A first look at auditing in a Blockchain world

No Author Given

No Institute Given

Abstract. The emergence of cryptocurrencies, like Bitcoin, and blockchain technologies, like Ethereum, have matured to a point that commercial firms operating in this space have begun to seek financial audits. 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

In certain common circumstances, firms operating in the blockchain space will require their financial statements to be audited by an external firm. 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 lack experience in this sector and therefore are 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 on 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 of companies deploying blockchain technologies, 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 were established, we vetted our results through informal discussions with over a dozen individuals working in the field, including at the Big Four 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 which we initially missed.

Relevance. Our work can viewed as a case study of cryptographers working with an outside profession for addressing a real-world problem. The result is not a new protocol but a two-way knowledge transfer between professions that we hope is interesting to this audience. While displacing auditors is occasionally a target of cryptographers [9,5], auditing itself is also occasionally studied directly 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 firms income/profits, expenses/losses, 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. In addition to an 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 seek 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 a market where auditors are reluctant or audits are expensive, firms can use their ability to obtain audited financial statements as a barrier against new entrants to the blockchain sector.

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 [8].

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* is an important 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 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 firms balance sheet which lists assets and liabilities. We use the term *cryptoasset* and *cryptoliability* to refer to items whose value are 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. Bitcoin and Ether are examples. For blockchains that allow developers to deploy custom decentralized apps, the apps might issue and manage the ownership of a custom tokens. In the case of Ethereum, these tokens are often ERC20 tokens, where ERC20 is sometimes misunderstood to mean what the token represents; rather, ERC20 is a technical standard about how token transactions are invoked.

What a token represents varies across applications but includes at least of the following major categories. (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 collectors item. Digital tokens of these types predate blockchains; for example, (1) Linden dollars, (2) E-Gold, and (4) URLs are arguably examples. Equities (3) are almost entirely dematerialized (*e.g.,* paper stock certificates are rare) but operate closer to (2) with a central depository.

Tokens and cryptocurrencies are issued to an initial set of owners through any mechanism of the issuers 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 firms 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 obtain such tokens to lock in the purchase price (hedging) or for speculation.

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 its possession) and a liability (the obligation to repay its clients). 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. 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).

Bitcoin and Ether are native to their blockchains. Other assets or liabilities 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.

To illustrate how a firm might come to possess a cryptoasset, consider four examples of firms that have actually sought audits or regulatory exemptions from audits[1]. 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 [c]) 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 (American Generally Accepted Accounting Principles in the United States and International Financial Reporting Standards (IFRS) in many other countries). The following discussion will apply IFRS although the considerations under US GAAP are similar.

Cryptoassets. IFRS do not provide specific standards for how to account for cryptoassets therefore their presentation is based on existing standards that were not

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

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 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 net profit.

The Bitcoin, on the other hand, would be presented as an intangible asset. This investment 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 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 value of Bitcoin or other cryptoassets are not recorded as part of 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 holder is owed some type of obligation, like access to a marketplace or participation in an, 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 ICO holder. However, we expect these instances to be fairly rare as it is unlikely that an investor would contribute to an ICO and not expect something of value in return.

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 [4]. In Canada, securities regularities have approved several ICOs through a regulatory fast-track program.

In Quebec, the provincial regulator approved the ICO of Impak Finance. In doing so, the regulator labeled the ICO's token, *ImpakCoin*, as a security and waived several filing requirements, including the need for a prospectus, to facilitate the launch. 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 [1].

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.

The following sections will present key issues that currently are troubling auditors and provide solutions or directions for future research.

3 Key Issue: Existence of Assets and Occurence of Transactions

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). This issue also underscores how, despite the immutability of the blockchain, the auditor remains necessary to validate the legitimacy of transactions.

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.

Given that financial statements report the summary of a company's activities at a point in time or over the course of a certain period, the cutoff of transactions is also an important consideration. For instance, in the example above, if the auditor is verifying a company's transactions for the year ended December 31, 2017, they must ensure that the Bitcoin was paid and the raw material was received before the end of the year to record the purchase in the 2017 fiscal year. Although the blockchain confirms the date the Bitcoin was paid, it cannot guarantee when the merchandise was received as this happens off-blockchain. Therefore, the cutoff of the transaction would be subject to traditional auditing methods.

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 [7]. The challenge of finality was an important design consideration in the Bank of Canada's Project Jasper which sought to establish a Distributed Wholesale Payment Systems. “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 can be reversed, 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.” [3].

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 much estimate the percentage 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, number of days) 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 possess other, unreported keys, or have entered into side-arrangements with related parties. This risk is also present in traditional audits. While these challenges are magnified on a blockchain is magnified 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 [7]. Another example would be the Lightning Network poon2016bitcoin which is second layer, off blockchain payment network that was implemented for scaling Bitcoin to increase throughput. The Lightning Network is more complex than simple Bitcoin payments and involves payment channels and routings.

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, may 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 broadcasted with one identifier might end up in the blockchain with a different identifier, which could lead a firm to conclude a transaction did not take place when in fact it did, but under an unexpected identifier [2] Some firms went bankrupt when their automated system kept honouring refund requests from a malicious entity claiming the refunds were not going through [10,6]. The larger lesson here is that auditors cannot always safely abstract away low level implementation details.

Issue: Occurrence. In order to validate that cryptoasset transactions actually took place during the year, auditors will look to reproduce the transactions carried out. By obtaining a listing of the client's cryptographic keys, the blockchain can provide a complete history of the transactions that occurred during the year. Due to the immutable nature of the blockchain, the auditor can be assured that the transaction did take place as described. However, the auditor will still need to validate meta-information surrounding the transaction (see above) to validate the transaction's reasonability.

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 companys 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 firms 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). Thus demonstrating knowledge of this key is necessary (but not sufficient, as we will discuss shortly) to demonstrating ownership. The most direct 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[2]. 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 (and used in at least one occasion [cite]). 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.

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

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 audit, which will in this case involve a physical visit and inventory check by the auditor. 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 [5].

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 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 key to its appeal [cite: CHI paper]. 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 it might more quickly specialize in security than end users, and this is certainly true for some users [cite: MIT]. 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. Further, custodianship over cryptographic keys is a financial factor in other sectors, such as certificate authorities like Versign or Symantec which maintain keys critical to HTTPS and DNSSEC [cite]. 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.

References

1. 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.

2. M. Andrychowicz, S. Dziembowski, D. Malinowski, and Ł. Mazurek. On the malleability of bitcoin transactions. In *International Conference on Financial Cryptography and Data Security*, pages 1–18. Springer, 2015.
3. J. Chapman, R. Garratt, S. Hendry, A. McCormack, and W. McMahon. Project jasper: are distributed wholesale payment systems feasible yet? *Financial System*, page 59, 2017.
4. 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.
5. G. G. Dagher, B. Bünz, J. Bonneau, J. Clark, and D. Boneh. Provisions: Privacy-preserving proofs of solvency for bitcoin exchanges. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, pages 720–731. ACM, 2015.
6. C. Decker and R. Wattenhofer. Bitcoin transaction malleability and mtgox. In *European Symposium on Research in Computer Security*, pages 313–326. Springer, 2014.
7. 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.
8. FinancialTimes. Deloitte in $150m settlement over mortgage broker collapse. `https://www.ft.com/content/692cda3e-1ce1-11e8-aaca-4574d7dabfb6`, 2018. Accessed: 2018-09-20.
9. N. Narula, W. Vasquez, and M. Virza. zkledger Privacy-preserving auditing for distributed ledgers. *auditing*, 17(34):42, 2018.
10. 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.