Systemizing the Challenges of Auditing Blockchain-Based Assets

Erica Pimentel*
PhD Candidate
John Molson School of Business – Concordia University
erica.pimentel@mail.concordia.ca

Emilio Boulianne
Professor
John Molson School of Business – Concordia University
emilio.boulianne@concordia.ca

Shayan Eskandari
PhD Student
Gina Cody School of Engineering - Concordia University
s_eskand@encs.concordia.ca

Jeremy Clark
Associate Professor
Gina Cody School of Engineering - Concordia University
jeremy.clark@concordia.ca

*Corresponding author

Acknowledgments: Pimentel thanks the Social Science and Humanities Research Council of Canada (SSHRC) and the Quebec CPA Foundation for financial support. Boulianne thanks the KPMG Entrepreneurial Research Studies, and the Manulife Professorship in Financial Planning, at the John Molson School of Business. Clark thanks the National Science and Engineering Research Council (NSERC). All authors thank the Autorité des Marchés Financiers (AMF) for funding this research. Finally, we thank the interview participants for their candour and insights. The information, opinions and advice presented in this paper are the sole responsibility of the authors.

SYSTEMIZING THE CHALLENGES OF AUDITING BLOCKCHAIN-BASED ASSETS

ABSTRACT

Presently, auditing firms are hesitant to accept mandates from companies that hold a significant amount of cryptoassets, primarily because the blockchain sector introduces novel, technically sophisticated and risky propositions that auditors are unequipped to handle. Abrupt recusals by auditors operating in this sector have led to several enterprises being placed on cease trade by securities regulators for failure to produce audited financial statements on time, thus impeding these companies from raising capital and bringing new investment to fund innovation in this space. Through an iterative process of interviews with senior accounting professionals, structured brainstorming among a multidisciplinary team of accountants and blockchain experts, and a focus group with experienced auditors, we critically analyze the purported roadblocks to auditing blockchain firms and map them to traditional auditing practices. We urge auditors to reconsider their resistance to the blockchain sector by demonstrating that providing an audit opinion is challenging but not insurmountable.

Keywords: blockchain, financial audit, cryptoassets, accounting firms, auditors, cryptocurrencies

INTRODUCTION

The blockchain industry is comprised of firms (raising more than $15B in unregulated funding and $2.5B in venture capital in 2018 (Coindesk 2018)) that issue and manage cryptoassets (worth a combined $260B at the time of writing (CoinMarketCap 2019)). While this market is experiencing rapid growth, it is dominated by startups that lack the financial sophistication and maturity of similarly valued traditional firms, and that rely on outside funding to develop and grow. These small firms will require audited financial statements to obtain traditional forms of credit such as bank loans or to gain access to public markets. For instance, SEC registrants must file audited financial statements that have an unqualified audit opinion (except under limited circumstances) (SEC 2009). If registrants are unable to provide unqualified audited statements, they will be unable to raise capital on public markets. At the time of writing, auditing firms are hesitant to provide audit opinions to the blockchain sector. Furthermore, several crypto companies such as Impak Finance (who undertook the first legal ICO in Canada; Impak Finance 2018), Hut 8, Vogogo Inc. and DMG Blockchain Solutions, were placed on cease trade for failure to produce timely financial statements when their auditors abruptly stepped down and the companies were unable to find replacement auditors (Posadzki and Milstead 2019). Therefore, the inability to obtain audited financial statements is a pressing issue as both new and existing firms are having difficulty finding auditing firms who wish to provide opinions to crypto companies.

Our research has uncovered that major accounting firms are hesitating to provide certification in the blockchain sector due to a perception of insurmountable business risk associated with these clients. Auditors believe that due to a complex and rapidly changing

technological environment, they have yet to develop the in-depth knowledge of their clients' blockchain businesses in order to perform an audit. Due to the lack of guidance, standards and regulations in this space, auditors are reticent to take on new clients in a sector that has been subject to numerous frauds (Abreu, Aparicio, and Costa 2017). Accordingly, the inability to obtain audited financial statements presents a key barrier to investment and growth in the blockchain sector.

To perform our data collection and analysis, we deployed a methodological framework for conducting inductive research that aims to address challenges raised from practice, brainstorm solutions to those problems and validate the recommendations with practitioners. Our research was conducted in two phases. In the first phase, we generated ideas relating to the primary challenges of auditing blockchain-based assets from twelve semi-structured interviews with practitioners and five brainstorming sessions within our multidisciplinary research team of accountants and blockchain experts. This process allowed us to curate a centralized list of the main issues to address in our research project. In the second phase, we conducted eight additional interviews with practitioners and four more brainstorming meetings to develop solutions to the issues raised. Finally, we validated our recommendations with a focus group of five experienced auditors to ensure that our recommendations were practicable.

In order to address the auditors' concerns, this paper aims to systematize the issues associated with auditing blockchain-based assets by making parallels to traditional financial statement audits. Our respondents expressed concern over being able to comprehensively understand the potential issues relating client acceptance and engagement performance. This paper aims to provide a synthesis of the potential

considerations relating to the audit of blockchain-based assets as well as offer recommendations on how to address these issues in order to be able to issue audit opinions in the blockchain sector.

Next, we present relevant literature, our research method, the results, the discussion and the conclusion.

BACKGROUND AND RELATED WORK

The blockchain was initially proposed as a technology to support a new form of electronic cash, namely bitcoin, without the involvement of a third-party trust provider such as banks (Nakamoto 2008).[1] We assume the reader is familiar with the basic concept of a blockchain, and refer to Dai and Vasarhelyi (2017) for an introduction on the topic.

Cryptoassets

We use the term cryptoasset and cryptoliability to refer to listings on a firm's balance sheet that exist and are transacted using blockchain technology and have some tradeable value. This includes cryptocurrencies (e.g., bitcoin and ether) as well as tokens[2] issued by smart contracts running on a blockchain. Among others, the main categories of tokens are: (1) *Access tokens*: a service is developed which requires its own custom tokens for using the service; (2) *Backed tokens*: a token issuer claims to be holding something valuable (material or digital) in reserve, and the token represents a claim on these reserves; (3) *Equity tokens*: a firm issues tokens to represent ownership shares of

[1] According to coinmarketcap.com, in addition to Bitcoin, there are currently more than 2,100 cryptocurrencies.

[2] In the case of Ethereum, these tokens are often called ERC20 tokens, where ERC20 is sometimes misunderstood to mean what the token represents. Instead, however, ERC20 is a technical standard about how tokens are implemented.

the company; and (4) *Collectable tokens*: the token itself is offered as a contemporary collector's item.

Blockchain as a Source of Verification

Several observers have touted the role of the blockchain as a source of "verification" where transactions are validated by the nodes—called miners—in the network (Kokina, Mancha, and Pachamanova 2017). However, the degree and type of verification provided by the blockchain compared to that which is provided by financial statements auditors is often conflated in the literature. Catalini and Gans (2016) propose that the blockchain provides an opportunity for "costless verification" as transactions are authenticated on a blockchain using a consensus mechanism. Others also describe the blockchain as an irrefutable record-keeping system (Crosby, Pattanayak, Verma, and Kalyanaraman 2016). In fact, the blockchain does not verify whether a transaction was correctly accounted for under financial reporting rules or has a legitimate business purpose. While a blockchain verifies whether a transaction occurred and at what amount and on what date, it does not provide an examination of the internal controls which underlie the financial reporting process to prevent or detect fraud and errors, as would a financial statement audit. An audit is much more than a verification of routine transactions, being a holistic assessment of the robustness of a firm's internal controls, financial reporting policies and the reasonability of significant estimates. This activity cannot, in our view, be supplanted by a blockchain.

