The Financial Auditing of Distributed Ledgers, Blockchain and Cryptocurrencies

Journal of Financial Transformations

Daniel Broby and Greig Paul

daniel.broby@strath.ac.uk

greig.paul@strath.ac.uk

Abstract

The internet and digital transfer of money is set to fundamentally change the way financial audits are conducted. This paper critically assesses the way that such assets are currently audited when stored in distributed ledgers, transmitted via a blockchain or whose value is stored in crypto rather than sovereign currency form. In it, we identify the self-verifying nature of such financial data which negates the need for traditional audit methods. Despite the promise of such methods, we highlight the many weaknesses that still exist in the blockchain and how these presents issues for verification. We address distributed transaction and custody records and how these present auditing challenges. We suggest how auditors can use smart contracts to address these and at the same time provide arbitration and oversight. Our contribution is to propose a protocol to audit the movement of blockchain transmitted funds in order to make them more robust going forward.

Introduction

An audit is an official examination and verification of financial accounts and records and is summarised well in (Whittington & Pany, 2012). It can be conducted either internally and/or externally by a qualified third party. The principles of modern auditing, as first laid out in (Brink, 1988 (Reprint 1941)) revolve around a statement of responsibilities, a common body of knowledge and standards alongside a code of conduct. These collectively encompasses the pre and post examination of a corporation's financial revenues and disbursements, a review of its soundness, its effectiveness and its compliance with both internal and external controls. We argue the application of these in a corporate setting needs to adjust and evolve to take into account the distributed nature of financial information stored on distributed ledgers, blockchain and/or in cryptocurrencies. All the current norms are being challenged by the advent of these three new modes of digital asset storage and transmission. This paper investigates these phenomena and addresses the problem of how financial audits have to adapt to reflect this.

The International Standards of Auditing are captured in ((IFAC), 2009). These were devised by financial practitioners, not experts in distributed technology and software protocols. (Francis, 2004) summarised the scholarly view of auditing, namely that it is inexpensive, informative, and positively associated with earnings quality but impacted by the legislative framework. Despite this positive assessment, audit risk exists, and is intensified when technological complexity is taken into account. (Dusenbury, Reimers, & Wheeler, 2000) defines such risk as coming from a field auditor not being able to detect material misrepresentations in financial statements. In a distributed online world, such risk is amplified.

The new audit challenges herald from peer to peer networking, as explained by (Koshy et al, 2014). Technology has allowed corporations to develop self-auditing systems. Blockchain, the most widely used, as first introduced by (Nakamoto, 2008). Its use presents auditing with unique challenges due to its distributed nature. Its properties, immutability and verification, are concepts familiar to auditors and we shall expand on them further.

In order to understand the auditing challenges, we offer a brief explanation of blockchain. Each block in a blockchain may contain one or more transactions, with the block header referencing the contents of the previous block in the chain. This ensures that the content of a block cannot be tampered with after its creation, without other parties being able to detect and reject this manipulation. The chain therefore acts as a distributed ledger, where each party holds and validates it on an ongoing basis. Indeed, the processing of each transaction is, to some extent, an audit in itself, since every participant in the network ensures that all credits are a result of permitted debits. As a result, (Rezaee & Reinstein, 1998) argue that electronic data and the Internet *"signal the end of the traditional audit."* That said, the need for corporate audits for financial purposes is self-evident and we argue that it is just the nature of the audit that must change.

Transaction Malleability

The primary function of financial reporting, according to (Rogers, Marsh, & Ethridge, 2004), is the recognition of revenue, safeguarding of cash, recognition of expense and control over procurements. A major challenge to this process, and hence for auditors in a blockchain world, is that of transaction malleability. This is where a transaction can be changed after it has occurred. The issue was addressed by (Andrychowicz, Dziembowski, Malinowski, & Mazurek, 2015). They showed that the issue arises due to the implementation of the transaction ID algorithm within bitcoin. Malleability makes it possible for a party relaying a transaction (such as a miner or other relay) to modify the transaction in a trivial manner, such that the contents of the transaction remains materially unchanged (with the transaction signature remaining valid). The transaction ID (which is a hash of the transaction data itself) is altered to differ from that originally produced by the party generating the transaction [2].

The malleability of bitcoin transactions can have two potential impacts when auditing a blockchain. Firstly, malleability makes it possible for a transaction to be generated under one ID, yet broadcast and incorporated into the blockchain under another transaction ID. This naturally presents a challenge for auditors, since typically a transaction ID would be considered as a unique identifier. If malleable blockchain payments were frequent occurrences, the reconciliation of payment authorisations from sender against blockchain entries may be difficult.

