CHARTERED PROFESSIONAL ACCOUNTANTS CANADA

Audit Considerations Related to Cryptocurrency Assets and Transactions

CPA CHARTERED PROFESSIONAL ACCOUNTANTS CANADA

Audit Considerations Related to Cryptocurrency Assets and Transactions

DISCLAIMER

This paper was prepared by the Chartered Professional Accountants of Canada (CPA Canada) as non-authoritative guidance.

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

Table of Contents

Executive Summary

An entity's financial statements may include material cryptocurrency items. This paper is intended to be useful to auditors who have little or no experience with cryptocurrencies and may not fully appreciate the challenges presented when auditing these items. Highlights of matters described in this paper are set out below.

- *Client Acceptance and Continuance Considerations*
  Matters to consider include, for example:
  - integrity of the client, including the business purpose for which the entity is entering into cryptocurrency transactions (e.g., that transactions do not involve money laundering or other illegal acts)
  - management's level of understanding of cryptocurrency risks and internal control over cryptocurrency transactions and balances
  - whether the audit engagement partner is satisfied that those involved in the engagement (including members of the engagement team and any auditor's external experts) collectively have the appropriate competence and capabilities in information technology (IT) and cryptocurrencies to perform the engagement in accordance with professional standards.

- *Obtaining an Understanding of the Entity's Information System for Cryptocurrency Transactions*
  Matters such as cryptography and **blockchains** are complex. Reference sources are provided to enable readers to obtain information on these topics. A simplified example of a process to purchase **cryptocurrency** is provided. There is also a brief description of various types of cryptocurrency **wallets**. These contain the entity's private and public cryptographic keys used in selling cryptocurrency and are used to monitor the entity's cryptocurrency balance.

- *Examples of Matters to Consider in Identifying and Assessing Risks of Material Misstatement in Cryptocurrency Transactions and Balances*
  Nine examples are provided of conditions or events that may result in a material misstatement. The material briefly describes matters related to the condition or event, notes the related assertions, and provides examples of internal control considerations. The nine conditions or events are as follows:
  1. The entity chooses to use a cryptocurrency exchange that does not have effective controls over the transactions it enters into on behalf of the entity or over the balances of cryptocurrency maintained in the entity's accounts.
  2. The entity has a cryptocurrency wallet that has not been accounted for.
  3. The entity loses a private key and therefore can no longer access the related cryptocurrency.
  4. An unauthorized party obtains access to the entity's private key and steals the entity's cryptocurrency.
  5. The entity misrepresents ownership of a private key and therefore of the related cryptocurrency.
  6. The entity sends cryptocurrency to an incorrect address and the cryptocurrency cannot be recovered.
  7. The entity enters into and records a cryptocurrency transaction with a related party that cannot be identified because of the anonymity of parties to blockchain transactions.
  8. There are significant delays in processing cryptocurrency transactions at the end of a period.
  9. Events or conditions make it difficult to determine the value at which a cryptocurrency should be recorded for financial reporting purposes.

Introduction

Holdings of **cryptocurrencies** allow individuals and businesses to transact directly with each other without an intermediary such as a bank or other financial institution. These cryptocurrency transactions rely on blockchain technology. For an introduction to blockchain technology and the related audit implications, refer to the CPA Canada publication, **Blockchain Technology and Its Potential Impact on the Audit & Assurance Profession.**

The rapid rise and volatility of cryptocurrencies have led to increased global interest and scrutiny by organizations, investors, regulators, governments and others. During 2017, the market capitalization of cryptocurrencies increased by US$547 billion or 3,038%.[1] The most popular and widely used cryptocurrency is Bitcoin; however, there are over 1,600 cryptocurrencies in circulation.[2] Each of these cryptocurrencies has its own unique features and characteristics which makes understanding, accounting and auditing them particularly challenging.

It is becoming common for financial statements to show cryptocurrency balances and to reflect the results of cryptocurrency transactions. However, many auditors may have little or no experience with cryptocurrencies and therefore may not fully appreciate the challenges that auditing these items may present. This non-authoritative publication is intended to provide auditors with examples of matters to consider when:

- deciding whether to accept or continue an audit engagement when an entity has engaged in material cryptocurrency transactions
- identifying and assessing risks of material misstatement in financial statements related to cryptocurrency transactions and balances.

1 https://coinmarketcap.com/charts.

2 https://coinmarketcap.com as at June 19, 2018.

We encourage auditors to continue to monitor developments in this space and we invite readers to contact us with any feedback or insights that could help us develop future publications on this topic.

Taryn Abate, CPA, CA, CPA (IL)
Director, Audit & Assurance
Research, Guidance and Support
CPA Canada
277 Wellington Street West
Toronto ON M5V 3H2
Email: tabate@cpacanada.ca

Scope

This publication focuses only on engagements to audit financial statements that show material cryptocurrency balances. It does not discuss other types of engagements, such as review of financial statements containing material cryptocurrency items. However, matters discussed in this publication may be adapted as necessary by practitioners performing other types of engagements.