Using Blockchain as an Accounting Tool

Some have explored how to exploit the blockchain's decentralized ledger technology for accounting purposes. Grigg (2005) describes a system he refers to as "triple entry accounting," whereby a digitally signed receipt is created to represent a form of mutual authorization for a transaction between a buyer and a seller that a transaction has been carried out according to their specifications. This digitally signed receipt, coupled with a double entry accounting system, complete a "triple entry system," which can leverage the power of financial cryptography to provide confidence over each accounting transaction entered into a company's accounting records. Yet, Dai and Vasarhelyi (2017) argue that "this [triple entry accounting] mechanism requires an independent and reliable intermediary to 'verify' each individual transaction. In addition, entries stored by the intermediary are also exposed to the risk of loss or unauthorized changes due to cyber-attacks" (p. 10). A blockchain could be used to take on this intermediary role and act as a centralized, secure repository for accounting records. Our paper aims to expand on this work to explore the procedures auditors could carry out to validate the occurrence, measurement and rights and obligations associated with these recorded transactions.

Coyne and McMickle (2017) take issue with using a blockchain in accounting settings, namely due to challenges surrounding confidentiality and the ability for a consensus mechanism to accurately verify transactions. An important argument is that although two sides of a transaction can verify that a transaction occurred, at what amount and on what date, the counterparty may be unable to verify that the transaction has correctly followed financial reporting rules. Ru□ckeshäuser (2017) argues that

blockchain systems based on a proof-of-work model provide an opportunity for management override of internal controls as the firm will likely hold a majority of a private blockchain's computing power. In this instance, managers could use their majority control of the network to circumvent controls by authenticating fraudulent transactions in a way that is more difficult to detect than traditional control override. Therefore, while the blockchain has important potential to support the accounting function, it is faced with challenging issues, which undermine its full deployment.

Using Blockchain as an Audit Tool

Dai and Vasehelyi (2017) raise the potential for the blockchain to support the audit function by enabling continuous assurance. For instance, the use of a blockchain as a data depository could allow information to be updated (and audited) in real time. Abreu, Aparicio and Costa (2017) and Smith (2018) describe opportunities to replace traditional audit procedures such as bank confirmations with blockchain-enabled solutions. However, the deployment of these tools remains a challenge due to their lack of widespread acceptance. Broby and Paul (2017) provide a broad outline of issues that the auditor faces, such as forks, transaction malleability and third-party custody, among others, coming to the conclusion that audits are not sufficiently robust in their current format to tackle the challenges of blockchain. We, however, disagree and will demonstrate how many of the issues with auditing the blockchain are surmountable, subject to certain caveats.

Obtaining Relevant Technical Knowledge for Blockchain Mandates

A challenge for any auditor taking on a mandate in this space is demonstrating that they have sufficient competence to address the relevant IT risks. One way to achieve this would be for auditors to obtain the necessary level of IT knowledge through training (Curtis, Jenkins, Bedard, and Deis 2009). Another way would be to engage IT specialists to join the audit team. Bauer and Estep (2019) explore the relationship between IT specialists and audit teams to find that the quality of the relationship between these parties can impact the quality of the audit evidence gathered. Hirsch (2020) studies the spatial distance and domain knowledge distinctiveness between auditors and IT specialists to suggest that auditors will rely differently on IT specialists whether they possess similar or different knowledge levels, and whether or not the specialists are in-house. In our research approach, we combine a multi-disciplinary group of blockchain experts and auditors to demonstrate that it is possible for accountants and technology professionals to work together to combine their mutual knowledge.

METHODS

This study employed a qualitative approach (Patton 2002; Taylor, Bogdan, and DeVault 2016). Since the purpose of this study was to systematize the issues relating to the audit of blockchain-based assets, we developed a process that would allow us to at once include the input of practitioners, brainstorm ideas from a multi-disciplinary research team, and validate solutions with experts in the field (see Figure 1).

Phase I: Issue Generation

In order to develop a comprehensive list of issues to address in our paper, we took two approaches. First, we conducted twelve semi-structured interviews with Canadian professional accountants (from Big 4 and non-Big 4 firms) in Canada.[3] The purpose of these meetings was to ask open-ended questions about the practitioners' concerns regarding auditing blockchain-based assets and why they believe mandates were not being accepted in this sector. In order to select interviewees for our study, we took a two-pronged approach. First, we selected practitioners who were recognized as experts at the intersection of audit and blockchain. Based on discussions with financial regulators as we were designing our study, we learned that certain firms and practitioners were particularly active in this space. We engaged in purposive sampling when selecting interviewees to target those auditors who had a particular interest and developing expertise in this area (Saunders and Townsend 2018). Our initial interview targets were selected among individuals who have contributed to conferences, panels and publications on blockchain auditing. In total, we selected nine blockchain experts. Second, we selected three auditors who did not consider themselves to be experts in the blockchain sector. Of those, one had worked on clients in this space but did not consider himself to be an expert in the technology. Given that many auditors are reticent to take on audits in this new field, our belief was that by combining the insights of experts and non-experts, we could

[3] While this paper focuses on the Canadian context, most interviewees are partners and senior managers at Big 4 accounting firms. Accordingly, issues raised with the audit of blockchains and cryptoassets, and initiatives undertaken in these firms, are reflective of the global trends. In other words, interviews conducted and documentation examined suggest important similarities within a North American context. Carter and Spence (2014) document how Big 4 partners may be similar across countries, being alike across different cultures, overcoming national and geographical contexts (Loveridge and Mueller 1999).

have greater insights into the thoughts of those who will be working on the frontlines of blockchain auditing. Table 1 provides the profiles of the interviewees. Confidentiality was provided to ensure that interviewees speak freely to give us the most accurate information of the phenomenon.[4]

Insert Table 1 here

As we conducted these interviews with our respondents, our multidisciplinary research team of accountants and blockchain experts held structured brainstorming meetings where we aimed to devise a list of potential issues that could arise relating to the audit of blockchain-based assets. See Table 2 for the profiles of the members of our research team. The list of issues arose from our own experience, a review of relevant blockchain and accounting literature and ideas stimulated from our participation in conferences, panels and symposia. Over the course of five meetings between July 2018 and August 2018, we consolidated the knowledge obtained from our interviews with our own brainstormed ideas to curate a final list of main themes for our research project. These issues have been summarized in Table 3.

Insert Table 2 here

Insert Table 3 here

[4] This study has been approved by the authors university's ethics office. Interviewees were provided with a consent form including details of the study.

Phase II: Analysis

Once we had put together a list of issues for purposes of our analysis, we performed a literature search in both the blockchain and accounting areas but found few resolutions for our issues, as little has been written about how to solve the auditing issues identified. We conducted eight additional semi-structured interviews with auditors to understand how their firms are attempting to address the issues raised and generate solutions. This sample included six experts in the blockchain technology and two non-experts. We again believed that by combining the insights of experts and non-experts in blockchain technology, we could bring together the insights of the different profiles of auditors who will engage in mandates in this space. We also conducted four additional brainstorming meetings among our multidisciplinary research team between September 2018 and February 2019 to attempt to develop solutions to the issues raised.