As a consequence of the above, there is potential for double-payment fraud; something which auditors have to be vigilant about. For example, a participant in the blockchain, particularly one using simple payment verification (SPV) rather than downloading and monitoring the full blockchain, could be tricked into issuing payment twice, with a party claiming the payment did not go through, showing the lack of existence of a transaction under the ID generated by the sender. If the sender does not verify their previous transactions properly, checking the blockchain for all recent transactions, they may not see the transaction appear under an additional transaction ID, resulting in a double payment being

made. Accounting for such double payments in an audit may be a challenge, particularly where auditors are not familiar with the technical constraints and restrictions in the implementational quirks of blockchains, such as Bitcoin in this case.

DAO type Issues

The world of digital money not only covers transmission and storage but also smart contracts and the concept of a DAO (digital autonomous organisation) has been floated. A DAO is designed to resemble in many ways a conventional corporation, with its own rules and regulations, although it does not inherently exist as a legal person within any given jurisdiction. The issue was covered by (Ringelstein & Staab, ICWS 2009.). This clearly presents an issue for an audit which is focused on a legal entity. The original DAO within Ethereum was built as a form of organisation, whereby those who "bought into" the DAO became stakeholders. Those holding tokens issued from the original sale were then viewed as shareholders, able to vote on various different kinds of proposal. The rules of the organisation (themselves able to be altered through a voting process) would then be used to vote on proposals for the organisations funds to be spent. In essence, a DAO presents a form of cryptographically enforceable articles of association; DAO-controlled funds cannot be spent without the cryptographic agreement of stakeholders, per the rules defined and voted on by stakeholders.

Various audit challenges are posed by DAO-type structures, not least that of jurisdiction of the entity, and how judgements could be enforced against it. Since the DAO in itself is not a legal entity, its position in law is unclear. In addition, were a judgement to be issued against a DAO, the means of enforcement against it would also be unclear; without agreement of a majority of shareholders, or whatever is defined in the DAO's smart contract rules, it would not be possible for funds to be taken from the organisation. Therefore we recommend that assets held within a DAO should be carefully considered, in particular around the requirements needing satisfied for them to be accessed or spent.

Long-term blockchain forks

Another challenge to the soundness of an audit is the potential for long term blockchain forks. For a comparison of different forks see (Gervais, et al., 2016, October.). A fork is formed when a blockchain has two potential paths forward, either with regard to its transaction history or a new rule. While transient blockchain forks are a fairly regular occurrence, where more than one valid block is produced as the next block in close time proximity, there is another scenario, potentially of concern to auditors. In the event of a blockchain (itself inherently decentralised with no one party in charge) sees a breakdown in relations within portions of the community, a long-term fork is a potential outcome. In this scenario, two or more distinct groups each recognise their own version of the blockchain as the correct chain, and refuse to recognise the other's. This would typically occur as a result of network enforcement of rules. Examples of this may include alterations to validity requirements on transactions, or of blocks. For example, the Bitcoin maximum block size is 1 megabyte, and raising this would require a fork to the blockchain, since larger blocks would be viewed as invalid by those following the older rules.

Auditors need to be cognisant of situations where a community formed around the concept of larger blocks at a given raised limit (say 2 megabytes for the sake of example). In such a scenario one group of miners may decide to mine and produce larger blocks, while others reject these blocks and continue

to produce their own blocks with a maximum size of 1 megabyte. At this point, a divergence would occur. Transactions taking place prior to the fork would be present on both chains. Transactions taking place after the fork may appear on one, or both, chains. To further complicate matters, blocks mined on one chain may also be valid on another, depending on the nature of the fork. For example, in the scenario of a block size increase, blocks mined while adhering to the 1 MB size limit would presumably also be valid on the fork permitting larger blocks, provided they were mined with the correct parent block header hash, thus advancing the chain correctly.

Short-term blockchain forks

Short-term blockchain forks are a somewhat more regular occurrence. As a result, they present auditors with more frequent issues. In Bitcoin, this happens in the period between blocks being produced (the mean inter-block period is regularly recalibrated through block difficulty adjustments to be 10 minutes). Where two miners near-simultaneously discover a valid solution for the next block, one block will become the successor block, and the other will become an orphan block. The block which is propagated to the majority of nodes first will most likely become the valid successor, since they will attempt to build upon that block, and more parties attempting to mine upon it means that this block is most likely to have a successor. Once one side of the chain becomes longer, one block will orphan, with its transactions returned to the pool of pending transactions, and the block recognised as invalid, due to a longer chain existing without incorporating that block.

The risk of short-term forks, referred to as orphan blocks, is minimal, since it occurs regularly in the Bitcoin blockchain (around once per day is not uncommon), and participants can handle the scenario elegantly. For an auditor however, the potential for orphan blocks makes it important to ensure that the audit only covers blocks which have sufficient proof of work upon themselves to make any future re-arrangement orphaning those blocks infeasible. One significant factor to note is that Bitcoin will accept any longer chain at any point in future, if such a chain exists. Therefore, there is no time period beyond which it can be guaranteed that no alternative longer chain will emerge. At any time, a longer chain being announced to the network would result in the adoption of the longer chain. While past transactions could then be re-broadcast to the network for inclusion, since they were already signed, this introduces the potential for double-spends to occur, whereby the (previously hidden) chain incorporated a transaction to spend funds which were spent in the (broadcast) chain. This would result in the recipient of the broadcast transaction to lose the received funds in the subsequent reorganisation to accept the longer (previously hidden) chain.

