CURRENT ISSUES IN AUDITING
Vol. 14, No. 1
Spring 2020
pp. A46–A58

American Accounting Association
DOI: 10.2308/ciia-52675

Challenges when Auditing Cryptocurrencies

Nishani Edirisinghe Vincent
Anne M. Wilkins
The University of Tennessee at Chattanooga

SUMMARY: The novelty, ambiguity, and the lack of official guidance surrounding cryptocurrency transactions impose additional audit risks that should be considered during client acceptance and retention and planning audit procedures. We develop a four-quadrant model to assist auditors in client acceptance and continuance decisions and identify cryptocurrency risks that should be considered during audit planning and audit evidence gathering.

Keywords: cryptocurrency; audit; client acceptance and retention; cryptocurrency risks.

I. INTRODUCTION

The lack of relevant official guidance from standard setters dealing with emerging issues related to cryptocurrencies is a major challenge for auditors. Indeed, the Public Company Accounting Oversight Board (PCAOB) lists digital assets as a key area of focus in its Inspection Outlook for 2019 (PCAOB 2018). Given the rapid public acceptance of cryptocurrencies, the PCAOB plans to increase its understanding of public accounting firms' client acceptance and continuance policies, resource deployment, and planned audit procedures with respect to cryptocurrency.

We identify cryptocurrency issues and risks that auditors need to consider during client acceptance and retention (Figure 1) as well as a cryptocurrency framework for audit planning and gathering audit evidence to support management assertions regarding their financial statements. Subsequent discussion of issues related to cryptocurrency is limited to cryptocurrency assets used as a medium of exchange in a public blockchain. The framework (Table 1) summarizes commonly used financial assertions, current audit procedures, and additional risks/challenges inherent in cryptocurrencies that should be considered when planning and performing an audit. These considerations could potentially help standard-setters and regulators to provide authoritative guidance in the near future.[1]

The authors thank Lisa Milici Gaynor (editor) and two anonymous reviewers, as well as the support of a research grant from The University of Tennessee at Chattanooga.

Editor's note: Accepted by Lisa Milici Gaynor.

Submitted: August 2019
Accepted: November 2019
Published Online: November 2019

[1] As this is a rapidly evolving industry, we present a starting point in our framework, therefore, readers should consider emerging technology advances when using this framework for cryptocurrency auditing in the future.

TABLE 1

Cryptocurrency Risk Framework

Financial Assertions	Description	Typical Audit Procedures used for Testing at Assertion Level	Additional Considerations for Auditing Cryptocurrency
Existence testing	Is the asset there? The purpose of this procedure is to verify whether an asset exists.	• Confirmation by a third party. • Inspection of the asset. • Inspection of documents supporting ownership of the asset. • Inquiry of management. • Subsequent conversion of an asset to currency.	• How to get a list of different wallet accounts? • How to verify the balance on each wallet? • How to verify that the wallet has not been breached? • What is the risk that an unauthorized party accesses the account and depletes the balance? • How do you verify the existence of digital currency accounts with the multitude of exchanges in various jurisdictions? • What source/contractual documents are there to indicate the opening of a wallet? • What controls have been implemented to ensure the security of the private key used to access the cryptocurrency asset?
Rights and Obligations testing	Do we own the asset? This is an audit procedure that requires the auditor to verify the ownership of the asset.	• Confirmation by a third party. • Inspection of legal documents. • Inquiry of management. • Inspection of BOD minutes.	• How do we verify the ownership of the wallets without supporting documentation? • What party controls the cryptocurrency and the accounts held at digital asset providers (exchanges)? • How to assess controls for the exchange? • What controls have been implemented at the audit client to support rights and obligations for cryptocurrency? • What party controls the wallets and what access controls are established? • Is there proof of ownership for the cryptocurrency and private key?