Once we completed our brainstorming sessions and interviews, we developed a comprehensive set of recommendations to address the issues raised in our issue generation phases. In order to validate these findings with practitioners, we conducted a focus group in July 2019 with five auditors who work for a specialty audit practice within a national firm that is devoted to blockchain auditing (see Table 4 for focus group composition). This group was selected because their specialized knowledge would allow focus group participants to challenge our findings against what they had seen in the field.

Insert Table 4 here

In this case, our focus group participants were limited to blockchain experts as this would allow us to assess the validity of our recommendations. Overall, the focus group allowed us to challenge our findings and conclude that our recommendations were actionable, relevant and accurate. We now turn to the results and discussion section.

RESULTS AND DISCUSSION

The following sections cover client acceptance and executing the audit engagement, taking into account the challenges related to the *existence*, *ownership* and *valuation* of cryptoassets.

Client Acceptance

To carry out an audit, auditors must possess sufficient knowledge in a subject area to understand the subject matter under audit and be able to question its underlying assumptions. This can be achieved through industry specialization, training or by relying on subject matter experts to provide knowledge in a particular area. Presently, many auditors are refusing mandates in the blockchain sector due to a lack of technical competence regarding how to effectively carry out these audits. As Interviewee #15 explains:

> I can't even think of a single client we have that operates on a blockchain. I think it's clear that we don't have any clients in (the blockchain) space just because we can't take them on. We're just not in a place where we can audit these clients. (…) I

> think that when it comes to blockchain, it will be difficult to train people on this. People who have tried to understand what blockchain is have difficulty understanding what it is.

Interviewee #15's comments reflect a broader concern that auditors lack the background and training in information technology, more specifically on blockchains, in order to effectively assess the risks and question their client's assumptions, a phenomenon that has already been documented (Tschakert, Kokina, Kozlowski, and Vasarhelyi 2016; Richins, Stapleton, Stratopoulos, and Wong 2017). Our investigation indicates that many auditors are refusing mandates in the blockchain sector due to a perception of insurmountable risk from these clients. As someone who is not an expert in blockchain technology, Interviewee #15 echoes a concern raised by several of our non-expert respondents, namely, that not only is there a substantial gap between their knowledge as auditors and the fundamentals of blockchain technology, but that they question the possibility of ever closing this gap. Auditors wonder whether they will ever be able to obtain the requisite level of knowledge to provide assurance to the blockchain sector since they lack a foundation in areas like computer programming, information security and cryptography. Professional bodies like CPA Ontario and the AICPA have devoted substantial resources to developing new materials to train auditors in this new technology (CPA Ontario 2018; AICPA 2020). Additionally, several universities are integrating additional coverage of information technologies such as blockchain into their curricula to address this knowledge gap for new auditors entering the profession (e.g., RMIT Online 2020; CPA Canada 2019). However, the issue remains that many auditors are refusing mandates on the basis that they believe the gap between their extant

knowledge base and the level of proficiency required to audit clients in this space to be too large.

Other respondents expressed concerns about "getting things wrong," or about what would happen if they incorrectly issued an unqualified opinion when there were material misstatements that the auditor did not identify because they simply lacked an understanding of the technology and its risks. As Interviewee #17 explains:

> It ultimately comes down to risk. If I'm speaking candidly, an audit firm the size of X isn't going to do something unless they are 100% sure about it. I'm not going to go over a 100% but unless we know nothing bad is going to happen, we won't do it. The only thing worse than not doing it is doing it and ending up on the news the next morning because you guys committed fraud, or you didn't know what you were doing and you missed something.

Although Interviewee #17 is very much an expert in both auditing and blockchain, he shares many of the same reputational concerns as our non-expert respondents. One solution would be to engage experts to assist the auditor in obtaining the necessary competence, similar to the use of actuaries in assisting in the valuation of pension assets and liabilities (Himick 2016) and/or business valuators for fair market value assessments (Smith-Lacroix, Durocher, and Gendron 2012). In fact, this is something our respondents believe would be beneficial to their practice:

> One of the solutions is cross-disciplinary teams. So, I'm the auditor, and then I'm working with expert in computer engineering. (…) I think your focus as an auditor turns to your IT controls. But the thing is that with some [technologists], they don't understand audit at all. They don't get it. And we end up working as two teams. You have your audit team and your IT team, and the knowledge is separate. (Interviewee #11)

A challenge remains in ensuring that auditors and IT professionals work together effectively, as poor integration between these professionals can undermine audit outcomes (Bauer and Estep 2019; Hirsch 2020). As someone who is not an expert in

blockchain, Interviewee #11 worries that she would be dependent on these subject matter experts and that she might not be able to develop the necessary expertise to obtain a sufficient and appropriate knowledge of the business to challenge the specialists' conclusions, as the auditing standards require. Her concerns are shared by Interviewee #12 (likewise not an expert in blockchain):

> Auditors are becoming very reliant on specialists. You become so reliant on advisors that you can't make decisions yourself. It's kind of scary when you start to rely on so many different experts like the IT team and the valuation team and the tax team. I have no clue what (the specialty team) does. The technicality of it. In one meeting, I recorded the conversation because I didn't understand. Honestly, I have no idea what they were talking about and thank god (the expert) was there. I think that's the problem. He doesn't know what I'm doing, and I have no idea what he's doing.

One of our interviewees who does not consider himself to be an expert in blockchain technology (Interviewee #20) has in fact taken on a mandate in this space. Since his expertise is in auditing investment funds, he felt comfortable taking on clients who held portfolios of cryptoassets. He felt that given his in-depth knowledge of the financial services industry, he was able to audit this client as a traditional portfolio company that simply held a unique type of asset. He was able to rely on experts to assist with the crypto portion of the audit but relied on his own knowledge of portfolio companies to assess the risks of the client's operations. He stressed that he was not comfortable taking on other types of clients in the blockchain sector as this would be too removed from his skillset. Therefore, one way for auditors to gain a toehold into this industry is to take on blockchain companies whose business models are similar or tangential to their existing client base. Unfortunately, given that the objective of the

blockchain sector is to disrupt business as usual, there may not be many opportunities to approach the sector in this way.

Altogether, our conversations with auditors who are not experts in blockchain technology centered around their challenge in addressing their perception that they would resist taking on clients in this sector because they lacked the requisite knowledge to effectively address the client's risks. While they agreed that relying on experts offered the potential to bridge the knowledge gap, there remained important concerns that they would not be able to adequately supervise these experts given their lack of foundational knowledge. This presents an important opportunity for professional bodies and universities to fill this gap by offering training to bring auditors up to speed in order to take on these new mandates.

Our interviewees also indicate that many clients in this sector are rejected at the client acceptance phase because the clients lack an awareness of the internal controls required to safeguard against errors or misappropriation of assets and fraud (we discuss the sufficiency of various controls later in the paper). These clients often have technologically novel ideas but have not implemented an adequate internal control environment to permit the entity to be auditable:

> At some point we have to say, 'Look, you want to go public. You want to have an audit. You have to have this.' [...] We're comfortable at least in saying it's not just us. None of the other Big Four are going to do this either. (The client) might be able to get like some small niche boutique accounting firm to come in and look over (their) financials but unless (they've) got proper controls and a well thought out risk matrix in place, no one will accept them. (Interviewee #13)

Therefore, the onus is on auditors to become more familiar with blockchain technology and for firms to implement rigorous internal control procedures over the financial reporting process in order to become auditable.

