Designing and Auditing Accounting Systems Based on Blockchain and Distributed Ledger Principles

Deniz Appelbaum, Rutgers University
Robert A. Nehmer, Oakland University

Abstract:

Much has been said recently about Bitcoin, blockchains and distributed ledger technologies (DLT). The legendary Satoshi Nakamoto is given credit for instigating these discussions. In this research, we refer to Nakamoto's seminal paper "Bitcoin: A Peer-to-Peer Electronic Cash System" (2008) to apply his proposed characteristics to the accounting systems domain. We find that the requirements are that the system must be peer-to-peer (no trusted third party), transactions are publicly announced, there is a single history of the order of the transactions, there is a time-stamp server, and there needs to be a system of proof-of-work. We then take these design requirements and using Design Science Research (DSR), we consider the transaction processing and contracting contexts which match those requirements. We then consider the issues of data reliability, data security and transaction transparency in those classes of accounting transactions and contracts which lend themselves to a blockchain or distributed ledger solution approach using DSR as our criteria (Hevner et al 2004, Peffers et al 2008). This DSR approach for blockchain and DLT is then viewed from the aspect of designing auditable systems (Alles et al 2008, Appelbaum and Nehmer 2017). We discuss transactions, contracts and workflows for classes of viable accounting systems in this context. After this, we consider how auditors would go about providing assurance on systems which have these characteristics. We consider how DLT technologies pertain to the evidence standards of both internal and external auditors. We also consider how such systems would affect confirmations. We also provide a proof of concept using a cloud computing environment. Finally, we consider the challenges that DLTs pose for both accounting and auditing and suggest some avenues for future research.

Introduction

The Advent of Blockchain

Much has been said recently about Bitcoin, blockchains and distributed ledger technologies (DLT). The legendary Satoshi Nakamoto is given credit for instigating these discussions. In this research, we refer to Nakamoto's seminal paper "Bitcoin: A Peer-to-Peer Electronic Cash System" (2008) to apply his proposed characteristics to the accounting systems domain. We find that the requirements are that the system must be peer-to-peer (no trusted third party), transactions are publicly announced, there is a single history of the order of the transactions, there is a time-stamp server, and there needs to be a system of proof-of-work. The foundation of bitcoin is that of DLT, or more precisely, blockchain. Blockchain is a decentralized, distributed ledger of transactions in which all participants can log, view, monitor, and approve an identical common copy in a real- time basis. Since it is decentralized, the ledger is not owned by any one business or participant, nor is it monitored and regulated by a trusted third party. Instead, these functions are distributed among all participants. Any changes must be approved by a majority of participants and once recorded, a transaction or input cannot be altered or destroyed. The fact that a blockchain can be observed and any new entries confirmed by many diverse participants simultaneously purportedly reduces the risk of security breaches and fraud. Politically, blockchain could be regarded as a pure form of democracy, in that all participants are granted equal rights of observation and approval, and it is the consensus of the parties that legitimizes a transaction.

Blockchain provides a means for many different participants, regardless of location, to record their transactions in a jointly shared "master" digital ledger that exists as linked and synchronized copies in their respective computers. Every transaction is time stamped at different intervals and linked to the previous event via a cryptographic hash. Instead of keeping separate records based on receipts and vouchers, participants can enter their transactions directly into the shared blockchain ledger. This entry, once confirmed by a consensus of the participants, is then cryptographically locked and almost impossible to alter. These blockchain features of consensus approval of transactions and of the immutability of records could potentially render the double entry accounting system outdated and irrelevant.

Accounting records are examined by external auditors on behalf of investors to provide reasonable assurance as to their accuracy and integrity and to ensure compliance with accounting regulations. These examinations can be lengthy and laborious, often requiring manual reviews and obtaining paper documentation. Blockchain should be able to reduce this reliance on manual tasks and duplication of records, as has been recently demonstrated by Deloitte (2017). Deloitte states that "Every transaction becomes 'notarized'" (Bacani 2017).

Technology and automation are accelerating auditing processes. When businesses can record their transactions directly to a shared blockchain that is synchronized on a real-time basis with other participants either internal or external to the business, the requirement for double entry accounting goes away (Dai and Vasarhelyi 2017). In theory, financial statements, budgets, benchmarks, and forecasts can be generated on real time, on demand basis. The processes of generating and examining annual financial statements become irrelevant.