(continued on next page)

TABLE 1 (continued)

Financial Assertions	Description	Typical Audit Procedures used for Testing at Assertion Level	Additional Considerations for Auditing Cryptocurrency
Completeness testing	Are there any missing transactions? In completeness testing, the auditor attempts to determine whether all transactions have been recorded in the accounting system.	• Trace transactions from supporting documents to a journal or ledger. • Accounting for the numerical sequence of source documents. • Inquiry of management. • Inspection of legal documents. • Testing client internal controls for completeness.	• Can there be transactions that are not yet added to the blockchain? • Are there any hidden wallets? • Are inactive wallet accounts deactivated or deleted? • What minimum access controls are at the exchange or third-party level? • What is the risk that parties in the cryptocurrency transaction are related parties given the anonymity? • What internal controls have been implemented at the client level to ensure completeness? • What internal controls have been implemented to ensure compliance with cryptocurrency laws and regulations given the lack of consistency of the laws throughout jurisdictions?

(continued on next page)

TABLE 1 (continued)

Financial Assertions	Description	Typical Audit Procedures used for Testing at Assertion Level	Additional Considerations for Auditing Cryptocurrency
Accuracy and valuation testing	Are the transactions accurate? Here the auditor needs to verify that the recorded transactions are free from errors, recorded at the correct dollar amount, posted to the correct vendor/customer account, and/or posted to the correct general ledger and other subsidiary ledgers and journals.	• Select a sample of transactions and reperform the accuracy. • Trace the source documents to verify the validity of the amount and vendor/customer details. • Trace the transaction to the account. • Test the controls—what is the process? Did the employees follow company policies such as taking and giving discounts and/or obtaining approvals?	• Can we do a population test rather than a sample? • Can we verify that the currency was received from a legitimate ordinary business transaction? • Can we determine the payment was sent to the correct vendor? • What is the risk exposure if the cryptocurrency came from an exchange with low liquidity and/or low trading volume that makes valuation less reliable? • Can we obtain an understanding of how prices of cryptocurrency are reported on various exchanges? • What unit of measure is being used to value cryptocurrency? • Once entered and a transaction in the wallet is permanent and cannot be changed, can we verify using source documents that the correct amount and/or correct address was entered? • What internal controls are implemented at the client to ensure the accuracy of data entered in the blockchain? • Can we assess controls at the exchange or third-party level?

(continued on next page)

TABLE 1 (continued)

Financial Assertions	Description	Typical Audit Procedures used for Testing at Assertion Level	Additional Considerations for Auditing Cryptocurrency
Authorization testing	Are the transactions authorized? This is a test to make sure that the recorded transactions are valid and not fraudulent.	• The auditor needs to understand the business process and pay attention to who does what in the firm. • The auditor would obtain a sample of transactions and look at who has signed the source documents such as invoices, disbursement vouchers, cash receipts, and checks.	• Can we verify who authorized a transaction, creation of a wallet, or opening an account with an exchange? • Can we verify that the cryptocurrency was received from a legitimate ordinary business transaction? • Can we assess controls at the exchange or third-party level?
Cutoff testing	Are the transactions recorded in the correct period? Here the auditor will focus on transactions that occur during the end of the month and the beginning of the subsequent month to determine the period to which a transaction belongs.	• The auditor will examine the transactions at the end of the month, beginning of the month, and supporting documents to determine whether the transactions are in the correct period.	• Can we assess whether there were any delays in processing and confirming the cryptocurrency transactions? • Can we obtain a list of transactions from a wallet, exchange, or crypto-explorer given a certain cutoff date? • What is the impact and risk of a lack of controls at the exchange or third-party level with regard to processing integrity?

(continued on next page)

TABLE 1 (continued)

Financial Assertions	Description	Typical Audit Procedures used for Testing at Assertion Level	Additional Considerations for Auditing Cryptocurrency
Occurrence testing	Did the transaction actually happen? If a client claims that a payment was made to a vendor, the auditor needs to verify that the check was written, payment was recorded in the accounts, and the check was mailed. Is revenue earned before recognition? Are transactions with related parties adequately identified and disclosed?	• Select samples of transactions from source documents and trace them to the recording of the transaction. • Scan through journal entries and review any unusual items. • Inquiry of management. • Inspection of documents supporting the transactions.	• Can we obtain confirmation of transactions? • What source documents are available for examination? • Should we recommend creating new source documents and establishing new procedures related to cryptocurrency? • What internal controls have been implemented at the client to ensure occurrence? • What is the risk and impact of a lack of controls at the exchange or third-party level?
Adequate Disclosure testing	Are all disclosures required included?	• Completion of the disclosure checklist. • Inquiry of management. • Obtaining a legal letter from attorneys engaged by the client. • Obtaining a management representation letter. • Inspection of documents.	• Are the relevant accounting policies for cryptocurrency disclosed? • Are all loss contingencies relating to cryptocurrency disclosed? • If required, is fair value information disclosed? • Is the method of valuing the cryptocurrency adequately disclosed? • Are the rights and obligations of cryptocurrency adequately disclosed? • Should the business purpose for holding cryptocurrency be disclosed? • Are the additional risks involved in holding cryptocurrency adequately disclosed?