Independence

One issue raised during our focus group was the difficulty of performing independence procedures in an anonymous environment. The group members relayed their experience in different client acceptance processes where the routine independence confirmation procedures were insufficient due to the inability to ascertain the full extent of who had a substantial stake in the enterprise:

> If John owns shares of Bell Canada, then that will be disclosed, and I can find that out. If Bob owns Bitcoin and we're auditing a Bitcoin mining company, does that impact Bob's independence? Well for Bitcoin, probably not. But if we're talking about an altcoin that is very specific and held by a small number of people, and it happens that a fund that we're auditing is a whale in that space, well, it could impact independence. [Focus Group #1]

The same discussion would also apply to related parties. In an anonymous environment, auditors may have difficulty identifying the scope of related parties, and therefore the auditor will have to design alternative procedures to ensure that they have obtained the full scope of related parties and related private keys under the entity's control.

Executing the Audit Engagement

Our investigation indicates that the three main issues identified by auditors when auditing clients with a material amount of cryptoassets are *existence*, *ownership* and *valuation* of those assets. However, some auditors remain confident that these issues are eventually surmountable. As Interviewee #18 describes:

> I think we could work our way through the audit risks and obtain evidence around the existence, and the ownership rights, and the valuation to be able to say, 'We can issue an opinion.'

However, getting there may be a challenge as firms are presently, by and large, unwilling to issue audit opinions. These three issues (*existence*, *ownership* and *valuation*), collectively, were consistently identified throughout our interviews. In the next sections, we describe the challenges related to these items, but more importantly, we suggest how to address them.

Existence of Cryptoassets

Auditors need to establish that financial statements, as reported, are free of material misstatements. One area that was repeatedly cited as a challenging area for our respondents was the existence of cryptocurrencies. The major challenges to verifying existence are related to the reliability of a blockchain and the custodianship of assets.

Reliability of a Blockchain

One challenge of auditing the existence of cryptoassets is simply due to their non-physical nature [Auditor #6]. Unlike inventory or land which auditors can observe, auditors are required to find alternative evidence for these intangible assets. Evaluating the existence of a cryptoasset necessarily requires relying on a blockchain upon which a cryptoasset resides. Further, determining whether a given blockchain is reliable or not can prove difficult. Our interviewees indicated that simply relying on the blockchain is not an option. Although blockchains are touted as immutable, not all blockchains are created equally. Hence, the ability to rely on a blockchain will depend on factors such as the robustness of the consensus mechanism, depth of the community supporting the blockchain, and reliability of the cryptography involved, among other things.

> A fundamental question is the reliability of that blockchain to be used as audit evidence. Blockchain is viewed as trustless but it is still a piece of code. For instance, if we're talking Bitcoin, there is a larger community supporting it, resulting in a longer chain, more mining, more hashpower, more robust cryptography, more robust consensus mechanism, quicker resolution of forks. Not just because of the size of the community, but the manpower to resolve these issues makes the blockchain more reliable. If we're talking about an obscure altcoin, then it's something different. In that case, maybe it's a weaker protocol, a weaker consensus mechanism. There is less support. [Focus Group #1]

Respondents mention that the challenge lies in determining how much work is involved in validating the blockchain itself. Whether a full code review or investigation of the underlying blockchain's cryptography is necessary will be a case by case decision [Focus Group #1]. However, this may result in duplicate work if each firm is providing an in-depth review of each blockchain for each mandate. Best practice would involve firms developing a library of blockchains which have been tested (for instance, blockchains for which a code review has been done at a certain date) and which future engagement teams within the firm network can rely on to reduce the duplication of work.

Another challenge remains determining how to rely on transactions that are not on the blockchain. For instance, many exchanges pool or commingle the accounts of several clients. In a secondary ledger (not on the blockchain), they record the positions of each client and then may record offsetting positions of those clients in this secondary ledger and not actually record the exchange on the blockchain:

> A number of custodians just pool all the assets together and then sometimes they do trades where the trade isn't recorded on the blockchain. It's just a movement from ledger A to ledger B. If you have one client of your exchange and another client of your exchange that have equal, offsetting trades, they will match them without involving the blockchain. Somebody might say, "Well, all the trades are on the blockchain." No, they're not. [Auditor #6]

Auditors must be careful when evaluating audit evidence to verify the source for their existence support. While there are procedures that will allow the auditor to rely on the blockchain to validate existence, the auditor must validate that the transaction actually took place on that blockchain. If not, the immutability of the blockchain is irrelevant.

Finality

While blockchains are touted as immutable, the finality property (like all security properties) is subject to assumptions. Immutability of a blockchain is subject to consensus taken across miners according to computational ability. Consensus is not instant: a transaction might be included and then quickly dropped as consensus forms between different proposed chains. And it is never guaranteed to be final: an agreement within the computational majority of miners can unroll past transactions to some extent. For example, this was raised as a significant drawback by the Bank of Canada, who built a pilot large-value transfer system for its member banks using blockchain technology (Chapman, Garratt, Hendry, McCormack, and McMahon 2017):

> Finality is probabilistic in this setting. For instance, in Bitcoin, if a miner waits less than 6 blocks [about an hour], there is less than a 1% chance of reversal. If he waits more than 120 blocks [about 48 hours to three days], then there is less than a 0.01% that the transaction will be reversed. [Focus Group #3]

While auditors are concerned about the reversibility of transactions on a blockchain, this is another manifestation of the issue of immutability of the blockchain [Focus Group #1]. In their validation of the blockchain itself, auditors must verify that the

blockchain is tamper-proof and the degree of testing required for each blockchain will differ. For blockchains that have less robust mechanisms, accountants may wish to consider revocability, like in the case of sales agreements that provide customers with the option to return merchandise within a pre-established period. When recording revenue, the accountant must estimate the expected number of returns and factor this into the amount of revenue to be recorded. The same concept could be applied for the issue of finality. The firm could estimate the amount of returns or reversals that are likely to occur and factor this into their transaction recognition.

The above section aimed to demonstrate that due to the immutable nature of the blockchain and its ability to report the totality of transactions conducted during the period, this technology provides a record upon which the auditor can obtain a certain level of evidence to ascertain the occurrence of transactions. However, the auditor cannot blindly rely on the blockchain but must perform procedures to validate its reliability.

Completeness

Firms generally do not hide assets as this undermines their reported financial health. However, a firm might hide an asset to shift its acquisition forward in time. Additionally, hiding liabilities promotes a firm's solvency. Therefore, auditors are charged with determining that they have obtained the full measure of a firm's transactions to ensure the completeness of the information under analysis.

In a blockchain-enabled world, the blockchain contains the record of all transactions by all participants carried out during the year. If the auditor has a complete and authentic list of all the keys that belong to the entity under audit, they can easily

obtain an account of all the transactions carried out on the blockchain during the period. However, there is always the possibility that a client has not reported all keys in his possession to the auditor. Therefore, transactions on those keys would not be part of the known set of information under audit:

> For completeness, this is not a blockchain problem, it's a regular audit problem. We would do the search for unrecorded liabilities but instead of finding a liability that wasn't in the books, we would find a key that we didn't know about [Focus Group #4].