However, the integration of blockchain within the auditing process will most likely be one of gradual adoption and not a large-scale disruption. As a first step to illustrate, we take the design requirements for a blockchain and using Design Science Research (DSR), we consider the possible accounting systems which match those requirements. We then consider the issues of data reliability, data security and transaction transparency in those classes of accounting systems which lend themselves to a blockchain or distributed ledger solution approach using DSR as our criteria (Hevner et al 2004, Peffers et al 2008). This DSR approach for blockchain and DLT is then viewed from the aspect of designing auditable systems (Alles et al 2008, Appelbaum and Nehmer 2017). We discuss transactions, contracts and and workflows for classes of viable accounting systems in this context. . After this, we consider how auditors would go about providing assurance on systems which have these characteristics. We consider how DLT technologies pertain to the evidence standards of both internal and external auditors. We also consider how such systems would affect confirmations. We also provide a proof of concept using a cloud computing environment. Finally, we consider the challenges that DLTs pose for both accounting and auditing and suggest some avenues for future research. Throughout our discussion, we assume that an adequate system of governance and control is already in place for both the business and for IT. Our discussion is meant to be incremental in character.

Methodology

The methodology used in this paper is design science research (DSR). The paper follows the DSR approach introduced by Hevner et al. (2004) and Peffers et al. (2007). Other AIS research using the DSR approach include Geerts (2011), Nehmer and Srivastava (2016) and Appelbaum and Nehmer (2017). This paper uses Geerts (2011) application of DSR which categorizes the methodology into six major activities. The six activities are:

1. Problem identification and motivation
2. Define the objectives of a solution
3. Design and development of an artifact which meets (some of) the solution objectives
4. Demonstration of the solution
5. Evaluation of the solution
6. Communication of the problem and the solution (usually an article)

As stated in the introduction, blockchain or distributed ledger technology (DLT) is becoming a popular design for software, especially in financial applications. This will instigate the need for auditors to assess the risk to the financial statements or other management information used for decision making purposes. The motivation for this research is to get ahead of this situation and consider ways in which the auditor can make such an assessment. In order to do so, auditors must understand DLT and how it affects business and audit risk. Any solution to the problem will need to consider the seven components of DLTs considered in the next section. The paper designs both generic audit solutions and some which relate more specifically to DLT designs in cloud computing environments. These solutions are demonstrated and evaluated against the seven components of DLT designs. As is usual, the final step of the DSR process is incorporated in the content of this research article itself.

Discussion on Blockchain and Distributed Ledger Technology

The following discussion of distributed ledgers is based on Nakamoto's original paper on Bitcoin (Nakamoto 2008). We study that paper to derive the core components of distributed ledger technologies (DLTs). We use those components as our starting point in modeling the audit processes which are in play when auditing DLTs. Essentially, we look at the generic DLT business process definition and then, using a risk-based approach, determine the audit risks in that process and the audit procedures that can be used to collect evidence about those risks. The components which make up the DLT process are as follows:

1. There is no trusted third party required instead, the network is peer-to-peer.
2. New transactions are timestamped and hashed onto an on-going chain of transactions.
3. The hash algorithm is designed to provide a proof-of-work.
4. The record, the hashed chain of transactions, cannot be changed without redoing the proof-of-work.
5. The proof-of-work is accomplished by a pool of CPUs from the peer-to-peer network through computation.
6. The longest chain (block of transactions) includes the latest transaction and requires the most CPU work to create the hash, therefore it takes the most time, to date, to compute the hash.
7. The system works as long as the majority of peer-to-peer nodes are not cooperating to subvert the chain since they represent the majority of the computing power and so can compute the hash faster than any other group.

We will work through each of these components in turn

First, as a design requirement for whatever system is using the DLT, avoidance of using a third-party countersigner or oracle must be preferable from a design point of view. Use of a third party in the design must impose a cost or add risk to the system under design. The rest of the process is largely required to provide a level of trust between the peers on the network that substitutes for the lack of a third-party trust guarantor. This is done in two principle ways: timestamping individual transactions and hashing the transaction sequence or block using an algorithm with special properties. The transaction types which lend themselves to this type of processing must have certain properties. Usually they are either an asset or record of an asset or they are a type of economic contract. The transaction sequence then either shows the record of ownership of the asset or the record of contractual obligations fulfilled to date in the execution of the contract, such as the number and timing of mortgage payments already made on a mortgage contract. So the timestamp provides a recorded 'history' of the asset or contract.

