A first look at auditing in a blockchain world

Erica Pimentel[1], Emilio Boulianne[1], Shayan Eskandari[2], Jeremy Clark[2]

[1] John Molson School of Business, [2] Gina Cody School of Engineering and Computer Science
Concordia University

Abstract. The emergence of cryptocurrencies (*e.g.,* Bitcoin) and blockchain technologies (*e.g.,* Ethereum) have matured to a point that commercial firms operating in this space are seeking audits of their financial statements. At the time of writing, auditing firms are hesitant to audit such firms for a variety of reasons with a common underlying theme: the blockchain market introduces novel, technically sophisticated, and risky propositions. In this paper, we critically analyze the purported roadblocks to auditing blockchain firms, using a cross-disciplinary approach to bring cryptographers and auditors on the same page.

1 Introductory Remarks

A number of firms operate with blockchain-based assets, liabilities, and/or transactions. In certain common circumstances, these firms will require their financial statements to be validated by a financial auditor. Annual audits are legally mandatory for publicly traded companies in most countries, and audits might also be required when a firm borrows from a bank or raises capital from investors. Auditing is a timely subject as, at the time of writing, major auditing firms are hesitating to provide certification to a wide range of businesses in the blockchain sector due to a perception of insurmountable business risk associated with these clients. This creates friction for firms wanting to raise capital in traditional ways.

When assessing whether or not to take on a new client, auditors who lack experience in this sector will be unable to develop expectations of financial performance as a way of challenging financial statement assumptions. Due to the complex and rapidly changing technological environment, auditors are also unable to keep pace with the changes and develop the in-depth knowledge of their clients' businesses required for performing an audit. Finally, auditors are wary of accepting clients that hold a significant amount of cryptoassets as this space is largely unregulated. A lack of third-party oversight puts an onus on the auditor, further increasing their risk exposure.

In this paper we explore why and provide a comprehensive overview of the challenges auditors perceive as novel, we form parallels to auditing approaches used today, and critically assess the extent to which these challenges are barriers. Altogether, we find that while this environment is new, the challenges presented are different incarnations of issues already addressed with traditional audit clients. Therefore, we conclude that many entities in this space are auditable, subject to certain caveats.

Methodology. To ensure a comprehensive overview of the changes facing auditors, we first used structured brainstorming within our multidisciplinary research team, which includes expertise in both auditing and blockchain technologies. Once our preliminary list of challenges was established, we vetted our results through informal discussions with over a dozen individuals working in the field, including at the Big Four[1] and mid-sized accounting firms, and used these interviews to augment our list. The contribution of this paper is to provide a comprehensive list of challenges, rather than determining the relative importance of each or any broader concepts across the industry—thus we did not find it necessary to apply qualitative data analysis (*e.g.,* grounded theory) to the interviews; instead, we simply extracted the challenges raised.

Relevance. Our work can be viewed as a case study of cryptographers working with an outside profession to address a real-world problem. The result is not a new protocol but a two-way knowledge transfer between professions. While displacing auditors is occasionally a target of cryptographers [10,24], auditing itself is also occasionally studied directly [17] or indirectly [29,6] at venues like Financial Cryptography.

2 Preliminaries and Related Work

Financial statements are prepared by a firm to summarize: its assets and liabilities at year-end, the resulting changes in firm equity, and the firm's revenue, expenses, and cash flows across the year. Because the firm generally wants to present the most optimistic view of its financial health, the firm may hire an auditor to ensure it is a realistic picture of the company's financial performance. In doing so, auditors are expected to comply with Generally Accepted Auditing Standards (GAAS) and the Code of Conduct of their professional order [28]. In addition to an annual audited statement, the firm will produce quarterly statements that are reviewed by a third party auditor to a less rigorous standard.

2.1 Primary Stakeholders in an Audit

Firm Management. Financial statements are prepared by and remain the responsibility of firm management. Many assumptions and estimates are required to prepare this report. A firm's CEO and CFO must certify the adequacy and effectiveness of the firm's internal controls over financial reporting, which poses a reputational risk for firm directors as they will be held accountable for financial statements that are misstated. Management will agree to an audit to comply with regulatory requirements, or because they feel it will give them a competitive advantage over non-audited firms in raising capital and lowering their lending rates. In the blockchain market where auditors are reluctant and/or audits are expensive, firms can use their ability to obtain audited financial statements as a barrier against new entrants to the sector.

[1] The Big Four are the four biggest auditing firms in the world which includes, Ernst & Young (EY), Deloitte & Touche, KPMG and PricewaterhouseCoopers (PwC).