We will next address how custodianship is an important issue for both existence and ownership of cryptoassets.

Ownership of Cryptoassets

Auditors must be satisfied that the assets reported on the company's balance sheet do in fact belong to the company, or if the client is operating as a custodian for third parties (for instance, as an exchange who holds cryptocurrencies received from third parties), that the assets held do in fact belong to the third party who claims to possess them. For traditional assets, firms might overcome the ownership issue in several ways. First, a client can demonstrate ownership of an asset with reference to a generally accepted official document. For instance, a property owner can demonstrate ownership of their building with reference to a deed. However, in a blockchain environment, no central authority exists to produce such official documents. The sheer anonymity of a blockchain precludes this type of investigation [Auditor #6]. Secondly, firms may engage a custodian to hold assets on their behalf, like a bank. This does not eliminate the issue of ownership but simply shifts the concern from the firm's audit to the audits of central custodians:

> One of our first considerations as it relates both existence and ownership is just to think through how the entity is maintaining custody of their assets. And in particular, what's the security mechanism around access to the private key? Which can vary from being held [in many ways] from online to some type of hot storage to on a piece of paper somewhere to in a software tool that is not connected to the internet and kind of offline. Which of course, brings down the risk of it being hacked but then increases the risk of physical loss of the private key. We want to understand what our potential clients are doing related to that. Then, as many of them seem to do, we start to gather that they're using a third party around custody [Auditor #19]

Therefore, addressing whether or not a client maintains ownership over their cryptoassets will depend on whether they hold their cryptoassets themselves (self-custody) or through a custodian.

Self-custody of assets

In the absence of legal registers to support ownership or documents bearing the name of the firm, the auditor must rely on the internal controls of the entity to obtain comfort over the ownership assumption [Focus Group #3, #4]. A question emerges about what ownership means in this context both temporally and in terms of access to a private key. Temporally, auditors must distinguish between whether they are able to provide support for ownership over an asset at the date of conducting the audit procedure or at the end of the fiscal period under audit [Focus Group #4]. For example, if an auditor verifies that a client owns bitcoin one month after year-end through procedures like signing messages or transferring small amounts to and from the key, this proves that the client controlled the asset on that date but says nothing about whether the client owned those assets at year-end. With inventory, in the absence of performing a count at year-end, the auditor may perform roll-back procedures to verify the transactions between the count date and the year-end date to obtain comfort over the year-end balance. To do so, this

would require that the auditor ensure that ownership was maintained over the subsequent events period even if this is not what is required by the auditing standards:

> Do I need to prove that they retained ownership over the subsequent events period? The auditing standard doesn't say that I do. If the client loses ownership during the subsequent events period, do I need to unrecord the whole thing at year end? Likely, this would be an issue of note disclosure. In the past, this has been used before for some fraud cases, but in those cases, it was because those transactions never really occurred [Focus Group #1].

Determining when to test ownership to ensure that evidence is obtained at the correct date becomes a challenge. Best practice would indicate that, like inventory, auditors should test ownership as at the balance sheet date and may wish to provide note disclosure for significant events where ownership is lost.

A question emerges about what ownership really means in this context. A client may demonstrate that they have access to a private key, but this in and of itself does not demonstrate ownership [Interviewee #17]. "*With ownership, the risk of giving someone else access to the private key is no different than the corporate controller sharing his password to the company bank account with his spouse" [Focus Group #4]*. Auditors must determine what types of procedures they can do to validate control and ownership in this context:

> If a client uses self-custody, we can do different procedures to be able to approve ownership like small amount transfers or secret messages, depending on the protocol they're using. [Focus Group #3]

These practices like small value transfers or the sending of secret messages are part of what are referred to as cryptographic proofs.

Cryptographic keys

For most cryptoassets, the asset is considered owned by Alice if Alice possesses a private signing key that can be used to digitally sign a transfer of the asset. Although alternative notions of ownership are possible to define, the idea of a signing key is foundational and seen with bitcoin, ether and ERC20 tokens. Thus, demonstrating knowledge of this key is necessary, but not sufficient, to demonstrating ownership. The most direct cryptographic technique is to use a so-called zero-knowledge proof of this private key, and to staple in some information identifying the context of the proof. For standard proofs, this is cryptographically equivalent to simply signing a challenge message with the key. Folklore protocols of sending small cash amounts from an allegedly owned account to the auditor to demonstrate control are also commonly noted in the literature. This offers similar security but may add ethical complexities for the auditor in accepting the amount transferred.

We note that while cryptographic proof is necessary, it is not sufficient. A cryptographic proof simply demonstrates that the purported owner has access to the person holding the signing key. A malicious company might arrange for the owner of cryptoassets to engage in signing statements or moving test amounts fraudulently on their behalf. This issue is not new: an insolvent retail store might borrow inventory from elsewhere to inflate its assets during an inventory count. Auditors mitigate this by arranging a common date for all audits of physical inventory and, similarly, cryptographic audits could be synchronized on a fixed schedule to prevent the same assets from being counted for different companies in different audits (Dagher, Bünz, Bonneau, Clark, and Boneh 2015).

One type of proof includes sending a small amount of money to the auditor from the private key, while another proof involves demonstrating that the client can respond to a cryptographically-protected message that only the private key holder could open. Independently, neither of these procedures demonstrate that the client owns the private key. However, auditors rely on the sum of several procedures to obtain reasonable assurance over this assertion:

> With ownership, it's not a specific procedure but rather the body of evidence that can be performed by signing messages, by testing internal controls, by understanding how the client protects passwords. The clear expectation of ownership is changing. In a traditional audit, the client represents that they own certain things. We see an invoice and we see that they own it. But did they really pay for it? Was it paid for by another company and consigned to them? We perform several procedures to feel comfortable enough to say that they have ownership at that point in time. Our expectations of what ownership means in this area is evolving. [Focus Group #1]

Many clients are concerned about self-custody due to security risks over holding their own private keys and are turning to custodians to fulfill this function for them [Auditor #19]. Auditors must adapt their audit procedures to their clients' unique internal control environments and consider competing sources of evidence before coming to a conclusion about ownership.

Third-party Custodianship

In a traditional audit context, the reliance on a third-party custodian is commonplace. Clients might have bank accounts with multiple banks or investment accounts with various brokerage houses. Obtaining confirmations from these custodians is valued as a high-quality evidence due to its provenance from a regulated third party.

Confirmations in the cryptoasset space are not as straightforward because the entities the auditor would be requesting confirmations from, such as a crypto-exchange, are not regulated [Focus Group #1]. This raises questions over the reliability of their responses.

In order to address the reliability of the confirmations from service providers such as cryptocurrency exchanges or other types of custodians, auditors look to the robustness of the internal controls at the service organization. The robustness of these controls is evidenced by the presence of a service organization control (SOC) report. In order to rely on the controls of a service organization such as a payroll provider or investment custodian, auditors often obtain SOC reports which provide assurance over the processes and data security at the custodian. Two types of reports are available: an SOC 1 report provides assurance over the controls used by a service provider who processes financial data; an SOC 2 report provides assurance over controls over the processing of non-financial data in accordance with Trust Services Criteria (BDO 2019).