This publication does not discuss procedures that might be performed in response to assessed risks (i.e., tests of controls and substantive procedures). Some auditing firms are exploring the nature, timing and extent of such procedures. Practice will likely evolve as more experience is gained.

This publication also does not discuss matters such as auditing:

- liabilities resulting from agreements to pay amounts owing using a cryptocurrency
- financial statements of a cryptocurrency exchange
- financial statements of entities that:
  - validate cryptocurrency transactions on a blockchain (i.e., cryptocurrency miners)
  - issue Initial Coin Offerings (ICOs) or Initial Token Offerings (ITOs)
- investments in ICOs and ITOs
- controls related to the infrastructure supporting a blockchain, such as the hardware and software used in operating a node
- aspects of income tax expense and liability that may be affected by a lack of clarity in how tax laws and regulations apply to cryptocurrency transactions and balances
- controls implemented by a service organization (perhaps a cryptocurrency exchange) and complementary controls designed and implemented by the entity. For example, any entity's cryptocurrency wallet(s) may be hosted by a cryptocurrency exchange or other type of entity providing this service, resulting in that organization being significantly involved in cryptocurrency transactions and custody of an entity's cryptocurrency.

Client Acceptance and Continuance Considerations

Canadian Standard on Quality Control 1 (CSQC 1) requires a firm to establish policies and procedures for the acceptance and continuance of client relationships and specific engagements.

These policies and procedures are designed to provide the firm with reasonable assurance that it will only undertake or continue relationships and engagements where the firm:

1. Is competent to perform the engagement and has the capabilities, including time and resources, to do so;
2. Can comply with relevant ethical requirements; and
3. Has considered the integrity of the client, and does not have information that would lead it to conclude that the client lacks integrity.

Auditing cryptocurrency transactions can be complex:
Have you considered all relevant matters before accepting or continuing an engagement?

An entity's use of cryptocurrency is likely to be relevant to the auditor in deciding whether to accept or continue an engagement to audit an entity's financial statements. An auditor may encounter circumstances where, for example, the entity has:

- entered into material cryptocurrency transactions for the first time
- significantly changed the nature or increased the extent of its cryptocurrency activities from previous years. For example, an investment entity that previously focused primarily on traditional investment vehicles may decide that a significant part of its investment portfolio will now include cryptocurrencies.

Examples of matters to consider regarding client acceptance or continuance are set out below.

Integrity of the Client Including Its Business Purpose in Entering into Cryptocurrency Transactions

An example of a matter for the auditor to consider regarding client integrity is whether there are indications the client might be involved in money laundering or other criminal activities. There are legitimate business reasons to use cryptocurrencies. However, cryptocurrencies have also been used to launder the proceeds of criminal activities and to finance terrorism and other illegal acts. These types of activity are enabled by the anonymity of participants in blockchain transactions. Also, exchanges where cryptocurrencies are traded for fiat currencies remain largely unregulated (e.g., some are not subject to regulations that apply to banks such as know-your-customer (KYC) and anti-money laundering (AML) rules and requirements to keep a record of unusual transactions).

The auditor's engagement acceptance or continuance procedures would therefore likely include inquiries and related procedures to obtain an understanding of the entity's business purpose in entering into cryptocurrency transactions for the first time or significantly changing the nature or extent of its cryptocurrency activities. A key consideration is whether the entity's significant cryptocurrency transactions are in the normal course of its business. If the auditor identifies significant cryptocurrency transactions that are outside the normal course of business, the auditor is required to:

- evaluate whether it gives rise to significant risks[3]
- inquire of management about the nature of these transactions and whether related parties could be involved,[4] and
- whether the business rationale (or the lack thereof) suggests that they may have been entered into to engage in fraudulent financial reporting or to conceal misappropriation of assets.[5]

The auditor is also required to remain alert to the possibility of instances of non-compliance or suspected non-compliance with laws and regulations, including money laundering or other illegal activities.[6]

3 Paragraph 27 of CAS 315, *Identifying and Assessing the Risks of Material Misstatement through Understanding the Entity and Its Environment.*

4 Paragraph 16 of CAS 550, *Related Parties.*

5 Paragraph 33(c) of CAS 240, *The Auditor's Responsibilities Relating to Fraud in an Audit of Financial Statements.*

6 Paragraph 16 of CAS 250, *Consideration of Laws and Regulations in an Audit of Financial Statements.*

Client's Level of Understanding of Cryptocurrency Risks and Relevant Aspects of Internal Control

To establish whether the preconditions for an audit engagement are present, the auditor obtains the agreement of management that it acknowledges and understands its responsibility for certain matters, including:

- the preparation of the financial statements in accordance with the applicable financial reporting framework, including, where relevant, their fair presentation
- internal controls necessary to enable the preparation of financial statements free from material misstatement whether due to fraud or error.[7]

Ideally, the client would have an understanding of matters related to cryptocurrency, including its financial reporting implications. The client also would have designed and implemented controls related to its cryptocurrency transactions and balances. However, an auditor may encounter circumstances where the prospective client has not even implemented a process to track its cryptocurrency transactions. In these circumstances, it may be very difficult or not practicable to audit the entity's financial statements.

