's IT environment relevant to a) through c) above.

Traditionally, financial statement auditors have not considered certain functions performed by banks or stock exchanges to be that of service organizations. In these cases, the services provided are typically limited to executing transactions that are specifically authorized by the client, such as a bank processing chequing account transactions or a broker executing securities transactions.

Similarly, in a crypto-asset environment, an entity may authorize a transaction to occur through a third-party trading platform while maintaining responsibility for ensuring that the transaction was executed as intended (e.g., evidence of the completed transaction on the blockchain), without relying on information received from the third-party platform to support recording the transaction in their books and records. In these circumstances, the auditor may not view these third parties as service organizations.

Alternatively, bank trust departments that invest and service assets for others may initiate, execute and maintain the books and records for certain transactions. In these circumstances, the transactions that affect the user entity are, at least in part, physically and operationally separate from the user entity. Depending on the nature and materiality of these transactions, it may not be practicable for the user entity to implement effective controls for those transactions. In this case, these bank trust departments may be considered a service organization to the user entity.

In a crypto-asset environment, the following circumstances may arise:

- The user entity may engage a third-party trading platform to perform similar functions, such as record-keeping for transactions executed and assets held. The user entity may then periodically (e.g., monthly, quarterly) update their own financial records based on statements provided by the third-party trading platform.
- The user entity may be transacting directly with the third-party trading platform. For example, the user entity may wish to sell crypto-assets at a particular price, and the third-party trading platform may buy the assets directly rather than facilitating a trade with another independent party. In this circumstance where there is not a transaction on the blockchain, the user entity may have no record that the transaction has occurred as requested and therefore relies on a statement from the custodial trading platform.
- The third-party trading platform may commingle all crypto-assets into a single wallet that also includes assets of other entities and track the allocation of the account's holdings to each entity internally. The transaction may not involve a movement of the asset and may not generate a transaction record on the blockchain, and so the user entity is reliant on the third-party trading platform.

In these cases, the user entity is likely relying on the controls at the third-party trading platform as part of the user entity's information system relevant to financial reporting.

Asset custodians have often been viewed as service organizations based on the functions that they perform. Specific to crypto-assets, user entities may engage a third party to provide a secure storage facility for their assets in exchange for a fee. In determining whether the third party is a service organization, you may need to consider who effectively controls the safeguarding of the assets.

Some trading platforms that hold an entity's crypto-assets on their behalf to support trading are performing an asset custodian role in addition to their trading role. For example, you may establish that the trading platform is just playing an intermediary role to transactions (similar to an exchange), but you still need to consider whether the platform is an asset custodian given that the platform may hold a material amount of the entity's crypto-assets.

There may be some limited circumstances where no service organization relationship exists. The user auditor may determine this to be the case when all of the following apply:

- A user entity authorizes transactions to be executed by an independent trading platform or custodian.
- The trading platform or custodian activities are limited to processing transactions for the user entity account.
- Neither the trading platform nor the custodian maintains the user entity's accounting records, manages any assets, or initiates, records or processes transactions as an agent of the user entity.

Even when you conclude that no service organization relationship exists, you must still satisfy the requirements of CAS 315[6] and CAS 330[7] in ensuring that you obtain audit evidence to address the risks of material misstatements.

There is an element of judgment in assessing whether a third party is a service organization. A third party may be considered a service organization to one entity and not to another depending on the nature of transactions that occur between the different entities.

If you have determined that the third party is a service organization with controls relevant to the audit, you will then use your understanding of the nature and significance of services provided to:

- identify and assess the risks of material misstatement
- design and perform audit procedures responsive to those risks

Approaches to Obtaining an Understanding of and Evaluating the Relevant Controls at a Service Organization

As the user auditor, you may be able to address your assurance needs related to service organization controls relevant to the audit by obtaining and reviewing a SOC report that addresses reporting on controls at a service organization relevant to user entities' internal control over financial reporting.

6 CAS 315, *Identifying and Assessing the Risks of Material Misstatement*

7 CAS 330, *The Auditor's Responses to Assessed Risks*

SOC 1 reports are typically more likely to be relevant, as they address internal controls over financial reporting. However, a SOC 2 report on security, availability, processing integrity, confidentiality or privacy controls may also provide information relevant to you as the user auditor, depending on its scope.