Financial custody

Custody and distributed ledgers need to be audited. Traditional audit inspects the custodial assets held by a legal entity. The role of custodians in the context of distributed ledgers will clearly evolve and as such presents auditors with new challenges. As it currently stands, market infrastructure currently relies on a hierarchy of custodians. A number of legal issues arise from such intermediation. Neoclassical economic theory suggests that we don't know enough about this infrastructure. Financial intermediation chains have contractual ring-fencing from the responsibility of the sub-custodians in this hierarchy. There is, in effect a behavioural problem at the investor level because of the different bargaining power between the institutional and the public market. The

explanation for this is that the public investors are time poor, have a bias against long term risk, have tax issues, and have a tendency to believe that the future is like the past.

Blockchain technology provides the ability for money to be disintermediated and connected to a central asset ledger via the Internet. Current investors in the public market, who would most benefit from this, don't have the bargaining power to fund such developments. As a result, institutions still have the upper hand. There is a role for auditors in this respect. We need to be aware that even such things as cryptocurrencies involve intermediation. Where the cryptography is provided centrally, the wallet holder effectively being the intermediary.

The role of a central third party is not just keeping a ledger, it is in ensuring they are valid. An auditor has to verify this. In other words, are the distributed ledgers reliable and how do they link to reality. Blockchain explorers can be adapted to provide tools to make it easier to achieve this. Current custody platforms such as Euroclear can clearly improve by adopting and adapting their technology but would be at risk of undermining their current business model.

In addition to custody and ownership, the detail behind auditing includes the timestamping of the blockchain, its validity and is robustness. In the distributed world, there are in fact multiple blockchains, not a single immutable record as the public perceives. As such, a traditional audit of a false fork only provides a detailed record of the records. We return to the latter. In the case of closed, permissioned blockchains, what is required is an audit of who permissions the permissioned blockchain. In other words, the audit process should go to the creation of a chain, not give insights into a snapshot in time. At present, reconciliation only occurs at the individual custodian level.

Challenges for Audit

There are many challenges in auditing financial data within a blochchain. One of these is accounting year ends. These are reported at a static point in time. In a blockchain, however, the most recent recent transactions cannot be guaranteed to be irreversible at a given point in time; their irreversibility is a property of the quantity of mining work carried out on top of those transactions. Each subsequent block mined beyond a given block is referred to as a "confirmation", signifying that other miners have agreed that this block is valid, following the necessary rules, and containing only validly signed transactions. We highlight other more technological issues next.

Multi-location audit risk

The Internet is cross jurisdictional. This audit issue is addressed by Statement of Auditing Standards (SAS) No 107. This states that an auditor facing such jurisdiction issues has to take into account the nature of the assets and transactions, the centralization of records, the effectiveness of the control environment, the frequency of monitoring and the materiality of location. That said, the auditing standards incorporate digital storage of value when they were first drafted.

The issue of multi-location was highlighted in July 2017 when a French court gave Alphabet Inc (Google's parent company) a reprieve from a 1.11bn-euro ($1.27bn) tax bill. The Paris administrative

court noted that its subsidiary, Google Ireland Limited, didnt have a “permanent establishment” in France. The audit trail, in this instance, being critical in determining jurisdiction.

The need for better auditing standards for digital assets is a fairly new issue. There are a lot of participants in the distributed ledger ecosystem who want credibility and a lot who want reassurance. Clearly, some things are easier to audit than others. The auditing industry needs to define the level of that reassurance. If you go into any form of distributed ledger environment, the cost of audit and regulation currently outweigh the development costs. The current ledger audits are done by the data departments of accounting firms, there being no dedicated audit function that oversees the technological aspect of financial audits.

Current audit practice revolves around accountants entering an organisation as external auditors, and carrying out a process of verification of the accounts. With the rise of blockchain, and the potential for non-trivial quantities of assets to be held within, or transferred through, a blockchain, auditors will increasingly find it difficult to ignore these ledgers. The blockchain gives rise to a distributed set of ledgers which bring with them the sort of multi-location audit risks identified by (Allen, Loebbecke, & Sorensen, 1998) and (Hegazy & Nahass, 2012).

Auditing permissioned ledgers involves interrogation of the system. The technology can be audited in real time, but auditing requires an understanding of the context. When you look at a distributed ledger from the perspective of ownership, the coding of a transaction might not be as aligned to the underlying ownership as it exists in the physical world. In a digital context, ownership can also be broken down into describing ownership, protecting ownership, storing ownership, preparing ledgers, the addition of transactions to a ledger, and deciding which ledgers are deemed true and accurate.