> The issue that we have here is that there aren't generally service organization control reports available. We'd be looking around kind of what controls are in place. And often, the entities don't understand what those things are and might be placing undue reliance themselves on what the custodians are doing with their assets. [Auditor #19]

> There is a question of quality of the SOC 1 and SOC 2 that are coming out now. If we compare them to current practice in other sectors, the reports that we see in those areas are extremely well standardized. It's very easy to what is being covered and tested. However, for the few that have been released in this sector, there are things missing. There is certainly an effort being made but just because there is a SOC 1 or SOC 2 report doesn't mean that it is enough. [Focus Group #2]

While some firms have been able to obtain SOC reports, albeit the mere fact of having the report is, according to our interviewees, insufficient. Our interviewees caution that obtaining an SOC report is not a box-checking exercise and that the auditor must

review the report carefully to understand which controls it has addressed and can be relied on [Focus Group #2].

A related issue to the robustness of the internal controls relates to how the custodian segregates the assets in their possession:

> We also have heard that many of these custodians are co-mingling or combining assets into a single account or wallet. That muddies the water a bit and it's difficult in some type of SOC reports to understand what they are really doing to maintain a client's assets. There's a chance that there actually are no assets. If you've given your assets to someone else to hold for you, you may think that they still are yours and that they still exist, but that can be difficult to ascertain. [Auditor #19]

When evaluating whether or not they can rely on the representations from a custodian, the auditor should evaluate how the custodian segregates the assets in their possession.

In short, in order for auditors to validate ownership, their procedures will depend on whether the client has custody of their keys or uses a third party. Self-custody will depend on the client's internal controls, while reliance on a custodian will depend on the ability to obtain comfort over the reliability of the custodian. Additionally, cryptographic proofs play an important role in the ability to rely on either party. In order to avoid double-counting of keys, an industry standard common date should be arranged to provide a generally agreed upon "state of the world" where keyholders can demonstrate ownership.

However, not all auditors may be as aware of the importance of SOC reports. Interviewee #3 (who does not consider himself to be an expert in blockchain) had taken on a mandate in the blockchain sector as he believed he had sufficient support from resources within his firm to take on the mandate. However, he described relying on confirmations from exchanges as a way to corroborate the existence and ownership of his

client's assets, since third-party audit evidence is traditionally viewed as the highest quality of audit evidence for addressing these assertions.

This finding raises two issues. First, this respondent took on an audit recognizing that he is not a blockchain specialist, believing he could rely on technologists at his firm to compensate for his lack of knowledge (he is part of a Big 4 firm). However, having access to expert knowledge is not the same as deploying it. As we have cautioned throughout the paper, it is incumbent on auditors to develop a fundamental knowledge of blockchain technology to be able to leverage the skills of specialized professionals. And this synergy is only possible when auditors and technologists collaborate (Bauer and Estep 2019). Second, in our conversation with this respondent, he bemoaned the lack of guidance on how to audit cryptoassets. Since our interviews, considerable thought leadership has been released by the accounting firms, professional organizations and standard setters on the accounting and audit of cryptoassets. We believe that by providing rigorous sets of standards and through ongoing inspections by audit oversight bodies, a corpus of generally accepted auditing standards for this sector will develop. These standards will provide guidelines which auditors who are not blockchain experts can use when attempting to make inroads into this sector.

Valuation of Cryptoassets

When values are reported on financial statements, they must be reported in the functional currency of the firm, meaning the primary governmental currency used. A challenge for blockchain entities is to determine the valuation of cryptoassets on the financial statement date or the conversion rate for sales and expenditures made

throughout the year. Auditors must be satisfied that the values reported in the financial statements are accurate and represent the underlying economic reality.

Fair Value of Cryptoassets

A significant obstacle for obtaining audited financial statements is the determination of a fair value for cryptoassets. Auditor #19 describes this challenge as follows:

> The only way in my view to reliably determine the fair value of a cryptocurrency is to observe actual exchange transactions in the market. There's no other way to derive a fair value, because I can't look at the intrinsic value of that cryptocurrency and come up with some sort of valuation model to derive a value.

Cryptoassets are often difficult to value because it is challenging to determine their underlying value and there may not be a generally accepted, quoted value to use as a reference. As an analogy, firms value foreign currencies at the closing rate on the transaction date, as reported by the central bank servicing the firm's area. No universal central bank offers rates for currency-like cryptoassets. At the time of writing, one Fortune 500 financial firm, CME (Chicago Mercantile Exchange), offers a daily reference rate for bitcoin, but not for other cryptocurrencies or cryptoassets.

While bitcoin and ether enjoy around-the-clock trading across many markets, lesser-known coins, tokens, assets, or liabilities may trade slowly, and in low volumes. Generally speaking, low liquidity results in stale last sale prices and large bid-ask spreads. This is challenging but not unprecedented in financial auditing: privately held stocks and over-the-counter financial instruments share a similar profile. Auditors must

familiarize themselves with the exchange markets for the cryptocurrencies held by their client to assist in validating their valuation.

Geographical variation

The same cryptoasset might have different market values across different jurisdictions [Focus Group #1, #4, #5]—because of market frictions, arbitrage does not resolve these differences (Kroeger and Sarkar 2017). If a firm applies International Financial Reporting Standards (IFRS), any financial assets measured at fair value that they hold must be determined with reference to their principal market (if available), which refers to the "market with the greatest volume and level of activity for the asset" (Deloitte 2013). Therefore, this standard precludes a firm from using the valuation of a cryptocurrency based on an obscure market price. Auditors will need to look carefully at the record of a client's trading activity to determine the location of a client's principal cryptoassets market and ensure that the assets are valued accordingly on the financial statements.

Figure 2 summarizes the three core issues auditors will have to face to provide audited financial statements to blockchain firms.

Insert Figure 2 here

CONCLUSION

This paper has aimed to demonstrate that, in comparison to traditional audits, audits of clients who hold material amounts of cryptoassets are complex but not

impossible. Once a client has been accepted, the three most cited stumbling blocks to providing an audit opinion are the *existence*, *ownership* and *valuation* of cryptoassets. However, we argue that these issues are not insurmountable if industry guidelines are put into place to allow auditors to verify their client's cryptographic keys against a "state of the world" at a generally accepted point in time. Verifying existence and ownership largely hinges on an auditor's ability to verify the possession of cryptographic keys. However, the auditor must be certain that these keys in fact belong to the client and do not simply represent access to an account. Once ownership has been proven, the auditor can rely on the immutable properties of the blockchain to verify existence as the blockchain provides the entire record of transactions since the blockchain's inception. The issue of key sharing is important but is not unlike a situation in the real world where a related party could give the entity under audit a large sum of cash to hold at year-end and report on their financial statement to buoy their financial performance. Volatility complicates the valuation of altcoins and other coins with low trading volumes. However, many other exotic securities exist where accountants rely on complex financial modelling to determine a price.

In sum, this paper argues that although auditors are rightly cautious when approaching a new sector where clients have not been initiated to the importance of internal controls and where numerous frauds have recently been perpetrated, audits are possible. Audit risk can be reduced through proper vetting of clients and management teams. Additionally, by collaborating closely with blockchain experts from client acceptance through to the issuance of an audit opinion, auditors who themselves are not

experts in blockchain technology can come to a place where they can provide assurance to this sector.