Auditor. The auditor for a given firm is selected by the firm itself. When an auditor provides an audit opinion, there is always a chance that fraud or misrepresentation went undetected in the statements. If this fraud is subsequently uncovered, the auditor could be liable for substantial penalties. For instance, Deloitte LLP paid a settlement of $150M for failure to find fraud at mortgage broker Taylor, Bean & Whitaker [14].

Investors. The primary users of financial statements are external investors who make decisions about whether or not to lend money or invest capital in a target firm. Investors use financial statements to assess their potential return on investment. Although *caveat emptor*[2] is a consideration, investors rely on the existence of an auditor's report as a signal of the reliability of financial disclosures.

Financial Regulators. Regulators span different government agencies with a spectrum of concerns including financial fraud, taxation, anti-money laundering, and know your customer (KYC) rules. Financial audits are central to the role of security regulators, who require publicly traded firms to obtain an annual unqualified audit opinion on their financial statements for consumer protection. Failure to do so, would put the company offside with the regulators' requirements and could result in the company's shares being placed on cease-trade.

2.2 Cryptoassets and firms that hold them

The central component of a financial report is the firm's balance sheet which lists assets and liabilities. We use the term *cryptoasset* and *cryptoliability* to refer to items contingent on blockchain technologies. Cryptoassets include cryptocurrencies and other tokens of tradeable value. Without loss of generality, we assume cryptocurrencies are native to their underlying blockchain, can be transacted directly, and are used to pay fees for transaction execution (*e.g.,* bitcoin and ether). For blockchains that allow developers to deploy custom decentralized applications, the applications might issue and manage the ownership of custom tokens. In the case of Ethereum, these tokens are often *ERC20* tokens [33], where *ERC20* is sometimes misunderstood to mean what the token represents; rather, *ERC20* is a technical standard about how token transactions are invoked.

What the token actually represents depends on the application, but major categories include the following. *(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 the company; and *(4) Collectable tokens*: the token itself is offered as a contemporary collector's item (*e.g., ERC721* [13]). Digital tokens of these types predate blockchains; for example, Linden Dollars, E-Gold, and URLs are arguably examples of (1), (2), and (4) respectively. Equities are almost entirely dematerialized (*e.g.,* paper stock certificates are rare)

[2] Latin: Let the buyer beware.

but operate closer to (2) with a central depository (*e.g.,* DTCC) and holding company (*e.g.,* Cede & Co.).

Tokens are issued to an initial set of owners through any mechanism of the issuer's choosing. A popular option is auctioning a set of tokens to the public in an "Initial Coin Offering" or ICO. This is intended to resemble the "Initial Public Offering" (IPO) of a firm's stock, but ICOs often lack any consumer protection or regulatory compliance. An ICO of an access token might raise capital for developing or improving the service that will use these tokens. Buyers seem to obtain such tokens to lock in the purchase price (*i.e.,* utility hedging) or because they believe they can sell for a profit (*i.e.,* speculation). Backed tokens are digital representations of an off-blockchain asset or liability. One example would be the recognition of a land deed on a blockchain in the form of a token. The blockchain must be invoked during the audit to validate ownership, the land itself is obviously not on the blockchain. The token issuer is trusted to ensure the token is a valid claim on what it represents.

Any action that results in a firm borrowing a cryptoasset results in an offsetting cryptoliability. For example, an exchange service that holds bitcoin or tokens on behalf of its clients has both an asset (the cryptoasset it holds 'in street name') and a liability (the obligation to repay it's client the cryptoasset on-demand). In the future, tokens could represent a debt instrument, like a bond, commercial paper, or repurchase agreement. In a recent pilot, a blockchain-based certificate of deposit was issued [2]. This creates an asset for the investors (Western Assets, Pfitzer, etc.) and a liability for the issuer (National Bank of Canada with J.P. Morgan).

It might seem esoteric for a real-world, profitable firm today to actually be holding a material amount of cryptoassets. Consider four illustrative examples of firms that have actually sought audits or regulatory exemptions from audits.[3] A mining firm will invest in specialized computing equipment and electricity to generate cryptocurrencies it will hold as assets. An exchange service will hold demand deposits of cryptocurrencies or tokens, as well as governmental currencies, and allow its users to trade them. An investment fund will hold a portfolio of cryptoassets (*e.g.,* TIQ101-CF is 50% bitcoin, 35% ether, 15% litecoin [1]) and sell shares to investors through a standard financial platform. Finally, a firm initiating a token sale will raise capital in cryptocurrencies, held as an asset, in return for tokens that are not generally liabilities (it may also reserve some tokens as an additional asset).