Issues with Self Verification

While the design properties of a blockchain being immutable and self-verifying are beneficial to audit, the robustness and reality need to be explored by the auditor. In this respect, (Buyya, et al., 2008) illustrated how blockchains can be used with cryptographic hashes within decentralized networks. Transactions on a bitcoin-like blockchain are inherently self-verifying. Each transaction is digitally signed, to prove its authenticity, and based upon the outputs of a previous transaction. A transaction can therefore be checked by any interested party with access to the blockchain, to ensure that the signature on it is valid, and that it only spends available and unspent funds, satisfying the requirements of the ledger rules.

For example, if party A transfers an asset to party B over a blockchain using this model, a transaction record will be created, whereby party A takes one or more received transactions which they have not yet spent, and specifies party B as the recipient. Any surplus funds can be returned back to party A. The resulting transaction must then be signed by the private key corresponding to each incoming transaction which is used within the transaction. Any party with access to an address' public key is able to verify if a signature was issued by the corresponding private key holder for that address.

We argue that it is desirable to audit only transactions contained within blocks with a number of confirmations. This indicates when the likelihood of reversal is minimal due to a fork having emerged in the blockchain. It is difficult to quantify the number of confirmations necessary. That said, we suggest that 6 confirmations is usually sufficient for most large transactions, which would correspond to around a 60 minute delay after a transaction was featured in a block. Despite this, in times of adverse conditions on the blockchain, such as large numbers of mining nodes not properly validating blocks, users have been advised to wait for considerably higher numbers of confirmations. In one case, this was as high as 36 confirmations, reflecting a 6-hour delay [1].

Ability to transact silently

Audit helps to detect fraud. Within blockchain-based crypto-currencies, it is possible for parties to create transactions silently, as well as to generate them from any location where the appropriate keys are accessible. Therefore, if a malicious party were to gain access to the private keys for a Bitcoin or other wallet, they would be able to generate validly signed transactions from that address at any point in the future, without being located physically within the organisation in question. The transactions could be broadcast from any node connected to the Bitcoin network, as there is no such concept of authorised signatory, beyond that of anyone holding the correct cryptographic keys. While multi-signature wallets, such as those discussed below as a form of contract, fundamentally if a party can satisfy the requirements of any given incoming funds, a transaction can be generated from anywhere. Auditors have to find ways to address this issue when ensuring transactions are valid.

In contrast, a regular bank account may require transactions to be initiated from a particular terminal, or have certain approved signatories physically present themselves at the bank to sign a large transaction. Within blockchain, possession of the necessary private keys, or knowledge of the appropriate hashlock condition is all that is required to make a transaction from anywhere.

Ability to hide transactions

For an audit to be effective, it must be bounded to cover a finite period of time, from a starting point to an ending point. The audit should begin at the end of the previous audit, to ensure that transactions do not fall between audits. Within a blockchain, time becomes discrete, rather than continuous, making this process slightly easier. The mean inter-block generation time becomes the increment of time in the chain.

Transactions are not themselves individually timestamped however, so the presence of a transaction within one block doesn't guarantee that was when the transaction was produced and broadcast. This presents issues for an audit. A time stamp may have been included in an orphan block and now is being included in a new (valid) block. Alternatively, the transaction may have been generated in the past, and then broadcast at a later date. This makes the audit process more complex, particularly if auditing internal controls and procedures needed to initiate transactions, since pre-authorised transactions could be broadcast at any later time, thus transmitting the funds long after the authorisation was granted.

The timestamping highlights a key risk for those auditing a blockchain; namely that not all approved transactions may be visible to the auditors. If an authorised party acting maliciously was to generate

validly signed transactions from corporate-controlled funds, without broadcasting these to the blockchain, the auditors may be unable to detect their existence if internal processes around signing and auditing access to keys were breached or bypassed. These transactions could then be presented to the network after-the-fact.

The Bitcoin protocol does not feature a per-transaction timestamp, introducing a challenge for auditors attempting to identify all transactions which were generated during a given audit period. There is no time-stamp on transactions, and indeed no way to prevent old transactions from being successfully broadcast on the network and included in a block. Old transactions which fell out of the pool of pending transactions could be later re-broadcast by any party holding a copy of the old transaction, whether maliciously or well-intentioned.

Therefore, we propose the audit process should also include the movement of all blockchain-based funds between wallets (public keys). This addresses two of the main challenges of the audit; ensuring funds are indeed under control of the organisation, and preventing historical fraudulent transactions from being re-broadcast in the future. By moving all business funds to a new wallet and address during the process of audit, auditors can be satisfied that the funds are indeed under the control of the organisation, since they were transferred to a new account, thus proving the possession of the old private key. By transferring to a new wallet, this transaction will prevent the successful execution of any old, hidden (and thus unaudited) transactions during the previous audit period, since it would be rejected by the network as a double-spend attack, since the funds had already been moved to a new wallet. Secondly, it will ensure that the process of generation of the keys for the new wallet is secure, and compliant with best-practice, for the audit period going ahead, without any transactions generated prior to transfer of funds for future replay.