Competence and Capabilities of Those Involved in Performing the Engagement[8]

Cryptocurrency transactions and management of cryptocurrency assets often involve the use of highly complex cryptography and information technology (IT). In some cases, it may not be practicable to audit cryptocurrency-related assets and transactions without relying on the effective operation of relevant controls. In addition, matters such as the valuation of cryptocurrency items for financial reporting purposes may require the use of valuation experts. Therefore, when deciding whether to accept or continue an engagement to audit financial statements that include material cryptocurrency items and transactions, the engagement partner has to determine whether those involved in performing the engagement (including both members of the engagement team and any auditor's external experts) possess appropriate competency and capabilities.

7 Paragraph 6 of CAS 210, *Agreeing the Terms of Audit Engagements.*

8 Paragraph 31 of CSQC 1, *Quality Control for Firms that perform Audits and Review of Financial Statements, and Other Assurance Engagements.*

The Entity's Information System for Cryptocurrency Transactions

Canadian Auditing Standards (CASs) require the auditor to obtain an understanding of the entity's information system[9]. This includes, for example, the entity's procedures, within both IT and manual systems, by which transactions are initiated, recorded, processed, corrected as necessary, transferred to the general ledger and reported in its financial statements.

Major cryptocurrencies use transparent public blockchains. All transactions are permanently recorded on the blockchain. Anyone can read or aggregate recorded transactions. These transactions can be tracked, for example, by using a transaction identification number or an address. It is sometimes claimed that blockchain technology eliminates the need for trust among transaction participants. Even if this is true to some degree, nevertheless, there are challenges and risks to using blockchain technology and cryptocurrency.

Some aspects of the entity's procedures regarding cryptocurrency transactions will differ significantly from those for fiat currencies. For example, cryptocurrency transactions involve the use of cryptography, **cryptocurrency wallets** and a blockchain. It is possible (although rare) that a cryptocurrency organization may use a cryptographic system other than a blockchain (e.g., Ripple).

To help obtain an understanding of these complex matters, readers may refer to sources such as the following:

- **OSC — Ontarians and Cryptocurrencies — A First Look**
- **Bank of Canada — Briefing on Digital Currencies**
- **US Congressional Research Service — Bitcoin Q&As**

9 Paragraph 18 of CAS 315.

- UWCISA Bitcoin Process Flow — Accountants Guide
- Nasdaq article — Cryptocurrency-and-your-small-business-what-you-need-to-know

Example of a Cryptocurrency Purchase

Exhibit 1 shows a simplified example of how cryptocurrency might be purchased and the transaction recorded. This exhibit and the subsequent discussion of cryptocurrency wallets are aimed at readers not already familiar with cryptocurrency transactions. The Exhibit is generic; individual entities may follow a process different from what is illustrated.

A process similar to that shown below might be followed when selling cryptocurrency. For example, the cryptocurrency might be exchanged for another cryptocurrency or a fiat currency.

Other transactions might involve, for example, using cryptocurrency for the sale or purchase of goods or services.

EXHIBIT 1—SIMPLIFIED EXAMPLE OF A CRYPTOCURRENCY PURCHASE TRANSACTION

- Management determines the type of cryptocurrency to be purchased.
- A **cryptocurrency wallet** is downloaded from a service provider. A password or passphrase and other security measures considered appropriate are used to secure the wallet against unauthorized access. (See information on types of wallets in the next section of the paper.)
- The wallet software is used to generate the entity's cryptographic private key. A public key is generated using the private key, and the entity's address (single-use identifier) for each cryptocurrency purchase transaction is generated from the entity's public key.
- Management establishes an account with a **cryptocurrency exchange or broker**.
- The desired amount of cryptocurrency is purchased using the entity's cryptocurrency hot wallet (see next section).
- The transaction is authenticated and then irreversibly recorded on a blockchain. Transactions may be viewed using a blockchain or block explorer (when available).

- To protect the entity's private key from unauthorized access through the Internet, the entity may use one or more methods of cold storage (i.e., cold wallets) to store the private key and related information (e.g., addresses to which the private key is linked).
- Backup copies of the entity's cryptographic keys, particularly the private key, as well as passwords or passphrases needed to access a wallet, are made and safely stored.
- The cryptocurrency transaction is recorded in the company's financial reporting system then, if applicable, translated into the entity's functional currency at an appropriate exchange rate.
- In preparing the entity's financial statements, any adjustments needed are made to the recorded amount of the cryptocurrency asset and related transactions to comply with the applicable financial reporting framework (e.g., IFRS® Standards). For additional guidance on the accounting implications of cryptocurrencies, see CPA Canada's paper, ***An Introduction to Accounting for Cryptocurrencies***.