2.3 Presentation of Cryptoassets

A financial report will classify assets and liabilities according to categories established by the auditing standards adhered to in the firm's reporting country. This is the *American Generally Accepted Accounting Principles* in the United States, and the *International Financial Reporting Standards (IFRS)* in many other countries. Without loss of generality, we will consider IFRS.

[3] [Anonymized] Based on data provided to us by the financial regulator in the region where the authors work.

Cryptoassets. IFRS does not provide specific standards for how to account for cryptoassets, therefore, their presentation is based on existing standards that were not conceived with the nature of these assets in mind. This results in a presentation of cryptoassets that does not necessarily reflect the underlying economic reality of the assets at hand. For instance, an investment portfolio that holds a combination of bitcoin and Google stock for long-term capital appreciation purposes would report the bitcoin as an intangible asset [30] and the Google stock as a short-term investment. The Google stock would be presented at its fair market value and any gains and losses on this investment would be immediately reported as part of the net profit. The bitcoin, on the other hand, could either be presented at historical cost (what the company paid for the bitcoin) or revalued to its fair market value. If the bitcoin is reported at cost, any increases in value would not be recorded until the asset is sold (decreases in value below cost would be reported immediately). If the bitcoin is reported at fair market value, any increases in value would be reported in *Other Comprehensive Income*, a special category that does not fall into the net profit. This means that while the investment fund holds two investments, bitcoin and Google stock, both for long-term growth purposes, the current standards would not allow these investments to recorded on the same basis. This also means that increases in the value of bitcoin or other cryptoassets are not recorded as part of the net profit, which obfuscates a company's annual reported earnings and undermines their usefulness for investors.

ICOs. Currently, there is no guidance on how to account for proceeds raised during an ICO. During an ICO, a company issues its tokens in exchange for fiat or other cryptoassets, depending on the offering. However, the presentation of these funds will depend on what the ICO holder is entitled to receive in exchange for whatever they have given up.

If the tokens received represent a residual interest in the issuing firm, the tokens would be presented as part of share capital, like would be the case for traditional share issuances. However, most ICOs are not set out to give the holder an interest in the company as a whole, but rather represent an interest in a specific project. If the token holder is owed some type of obligation, like access to a marketplace or participation in application, then recognition of the funds received as a liability would be appropriate. Under rare cases, the proceeds could be reported as revenue if the funds received do not qualify as either share capital or represent some ongoing obligation towards the token holder.

Legal Status. One challenge for regulators can be determining whether or not a token is, in fact, a security for legal purposes and, therefore, whether or not regulation applies. Existing securities law is not clear on how to classify tokens and different classifications will apply to coins with different characteristics. To date, not a single ICO has been approved by the SEC [9]. In Canada, securities regularities have approved several ICOs through a regulatory fast-track program [27]. Despite a desire for Canadian regulators to foster innovation through fast-track

programs, securities regulators remain skeptical and have issued a notice cautioning investors of the risks in this sector [3].

2.4 Takeaway

Several parties, including auditors, management and regulators, have an interest in ensuring that entities in the crypto space can obtain an audit, namely to satisfy regulatory requirements in order to attract capital. However, issues surrounding the presentation and measurement of these items on the financial statements undermine the potential information content of these statements. In the rest of the paper, we will present key issues that currently are troubling auditors.

3 Key Issue: Existence of Assets

Auditors need to establish that assets and liabilities reported at a point in time are real and that the transactions reported over the year did, in fact, take place. The auditor must also ensure that the transactions were neither fraudulent nor illegal and had a legitimate business purpose.

Issue: Meta-information. Assets and liabilities that are transacted on a publicly readable blockchain record basic details, like times and values, but auditors require further information to validate the nature of a transaction. For example, assume an employee's salary is paid in bitcoin. Bitcoin's blockchain shows that a transaction occurred but it does not specify it as a salary; nor does it confirm basic details like the number of hours paid, if the nominal amount is BTC or a spot conversion from a governmental currency, and what deductions for tax or benefits were applied. Most importantly, it does not confirm the amount the employee was paid accurately reflects the number of hours worked at the authorized pay rate. Therefore, the company either requires a verbose secondary ledger to track these details or a decentralized application (DApp).

Issue: Off-Blockchain Transactions. Transactions may involve the exchange of cryptoassets for off-blockchain assets. For instance, a company may pay its supplier in bitcoin for a shipment of raw materials. Although the bitcoin is blockchain-native and that side of the transaction benefits from the consensus algorithm, the blockchain cannot verify that the right quantity or quality of raw materials were received in exchange for the consideration paid. Therefore, given that half of this transaction occurred off-blockchain, it would need to be audited like a traditional raw materials purchase.