Although in March, 2019, the International Financial Reporting Interpretations Committee (IFRIC) issued *Holdings of Cryptocurrencies—Agenda Paper 4* (IFRIC 2019) stating the accounting treatment for holding cryptocurrency follows the International Accounting Standard (IASB 38) on Intangible Assets (IASB 2004), neither the Financial Accounting Standards Board (FASB), the Auditing Standards Board (ASB), nor the PCAOB have issued formal guidance for accounting or auditing cryptocurrency. The Internal Revenue Service (IRS) has issued guidance on the United States tax treatment of cryptocurrency transactions (IRS Notice 2014-21, 2014). Thus, the profession is relying on concept statements, principle-based accounting, and non-authoritative information such as white papers and other accounting and auditing publications.[2] By developing a client acceptance and retention model and a framework of additional risks inherent in audits of clients with cryptocurrency transactions, we provide an additional resource for those auditors experiencing emerging cryptocurrency audit challenges.

II. CLIENT ACCEPTANCE AND RETENTION

PCAOB auditing quality control standards require audit firms to have quality control procedures on audit client acceptance and continuance; specifically, audit firm policies should provide reasonable assurance that the firm has the competence to perform the engagement and consider relevant risks appropriately (PCAOB 2003). Therefore, when considering whether to accept and/or retain a client with cryptocurrency, the auditing firm should consider whether the firm has the competence and resources required to complete the engagement. The absence of consistent legal and regulatory guidance for cryptocurrency is a major challenge when determining whether the audit firm has the required competence. For example, does the firm audit staff have the required knowledge to identify and avoid independence threats that may occur when performing auditing procedures?[3] Further, the lack of prior experience can hinder the audit firm from determining adequate resource requirements for an engagement. Particularly, as cryptocurrency transactions create digital data, lack of prior experience with digital data and technical expertise can significantly influence the estimation of resource requirements for an audit engagement.

Quality control standards also require the auditor to consider risks associated with the engagement. Auditors need to consider whether cryptocurrency transactions have a business purpose related to the client's overall business strategy or whether the use of cryptocurrency is driven by other motives that benefit from maintaining anonymity.[4] Further, auditors should consider their clients' competence in cryptocurrency accounting and reporting, cryptocurrency risk management, as well as the audit client's ability to establish and maintain appropriate internal controls to mitigate the identified risks associated with cryptocurrencies. Lack of cryptocurrency competence in the client firm will impose an additional burden on the audit firm with regard to assessing risks and gathering audit evidence.