Cryptocurrency Wallets

Cryptocurrency transactions involve the use of a software program known as a cryptocurrency wallet. A wallet is used, for example, to:

- store the entity's private and public encryption keys used for cryptocurrency transactions
- interact with one or more blockchains to send and receive cryptocurrency
- show the entity's balance in each cryptocurrency that results from the various transactions.

If the entity loses a private key and it cannot be recovered, the entity will no longer be able to access the cryptocurrency linked to that key. Therefore, in effect, the cryptocurrency is lost. Also, if an entity's private key is obtained by an outside party, it can be used to undertake unauthorized cryptocurrency transactions which cannot be reversed. The entity's wallet would show transactions not authorized by the entity. The stolen cryptocurrency may never be recovered.

Types of Cryptocurrency Wallets

Hot Wallet

A "hot wallet" is located in a device connected to the Internet (whether hosted or entity-controlled). A hot wallet is required to send cryptocurrency to another address (e.g., spend cryptocurrency) and to obtain an up-to-date snapshot of all the entity's recent cryptocurrency transactions and balances.

Cold Wallet

A "cold wallet" (or "cold-storage wallet") is not connected to the Internet. The following are examples of cold wallets:

- **Hardware Wallet**
  A "hardware wallet" is located on a USB or other device. The entity's private and public keys are generated in the device when it is offline by using a random number generator. When the wallet is not connected to the Internet, the entity's private key is, of course, not accessible by outside parties via the Internet. However, a private key is still susceptible to loss or theft by other means. For example, the device containing the cold wallet may be lost or damaged. Also, a cold wallet temporarily becomes a hot wallet (and therefore less secure) whenever the device containing the cold wallet is connected to the Internet. The private key that was generated offline is now being used online in the process of sending cryptocurrency to another address and is therefore temporarily exposed, for example, to viruses or malware. However, some hardware wallets have a process that generates a digital signature offline in the device so the private key never appears on the computer or other device used to execute the sale transaction.

- **Paper Wallet**
  A "paper wallet" is a paper record of the entity's private key and related information. When the entity's computer or other devices and printer are offline, software is used to generate a set of private and public keys and related addresses for its cold wallet. The public and private keys for the wallet are printed out on paper. The desired amount of cryptocurrency is sent from the entity's hot wallet to its paper wallet address. The amount transferred to the paper wallet can be written down. Cryptocurrency can subsequently be sent from the paper wallet. This may be done by entering into the entity's hot wallet the address to which cryptocurrency is to be sent, then scanning or typing the paper wallet private key into the hot wallet. This private key will then be used to generate the digital signature

for the transaction. For the short period of time it takes to send the cryptocurrency, the paper wallet's private key is no longer "cold" and therefore is exposed, for example, to viruses and malware.

Exchange-Hosted Wallet

An "exchange-hosted wallet" is hosted by a cryptocurrency exchange on its server. The wallet is linked to the entity's account with the exchange. That account contains information identifying the entity. Access to the account and wallet requires a password. The exchange knows the entity's private key stored in the wallet, but the entity itself does not know its private key. The exchange undertakes the cryptocurrency transactions on behalf of the entity (based on the entity's instructions or what has otherwise been agreed).

Examples of Matters to Consider When Identifying and Assessing Risks of Material Misstatement in Cryptocurrency Transactions and Balances

For the purpose of identifying and assessing risks of material misstatement, the CASs require[10] the auditor to:

- Identify risks throughout the process of obtaining an understanding of the entity and its environment, including relevant controls that relate to the risks, and by considering the classes of transactions, account balances, and disclosures (including the quantitative or qualitative aspects of such disclosures) in the financial statements;
- Assess the identified risks, and evaluate whether they relate more pervasively to the financial statements as a whole and potentially affect many assertions;
- Relate the identified risks to what can go wrong at the assertion level, taking account of relevant controls that the auditor intends to test; and
- Consider the likelihood of misstatement, including the possibility of multiple misstatements, and whether the potential misstatement is of a magnitude that could result in a material misstatement.

10 Paragraph 26 of CAS 315.

A risk of material misstatement of a cryptocurrency balance or transaction may be identified when:

- a condition exists or an event occurs that is relevant to one or more of the assertions related to the entity's cryptocurrency balances and transactions
- the entity has not implemented internal control to provide reasonable assurance the results of these events and conditions are recorded in the entity's accounts and reflected in its financial statements as required by the applicable financial reporting framework.

Set out below are nine examples of events or conditions an auditor would likely consider as part of performing procedures to identify and assess risks of material misstatement in cryptocurrency transactions and balances whether due to fraud or error. The information provided for each example includes:

- a brief description of the condition or event
- related assertions
- examples of aspects of internal control that could help prevent or detect and correct a material misstatement. These examples are not a complete list of internal control considerations.

This list is not intended to be exhaustive; other conditions and events may give rise to a risk of material misstatement in cryptocurrency transactions or balances.

Exhibit 2 summarizes these conditions or events and the assertions that may be affected.