Issue: 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, For example, Ethereum's miners branched the main blockchain to modify some past transactions to reverse a hacked DApp transactions [12]. The challenge of finality was an important design consideration in the Bank of Canada's Project Jasper [7] which sought to establish a distributed large value payment system. "Project Jasper was structured so that a transfer of [digital currency] was equivalent to a full and irrevocable transfer of the underlying claim on central bank deposits." Given that on the Ethereum blockchain, transactions could be reversed with consensus of the miners, the work around for Project Jasper was to implement a "design feature (which) relates to the issuance of (digital currency) and is therefore independent of the platforms upon which Jasper was built."

The issue of revocability is not uncommon for accountants. In many cases, sales agreements 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. Alternatively, auditors could establish a generally accepted threshold (for instance, 6 blocks is commonly used in Bitcoin) after which a transaction would be considered final.

Issue: 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 carried out during the year. If the auditor has a 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, this still raises the issue that the client may have entered into side-arrangements with related parties. While these challenges are magnified on a blockchain due to the pseudo-anonymity of this environment, the underlying challenge remains the same as it would in a traditional audit.

There is always the possibility that, for instance, 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. However, this situation is not unlike a traditional audit. The client may have unreported bank accounts at a different bank than their usual institution that the auditor would not know about.

Issue: Transaction Complexity. Bitcoin and Ethereum transact native currency according to established protocols, and Ethereum-based tokens gravitate toward standards as well. However nothing prevents DApps from transacting in complex

ways. For example, one proposed DApp for crowdfunding projects would allow stakeholders to split off into a smaller DApp, taking a share of the assets from the parent DApp with it [12]. Another example would be the Lightning Network [26] which is a second layer, off-blockchain payment network that was implemented for scaling bitcoin and enabling micro-transactions. Lightning transactions are more complex than simple bitcoin payments, involving payment channels routed through multiple parties that may not be finalized. While firms may complicate their transactions either for economic benefits in order to obfuscate the true nature of their transactions, the onus is on the firm under audit to operate in an auditable fashion. In other words, while it is the auditor's responsibility to design procedures to gain comfort over an entity's operations, it is the responsibility of management to implement controls and procedures to ensure that the entity is audit-ready. Therefore, some complex operations, while economically sound, might be avoided to ensure the audibility of operations.

Issue: Transaction Pointers. Blockchain transactions need to be uniquely identified to be pointed at by secondary financial records. Due to an implementation fault in Bitcoin, transactions broadcast with one identifier might end up in the blockchain with a different identifier. Known as transaction malleability, firms might erroneously conclude a transaction did not take place when in fact it did under an unexpected identifier [4]. Some firms went bankrupt when their automated system kept honouring refund requests from a malicious entity claiming the refunds were not going through [31,11]. The larger lesson here is that auditors cannot always safely abstract away low-level implementation details.

Takeaway. This section demonstrates 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 evidence to ascertain the occurrence of transactions. However, the auditor will continue to need to rely on external sources such as a verbose secondary ledger to validate the legitimacy and business purpose of those transactions.

4 Key Issue: Ownership

In addition to being satisfied with the existence of cryptoassets, auditors must be satisfied that the assets reported on the company's balance sheet do in fact belong to the company. For traditional assets, firms might store assets with a custodian. This does not eliminate the issue of ownership, it simply shifts the concern from the firm's audit to the audits of central custodians. Banks and organizations who provide custodial services are required to have robust internal controls over the safeguarding of assets in their care and provide audited report supporting the reliability of their controls.

Issue: Cryptographic keys. For most cryptoassets, the asset is considered owned by Alice if Alice possesses a private signing key that can be used to sign a transfer of the asset. Through decentralized apps, alternative notions of ownership

are possible to define, but this idea of a signing key is foundational and seen in bitcoin, ether, ERC20 tokens, etc. (not to mention earlier e-cash proposals dating back to the 1980s [29,6,20]). Thus demonstrating knowledge of this key is necessary (but not sufficient, as we will discuss shortly) to demonstrating ownership. The most direct cryptographic technique is to use a zero knowledge proof of knowledge of this private key, and 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.[4] 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 adds ethical complexities for the auditor.

We note that while this cryptographic proof is necessary, it is not sufficient. What it proves is 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 the physical visit and inventory check done when auditing retailers. Auditors mitigate this by arranging a common date for all audits of physical inventory, and similarly, cryptographic audits might be synchronized on a fixed schedule to prevent the same assets from being counted for different companies in different audits [10].