Business process

The development of blockchain, distrusted ledgers, or indeed any other technology, is done largely to improve the business process. As such, distributed ledgers, at present, are not subject of stand-alone audits. They are, instead, part of a typical corporate audit and thus not done from a technology robustness perspective.

Auditors have an issue with the ephemeral nature of money. Like fiat money, the value of cryptocurrencies relies purely on the assigned value to them of their users. It is not the ability to have a better currency that is the issue, it is the benefit of having it over a distributed computer that is linked into the supply chain. As such, which ecosystem is being audited that becomes the issue? Audit, in the traditional sense, is not appropriate for such an internet based environment.

When recording the balance of accounts holding crypto-currencies or other such commodities, one accounting challenge faced by auditors is that of ascertaining the currency in which the audit should report the overall balance of funds. While a balance could be reported in the native format of the blockchain-based protocol, this could lead to confusion or uncertainty in future. For example, were blockchain-backed bonds for gold or another physical asset to be used, the audit must highlight that these act as a form of promissory, rather than the tangible asset. In the event of a compromise of the blockchain, or the party holding the assets, the blockchain-backed variant may see a price variation or

devaluation due to a lack of confidence, or operation of a fractional reserve process by the physical asset holder.

Where a purely cryptographic currency is involved, the rapid volatility of such cryptocurrencies presents a challenge for audit. While the overall number of coins held may remain constant over a period of time, their value may significantly deviate due to fluctuations in pricing. Due to the relative immaturity of these markets, and the limited liquidity available, there remains the possibility of price and market manipulation. This could potentially be abused by either inside or outside parties for their own financial gain, resulting in a loss to the organisation. For example, if an organisation placed a stop-loss order on cryptocurrency funds, and a flash-crash was to occur as a result of third-party sell orders lowering the market price of a limited-liquidity commodity, this could lead to a sell being executed, permitting another party to acquire the asset from the stop-loss sale at a preferential price [3]. An audit should therefore seek to identify how funds held within exchanges are stored, and whether they are at risk from trading orders such as these, in the event of volatility.

Third Party Holding and Control

Third parties always present issues for auditors. Often in a distributed online environment, whether for increased usability, or due to shortage of technical skills, funds may be held within potentially insecure wallets, whereby the private keys are accessible to third parties. For example, funds may be on deposit with an exchange or other online wallet service. In these circumstances, it may be possible for discrepancies to occur, whereby the exchange was to end up in a deficit scenario, for example as a result of cyber-attack or insider stealing funds.

Where funds are held by a third party on behalf of the entity being audited, this naturally should raise concerns around the security of those funds; without the private keys being under the control of the organisation in question, the funds cannot be accessed in the event of the cessation of service of the third party. [4] This may lead to a material loss and deficit for the organisation concerned, and therefore this ought to be recorded during an audit. In addition, where funds are held in a third-party exchange or online wallet, the organisation concerned may be unable to demonstrate possession of the cryptographic keys controlling their wallet.

In particular, funds within online exchanges and wallets are often interchanged between accounts without any blockchain-based audit trail. For example, if two users of the same platform transact, this transaction can take place using the exchange software's internal record of balance on each account, avoiding a blockchain transaction being broadcast. In such a scenario, it becomes difficult for an audit to verify the true value of funds within the exchange or wallet, without requiring a full withdrawal to an external wallet where the keys are held by the organisation. This would permit identification of the true quantity of funds, and create an auditable blockchain entry showing proof of control of those funds at that point in time.

Verification of Parties

The verification inherent in blockchain presents issues in respect of the audit trail. Blockchain-based transactions occur between public key hashes (addresses) corresponding to cryptographic identities. Best practice in the use of keys dictates that each public key (address) should be used only twice; once

to receive funds, and once to transfers funds out. The justification for this is that one of the security measures of many blockchain-based currencies, including Bitcoin, are designed to conceal and protect the user's public key until a spend transaction is created. Prior to this point, only a one-way derivative of the public key is visible on the blockchain. This means that even compromise of the digital signing algorithms used in Bitcoin would not result in a compromise of funds, provided parties follow this guidance.

Where parties do follow this guidance, this creates a challenge for auditors, in that recurring transactions to a recipient will not necessarily (and indeed ideally should not) be directed to the same recipient address. The audit process therefore should cover ensuring the correct recipient was specified, and that the receiving address can be substantiated based upon documentation such as invoices. Further complicating matters, the private keys used to access a wallet may be transferred between parties simply. This means that an address used to receive legitimate funds by a business could be taken over by a party who was provided these keys by an insider after the funds had been received. This makes it difficult to ensure the identity of the party operating an address. The audit process therefore should both reconcile recipient addresses against invoices, as well as seek to locate duplicate receiving addresses for scrutiny. In many cases these may simply be explained by receiving parties using online third-party controlled wallets, or by a party who does not follow the best-practice guidance to use a new receiving address for every transaction. Nonetheless, repeat transactions should be scrutinised, to ensure that malicious actors do not attempt to transfer funds to previously-used addresses now under the control of a new beneficiary, for the purpose of money laundering or theft.