EXHIBIT 2—SUMMARY OF CONDITIONS, EVENTS AND ASSERTIONS THAT MIGHT BE AFFECTED

Examples of Condition or Events "What Can Go Wrong"	Examples of Assertions to Which a Possible Misstatement May Relate[11]					
	A	C	CO	E	O	R
1. The entity chooses to use a cryptocurrency exchange that does not have effective controls over the transactions it enters into on behalf of the entity or over the balances of cryptocurrency maintained in the entity's accounts.	×	×	×	×	×	×
2. The entity has a cryptocurrency wallet that has not been accounted for.		×				
3. The entity loses a private key and therefore can no longer access the related cryptocurrency.						×

11 Paragraph A129 of CAS 315.

Examples of Condition or Events "What Can Go Wrong"	Examples of Assertions to Which a Possible Misstatement May Relate[11]					
	A	C	CO	E	O	R
4. An unauthorized party obtains access to the entity's private key and steals the entity's cryptocurrency.				×		×
5. The entity misrepresents ownership of a private key and therefore of the related cryptocurrency.				×	×	×
6. The entity sends cryptocurrency to an incorrect address and the cryptocurrency cannot be recovered.						×
7. The entity enters into and records a cryptocurrency transaction with a related party that cannot be identified because of the anonymity of parties to blockchain transactions.	×	×				
8. There are significant delays in processing cryptocurrency transactions at the end of a period.			×			
9. Events or conditions make it difficult to determine the value at which a cryptocurrency should be recorded for financial reporting purposes.	×					

Legend:

A: Accuracy, valuation and allocation
C: Completeness
E: Existence
CO: Cut-off
O: Occurrence
R: Rights (ownership)

Note: Assertions related to presentation are not discussed therein. Also, auditors may use assertions other than those referred to in the paper.

What follows this is a description of example conditions or events that may result in a risk of material misstatement. **This is not a complete list**.

11 Paragraph A129 of CAS 315.

Do you have the appropriate experience needed to audit material cryptocurrency balances and transactions?

If you are auditing an entity with material cryptocurrency balance(s) or transactions, have you assessed all of the risks of material misstatements and related assertions?

Are you comfortable that you will be able to obtain sufficient appropriate audit evidence through designing and performing appropriate responses to those risks?

1. **The entity chooses to use a cryptocurrency exchange that does not have effective controls over the transactions it enters into on behalf of the entity or over the balances of cryptocurrency maintained in the entity's accounts.**

   Related Assertions: *there is a possibility that any of the assertions may be affected.*

   It is common for an entity to use an online exchange to enter into cryptocurrency transactions. Also, in some cases, the entity may use a cryptocurrency wallet hosted by the exchange.

   Attributes of the exchange selected may have important implications for all of the assertions related to cryptocurrency noted above. Considerations in selecting an online exchange may include the following:

   - who owns and operates the exchange, and its reputation (e.g., some exchanges have allegedly been associated with "pump and dump" schemes (i.e., pump up the price of an security through false stories then dump/sell to the new investors) to artificially affect cryptocurrency prices).
   - the country in which the exchange is located. This may determine, for example, the laws and other regulations to which the exchange is subject and could include money laundering regulations that require the exchange to follow "know your customer" protocols.
   - cryptocurrencies and fiat currencies for which the exchange allows trades
   - exchange's liquidity and trading volume
   - controls the exchange has in effect related, for example, to the security provided over exchange-hosted wallets.

- whether the exchange provides a service auditor's report on the effectiveness of its controls over cryptocurrency transactions and balances undertaken on behalf of its clients. Currently, appropriate service auditor's reports on these controls are rare. However, some cryptocurrency exchanges and auditors are exploring service auditor engagements. Therefore, it is possible that more service auditor's reports will become available in future years.

Internal Control Considerations

- The entity may assign responsibility for selecting the cryptocurrency to purchase and the exchange to use to knowledgeable personnel who are aware of the risks involved and how they might be mitigated.
- Senior management may review and, if appropriate, approve the choices made.
- The entity may decide to use at least two-factor authentication to access its account. This would somewhat mitigate the risk of unauthorized access to the entity's exchange-hosted wallet.

2. The entity has a cryptocurrency wallet that has not been accounted for.

Related Assertions: *Completeness in both recording the cryptocurrency assets and related transaction(s)*

An audited entity may fail to account for one or more of its cryptocurrency wallets (and the related cryptocurrency that it owns). The entity's cryptocurrency assets and related transactions will not have been recorded.

This risk of material misstatement regarding completeness of cryptocurrency assets and transactions may be difficult to assess. The public keys and related addresses in a blockchain do not make transparent the identities of the parties participating in transactions. Further, the entity may not have a long history of cryptocurrency transactions. As a result, the auditor may have difficulty obtaining useful information on which to base their expectation that significant cryptocurrency transactions may not have been recorded.