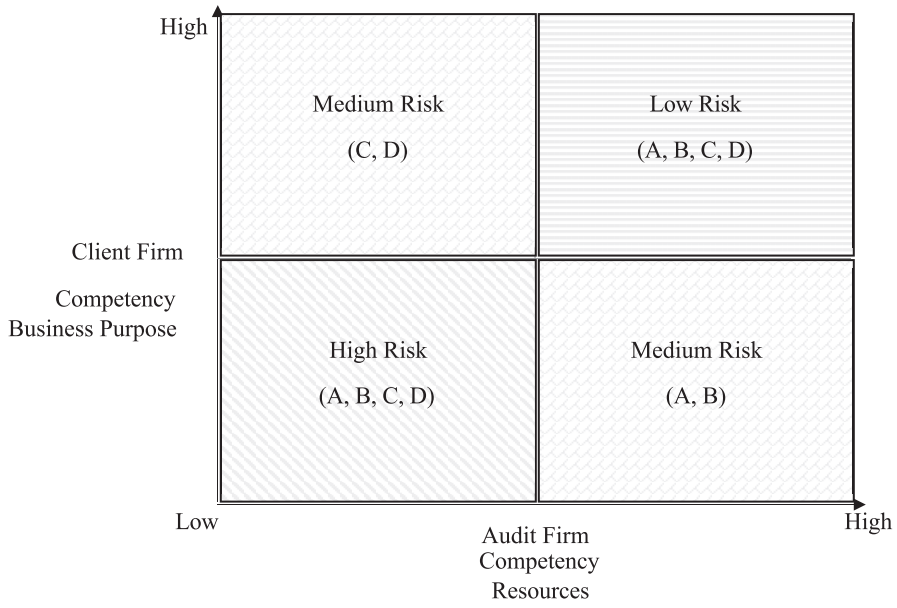
Figure 1 will help auditors identify the riskiness of a client acceptance/retention decision. By identifying where the audit firm falls on competency and resources and where the client firm falls on competency and business purpose of cryptocurrency, the audit firm can categorize whether an

[2] The most widely used white papers were issued by Chartered Professional Accountants Canada in May 2018, see CPA Canada (2018a, 2018b).

[3] The Accounting Blockchain Coalition (2019) discussed a possible threat to independence if the auditor obtains possession of the client's private key accessing the client's cryptocurrency assets during existence testing.

[4] Malik (2018) states that although cryptocurrency can provide financial empowerment reducing corruption risk, criminals can also adopt these technologies for their benefit.

FIGURE 1
Assess the Riskiness of a Client Acceptance and Retention Decision



Audit Firm
A. Audit firm's requisite competence in cryptocurrency to recognize risks and design appropriate auditing procedures is (high/low).
B. Audit firm's access to resources such as the appropriate mix of personnel and technology is (high/low).

Client Firm
C. The client's requisite competence in cryptocurrency to recognize and mitigate associated risks is (high/low).
D. The alignment of the client's cryptocurrency transactions with business purpose and the strategy is (high/low).

acceptance/retention decision is high, medium, or low risk. If an engagement is high risk, the audit firm should carefully consider the additional resources and expertise required to provide an audit opinion with reasonable assurance.

III. CRYPTOCURRENCY RISK FRAMEWORK

Audit procedures are used to gather audit evidence to support forming an opinion on whether the financial statements are fairly presented in accordance with a specific accounting framework. When designing audit procedures at the planning stage, auditors consider audit objectives, scope, approach, and risks. At the account level, risks considered would include managements' financial reporting assertions of existence, rights and obligations, completeness, valuation and accuracy, authorization, cut-off, occurrence, and adequate disclosure. We have developed a cryptocurrency risk framework (see Table 1) that includes a summary of common financial statement assertions, typical audit procedures, and additional considerations and risks relating to the assertion for account balances containing cryptocurrency transactions.

The auditor should consider the volume and/or dollar value of the cryptocurrency transactions and the valuation within the account(s). Risks would be higher for accounts with cryptocurrency assets or transactions exceeding the portion of overall materiality allocated to a specific account balance. The emerging nature of the currency, the lack of authoritative guidance for accounting,

reporting, disclosure and auditing, the lack of consistent laws and regulations, the relative anonymity of the parties to the cryptocurrency transactions, and the materiality of cryptocurrency transaction volume and/or amounts, increase the risk of material misstatement in an account balance.

Existence

One of the biggest challenges in determining whether cryptocurrency exists is verifying the number of crypto-wallets and digital asset accounts for a client at various exchanges. Since cryptocurrency is a digital asset, methods used to inspect inventory and property additions may not suffice. Confirmations are also traditionally used to verify existence. For example, a typical verification of cash will use confirmation letters from banks. However, since cryptocurrencies are maintained in a distributed ledger without a central authority, auditors may not be able to confirm the currency balance using a third party.[5] If the cryptocurrency is traded through an exchange (third party), a lack of proper assurance reporting mechanisms of the exchange's internal controls using service organization control (SOC) reports makes it difficult to assess, rely on, and verify cryptocurrencies with reasonable assurance.