There are several possibilities for the hashing algorithm as discussed in Back (2002). We will consider the publicly auditable cost function (hash) which Nakamoto uses. This hash has two primary features: it is guaranteed to take longer to compute the hash value as the length of the block increases and it is efficiently verifiable by anyone without any special information. The idea of efficient verifiability means that anyone can verify the validity of the block.

The computational time feature of the hash is used in the following way: if someone wanted to commit fraud and alter a transaction in the chain, they would have to go back into the chain to the point where they wanted to begin falsifying the record. But they would not only have to re-compute the hash for that transaction but they would also need to re-compute the hashes for every transaction which came after that. This is going to be computationally expensive. Essentially, the perpetrator would have to re-compute all of the hashes in the block between the time of the falsified transaction and the present. In the meantime, if valid transactions are added to the valid block and accepted by the peer network, then the perpetrator's work is again increased. The system does not guarantee that a change cannot be inserted into the block yet it makes it very time-consuming to insert that change.

The next design requirement is the hash as a proof-of-work. This is accomplished by requiring the hash algorithm to hash the entire new block, which is the original block history of transactions plus the new transaction and all of their timestamps. If the history is changed, the hash will need to be different, so having the hash proves that the hash algorithm was successfully run on that specific block including its specific history.

This also explains the fourth component of the DLT process. The block, the record of the chain of transactions, cannot be changed without re-computing a new hash. The next component requires some cooperation among the peers in the network to compute the hash. The idea is that the hash algorithm is computationally expensive enough to execute that it makes sense to decompose that task and share it on the network. The more peers who cooperate on the task, the faster the hash can be calculated. The fastest networks with respect to their ability to generate new hashes then will be those with the most members cooperating in the task of computing the hash algorithm. Since the latest un-hashed block contains all of the transaction history of the asset or contract plus a new transaction and since the hashing algorithm is chosen to take more time to complete with longer blocks, the time it takes to compute this latest hash will be the longest yet until the next transaction. This is the sixth component of the DLT process. And so the seventh component follows in that as long as a majority of the peer nodes are not actively trying to subvert the network, we are guaranteed that they can complete the valid hashes faster than the fraudulent peers can complete their fraudulent hashes to replace the valid ones. We now review the issues that auditors face when examining transactions and the attributes of Blockchain in this context.

Issues that challenge auditing

Data reliability

Data reliability pertains to the performance principle requirement that auditors obtain sufficient appropriate evidence about whether material misstatements exist, through designing and implementing appropriate audit tasks. Reliable evidence is that which can be trusted, verified, understood, and “seen” by the skeptical, independent auditor. The audit team is required to collect and evaluate sufficient audit evidence to arrive at an opinion. Evidence is all the information that the auditor observes, collects, or analyzes to arrive at conclusions with which to base the audit opinion. Evidence could include external sources as well as internal accounting data and any corroborating information such as confirmations, third party verifications, lawyer’s letters, board meeting minutes, invoices, analyst’s reports, and other paper documentation. To the extent that the information on the blockchain is produced in cooperation with peer network, the blockchain's source is also external to the firm.

Furthermore, data evidence sources that are external to the engagement client are considered by the standards to be more reliable than internal sources. These external data sources should be received/collected directly by the engagement team. Evidence collected from external sources with effective internal controls is more reliable than that collected from businesses with less effective controls. Evidence of proper governance of the peer network and the blockchain itself will therefore be more reliable than evidence from peer networks and blockchains which do not have adequate or adequately documented governance structures.

Data security

Data security provides assurance that the data has been protected from manipulation and has not been altered fraudulently. Data security refers to controls that are applied to prevent unauthorized access to computers, data bases, and websites. Data security also protects data from corruption. Data security is a facet of the requirement of data reliability. Data security ensures that the information continues to provide reliability – that is, it truthfully represents the originating event. Security of data is assured by input controls, processing controls, and output controls. These controls correspond to the following management assertions (Table 1):

Management Assertion	Control Objectives
Accuracy	Input of individual transactions and data is accurate
Completeness	All transactions are entered
Occurrence	Transactions are only entered once
Accuracy	Processing of transactions is accurate

Table 1: Assertions and their control objectives, adapted from Louwers et al, 2017 p 897

The use of a blockchain does not provide additional evidence that an individual transaction is more accurate since the provenance of the underlying event of the transaction originates from a single member or node of the peer network. A blockchain can provide evidence that the transaction trail is complete since it is, in effect, defining what completeness means: the peers agree that this is the sequence of transactions. It also will provide evidence of occurrence as testified to by the other members of the peer network cooperating to complete the proof of work. Evidence of processing accuracy is also provided by the blockchain by the cooperation of the peer network in agreeing to the transaction sequence. The methods of testing these controls, whether of input, processing, or output applications, typically entails inquiry, observation, examination, inspection, and reperformance. These processes are parallel to those in a manual processing environment.