Issue: Design transparency. For cryptoassets that are native to a blockchain, like bitcoin or ether, ownership is implemented at the protocol level and has been vetted over the lifetime of the blockchain. However many assets are created and owned through decentralized apps. Coding standards, such as the ERC20 token standard in Ethereum, might be followed but this standard only specifies necessary ways of transacting the tokens, not the mechanics of what ownership means. These mechanics can become complicated. For example, the DAO [19] maintained ether and two types of tokens (DAO tokens and reward tokens) across four different internal accounts, and holders of DAO tokens could split off balances from these accounts into a new (two token-, four account-) DAO, in addition to certain types of withdrawals. Establishing ownership requires understanding the internal accounting of the applications maintaining the assets.

Issue: Self-custodianship. Cryptocurrency advocates point to its non-reliance on trusted third parties as the key to its appeal [15]. Thus, the use of a custodian for cryptoassets (or more specifically, the private keys controlling the assets) is controversial. The advantage of a custodian is that one firm can specialize in security rather than all end users. Self-custodianship of non-digital assets, such as diamonds for a jewelry retailer or cash for a currency exchange, is already a concern for financial auditors. Custodianship over cryptographic keys is a factor in other sectors, such as certificate authorities like Verisign or Symantec which

[4] A Schnorr Sigma-protocol with the challenge hashed in using Fiat-Shamir is exactly a Schnorr signature and closely related to an ECDSA signature.

maintain keys critical to HTTPS and DNSSEC [8]. To date, no blockchain custodian or exchange has been able to produce a report that supports the reliability of their internal controls in order to provide auditors with comfort over the sufficiency of their systems. Therefore, auditors cannot rely on the internal controls present at custodians to obtain comfort over the ownership assertion.

Takeaway. In order for auditors to validate ownership, they must rely on cryptographic proofs as a first step. However, 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.

5 Key Issue: Valuation

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. While fair valuation is important for establishing a firm's financial health, it is also important for auditors to use in determining what to focus on during the audit itself. The objective of an audit is to certify that the financial statements are free of material misstatement. This does not mean that the statements are free of all errors; it merely means that the statements are free of errors that could substantially change the opinion of an informed user.

Issue: Fair value. A significant obstacle for obtaining audited financial statements is the determination of a fair value for cryptoassets. For foreign currencies, firms value them at the closing rate on the transaction date, as reported by the Central Bank in which the firm operates. No universal central bank offers rates for currency-like cryptoassets. At the time of writing, one Fortune 500 financial firm, CME, offers a daily reference rate for bitcoin, but not other cryptocurrencies or cryptoassets. Without an authoritative reference rate, current market quotes may be considered. According to IFRS 13 [18], fair value is measured using the "principal market for the asset or liability; or in the absence of a principal market, in the most advantageous market for the asset or liability." The principal market for a cryptoasset may not be apparent. For instance, a company may purchase cryptoassets from several different exchanges or parties.

Issue: Bans. There regulatory rules for cryptoassets differ based on the jurisdiction; for instance, cryptoassets are absolutely banned in Algeria, Bolivia, and Pakistan (among others), and implicitly banned under investor protection rules in Colombia, Saudi Arabia, and China (among others) [34]. Also, there are banking limitations for companies dealing directly with cryptoassets in some other countries such as Canada, India, and Thailand. This limitation impacts the valuation of cryptoassets on hand. For instance, assume a company acquires a token

when it is legal to do so, and several months later, the government prohibits companies in that nation from holding that token. While this token may be traded in other parts of the world, the fair market value to its holder in the restrictive nation is arguably zero as their ability to use or sell the token is limited. Therefore, when determining the fair value of assets at hand, the auditor must consider the regulatory environment surrounding cryptoassets.

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

Issue: Geographical Variation. Because cryptoassets (*e.g.,* bitcoin) can be moved digitally without any geographic restrictions, it should be the case that any variation in cryptoasset prices across exchanges would be consumed by arbitrageurs. However, empirically this is not the case due to fees, settlement delays, and other frictions with exchange services [21]. Reporting standards do not account for geographic variation.

Issue: Fungibility. Blockchains generally preserve a full transaction record for each (division of a) cryptoasset. This may lead to price discrepancies between equal amounts of cryptoassets, where assets with clear provenance might be preferred to assets with long transaction records involving unknown entities and possible fraud, theft, or other issues that might legally encumber the current holder of the asset [23]. The materiality of a premium for "clean" cryptoassets is an open research question; some markets for fresh bitcoin were announced but never materialized.