Further, cryptocurrency keys lost or stolen can render the asset worthless. Therefore, the existence of cryptocurrencies imposes an additional burden on the engagement to verify controls on access and storage of private/public keys. Given the successful attacks on wallets resulting in the complete loss of the cryptocurrency (Young 2019), auditors will want to examine internal controls around the safety of wallets.

Another way to confirm existence is to examine source or contractual documents supporting the asset. Unlike in the regulated banking industry, documentation between the holder of the asset (exchange) and the client organization may be minimal or nonexistent. Auditors also use subsequent receipt of fiat currency, in the case of payment settlement or subsequent sale of an asset, to obtain audit evidence for existence. Since such documentation may be nonexistent, the auditor will want to test whether the cryptocurrency wallet actually contains the specified amount.

Rights and Obligations

Traditionally, auditors assess the rights and obligations assertion through the inspection of other documents including third-party agreements, confirmations, and Board of Directors (BOD) minutes. While reviewing client cryptocurrency documents, auditors will want to consider: who is the legal owner of the cryptocurrency held by the client, is the cryptocurrency of the client held by an exchange segregated from the exchange's other holdings, what happens to the asset if the exchange goes out of business or loses the cryptocurrency assets, and what are the internal controls at the exchange to protect the security of the asset. Lack of third-party assurance reporting will increase the difficulty in assessing the risks involved.

The auditor will also need to assess the internal controls for cryptocurrency at the audit client as well as the exchange. Internal controls limiting access to private/public keys at the organization while safeguarding loss of the key(s) will need to be evaluated. Cryptocurrency holdings are relatively anonymous as the keys are digitally created and are not easily linked to the owner's identity. In addition, new addresses are easily created and do not require personal information,

[5] Information about the existence of cryptocurrency transactions was obtained by the Internal Revenue Service of the United States to investigate whether taxes had been paid on the profits (Aquilio 2018).

unlike new investment accounts that require owner identification. The auditor will have to ensure that the owner of the cryptocurrency is the audit client. Given the digital nature, audit firms may need to develop proprietary software to identify and verify cryptocurrency accounts belonging to their clients or hire specialists with such expertise.[6]

Completeness

The completeness assertion requires verifying whether all cryptocurrency transactions are recorded on the blockchain. Commonly, evidence of completeness is obtained by examining pre-numbered source documents, tracing source documents to ledgers, and understanding and testing operating effectiveness of client internal controls around completeness. Even though transactions entered into a blockchain are immutable over time, theoretically, there can be orphan transactions. Therefore, access controls at the client and/or exchange will need to be assessed.

Although there are blockchain explorers that can be used to track and/or aggregate transactions, auditors will need to increase their audit effort to track additional documentation to provide reasonable assurance of completeness. Reconciliations between the blockchain and the accounting records need to be maintained to determine whether there are transactions that have not yet been added to the blockchain. Indeed, sometimes there is a lag between the transaction date and the date the transaction appears on the blockchain due to technology limitations, controls, and volatility at the exchange. Further, auditors should verify that inactive wallet accounts are deactivated or deleted. Moreover, undisclosed wallets and transactions related to those wallets are difficult to identify. Since the identity of parties to the exchange is digitally masked, verifying that one or more of the parties to the exchange are related is difficult.

Last, auditors should consider whether the client firm will face potential losses from litigation and fines arising from inadvertently violating inconsistent laws and regulations between governments (e.g., state, federal, country) for cryptocurrency.