Transaction transparency

Audit performance standards require that the data generation process be transparent, observable, and verifiable. Date transparency provides assurance that the reported data is accurate and originates from the official source (provenance). Essentially, the output data should exactly match the input transaction without restriction or exception. Data transparency is assured by end-user processing controls, computer operations controls, data entry controls, processing controls, and systems development and modification controls. Using a blockchain in the design of a transaction processing system helps to improve transparency by providing a record of the series of blocks and by virtue of the properties of the hashing algorithm used as discussed above.

Discussion of Blockchain Accounting and Auditing

Evidence standards for Auditors

Audit evidence is “all of the information used by the auditor in arriving at the conclusions on which the audit opinion is based” (SAS No. 106, AICPA 2006; AS No. 15, PCAOB 2010). This information consists of the accounting records themselves and all other information obtained during audit procedures performed during the engagement. Furthermore, this evidence should be sufficient, appropriate, and reliable. SAS No. 106.08 clarifies that “the reliability of audit evidence is influenced by its source and by its nature and is dependent on the individual circumstances under which it is obtained.” (SAS No. 106.08, AICPA 2006). Generally, audit evidence is more reliable if it is obtained from sources external to the entity, if it is in documentary form, or if obtained directly from the auditor. SAS No. 106.20 - .42 describes the types of procedures that an auditor may undergo to obtain audit evidence, and these are illustrated in Table 2:

Procedure	**Method**
Inspection of Records or Documents	Pull samples of records and trace/verify/match
Inspection of Tangible Assets	Physical inventory, walk through, open boxes
Observation	Stand/sit with worker(s) and observe
Inquiry	Written or oral interviews
Confirmation	Verify account balances
Recalculation	Extract and recalculate figures to verify

Re-performance	Re-perform procedures to verify
Analytical Procedures	Scanning and statistics

Table 2: The clarification the audit procedures for obtaining audit evidence, based on SAS No. 106.20-.42

The audit procedures listed in SAS No. 106 are backward-looking in nature, providing verification via sampling of a small snapshot of the entity's financial data. This small sample is then extrapolated across the dataset from which the sample was pulled. Although the audit procedure activity itself is current, the sample it is testing may include transactions that are a year old.

Continuous evidence gathering (Teeter and Vasarhelyi 2010) enhances the audit by reducing the time span between the event occurrence and the audit procedure. Additionally, time series analysis may be readily performed, with which benchmarks and alert thresholds may be established (Vasarhelyi and Halper 1991). This process is more quantitative than the procedures in Table 2 and may require a reengineering of the audit evidence collection process (Alles et al, 2008). In a Blockchain and continuous evidence collecting environment, these more technical audit procedures stand in contrast to the earlier traditional approaches, as described in Table 3 and adapted from Appelbaum and Nehmer 2017:

Procedure	**"Traditional" Method**	**Blockchain enabled Continuous Method**
Inspection of Records or Documents	Pull samples of records and trace/verify/match	**Evaluate entire datasets in ERP using blockchain**
Inspection of Tangible Assets	Physical inventory, walk through, open boxes	RFID tagging
Observation	Stand/sit with worker(s) and observe	Use blockchains or process mining to verify work flows
Inquiry	Written or oral interviews	Monitor processes and controls, identify process violators for examination
Confirmation	Verify account balances	Link data streams using blockchain applications
Recalculation	Extract and recalculate figures to verify	Monitor all data and run calculations automatically at intervals desired

Re-performance	Re-perform procedures to verify	Automatically replicate all transactions and identify exceptions
Analytical Procedures	Scanning and statistics	Filter real-time data with continuity equations and statistics

Table 3: Audit procedures comparison of traditional manual procedures and Blockchain enabled continuous procedures (modified from Appelbaum and Nehmer 2017)