Smart Contracts and Time-locked transactions

Various types of smart contract can exist on blockchains. An auditor needs to look through the code to understand the nature of such contracts. Further reading on this can be found in (Corin, Etalle, den Hartog, Lenzini, & Staicu, 2005). In their simplest form, incoming Bitcoin payments can specify cryptographic conditions which must be satisfied before they may be spent, or even processed. For example, a Bitcoin transaction may specify a timelock, such that it will be rejected from the blockchain prior to a certain point in time. Such invalid transactions should not be encountered in the blockchain unless valid, as miners should reject them. Nonetheless, were transactions like this to be discovered due to a software bug in miner validation, these blocks would be invalid once the error was detected, and a chain reversal would occur, once miners had been updated to follow the correct rules.

A party being audited may hold non-submitted transactions, signed by parties, promising funds on a time-lock. These should not be considered as valid, however, since the initiating party can reverse these payments by transferring their funds away from the sending address prior to the time-lock condition being satisfied, and the block appearing in the chain. The previously-generated time-locked transaction would now be rejected as invalid due to a double-spend occurring, preventing the recipient from receiving their funds. Therefore, such transactions should be considered, at least from a cryptographic perspective, as little more than a non-binding form of IOU.

Multi-signature transactions

Auditors typically check authorized signatories in the physical word. With blockchain, once funds have been received, the unspent transaction output (UTXO), used as the input to a future outbound payment, may specify additional restrictions upon spending. Within Bitcoin, these restrictions are relatively constrained, and allow for split-signatures, requiring multiple private keys to be produced in order to spend funds. Funds held under such a system present strong protection against actions by any one individual, although an audit process should still ensure that keys are in place and funds are able to be used (i.e. that keys have not been lost, and funds can still be transferred to a new wallet with split-signature requirements).

An audit should ensure that funds are not held in wallets permitting signatures from any parties which have left the organisation, or who should no longer have control of those funds. Even where an N-from-M signature scheme is in use, perhaps requiring 2 keys from a group of 6 managers, it is important to audit those who have keys present in the release contract, to ensure that 2 people who have left the organisation cannot collude to steal funds prior to a re-keying of the accounts. Since copies may be taken of any keys which are not stored in dedicated hardware security devices, key rotation should take place before a group-based key-holder leaves the organisation.

Arbitration Contracts

The solution we propose for audit is "Arbitration-style contracts", an approach not dissimilar to that proposed by (Treleaven & Batrinca, 2017). These can be used on UTXOs, to allow two transacting parties to appoint a mutually-agreed arbitrator in a transaction. In such scenarios, the funds may be spent by any 2 of the 3 participants (including the arbitrator). Where both transacting parties are in agreement, they may transfer the funds as they wish, since combined they hold 2 of the 3 keys. Where the two parties enter dispute, the arbitrator can review the circumstances, and sign a judgement which, with the agreement of only one of the parties, will result in the transaction executing. The arbitrator cannot act alone without the consent of one of the parties, since they hold only 1 of the 2 required keys to carry out a transaction.

Where such contracts are in use, the audit process should carefully review the contracts in place, and establish the identity of those arbitrating any outstanding transactions. In the scenario where a party to a transaction recommends a non-independent arbitrator, it would be possible for that party to use the corrupt arbitrator to steal funds which the organisation under audit may feel they are owed. For this reason, funds which are contract-locked should not be considered to have been received, until a transaction takes place to move them to a wallet under the control of the organisation under audit.

Micropayment Contracts

Auditors have also got to get used to micro-payments. In some scenarios where small quantities of funds are being transacted, which would ordinarily be economically infeasible to carry out on the main blockchain, a micro-payment channel can be formed. This is done by parties, in order to permit repeated transactions to take place within the constraints of a larger transaction, which is updated dynamically as transactions take place, altering the funds owed. Under such a scenario, a time-locked transaction is combined with a 2-from-2 multi-signature contract. The end result is that the sending party holds a dual-signed "refund" transaction, granting themselves a full return of the funds paid out, but with a time-lock in place to prevent it from being processed prior to a certain time. A second

transaction is then created, forming a “bond” between the two parties. This bond requires both parties to sign to release the funds. Therefore the initial “refund” contract can be used (while adhering to the time delay) to return the funds to the initiating party. Only the second “bond” transaction need be produced and transmitted to the blockchain. Outwith the blockchain, as funds are owed to the recipient, an updated “refund” transaction is produced and signed by both parties, without the original timelock, allocating the outgoing funds between the two parties agreed. This transaction is again not broadcast to the network, but held by the receiving party. At any point prior to the original time-lock expiring, the receiving party can broadcast their copy of the most recent “refund” transaction, to receive the funds they are owed within the micropayment contract.