There are two types of reports available for SOC 1 and SOC 2 engagements:

- A **type 1 report** provides evidence of whether controls have been designed and implemented at a point in time.
- A **type 2 report** (which more commonly fits the needs of the user auditor) provides evidence of whether controls have been operating effectively throughout the period covered by the report.

Regardless of the type of SOC report you obtain, you will need to consider these factors as you assess and validate whether the SOC report does in fact address the risks relevant to the audit of the user entity:[8]

- the scope of the service auditor's work
- the type of report being issued and its appropriateness, given your requirements as the user auditor
- the time period covered, given that, with the rate of change in the crypto-asset ecosystem, the user auditor may require audit evidence about the controls up to or very close to the period end

You will also need to consider (and test as appropriate) complementary user entity controls.

As the user auditor you are responsible for obtaining audit evidence to address the risks of material misstatement irrespective of whether a SOC report is obtained.

For example, to provide a basis for the identification and assessment of risks of material misstatement, you are required to obtain a sufficient understanding of the nature and significance of the services provided by the service organization and their effect on the user entity's internal controls relevant to the audit. If you are unable to obtain a sufficient understanding from the user entity and a SOC report is not available, you must obtain that understanding in one or more of the following ways:

- Contact the service organization, through the user entity, to obtain specific information.
- Visit the service organization and perform procedures that will provide the necessary information about the relevant controls at the service organization.
- Use another auditor to perform procedures that will provide the necessary information about the relevant controls at the service organization.

You would typically carry out these procedures by making inquiries, combined with inspection or observation, sufficient to determine that the relevant controls have been implemented.

8 Part 2 of this paper includes illustrative risks and controls at a service organization in the crypto-asset ecosystem and may assist a user auditor in assessing whether the SOC report addresses risks relevant to the audit of the user entity.

Additionally, when your risk assessment includes an expectation that controls at the service organization are operating effectively, and a Type 2 report is not available,[9] as the user auditor you are required to obtain audit evidence about the operating effectiveness of those controls in one or more of the following ways:

- Perform appropriate tests of controls at the service organization.
- Use another auditor to perform tests of controls at the service organization on your behalf.

If you are unable to complete the necessary procedures to obtain audit evidence to address the assessed risks of material misstatement when a SOC report is not available, you would need to modify your opinion in the user auditor report in accordance with CAS 705.[10]

Part 2 of this paper provides practical guidance to assist you as the user auditor in two areas:

- obtaining your understanding of the services provided (including internal control) at a service organization in the crypto-asset ecosystem
- responding to the assessed risks of material misstatement

PART 2

Identifying Risks and Relevant Controls at a Service Organization

Before you assess the design and implementation of controls at the user entity's service organization, as the user auditor you first identify what those relevant controls may be. This section of the paper identifies possible topics of interest when auditing financial statements with material crypto-asset balances and/or transactions, including risk scenarios and related assertions as well as illustrative controls.

Where you as the user auditor are able to obtain a SOC report, this section provides some examples of possible risks and illustrative controls that may be relevant to the audit and that you would therefore want to ensure are included in the SOC report.

Where a SOC report is not available or the SOC report itself is not sufficient for the user auditor's purposes, this section provides some examples that you could consider in obtaining your understanding directly (e.g., performing your own testing of controls relevant to the audit at the service organization, where possible).

Please note that the topics and related risk scenarios are not exhaustive and identifying those that are relevant to a financial statement audit will depend on the individual facts and circumstances of the particular user entity.

9 A Type 1 report is currently more common in the crypto-asset ecosystem given the immaturity of the industry.

10 CAS 705, *Modifications to the Opinion in the Independent Auditor's Report.*

The legend for the financial statement assertions is as follows:

A	Accuracy, valuation and allocation
C	Completeness
E	Existence
CO	Cutoff
O	Occurrence
R	Rights (ownership)

Cryptographic Key Management

Engaging in crypto-asset transactions typically involves the use of cryptographic keys that must be securely generated, stored, used and ultimately retired. If cryptographic keys are compromised (e.g., security breach or inadvertent destruction) or lost, assets could become inaccessible or misappropriated, records could be altered, and unauthorized transactions could be processed. Thus, management of cryptographic keys through their lifecycle (that is, generation, storage, usage, and retirement) is a critical responsibility for trading platforms, custodians and wallet providers.