If the existence of a wallet not previously accounted for comes to the attention of the auditor during the course of the audit, there may be indications its existence was deliberately hidden. This may be indicative of a fraud risk, including the risk of management override of controls regarding cryptocurrency wallets.

Internal Control Considerations

The failure to identify a wallet owned by the entity may be inadvertent. An entity can have many wallets, such that controls regarding authorization for wallet creation and subsequent tracking of wallets may not have been operating effectively. The entity may therefore have lost track of one or more wallets. Establishing clear lines of responsibilities related to wallet creation and tracking may mitigate such risk.

3. The entity loses a private key and therefore can no longer access the related cryptocurrency.

Related Assertions: *Rights (ownership) of cryptocurrency assets*

If the entity loses a private key, or it is corrupted and it cannot be recovered, the entity will no longer be able to access the cryptocurrency linked to that key and will thus no longer be able to establish its ownership rights. The cryptocurrency connected to that private key will, however, continue to exist on the relevant blockchain. Nevertheless, the cryptocurrency linked to the private key no longer exists as an asset of the entity.

The loss of a private key gives rise to material misstatement if the effect of the loss is not properly accounted for. However, this risk of material misstatement may arise, for example, if those responsible for control over the private key are not aware of its loss when the financial statements are being prepared since they have not attempted to enter into any new cryptocurrency transactions. As another example, those at fault for losing the entity's private key may have a strong incentive to attempt to conceal the loss or not report it on a timely basis.

Internal Control Considerations

- Controls to reduce the risk of loss of access to a private key:
  For example, policies and procedures may be implemented to require that the private key (and perhaps related public keys and addresses) be backed up. Backups might be located on separate electronic devices. Another approach is to use a paper wallet. Private keys and passwords or passphrases stored on the backup device or paper wallet might in turn be backed up to help provide reasonable assurance the entity will not lose its cryptocurrency. In addition, the location of the backup device or paper wallet should be made known to several appropriate persons (i.e., not just known to one person).

- Controls to reduce the risk that the loss of a private key will not be communicated and the resulting loss not recorded:
  Policies and procedures implemented by an entity may include establishing appropriate segregation of duties (i.e., the responsibility for monitoring cryptocurrency assets from a financial reporting standpoint is performed by persons not involved in executing the entity's cryptocurrency transactions). Policies and procedures may also require that such monitoring be ongoing (e.g., through reviews of the entity's wallets or use of a blockchain (block) explorer when available).

4. An unauthorized party obtains access to the entity's private key and steals the entity's cryptocurrency.

Related Assertions: *Rights (ownership) of cryptocurrency assets and Existence of assets for the entity*

Matters relevant to the theft of a private key are similar to those for the loss of a private key noted in Example 3 above.

Internal Control Considerations
Risks of unauthorized access to a hot wallet may be mitigated by use of two-factor or multi-factor authentication to obtain access to a wallet. Encryption of wallet contents may add another level of security. Also, the use of a hot wallet only when entering into cryptocurrency transactions and using a cold wallet to store the entity's private key and related information may mitigate the risk of unauthorized access to the entity's private key over the Internet. Further, an entity may decide to have only a small part of its cryptocurrency accessible from a hot wallet, with most of it cryptocurrency stored in a cold wallet.

5. The entity misrepresents ownership of a private key and therefore of the related cryptocurrency.

Related Assertions: *Rights (ownership) of the cryptocurrency, occurrence (i.e., the event or transaction related to establishing ownership did not occur) and existence of the resulting balance.*

Addressing ownership risk is difficult since ownership of a cryptocurrency is not readily apparent from a blockchain because of the anonymity of the transacting parties. The possession of a private key is a clear indication, at a specific point in time, of the ownership of the cryptocurrency that can be accessed by use of that key. However, ownership of a private key

is not always attributable to one entity. There may be circumstances, for example, when a private key (and ownership of the related cryptocurrency) is legitimately shared between parties. It may also be difficult to determine whether the private key (and therefore the related cryptocurrency) is owned by the entity or owned personally by one or more individuals.

In addition, an auditor may also encounter circumstances indicating an audited entity is fraudulently representing that it alone controls a private key and owns the related cryptocurrency. The auditor is required to maintain professional skepticism throughout the audit, recognizing the possibility that a material misstatement due to fraud could exist, notwithstanding the auditor's past experience of the honesty and integrity of the entity's management and those charged with governance.

Internal Control Considerations
The entity's information system and related controls over creation of its wallets may provide documentation about the creation of private keys and their use in conducting the entity's cryptocurrency transactions. The entity's control environment, including policy statements and codes of conduct, may also be relevant.

6. The entity sends cryptocurrency to an incorrect address and the cryptocurrency cannot be recovered.

Related Assertion: *Rights (ownership) of cryptocurrency assets*

Each blockchain has its own process to verify that cryptocurrency transactions are authentic and not duplicated (i.e., their consensus algorithm). However, a feature common to all blockchains is that once a transaction is confirmed on the blockchain, it is irreversible. This feature may result in an entity losing cryptocurrency if it is sent to an incorrect address.