Issue: Volatility. Assuming the valuation of cryptoassets can be made, it is important to consider how stable this valuation will be over time. The cryptoasset with the richest historical data is bitcoin and by any standard measure of volatility, bitcoin's current volatility exceeds most traded currencies and commodities. If a firm's balance sheet contains large unbalanced[5] cryptoassets or cryptoliabilities, price movements significantly impact its financial health and even its solvency. A comparable scenario is a financial firm holding exotic, volatile securities or derivatives—in these cases, auditors might "stress test" the firm's balance sheet under different valuations. Starting with bitcoin and moving to other cryptoassets, researchers should consider procedures for the "shelf life" of valuations and design realistic stress tests.

[5] An exchange service that holds bitcoin on behalf of its users will have the bitcoin listed as both an asset and a liability, thus they are balanced and price movements have no impact on their solvency.

Issue: Financial Projections. Financial statements are prepared under the assumption that the reporting entity will continue operating for at least 12 months after the balance sheet date. Auditors are required to perform procedures to verify the reasonableness of this assumption. For instance, the auditors could examine projections where the cryptoassets the firm holds increase or decrease in value, however, this may be difficult due to the high volatility of cryptoassets. Bitcoin, for instance, increased 10-fold over the last half of 2017. The problem is even more substantial for companies that hold other cryptocurrencies, altcoins, which may have thin markets and short histories upon which to compare financial projections. A remedy would be the disclosure of significant assumptions underlying these projections to satisfy financial statement users of the company's projected financial health.

Takeaway. While the valuation of cryptoassets with large trading volumes like bitcoin and ether would be fairly straightforward by referring to values in an active market, the valuation of coins with low liquidity may be more difficult. However, by using financial modelling using different assumptions for volatility, this challenge is not insurmountable.

6 Other Auditing Issues

Issue: Technical Literacy of Accounting Professionals. 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 technological know-how regarding how to effectively carry out these audits. The risk of taking on such an audit (referred to as *audit risk*) is too high, especially given numerous recent frauds in this sector. For instance, PinCoin raised over $660M in an ICO before the management team vanished [5]. However, this issue can be overcome by engaging multidisciplinary teams that can leverage the business knowledge of auditors with the technical know-how of computer scientists. These types of teams will also provide auditors with increased awareness of security threats.

Issue: Financial Literacy of Technology Professionals. While auditors must learn more about the technology, managers of companies in the blockchain space must also learn about the internal controls required to safeguard against errors, misappropriation of assets and fraud. Given that financial statements are ultimately the responsibility of management and that senior management must certify the internal controls as part of the financial statement disclosures, managers have an incentive to implement a control environment that promotes a strong tone at the top, ethical conduct, and oversight of the financial reporting function.

Issue: Internal Controls. It is necessary for a firm to be able to demonstrate the existence and ownership of its crypto-assets, however it must further demonstrate that it has adequate procedures in place to prevent or detect fraud and theft. Consider a firm holding DAO tokens. Internally, it must ensure proper controls over the signing keys these DAO tokens are assigned to. External to the firm, the DAO application maintaining these tokens on Ethereum's blockchain must itself be secure (which in the case of the DAO, it was not [12]). Auditing internal procedures over cryptographic keys is not unprecedented—maintaining certificate authority keys for HTTPS is critical to some security firm's financial prospects (a security breach at one firm, *DigiNotar* led to its bankruptcy [35]). Symantec's self-custodianship over these keys involves elaborate security ceremonies whenever they are required [16].

Issue: Materiality. Materiality is considered to be any value that is significant enough to have an impact on the user's decision-making, and GAAS dictates that materiality for profitable entities be set at 5% of pre-tax income. This means that, in aggregate, the sum of identified and extrapolated errors identified by auditors during their audit cannot exceed 5% of pre-tax income for a clean opinion to be issued. However, companies may manipulate their selection of accounting policies to influence their net income in order to increase materiality. This means auditors would only look at items over a higher threshold, leaving smaller amounts subject to a lower level of scrutiny and greater opportunity for fraud or error. However, this issue is possible for all clients and therefore auditors would be aware of and design procedures to address this risk for all mandates.

Issue: Forks and Airdrops. Existing accounting standards do not contemplate how to account for non-reciprocal transfers of assets like in the case of forks or airdrops. For example, in August 2017, when a hard fork created Bitcoin Cash from bitcoin, holders of bitcoin had two types of assets on hand. Bitcoin Cash was not paid for but resulted from a split between the two cryptocurrencies. However, if existing accounting standards require the measurement of transactions at historical cost (what was paid for the assets), then recipients of Bitcoin Cash would report this new asset on their books at a value of $0. Certainly, this does not represent the true value acquired through the fork. Therefore, auditors must address the issue of an accounting standard that does not contemplate how to measure the value of cryptoassets when considering whether the financial statements they are reporting on are accurate in all substantial respects. More commonly for ERC20 tokens on Ethereum, the recipient of the tokens don't have the option to reject the deposits nor would get notified of the new tokens received, which could result in issues with completeness.