As the user auditor, you will need to obtain an understanding of controls related to the management of cryptographic keys when a service organization engaged by the entity employs blockchain technologies. This likely will be relevant to a user entity's internal control over financial reporting when cryptographic keys are used to authenticate and validate financial transactions, transfer assets between participants, and modify financially relevant data. The proper use and control of cryptography underpins the trust that blockchain networks seek to offer.

The following are examples of important matters that likely need to be considered in terms of managing cryptographic keys. This list is not intended to be comprehensive and you will need to consider the facts and circumstances specific to the user entity:

- What cryptographic objects (i.e., private keys, symmetric keys, hardware security modules, etc.) exist?
  - Cryptographic objectives involved in the blockchain network may include *hot storage* and *cold storage* of cryptographic keys, where differing technical tradeoffs are made involving speed-of-access vs. protection from loss or theft.
  - More sensitive cryptographic keys may be fully *air gapped* from any network connectivity at all.
  - Hardware security modules may also be used to enhance protection.
- How are cryptographic keys managed?
  - the controls associated with security of and access (logical and physical) to the cryptographic keys: These controls are needed at every stage in the lifecycle of the cryptographic object, which includes key generation, storage, usage and retirement.
  - the controls implemented by the user entity to manage access to the third-party platform: Unauthorized access to (or copying of) private keys can lead to unauthorized transactions, theft of associated assets and falsification of data.

— the segregation of duties controls over private keys: In some cases, private cryptographic keys may be split into multiple parts, where a subset of those parts can be used to recover the original cryptographic key. This process is called "*sharding*." The key "shards" can be distributed to responsible custodians to provide a more robust segregation of responsibilities.

— the creation of secure backups: If the original key is lost, the crypto-asset remains accessible.

TABLE 1: ILLUSTRATIVE RISKS AND CONTROLS – CRYPTOGRAPHIC KEY MANAGEMENT

Topic	Risk / "What could go wrong" scenario	A	C	CO	E	O	R	Example types of controls
Key management	Compromise or loss of cryptographic keys				X		X	Controls over secure key generation, storage, usage and retirement.

Custody, Recordkeeping, Order Execution and Customer Transactions

User entities may rely on the service organization to have controls related to custody, recordkeeping, order execution and effective performance of customer transactions. The service organization may therefore need to have controls that address:

- reconciliations between the blockchain and the entity's internal records
- effective recordkeeping
- authorization and validation of customer interactions and transactions (including deposits, transfers and withdrawals)
- prevention of commingling of assets (where held in separate wallets, or accurate recordkeeping where assets for more than one client are commingled in one or more wallets)
- account opening and order execution

In some cases, trading platforms may hold crypto-assets on behalf of the entity and transact with them solely through their own recordkeeping functions. This heightened level of involvement of the service organization impacts risk, particularly when transactions with that party occur off-chain.

You may consider whether control objectives and related controls that address consensus mechanisms and protocols associated with the blockchain are relevant to the user entity's internal control over financial reporting, and thus relevant to the audit. Where the blockchain-distributed ledger denotes ownership of assets, if the consensus mechanisms fail, this could result in asset loss. Similarly, if controls over the consensus mechanisms are not effective, it could lead to duplicate and inconsistent versions of the blockchain-distributed ledger among the participants, and the participants may end up disagreeing about who owns the assets or whether the data is valid.

In many public blockchain networks, the service organization (and the user entity) may be unable to control features of the blockchain that could impact them (and the user entity), such as the consensus mechanisms, forks and contract upgrades.[11] Because the operation of the consensus mechanisms is often beyond either organizations' direct control, the service organization's role may be limited to monitoring and responding to issues. The user entity may also need controls in place to monitor and confirm that there is no manipulation of the network, if the service organization does not already perform this function.