Micropayments are useful for avoiding the large transaction fees on major blockchains, such as Bitcoin and will become an increasing feature of audits going forward. Significant however is that the sending party should only engage in such a contract where the transfer of funds is uni-directional; a second contract must be set up if funds may be transferred in the other direction, as otherwise the receiving party could broadcast an outdated version of the release transaction from before a transfer back to the sender. Using two channels, with a clear recipient for each will avoid this.

Funds within a micropayment contract should be audited with care; until the contract completes, the exact outcome cannot be certain; if the audited party is the recipient, it is possible no funds will be received, if the recipient forgets to broadcast the most recent refund transaction, or broadcasts the wrong refund transaction in error, sending excess funds to the original sender. Likewise, in the event of an outage preventing the recipient from broadcasting their version of the transaction, the sender can broadcast their original refund transaction, and retrieve all of the funds once the time-lock condition is satisfied. Therefore, only micropayment contracts which have concluded through the broadcast and inclusion of a release transaction in a block on the chain should be considered to have completed.

We recommend, as a sending party, a micropayment contract should not be considered concluded by an auditor until a refund or release transaction has been made; if no release transaction is made, the refund may be made at any point after the time-lock condition expires, although if this does not occur, a release can be made at any point prior to the refund being broadcast, irrespective of time passed.

Hashlock (Pre-commitment) Contracts

Hashlocked transactions are another variation of contract-constrained transactions that auditors have to be cognisant of. In those a received transaction may only be spent when the corresponding pre-image to a cryptographic hash is provided as part of the transaction. This means that a transaction is created, which specifies that in order to spend the funds produced as an output, it is necessary to provide the input to a one-way function, such that a certain output (contained within the transaction) is yielded. Absent the knowledge of this input value, it is not possible to spend the funds, as the transaction will not be placed into a block by miners. With access to this value, the funds can be spent, as the transaction will be accepted by miners, and included in the blockchain. Once the input value is revealed in a transaction spending the funds held within the hashlock, any party may validate that the transaction is legitimate, by ensuring the hash matches the original requirement.

During an audit, UTXOs protected by a hashlock should be closely reviewed. Without access to the corresponding hashlock release value, funds cannot be spent and are thus inert. Therefore, as with the process detailed earlier for ensuring company funds are genuinely under the control of the entity being audited, an audit should consider whether hashlocked funds are accessible to the organisation. Since to demonstrate knowledge of the hashlock key, it must inherently be revealed to an auditor, the funds should be transferred to a new hashlock key, thus demonstrating possession and control of the funds, and ensuring that the funds are protected going forwards.

Chain Obfuscation and Coin Mixing

One potential challenge during an audit is the creation of transactions designed to obfuscate the intentions of the parties making payments, or the handling of coin mixing, in attempts to conceal the trail of transactions. In the first instance, transaction inter-mingling can be used to provide a level of deniability for those making transactions. Using the so-called CoinJoin technique [5], a contract-based release of coins is used to form a single transaction, incorporating multiple mutually distrusting parties' transactions. Potential participants can create a new receiving address for their new coins, and form one transaction between all three parties, requiring all participants to sign the transaction to release the funds. Each participant's inputs are then merged in the one transaction, with an output for each party.

The problem with the above weakness for auditors is that it separates the link between the inputs and outputs, since ambiguity is introduced on the blockchain as to which inputs correspond to a given output. If this process were repeated multiple times, blockchain-based analysis to trace funds would be significantly hindered. To establish what happened within each CoinJoin operation, it would be necessary for an auditor to identify and communicate with the other parties in the CoinJoin operation. With no easy way to establish communication with a pseudo-anonymous user of a cryptocurrency, this would be a significant challenge, especially if the process was repeated multiple times.

The technique of mixing or tumbling, while less common due to requiring trust in the provider of the service, is designed to hinder the tracing of transactions involving cryptocurrency coins. A party wishing to “clean” the past history of their coins would transfer these coins to a mixing service as part of a transaction. In return, providing the mixing service is honest, a set of coins would be returned to a new address, which have different origins. Without compromising the mixing service, an audit would be unable to trace funds through a well-implemented mixing service.

During an audit, techniques to obfuscate the true destination or origin of transactions may pose a challenge, as these may hinder the process of verifying the destination of funds is as stated. For example, an insider attempting to steal company funds would almost certainly attempt to mix their coins using one of these techniques, to avoid their purchases being traceable back to the original theft.

Cross-Chain Transactions

As a final, almost obvious point, the complexity of the audit increase where more than one crypto currency is involved. Different cryptocurrencies may have their own independent blockchains. Where transactions are used to carry out cross-chain trades, these may present a challenge during audit. Such transactions may be encountered when carrying out an exchange between two different

cryptocurrencies. For example, if an organisation were attempting to trade one cryptocurrency for another, and avoid the risk of the counterparty in the transaction taking their funds without paying the outstanding balance in the other currency, a cross-chain transaction is taking place. Hashlock-type contracts may be used here, since the same hash output value can be used across blockchains, with the corresponding input to unlock the transactions then able to be exchanged, thus making the funds available for release on both blockchains simultaneously. Auditing this transaction would require consideration of both blockchains, potentially significantly increasing the necessary scope of the audit.