Valuation and Accuracy

The financial statement assertion of valuation and accuracy is used to gather audit evidence that the transactions in the financial statements reflect the correct amount, the actual parties to the exchange, and the correct classification and allocation. Valuation of cryptocurrency is challenging due to a lack of comparable trades, differences in pricing between buy and sell orders, disparate methods in reporting exchange currency pricing, and the difference in pricing of a particular cryptocurrency depending on the exchange used for the trade. In determining the fair value of cryptocurrency assets or possible impairment, the unit of measure is important for valuation (per unit of currency or as a portfolio). In most instances, cryptocurrency will be valued per unit as coins are separable from each other (ASC 350, *Intangible Assets—Goodwill and Other*) and impairment testing will be performed per unit of account. Accounting records will need to be maintained to track the cryptocurrency cost basis for impairment testing (FASB 2014). Additionally, accounting policies used to value cryptocurrency will need to be identified and disclosed such as the market used in valuation, whether there is evidence of manipulation in the

[6] On June 19, 2019, PwC issued a press release announcing that the firm has developed software enabling private-public key pairing that can be used to establish ownership of the cryptocurrency as well as gain information about a client's transactions occurring on blockchains (PwC 2019).

market, and whether the market provides enough volume to assess the reliability and relevance of the pricing information. Further, the volatility of the asset market and the consistency of measurement should also be considered.

Typically, a review of reconciliation controls, re-computations, inspection of documents, and understanding and testing of internal controls are used to provide evidence of accuracy. Since cryptocurrency transactions are difficult to identify by looking at the addresses of the originator or receiver, it may increase the risk of failure to identify a related-party transaction or the ability to ascertain that the correct transferee or transferor was recorded.

Errors such as sending cryptocurrency to the wrong address or typographical errors in inputting transactions cannot be rescinded as blockchain transactions are permanent; hence, the client can lose their cryptocurrency through data input errors, increasing the risk of material misstatement. The auditor will need to examine client-level data entry integrity controls, access, and storage controls to ensure the accuracy of the cryptocurrency transactions. Further, auditors should consider the existence of such controls at the third-party-level (wallet providers/exchanges) to conclude there is reasonable accuracy.

Authorization

Internal control review and testing, re-performance, and inspection of source documents supporting recorded transactions are used to provide audit evidence that the financial statements are comprised of authorized transactions. Auditors should look for evidence that the client has established procedures for authorizing wallet opening, new private key creation, and the use of exchanges. Further, the clients should have separation of duties between authorization, custody, and recording of cryptocurrency transactions by both the client and the third party.

Cutoff

Cutoff testing provides audit evidence that the transactions are recorded in the proper period. Different exchange technology, market volatility, nexus regulation, blockchain consensus mechanisms, and internal controls at the exchange may cause delays in processing transactions. Cryptocurrency transactions also have to be confirmed by cryptocurrency miners before the transfer of assets and some exchanges require multiple confirmations before the transfer of balances. Further, when volatility is experienced in the cryptocurrency market or increased volume is experienced in the exchange, processing delays may occur. Therefore, auditors will have to gather evidence of client and exchange internal controls over processing accuracy to provide assurance of the cutoff assertion.

Occurrence

Occurrence for revenue accounts involves obtaining audit evidence that the transactions reflected in the financial statements are valid and occur only when the revenue is earned. Risks include fictitious transactions and recognition of transactions before all conditions are met. Audit procedures such as confirmation, understanding of internal controls, inspection of documents, and reconciliations are used to gather audit evidence to test occurrence. In auditing cryptocurrency transactions, auditors will need to examine evidence verifying ownership of the private key and evidence of the appropriate party to record the transactions. A sample of transactions in the wallet should be vouched back to supporting documents. Auditors should

obtain an understanding of the internal controls surrounding occurrence at the exchange and client level. Separation of duties between custody, recording, and authorizing of cryptocurrency transactions should be part of the audit clients' internal control processes. In addition, physical controls over private keys and information technologies used in the transactions should be part of the control activities related to cryptocurrency. Controls at the exchange or third-party level will also need to be considered, which will be a challenge due to the lack of third-party assurance reporting. IT application controls that prevent or minimize the risk of misidentification of a party to a transaction or the amount will reduce the risk of incorrect posting to the blockchain and resulting probable loss of assets.

Disclosure

The auditors' opinion on the fairness of the client's financial statements includes an evaluation of their presentation including disclosures. Typically, a disclosure checklist is completed to verify all disclosures required by a financial reporting framework are included in the notes to the financial statements. Since there is no guidance from standard setters around appropriate disclosures for financial statements containing cryptocurrency transactions, the auditor will need to assess the adequacy of the client's disclosures using principle-based accounting and white papers. These alternative guidelines are recommending greater transparency when assessing cryptocurrency disclosure. At a minimum, disclosures already required, such as the nature of the asset, accounting policies, fair value, contingencies, risks associated with cryptocurrency, and valuation should be included in the notes to the financial statements. Additionally, the business purpose of the cryptocurrency transactions, measurement basis, and volatility of the currency may also need to be considered for disclosure.