TABLE 2: ILLUSTRATIVE RISKS AND CONTROLS – CUSTODY, RECORDKEEPING, ORDER EXECUTION AND CUSTOMER TRANSACTIONS

Topic	Risk / "What could go wrong" scenario	A	C	CO	E	O	R	Example types of controls
Custody[12]	The service organization does not maintain custody of sufficient crypto-assets to satisfy customer deposits. As a result, they are unable to fulfill customer obligations.	X			X		X	The service organization performs a reconciliation between crypto-assets on the blockchain and its internal books and records. Note: this assumes that the user auditor has obtained audit evidence to validate whether the information stored on the blockchain is reliable. (see footnote 11)
Record-keeping	The user entity records crypto-assets or crypto-asset transactions that are inaccurate, do not exist, are incomplete or for which they do not maintain sufficient recordkeeping controls, including controls that address off-chain transactions.	X	X	X	X	X	X	The service organization has controls over sales and purchases of crypto-assets between the user entity and customers, such as having a system where, when transactions are executed, they are automatically recorded in the trading system. The service organization has controls over the appropriate maintenance of customer balances, including tracking movements in those balances.
Customer statements	The user entity relies on customer statements provided by the service organization which are incomplete or inaccurate.	X	X	X	X	X	X	The service organization has controls over whether the customer statements provided to the user entity are complete and accurate.

11 For further guidance, please refer to CPA Canada's *Relevance and reliability of information from a blockchain*

12 For further guidance, please refer to CPA Canada's *Are tests of controls needed regarding the ownership assertion?*

Topic	Risk / "What could go wrong" scenario	A	C	CO	E	O	R	Example types of controls
Validation of customer interactions	Due to the risk associated with changes to customer accounts, customers lose funds or are unaware of changes made to their account.	X			X			The service organization's customers receive an automated notification when a transaction is processed or a change is made to their account which includes contact details to report suspicious or unauthorized transactions.
Withdrawals of funds	The service organization does not identify instances where customers withdraw funds beyond their current balance.	X			X			Before performing the transaction, the service organization performs an automated validation to confirm that the customer account has sufficient funds.
Commingling of funds	The user entity does not have appropriate controls over commingling of funds	X			X		X	The service organization has controls to appropriately segregate each customer's crypto-assets from the other customers' and their own holdings.
Customer account opening	The service organization does not comply with Know Your Customer protocols.				X		X	The service organization has controls over the registration of customers, including identity verification procedures when they open the account.
Order execution	The service organization does not have effective controls for processing orders.	X		X	X			The service organization has controls to ensure open trades and/or orders are processed completely, accurately and on a timely basis when the appropriate triggering event occurs.
Consensus mechanisms and protocols	Undetected failure in the consensus mechanisms.				X		X	The service organization has monitoring controls to confirm there is no manipulation of the distributed ledger.

IT Infrastructure Security Operations

As with most systems, if fundamental security management fails, this can lead to a breakdown and loss of control over digital records. Effective controls over system access, change management and operations are essential.

You, as the user auditor may need to determine who has responsibility for managing access permissions on the third-party platform and whether controls adequately address:

- identity and access management, including participant account creation and maintenance, as well as privileged access
- infrastructure security (whether on-premise or in the cloud)
- data security of various data storage components (whether on-premise or in the cloud)
- security incident management

TABLE 3: ILLUSTRATIVE RISKS AND CONTROLS – IT INFRASTRUCTURE SECURITY OPERATIONS

Topic	Risk / "What could go wrong" scenario	A	C	CO	E	O	R	Example types of controls
IT infra-structure security	Failure of IT infrastructure controls results in loss of control over digital records				X		X	General IT controls that address system access, system security, system development, change management and IT operations

Once you have obtained an understanding of relevant controls at a service organization, including evidence that they are operating effectively (when your risk assessment includes this expectation), you may identify that there are substantive procedures for which you will need to obtain information directly from the service organization. In addressing the risk of material misstatement, you will need to consider whether that information is relevant and reliable.

Conclusion

The crypto-asset ecosystem continues to advance. The interaction of entities with trading platforms, custodians and wallet providers gives rise to risks that are relevant for financial statement auditors, particularly as it relates to matters such as (i) cryptographic key management, (ii) custody, recordkeeping, order execution and customer transactions, and (iii) IT infrastructure security operations.

As the auditor, you will need to continue to update your understanding of the entity, and specifically its use of third parties as it relates to any crypto-asset holdings or trades, to inform the risk assessment and plan further audit procedures to obtain audit evidence to address identified risks of material misstatements.

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, Deloitte, EY, KPMG, MNP, PwC and Raymond Chabot Grant Thornton.

CPA Canada gratefully acknowledges Deloitte for leading the authoring of this publication on behalf of the Working Group.

Additional Resources

1. CPA Canada. (2018). *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. (2020). *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. (2020). *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)
4. *CPA Canada Handbook,* CAS 315, CAS 330 and CAS 402

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