Observation/Inquiry

Any process that would directly connect the auditor with the audit process is more reliable (SAS No. 106. 08, AICPA 2006). Observation (SAS No. 106.30, AICPA 2006) consists of looking at a process or procedure being performed by others. For example, watching the process of inventory counting or controls processing constitutes observation. However, the observation is only valid for the point in time that it occurs and is constrained by the fact that being observed may affect how activities are performed. In a continuous real-time auditing environment, proponents of blockchain envision that the blockchain framework itself provides voluminous proofs of observation, thereby freeing the auditor from this task. However, the auditors can observe the timestamping of the transactions that are added to the block and observe whether the block is being hashed or not. They can also observe whether the lengths of the blocks are increasing over time to verify that the implications of the hashing algorithm exist. These are components two and six of the DLT process. The observation guidelines as audit procedures support the assertions of existence, occurrence, and valuation. Existence and occurrence are interchangeable and answer the questions if the assets really exist at the balance sheet date or did a transaction or physical control actually occur. These are all attributes of assurance that blockchain claims to provide by means of consensus. Inquiry can be used to obtain evidence from the peer network as to their understanding of the governance characteristics of both the network and the blockchain. This will provide evidence on the data reliability and security aspects of the information derived from the blockchain and will support the existence of component seven in the DLT process.

Confirmation

Confirmations for accounts receivable is usually regarded as a required audit procedure. Confirmations provide evidence for the assertions of existence and rights and obligations. That is, does the AR balance exist and what are the conditions of this relationship or obligation? Typically, confirmations are written inquiries regarding balances or other attributes. The inquiry may originate from the audit client but the response should ideally be mailed directly to the audit team. Absent confirmation evidence, auditors may examine cash receipts, sales orders, invoices, shipping documents, or other correspondence files. It should be noted that these sources of documentation would be already participating in an A/R blockchain of a business, thereby greatly reducing the burdens of confirmation processes in an audit engagement. A specific confirmation relating to the blockchain process components would be to confirm with members of the peer network as to the design and functioning of the hashing algorithm being used by the DLT (component three). They can also use confirmations to confirm that peers are participating in the calculations of the proof of work, component five of the DLT process.

Inspection of Records or Documents

Inspection of records and documents is one of the fundamental audit procedures and entails vouching, tracing, and scanning these evidence sources. In fact, these procedures are used predominantly in the engagement to ascertain the reliability of management's financial statement assertions. The inspected documents may originate outside or within the client. Vouching involves the process of verifying a financial statement number back to its originating transactions, whereas tracing involves tracking a process from its origin to its concluding number. Scanning is basically the way auditors will look at all the tables or documents for anything unusual. In a DLT application, the auditor can inspect the documents that support the configuration and governance of the peer network which is operating the DLT process. This would provide evidence that the first component of the DLT is in place.

Recalculation

Recalculation allows the auditor to verify the accuracy of the processed data within an application. If the hash in a DLT is designed with efficient verifiability, as it should be, then the peers of the network along with the auditor can verify the blocks stored in the blockchain simply and in support of component four of the DLT process. This will provide the auditor of evidence for the accurate processing of the stream of transactions included in the block. This in turn supports the accuracy assertion.

Demo of Cloud Application

Cloud Computing

Many business audit clients and their third-party providers have migrated to cloud -based ERP systems, as virtual shared protocols. The Cloud has become a popular pay-as-you-go location for data storage, due to its flexibility and scalability (Assuncao, Calheiros, Bianchi, Netto, and Buyya 2014). Clouds are known for their ability to scale dynamically upward or downward depending on demand and data load. However, the Cloud is perceived as being insecure (O'Driscoll, Daugalaite, and Sleator 2013; Armbrust et al 2010), providing scanty locational tracking due to this very same scalability and flexibility. Clouds are also viewed to be untrustworthy since the guarantees provided regarding data transformations and locations are minimal (Sakka, Defude, and Tellez 2010). Furthermore, most cloud providers offer clients little capability on data, application, and service interoperability. Most cloud storage services are not designed to effectively and efficiently store log file data, due to the cyclic nature of log file capture - its need to be stored separately yet linked to the data objects (Muniswamy-Reddy and Seltzer, 2006). Currently, tracking of data held in the Cloud persists as an open research problem

(Assuncau et al 2014). For auditors, the use of the Cloud by a client for either processing or storage of data may likely increase the risk that the relevant data is not reliable as audit evidence, due to the minimal recording of activity logs. Some initial investigations of how to manage this risk include Wilken and Chenhall 2010 and COSO 2012.