This objective of this paper is to systematize the issues relating to blockchain-based assets in order to provide a reference for practitioners and academics and to demystify the purported roadblocks associated with taking on clients in this space. We believe that by synthesizing these issues and providing actionable recommendations, we can provide insights that will invite auditors who are not experts in blockchain technology to consider how they can engage with this sector. Through an iterative process of building knowledge and obtaining input from practitioners, we deploy an approach that can be used to improve the collaboration across the research-practice gap. The approach used allow an in-depth understanding of the phenomenon but has limitations. Interviewees can speak freely, providing the opportunity to delve into otherwise hidden aspects of key technological and audit issues. In the end, we do not consider that these limitations undermine our contributions or reduce the relevance of conducting field studies in this domain. Too few studies have asked key practitioners about their concerns and solutions (Spraakman, O'Grady, Askarany, and Akroyd 2015). Overall, we hope our paper inspires future research on overcoming auditing and accounting challenges in the blockchain space.

Table 1. Description of Interviewees

#	Position	Date	Duration
Issues-focused interviews			
1	Mid-Sized Accounting Firm Partner	May 17, 2018	120 min.
2	Big 4 Accounting Firm Senior Manager	July 11, 2018	36 min.
3	Big 4 Accounting Firm Senior Manager	July 11, 2018	40 min.
4	Big 4 Accounting Firm Partner	July 18, 2018	39 min.
5	Mid-Sized Accounting Firm Partner	July 23, 2018	35 min.
6	Big 4 Accounting Firm Partner	July 27, 2018	36 min.
7	Big 4 Accounting Firm Manager	July 27, 2018	38 min.
8	Big 4 Accounting Firm Senior	Aug 2, 2018	140 min.
9	Big 4 Accounting Firm Manager	Aug 7, 2018	42 min.
10	Mid-Sized Accounting Firm Senior	Aug 8, 2018	35 min.
11	Big 4 Accounting Firm Partner	Aug 15, 2018	40 min.
12	Big 4 Accounting Firm Manager	Aug 21, 2018	45 min.
Solutions-focused interviews			
13	Big 4 Accounting Firm Senior Manager	Sept 12, 2018	54 min.
14	Big 4 Accounting Firm Senior	Sept 12, 2018	50 min.
15	Big 4 Accounting Firm Senior	Sept 12, 2018	55 min.

16	Big 4 Accounting Firm Senior Manager	Sept 27, 2018	47 min.
17	Big 4 Accounting Firm Senior Manager	Sept 28, 2018	55 min.
18	Big 4 Accounting Firm Partner	Oct 4, 2018	45 min.
19	Big 4 Accounting Firm Partner	Oct 4, 2018	55 min.
20	Big 4 Accounting Firm Partner	July 18, 2019	70 min.

Table 2. Description of Participants at Structured Brainstorming Meetings

#	Expertise in the area	Years of experience
1	CPA, CITP (Certified Information Technology Professional), MSc in MIS; expertise in information technology and accounting	19
2	CPA auditor, CA; expertise in auditing	10
3	PhD and Post-Doc in computer science; expertise in cryptography and blockchain	12 (9 on blockchain)
4	Master of engineering; expertise in information security and blockchain	11 (7 on blockchain)

Table 3. Themes Arising from Interviews

Main theme	Sub-theme
Client acceptance	- Auditor competence - Client internal controls
Existence	- Reliability of a blockchain - Finality - Completeness
Ownership	- Self-custody of assets - Cryptographic keys - Third-party custodianship
Valuation	- Fair value of cryptoassets - Geographical variation

Table 4. Focus Group: Description of Participants

#	Expertise in the area	Years of experience
1	Audit partner; Professional practice lead involved in national and international audit standard setting	19
2	Audit partner	15
3	Blockchain practice director	8
4	Audit manager	8
5	Audit manager	7

Figure 1. Research Approach

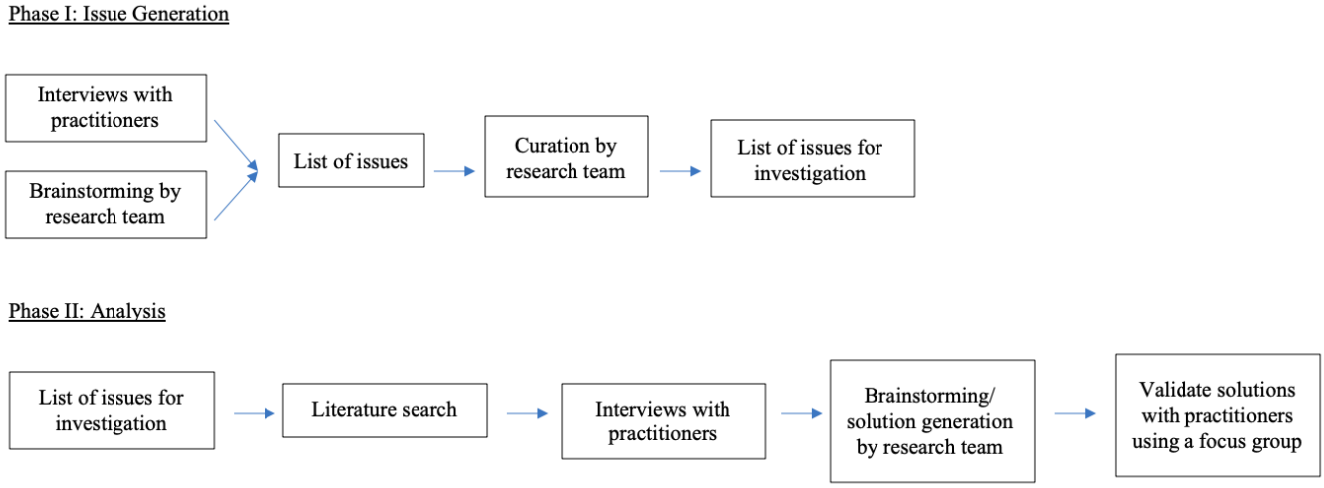
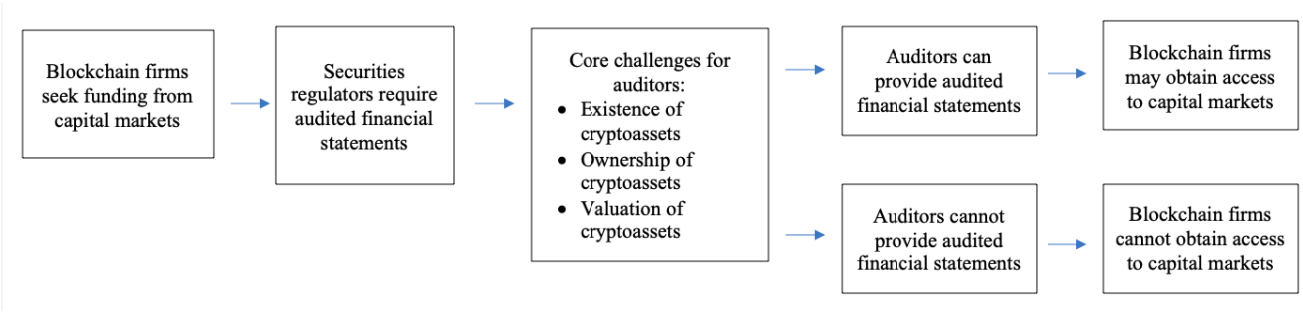


Figure 2. Core Issues Faced for Auditors when Providing Audited Financial Statements to Blockchain Firms



REFERENCES

Abreu, P. W., M. Aparicio, and C. J. Costa. 2018. *Blockchain Technology in the Auditing Environment*. 13th Iberian Conference on Information Systems and Technologies (CISTI).