Personnel of the audited entity may enter an incorrect address when sending cryptocurrency. The receiving party might voluntarily send the cryptocurrency back to the audited entity in a new transaction but might also decide not to do so. In that latter case, the cryptocurrency would be lost.

A misstatement would occur if the loss of the cryptocurrency is not appropriately recorded. This may occur, for example, when those responsible for managing the cryptocurrency have a strong incentive to attempt to conceal the loss or not report it on a timely basis.

Internal Control Considerations

- Controls to prevent use of incorrect addresses:
  The entity's policies and procedures could require both a careful review of each address before sending and the use of a checksum to help guard against typographical errors when entering an address. Also, some blockchains have encoded a checksum in each address. In addition, the entity may consider first sending a very small amount of cryptocurrency to the intended recipient. The recipient's address can therefore be confirmed before sending the larger amount. Use of a QR code (as opposed to typing the address or copying and pasting the address) may also help prevent errors.
- Controls to help reduce the risk that the loss of cryptocurrency is not communicated and recorded:
  Examples of controls are the same as those noted under Example 3 above.

7. The entity enters into and records a cryptocurrency transaction with a related party that cannot be identified because of the anonymity of parties to blockchain transactions.

Related Assertions: *Accuracy (including valuation and allocation) for assets and completeness for disclosures*

The identities of buyers and sellers of cryptocurrency are sometimes referred to as being pseudonymous rather than anonymous. Information such as their names cannot be determined from looking at addresses in blockchain. However, there are links between blockchain addresses and the identities of participants' transactions in, for example, the records of exchanges and brokers used by those parties. It is therefore possible that a regulator or other party might be able to obtain identities. However, in most cases, the names of participants in transactions will not be evident. Therefore, it may not be clear, whether the audited entity is entering into cryptocurrency transactions with related parties that management has not identified. As a result, related parties, transactions with related parties, and resulting balances may not be recorded and disclosed in accordance with the applicable financial reporting framework.

Internal Control Considerations

It is an overall consideration whether the entity's control environment and control activities regarding identifying related parties and authorizing related-party transactions apply to cryptocurrency transactions. These may include, for example:

- policies and procedures for obtaining an appropriate knowledge of the parties with whom the entity is entering into cryptocurrency transactions
- assigning responsibilities within the entity for identifying, recording, summarizing, and disclosing related-party transactions, including cryptocurrency transactions.

8. There are significant delays in processing cryptocurrency transactions at the end of a period.

Related Assertions: *Cut-off*

Cryptocurrency blockchains may vary significantly in the speed with which they process and confirm transactions. Often transactions are processed in minutes. However, in some cases, a transaction may be delayed for days. Such delays may occur, for example, when:

- blockchain miners give a low priority to the entity's transactions if the fee the sender agrees to pay to miners is significantly lower than that for other transactions, and the volume of these higher-fee transactions is large
- there has been a suspension of transactions by the exchange hosting the entity's cryptocurrency wallet.

Internal Control Considerations
The entity may implement procedures to monitor cryptocurrency transactions in the days before and after financial reporting dates to determine that transactions are recorded in the appropriate period.

9. Events or conditions make it difficult to determine the value at which a cryptocurrency should be recorded for financial reporting purposes.

Related Assertions: *Accuracy (including valuation and allocation)*

Financial reporting frameworks such as IFRS Standards do not currently contain explicit references to cryptocurrencies. CPA Canada's paper "*An Introduction to the Accounting for Cryptocurrencies*" notes that concerns have been raised that the application of IAS® 38 *Intangible Assets* and the measurement of cryptocurrencies at cost are not reflective of economic substance and do not provide relevant information to users of financial statements. In some cases, the fair value of cryptocurrencies may be accounted for or disclosed in financial statements.

Particular matters to consider regarding valuation of cryptocurrency include the following:

- Many cryptocurrencies are volatile, and markets may remain open 24/7. The time at which a reporting entity values the cryptocurrency may therefore be important. For example, is the valuation at 11:59 p.m. (time zone) on the last day of the reporting period or at the close of business on that day? This may represent a significant accounting policy. Consistency of application of that policy is required.
- As with stocks or commodities, there are "buy" orders and "sell" orders, often with a significant gap between the respective prices. At any given time, it may be difficult, to exchange a significant amount of cryptocurrency for fiat currency at a price the holder considers fair, within a reasonable time frame.
- Some cryptocurrencies are thinly traded.
- There may be significant variations in the price at which a cryptocurrency is concurrently being traded on various exchanges.
- The nature and extent to which cryptocurrency markets are regulated vary widely among jurisdictions. Often there is little regulation resulting, among other things, in lack of clarity as to how prices are reported.