Issue: Detection of Fraud. An auditor conducting an audit in accordance with GAAS is responsible for obtaining reasonable assurance that the financial statements taken as a whole are free from material misstatement, whether caused by fraud or error. Owing to the inherent limitations of an audit, there is an unavoidable risk that some material misstatements or fraud may not be detected,

even though the audit is properly planned and performed in accordance with GAAS. Due to the complex and rapidly changing nature of this sector, auditors are especially weary of fraud risk in this area. Not all frauds that occur this space are new kinds of fraud. For instance, Ponzi schemes have existed since they were perfected by Charles Ponzi in the early twentieth century [25]. In 2017, OneCoin was found to have raised over $350M of funds from investors for an ICO that was a Ponzi scheme [22]. Stories like this [32] only reinforce the perception in the auditing community of the dangers of operating in this space. However, auditors can protect themselves by ensuring that they only work with reputable clients. Managers can demonstrate their commitment to sound business practices by adopting controls that ensure KYC and AML rules are adhered to.

7 Discussion

Overall, this paper has demonstrated that, in comparison to traditional audits, audits of clients that hold material amounts of cryptoassets are complex but not impossible. For instance, while current accounting standards result in the presentation of an accounting fiction that is not always linked to the underlying use of crypto, adequate note disclosure can provide financial statement users with sufficient information in order to understand the underlying crypto operations.

From our discussions with practitioners, the three most cited stumbling blocks to providing an audit opinion were existence, valuation and ownership. 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 alt-coins 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 right to be cautious to enter a new sector where clients not be 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. Alternatively, accounting firms can provide advisory services to clients in anticipation of going public in order to ensure that these clients implement robust internal controls to support their financial reporting function.

8 Concluding Remarks

Blockchain technology provides novel, non-trivial issues for financial auditors, however these issues are in no way insurmountable and in many ways parallel challenging conditions seen in other sectors. We conclude that many entities in this space are auditable. We also wish to note that the firm is ultimately the entity seeking the audit, auditors are not seeking the firm, and therefore the onus to ensure financial disclosures are readably auditable by non-specialists auditors really lies with the firm itself. For example, a firm might not want to use a custodian for cryptocurrencies for philosophical reasons, and overtime, the technical literacy of auditors will advance to where self-custodianship may be commonplace, however firms seeking audits in the short-term may need to invest time and resources into internal controls, financial reporting mechanisms, and third parties to enable less friction for auditors.

Acknowledgements

The authors thank the Autorité des Marchés Financiers (AMF) for sponsoring this research through the Education and Good Governance Fund (EGGF). Additionally the first author acknowledges funding from SSHRC, the second author from the Manulife Professorship in Financial Planning at JMSB, and the fourth author from an NSERC Discovery Grant. The information, opinions and advice presented in this paper are the sole responsibility of the authors.

References

1. 3iQ global cryptoasset fund. Online, 2018.
2. National bank of canada (nbc) and j.p. morgan test blockchain technology with nbc debt issuance in the us financial markets. National Bank of Canada, 2018.
3. C. S. Administrators. Csa staff notice 46-307 cryptocurrency offerings. `http://www.osc.gov.on.ca/en/SecuritiesLaw_csa_20170824_cryptocurrency-offerings.htm`, 2017. Accessed: 2018-09-20.
4. M. Andrychowicz, S. Dziembowski, D. Malinowski, and Ł. Mazurek. On the malleability of bitcoin transactions. In *FC*, 2015.
5. J. Biggs. Exit scammers run off with $660 million in ico earnings. `https://techcrunch.com/2018/04/13/exit-scammers-run-off-with-660-million-in-ico-earnings/`, 2018. Accessed: 2018-09-20.
6. M. Blaze, J. Feigenbaum, and M. Strauss. Compliance checking in the policymaker trust management system. In *FC*, 1998.
7. J. Chapman, R. Garratt, S. Hendry, A. McCormack, and W. McMahon. Project jasper: are distributed wholesale payment systems feasible yet? Technical report, Bank of Canada, 2017.
8. J. Clark and P. C. van Oorschot. Sok: Ssl and https: Revisiting past challenges and evaluating certificate trust model enhancements. In *IEEE SSP*, pages 511–525. IEEE, 2013.
9. C. J. Clayton. Statement on cryptocurrencies and initial coin offerings. `https://www.sec.gov/news/public-statement/statement-clayton-2017-12-11`, 2017. Accessed: 2018-09-20.