Association of International Certified Professional Accountants, AICPA. 2020. *Blockchain and Distributed Ledger Technology*. Available at: https://www.aicpa.org/interestareas/informationtechnology/resources/blockchain.html

Bauer, T. D., and C. Estep. 2019. One team or two? Investigating relationship quality between auditors and IT specialists: Implications for audit team identity and the audit process. *Contemporary Accounting Research* 36 (4): 2142-2177.

BDO. 2019. *Third Party Assurance*. Available at: https://www.bdo.ca/en-ca/services/assurance-and-accounting/third-party-assurance/overview/

Broby, D., and G. Paul. 2017. The financial auditing of distributed ledgers, blockchain and cryptocurrencies. *Journal of Financial Transformation* 46: 76□88.

Carter, C. and C. Spence. 2014. Being a successful professional: An exploration of who makes partner in the Big 4. *Contemporary Accounting Research* 31(4): 949□981.

Catalini, C., and J. S. Gans. 2016. Some Simple Economics of the Blockchain (No. w22952). *National Bureau of Economic Research.*

Chapman, J., R. Garratt, S. Hendry, A. McCormack, and W. McMahon. 2017. *Project Jasper: Are Distributed Wholesale Payment Systems Feasible Yet?* Bank of Canada.

Coindesk. 2018. *State of Blockchains Q3 2018*. Available at: https://www.coindesk.com/research/state-of-blockchains-q3-2018

CoinMarketCap. 2019. *Total Market Capitalization*. Available at: https://coinmarketcap.com/charts/

Coyne, J. G., and P. L. McMickle. 2017. Can blockchains serve an accounting purpose? *Journal of Emerging Technologies in Accounting* 14(2): 101□111.

CPA Canada. 2019. *The CPA Competency Map Update, Outreach Package*. May, Toronto, Ontario.

CPA Ontario. 2018. *Navigating the Brave New World of Cryptocurrency and ICOs. Thought Leadership Series*. CPAOntario.ca.

Crosby, M., P. Pattanayak, S. Verma, and V. Kalyanaraman. 2016. Blockchain technology: Beyond bitcoin. *Applied Innovation* 2(6-10): 71.

Curtis, M. B., J. G. Jenkins, J. C. Bedard, and D. R. Deis. 2009. Auditors' training and proficiency in information systems: A research synthesis. *Journal of information systems* 23(1): 79□96.

Dagher, G. G., B. Bünz, J. Bonneau, J. Clark, and D. Boneh. 2015. *Provisions: Privacy-preserving proofs of solvency for bitcoin exchanges.* ACM CCS.

Dai, J., and M. A. Vasarhelyi. 2017. Toward blockchain-based accounting and assurance. *Journal of Information Systems* 31(3): 5□21.

Deloitte. 2013. *IFRS 13 Fair Value Measurement*. Available at: https://www.iasplus.com/en/standards/ifrs/ifrs13

Grigg, I. 2005. *Triple Entry Accounting*. Available at Research Gate: https://www.researchgate.net/profile/Ian_Grigg/publication/308640258_Triple_Entry_Accounting/links/57e99c4408aed0a291304588/Triple-Entry-Accounting.pdf

Himick, D. 2016. Actuarialism as biopolitical and disciplinary technique. *Accounting, Organizations and Society* 54: 22–44.

Hirsch, R. 2020. The effect of spatial distance and domain knowledge distinctiveness on auditor reliance on IT specialists.*Journal of Information Systems* 34(1): 81-103.

Impak Finance. 2018, Aug 28. *Impak Finance est en défaut de transmettre ses états financiers annuels audités* (Press Release). Retrieved from http://sedar.com

Kokina, J., R. Mancha, and D. Pachamanova. 2017. Blockchain: Emergent industry adoption and implications for accounting. *Journal of Emerging Technologies in Accounting* 14(2): 91□100.

Kroeger, A., and A. Sarkar. 2017. *The law of one bitcoin price?* Federal Reserve Bank of Philadelphia. Available at: https://www.philadelphiafed.org/-/media/bank-resources/supervision-and-regulation/events/2017/fintech/resources/law-of-one-bitcoin-price.pdf?la=en

Loveridge, R., and F. Mueller. 1999. Flagships, flotillas and corvettes: National business systems and sectoral dynamics in telecommunications. In *National Capitalisms, Global Competition and Economic Performance. Advances in Organization Studies (3).* Edited by S. Quack, G. Morgan, and R. Whitley. Amsterdam: John Benjamins Publishing Company.

Nakamoto, S. 2008. *Bitcoin*: *A Peer-To-Peer Electronic Cash System*.

Patton, M. Q. 2002. *Qualitative Research & Evaluation Methods*. (3rd ed.) London: Sage.

Posadzki, A., and D. Milstead. 2019, Mar 22. Crypto companies struggle to find auditors amid heightened scrutiny. *Globe and Mail.* p. B1 Available at: http://search-proquest-com

Richins, G., A. Stapleton, T.C. Stratopoulos, and C. Wong. 2017. Big data analytics: Opportunity or threat for the accounting profession? *Journal of Information Systems* 31(3): 63–97.

RMIT Online. 2020. *Blockchain*. Available at: https://online.rmit.edu.au/c/blockchain

Rückeshäuser, N. 2017. *Do We Really Want Blockchain-based Accounting? Decentralized Consensus as Enabler of Management Override of Internal Controls.* Proceedings of the 13. Internationalen Tagung Wirtschaftsinformatik (WI 2017).

Saunders, M., and K. Townsend. 2018). Choosing participants. In *The Sage Handbook of Qualitative Business and Management Research Methods,* edited by C. Cassell, A. L. Cunliffe, and G. Grandy, 480□492. London: Sage.

Securities and Exchange Commission (SEC). 2009, June 30. *Financial Reporting Manual Topic 4: Independent Accountants' Involvement*. Available at: https://www.sec.gov/corpfin/cf-manual/topic-4

Smith, S. S. 2018. Blockchain augmented audit Benefits and challenges for accounting professionals. *The Journal of Theoretical Accounting Research* 14(1): 117 137.

Smith-Lacroix, J.-H., S. Durocher, and Y. Gendron. 2012. The erosion of jurisdiction: Auditing in a market value accounting regime. *Critical Perspectives on Accounting* 23(1): 36–53.

Spraakman, G., W. O'Grady, D. Askarany, and C. Akroyd. 2015. Employers' perceptions of information technology competency requirements for management accounting graduates. *Accounting Education* 24(5): 403 422.

Taylor, S. J., R. Bogdan, and M. DeVault. 2016. *Introduction to Qualitative Research Methods: A Guidebook and Resource*. New Jersey: John Wiley & Sons.

Tschakert, N., J. Kokina, S. Kozlowski, and M. Vasarhelyi. 2016. The next frontier in data analytics − Why CPAs and organizations need to learn to use advanced technology to predict and achieve outcomes. *Journal of Accountancy.* August, 58–63.