If there has been a significant volume of recent trades of a cryptocurrency on exchanges, the trading prices might provide evidence of fair value. If there have been few or no recent trades, relevant observable inputs might include prices for buy or sell offers on a peer-to-peer exchange. However, there may be significant volumes of transactions for which the prices may not be readily available until a later date. For example, there are exchanges in which off-chain transactions are recorded temporarily in a private ledger until such time as the parties want the transaction to be recorded on a public blockchain. In addition, the entity might decide to use an economic model to estimate the fair value of a cryptocurrency.

Internal Control Considerations

The entity could implement policies and procedures related to valuations of cryptocurrency for financial reporting. These policies might require, for example, that the method of valuation and assumptions be made by competent personnel, and are reviewed and approved by personnel who are also not responsible for authorizing cryptocurrency transactions.

Conclusion

This paper is aimed at providing auditors with an initial awareness, at a high level, of various matters relevant to client acceptance and continuance and assessing risks of material misstatement related to cryptocurrency items in financial statements. As noted, a key matter for auditors to consider is whether the engagement team has the capabilities required to appropriately address the complex IT processes involved. Auditors may also wish to refer to other sources to explore in more depth the matters noted in this paper in order to be appropriately prepared to undertake audits involving material amounts of cryptocurrencies.

Appendix A — Where to Find More Information

This appendix provides links to additional resources that may be useful:

1. CPA Canada. *Technological Disruption of Capital Markets and Reporting? An Introduction to Blockchain.* www.cpacanada.ca/en/business-and-accounting-resources/other-general-business-topics/information-management-and-technology/publications/introduction-to-blockchain-technology

2. CPA Canada. *Blockchain Technology and Its Potential Impact on the Audit & Assurance Profession.* www.cpacanada.ca/en/business-and-accounting-resources/audit-and-assurance/canadian-auditing-standards-cas/publications/impact-of-blockchain-on-audit

3. CPA Canada. *An Introduction to Accounting for Cryptocurrencies.* www.cpacanada.ca/en/business-and-accounting-resources/financial-and-non-financial-reporting/international-financial-reporting-standards-ifrs/publications/accounting-for-cryptocurrencies-under-ifrs

Appendix B — Glossary of Terms

Blockchain

CPA Canada's publication "*Technological Disruption of Capital Markets and Reporting? An Introduction to Blockchain*", page 8 describes "*blockchain*" as a shared or "distributed" digital ledger of transactions over a network of participating computers. Since blockchain technology embeds peer-to-peer communications among the participating computers, the need for management of the network by a central third party such as a financial institution is eliminated. Computers participating in a blockchain use an automated process to validate the format of the transaction record to be included in the next "block". Once this "consensus" is reached, the information is recorded in a block.

Blockchain (block) Explorer

A blockchain (block) explorer is used to obtain information from a blockchain in a form easily readable by humans (rather than machines). The information obtained and the format used vary by explorer. Typically, an entity would use a blockchain explorer to, for example, check address balances, track histories of coin transfers, determine whether a transaction has been accepted and confirmed, and obtain statistics on the performance of the blockchain (e.g., time taken to confirm transactions).

Blockchain Miner and Mining

A blockchain miner is an entity that engages in blockchain mining. Mining is the act of adding new transactions to the blockchain by solving algorithmic problems with computing resources. The transactions include purchases and

sales of cryptocurrency and the creation of new cryptocurrency. Miners may be awarded cryptocurrency fees for the computational effort they expend in order to support the network.

Cryptocurrency

The Collins English Dictionary defines a cryptocurrency as "a decentralized digital medium of exchange which is created, regulated and exchanged using cryptography and (usually) open-source software". Descriptions of cryptocurrency sometimes emphasize its differences from fiat currency. For example, pwc. *IFRS news: Cracking the cryptocurrency code; or what is a 'bitcoin' anyway?* March 2017 states that "cryptocurrency represents a method of exchange that does not physically exist but rather exists digitally. Cryptocurrencies are not linked to any physical currency, nor are they backed by any government, central bank, legal entity, underlying asset or commodity."

Cryptocurrency Broker

A type of cryptocurrency exchange where cryptocurrencies can be purchased at a price set by the broker operating the exchange.

Cryptocurrency Exchange

An online platform that provides a digital marketplace for buying and selling cryptocurrencies and in some cases, for exchanging cryptocurrencies for fiat currencies.

Cryptocurrency Wallet

A cryptocurrency wallet is a software program used to:

- store the entity's private and public encryption keys used for cryptocurrency transactions
- interact with one or more blockchains to send and receive cryptocurrency
- show the entity's balance in each cryptocurrency that results from the various transactions.

Digital Signature

The entity sending the cryptocurrency to the purchasing entity signs the transaction using a digital signature. The digital signature establishes that the sender has the private key to which its public key is linked, but without revealing that private key. The sender's private key establishes its ownership of the cryptocurrency being sent (subject to verification by blockchain miners).

CPA CHARTERED PROFESSIONAL ACCOUNTANTS CANADA

277 WELLINGTON STREET WEST
TORONTO, ON CANADA M5V 3H2
T. 416 977.3222 F. 416 977.8585
WWW.CPACANADA.CA