IV. CONCLUSION AND LIMITATIONS

Financial statement audits are becoming more likely to contain transactions involving cryptocurrency. The lack of regulation and guidance when designing audit plans and procedures to form an opinion as to whether the financial account balance containing cryptocurrency increases the risk that a material misstatement or disclosure could be overlooked. In examining internal controls at both the entity and exchange level, the auditor should address what could go wrong (WCGW) at each step of the transaction and consider information technology controls, general and application, relating to cryptocurrency as a digital asset.

If an audit client engages in cryptocurrency transactions, the auditors should increase their cryptocurrency competence level through training and education, hiring experts to be on audit teams, and creating a crypto-aware culture within the audit firm. Further, audit firms may consider investing in developing proprietary software that will help address some of the concerns discussed in this paper. During the audit planning stage, auditors should assess and give careful consideration for compensating controls. If the client's existing internal controls environment is strong, the existing controls may act as compensating controls for cryptocurrency transactions. Given the rapid advancements and creation of new cryptocurrencies, audit procedures need to be consistently reviewed and updated to consider additional risks that have not been mitigated. Readers should be mindful that this is a preliminary analysis; hence, we do not consider all risks that may occur. Therefore, auditors should exercise caution, keep abreast of advancements in this field, and update audit plans and procedures accordingly.

REFERENCES

Accounting Blockchain Coalition. 2019. *Panel discussion on auditing, tokens, miners, exchanges, and wallets*. Available at: https://vimeo.com/showcase/6078562/video/344109070

Aquilio, M. 2018. *Court grants IRS summons of coinbase records*. Available at: https://www.journalofaccountancy.com/issues/2018/mar/irs-summons-of-coinbase-records.html

CPA Canada. 2018a. *Introduction to accounting for cryptocurrencies under IFRS*. Available at: https://www.cpacanada.ca/en/business-and-accounting-resources/financial-and-non-financial-reporting/international-financial-reporting-standards-ifrs/publications/accounting-for-cryptocurrencies-under-ifrs

CPA Canada. 2018b. *Audit considerations related to cryptocurrency assets and transactions*. Available at: https://www.cpacanada.ca/en/business-and-accounting-resources/audit-and-assurance/canadian-auditing-standards-cas/publications/cryptocurrency-audit-considerations

Financial Accounting Standards Board (FASB). 2014. *Intangibles—Goodwill and Other*. *Accounting Standards Codification (ASC) 850*. Washington, DC: FASB.

International Accounting Standards Board (IASB). 2004. *Intangible Assets*. London, U.K.: IASB.

International Financial Reporting Interpretations Committee (IFRIC). 2019. *Holdings of Cryptocurrencies. Agenda Paper 4*. London, U.K.: IFRIC.

Malik, N. 2018. *How criminals and terrorists use cryptocurrency: And how to stop it*. Available at: https://www.forbes.com/sites/nikitamalik/2018/08/31/how-criminals-and-terrorists-use-cryptocurrency-and-how-to-stop-it/#3c01cdee3990

PCAOB. 2018. *Inspection outlook for 2019*. Available at: https://pcaobus.org/Inspections/Documents/Inspections-Outlook-for-2019.pdf

PCAOB. 2003. *System of Quality Control for a CPA's Firm's Accounting and Auditing Practice*. Washington, DC: PCAOB.

PwC. 2019. *PwC launches solution supporting audit of cryptocurrency*. Available at: https://www.pwc.com/gx/en/news-room/press-releases/2019/cryptocurrenc-audit.html

Young, J. 2019. *Round-up of crypto exchange hacks so far in 2019: How can they be stopped?* Available at: https://cointelegraph.com/news/round-up-of-crypto-exchanges-hack-so-far-in-2019-how-can-it-be-stopped