10. G. G. Dagher, B. Bünz, J. Bonneau, J. Clark, and D. Boneh. Provisions: Privacy-preserving proofs of solvency for bitcoin exchanges. In *CCS*, pages 720–731. ACM, 2015.
11. C. Decker and R. Wattenhofer. Bitcoin transaction malleability and mtgox. In *ESORICS*, pages 313–326. Springer, 2014.
12. Q. DuPont. Experiments in algorithmic governance: A history and ethnography of "the dao," a failed decentralized autonomous organization. In *Bitcoin and Beyond*, pages 157–177. Routledge, 2017.
13. W. Entriken, D. Shirley, J. Evans, and N. Sachs. Erc-721 non-fungible token standard. `https://github.com/ethereum/EIPs/blob/master/EIPS/eip-721.md`, 2018. Accessed: 2018-08-31.
14. FinancialTimes. Deloitte in $150m settlement over mortgage broker collapse. `https://www.ft.com/content/692cda3e-1ce1-11e8-aaca-4574d7dabfb6`, 2018. Accessed: 2018-09-20.
15. X. Gao, G. D. Clark, and J. Lindqvist. Of two minds, multiple addresses, and one ledger: Characterizing opinions, knowledge, and perceptions of bitcoin across users and non-users. In *CHI*, CHI '16, pages 1656–1668, New York, NY, USA, 2016. ACM.
16. D. Goodin. A fort knox for web crypto keys: Inside symantec's ssl certificate vault. *Ars Technica*, 2012.
17. I. Grigg. Financial cryptography in 7 layers. In *FC*, pages 332–348. Springer, 2000.
18. I. IFRS. 13: Fair value measurement, 2011.
19. C. Jentzsch. Decentralized autonomous organization to automate governance, 2016.
20. R. Kohlas and U. Maurer. Reasoning about Public-Key Certification: On Bindings between Entities and Public Keys. In *FC*, page 18, 1999.
21. A. Kroeger and A. Sarkar. The law of one bitcoin price? Federal Reserve Bank of New York, 2017.
22. D. Z. MORRIS. The rise of cryptocurrency ponzi schemes. `https://www.theatlantic.com/technology/archive/2017/05/cryptocurrency-ponzi-schemes/528624/`, 2017. Accessed: 2018-09-20.
23. M. Möser, R. Böhme, and D. Breuker. Towards risk scoring of bitcoin transactions. In *FC*, pages 16–32. Springer, 2014.
24. N. Narula, W. Vasquez, and M. Virza. zkledger: Privacy-preserving auditing for distributed ledgers. In *USENIX NSDI*, 2018.
25. C. Ponzi. *The Rise of Mr. Ponzi*. Inkwell Publishers, 2001.
26. J. Poon and T. Dryja. The bitcoin lightning network: Scalable off-chain instant payments, 2016.
27. C. R. Sandbox. In the matter of impak finance inc. `http://www.osc.gov.on.ca/en/SecuritiesLaw_ord_20170824_212_impak.htm`, 2018. Accessed: 2018-09-20.
28. J. F. Strother. The establishment of generally accepted accounting principles and generally accepted auditing standards. *Vand. L. Rev.*, 28:201, 1975.
29. P. P. Swire. The uses and limits of financial cryptography: A law professor's perspective. In *FC*, page 20, 1999.
30. R. C. G. Thornton. Adviser alert - ifrs viewpoint - accounting for cryptocurrencies - the basics. `https://cdn.rcgt.com/app/uploads/2018/06/adviser-alert_ifrs-viewpoint_accounting-for-cryptocurrencies-the-basics-protected.pdf`, 2018. Accessed: 2018-09-20.
31. L. J. Trautman. Virtual currencies; bitcoin & what now after liberty reserve, silk road, and mt. gox? *Richmond Journal of Law and Technology*, 20, No. 4, 2014.

32. M. Vasek and T. Moore. Analyzing the bitcoin ponzi scheme ecosystem. In *FC*, 2015.
33. F. Vogelsteller and V. Buterin. Erc-20 token standard. `https://github.com/ethereum/EIPs/blob/master/EIPS/eip-20.md`, 2015. Accessed: 2018-08-31.
34. Wikipedia. Legality of bitcoin by country or territory. `https://en.wikipedia.org/wiki/Legality_of_bitcoin_by_country_or_territory`, 2018. Accessed: 2018-09-20.
35. K. Zetter. Diginotar files for bankruptcy in wake of devastating hack. *Wired*, 2011.