Conclusion

In this paper we have shown that the audit process, as it currently stands, is not sufficient robust to handle the challenges of digital money transfer and storage. The questions that auditors need to ask have to change and adapt. Our contribution is in offering some insights into the areas which must be addressed. Specifically, the financial audit must facilitate the distributed nature of blockchain assets, cryptocurrencies and online legers. The rules and process that auditors apply need to adapt to the complexity in such distributed systems. In particular, we identify the multijurisdictional nature of digital value and the time stamping of transactions as requiring special attention.

We further illustrated the many weakness and challenges in blockchain, despite the promise of self-audit. These include transaction malleability and both long and short-term blockchain forks. We also demonstrated the challenges presented by Digital Autonomous Organizations (DAO's) as well as accounting and auditing cryptocurrencies and distributed ledgers in multiple jurisdictions. We argue that dedicated audit professionals should consider how to address such issues.

In conclusion, we point out that audits are evolving to a more risk based and distributed model. In this context, distributed ledgers, in effect triple-entry book keeping, presents challenges to auditors previously focused solely on double entry book keeping. In this new environment, organizations have multiple counterparties to the same transaction. To address this, we propose that smart contracts be adapted to facilitate self-audit and that the skillset of auditors be adapted to face the new challenges.

Bibliography

(IFAC), I. F. (2009). Assurance and Ethics pronouncements. *Handbook of International Auditing*.

Allen, R., Loebbecke, J., & Sorensen, K. (1998). Multilocation audit risks. . *Journal of Applied Business Research*, 14(4), p.1.

Andrychowicz, M., Dziembowski, S., Malinowski, D., & Mazurek, Ł. (2015). On the malleability of bitcoin transactions. *International Conference on Financial Cryptography and Data Security* (pp. (pp. 1-18).). Berlin, Heidelberg.: Springer.

Brink, V. (1988 (Reprint 1941)). *Modern Internal Auditing.* New York, NY: Ronald Press.

Buyya, R., Yeo, C., & Venugopal, S. (2008). Market-oriented cloud computing: Vision, hype, and reality for delivering it services as computing utilities. In High Performance Computing and Communications. *10th IEEE International.* HPCC'08.

Corin, R., Etalle, S., den Hartog, J., Lenzini, G., & Staicu, I. (2005). *A logic for auditing accountability in decentralized systems. In Formal Aspects in Security and Trust (pp. 187-201).* Springer: Boston, MA.

Dusenbury, R., Reimers, J., & Wheeler, S. (2000). The audit risk model: An empirical test for conditional dependencies among assessed component risks. *Auditing: A Journal of Practice & Theory*, 19(2), pp.105-117.

Francis, J. (2004). What do we know about audit quality? . *The British accounting review,* , 36(4), pp.345-368.

Gervais, A., Karame, G., Wüst, K., Glykantzis, V., Ritzdorf, H., & Capkun, S. (2016, October.). On the security and performance of proof of work blockchains. *In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security.*

Hegazy, M., & Nahass, M. (2012). An analysis of multi-location audit risk factors and the improvement of the audit process: An empirical study. *Journal of Economics and Engineering*, 3(1), pp.35-48.

Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system.* Private distribution.

Rezaee, Z., & Reinstein, A. (1998). The impact of emerging information technology on auditing. *Managerial Auditing Journal*, 13(8), pp.465-471.

Ringelstein, C., & Staab, S. (ICWS 2009.). DIALOG: Distributed auditing logs. In Web Services. *IEEE International Conference* (pp. pp. 429-436). IEEE.

Rogers, V., Marsh, T., & Ethridge, J. (2004). *Internal controls: winning the battle against risks.* 2004: INTERNAL AUDITING-BOSTON-WARREN GORHAM AND LAMONT INCORPORATED-.

Treleaven, P., & Batrinca, B. (2017). Algorithmic Regulation: Automating Financial Compliance Monitoring and Regulation Using AI and Blockchain. . *Journal of Financial Transformation* , 45, pp.14-21.

Whittington, R., & Pany, K. (2012). *Principles of auditing and other assurance services.* McGraw-Hill Irwin.

[1] https://bitcoin.org/en/alert/2015-07-04-spv-mining

[2] https://bitcoin.org/en/alert/2014-02-11-malleability

[3] https://dcebrief.com/gdax-to-reimburse-traders-for-losses-during-flash-crash/

[4] http://www.coindesk.com/mt-gox-the-history-of-a-failed-bitcoin-exchange/

[5] https://bitcoin.org/en/developer-guide#coinjoin