For auditors to trust data applications in the cloud, the CSP will need to provide guarantees of data accountability, reliability, compliance, security, verifiability, auditability, and reperformance. To date, it would seem that these attributes cannot be associated with cloud computing (Gault 2017). There has been much research about cloud security and data provenance in the cloud, crumbs of research regarding blockchain, and even less research on blockchain and the cloud. Many of the businesses that are examining blockchain applications for their systems are also utilizing cloud computing. The integration of blockchain within cloud-based systems is an area that requires research if blockchain is to be adopted by businesses.

Demonstration

In this section, we illustrate a proof of concept for the design of an auditable blockchain application which is implemented in the cloud. The audit risks and procedures for DLTs discussed earlier should all be considered when the DLT application resides the cloud. The following discussion is in addition to those procedures. From the cloud assurance literature, we rely on Schmidt *et al.*, 2016 for our basic understanding of the issues or research questions. The demonstration proceeds as follows: 1) cloud computing ecosystem with a formal governance structure, 2) designs of a blockchain application in the cloud ecosystem, and 3) auditing the resulting design.

First, some terminology: following Schmidt *et al.*, 2016, a cloud ecosystem with a formal governance structure includes the cloud service user (CSU), one or more cloud service providers (CSP), one or more cloud service partners who provide services to the partners (CSN – cloud service network), the board of directors and the external auditors. Schmidt *et al.* Carefully consider the possible assurance risks to stakeholders in this ecosystem. The stakeholders include the CSU, the CSPs, the external auditors, and investors, trading partners and end customers of the CSU. We concentrate on the inherent risk of the CSU and the audit to its auditor in situations where a DLT is implemented in the cloud. For simplicity's sake, we consider a single DLT application and not multiple applications or multiple interacting applications.

When we consider the seven components of the DLT process which are discussed in this paper, the basic overarching consideration when designing such a process in a cloud environment is where in the cloud ecosystem does the peer-to-peer network fit from an IT architectural point of view. Consider some endpoints of that design: In the first, the cloud being used is entirely owned and operated by the CSU. The risks then are shifted to the other peers on the network and their architectural configuration on the cloud. The two end points here are either that none of them are using cloud services or that they are all on a single cloud. In between are all of the possible combinations of overlap of cloud service providers and members of the peer network. If the CSU is on an external cloud, then it becomes one of the peers in the combinatoric set of configurations. The auditor must consider the added risk that peer nodes operating on the same cloud may be easier to subvert by a potential fraudster attempting to take control of or rewrite the blockchain. The problem is that the auditor is unlikely to get evidence directly from the peer members as to their own contractual arrangements for cloud services.

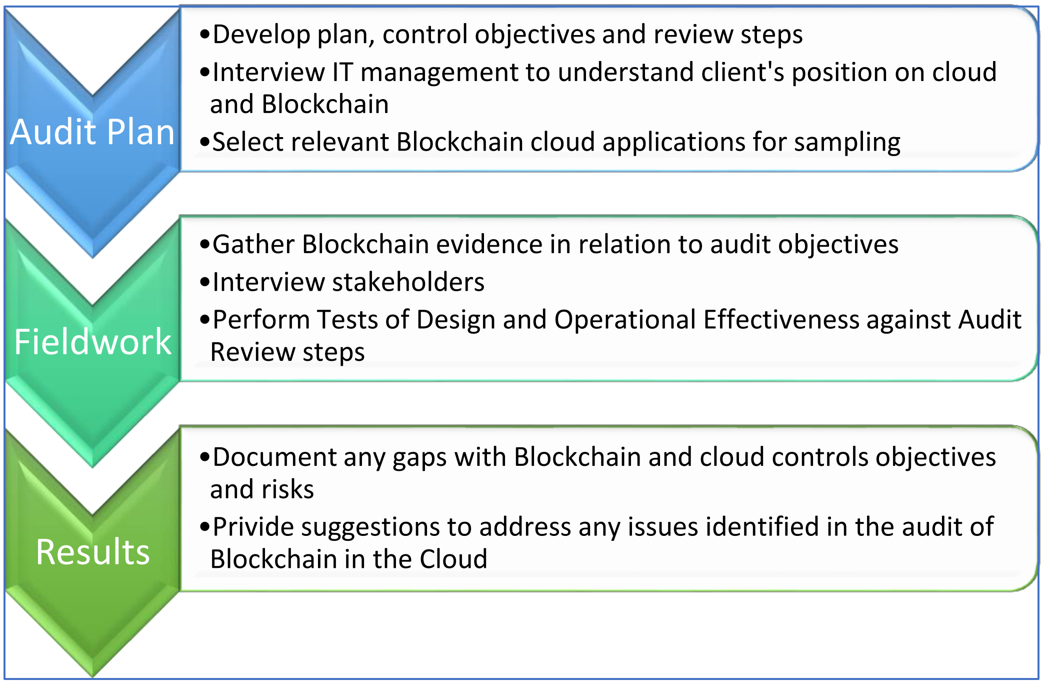
The main additional audit elements in a DLT cloud assurance engagement are the governance provisions that the CSU has in place with respect to the contracting and service provisioning of the peer-to-peer network on which the DLT operates. The CSU's risk is affected by these governance provisions while the auditor's risk is affected by both the provisions themselves and by their ability to gather evidence about those provisions. The evidence will be primarily documentary in the form of contract provisions including non-compliance provisions among the peers in the network. But the evidence can include inquiry and confirmation of peers as well. The nature and extent of the needed evidence should be related back to the risk assessment of the DLT cloud application, both from the CSU's point of view and from the auditor's point of view.

Some types of evidence include the policies on cloud computing provisioning and whether they include procedures for DLT implementations in the cloud. The contracting process will be key. Are there policies and procedures in place which guide the contracting process with respect to the analysis of risks and the negotiation of contract provisions which mitigate risk or provide for insurance against specific risks. Provisions regarding how companies enter and leave the peer-to-peer network, required audit provisions for member peers and the technical details of the hashing technologies employed may also be considered. Details of who is responsible for DLT contracts and how the DLT application development process interfaces with cloud computing development will also be important along with how the contracts and the DLT cloud applications will be monitored after implementation. The board's role or roles in the monitoring and risk management process will also be important. While DLT applications will not always be strategic in nature and can sometimes be managed at an operational level, in other cases they will be strategic to the way a firm conducts its business. In such cases the board will have to be educated on the DLT technology as well as its potential interactions with cloud services technologies. All these considerations lead to a broader discussion of the need for research in the Blockchain domain, both generally and specifically for auditing and accounting.

Areas for Future Research/Development

It could be said that Bitcoin and Blockchain are at the peak of the Gartner Hype Cycle. Blockchain appears to be gaining traction in the financial services industry, and even governments are exhibiting interest in adopting blockchain for land records, identity management systems, health-care record, and elections. Given the ever-growing interest in Blockchain technologies within the business and government domains, it is inevitable that auditors will encounter their use during the engagement. At the surface, it would appear that Blockchain transactions provide a perfect form of audit evidence – difficult to alter, credible, complete, obvious, and with evidence of approvals. Many of the characteristics of Blockchains are similar to the proposals for secure data provenance (Appelbaum 2016). However, there are challenges that should be examined further in the audit of businesses and government entities that are utilizing Blockchain:

- ✓ Although Blockchain may provide assurance of events of transactions in a chain-like fashion, the originating entry or origin of the chain may be suspect. That is, the auditor will still need to physically validate the originating event by means of verifications, observations, and recalculations/reperformance. Subsequent events along the chain will be approved by all participants – however, what is the structure and participation at the origination level? How can the auditor be sure that the origins of an event are truly representative of a transaction? This question is pertinent whether the blockchain is a twig of a vast tree of many forked chains or a stand-alone blockchain. Although the Blockchain may provide more reliable assurance about transaction permutations and pathways, the auditor might not be absolved from verifying the accuracy and validity of the chain origins.
- ✓ As mentioned earlier, the seventh component of DLT assumes that the majority of peer-to-peer nodes are NOT cooperating to subvert the chain. This situation may be less of a risk with a public chain, as such collusion might be difficult to conceal or pass consensus approval. However, with public/private or private Blockchains, the risk level is significant for collusion or other nefarious practices. In this scenario, the audit examination should include typical confirmations and recalculations of transactions.
- ✓ Many businesses utilize cloud computing services which require special audit considerations due to their complexity and deployment combinations (Elifoglu, Guzey, and Tasseven 2014). Blockchain in the Cloud exhibits the potential to address the essential audit issue of cloud computing (Gault 2017): How does the audit client comply with the regulations and trust its critical transaction data to an outsourced cloud who has little if any verifiable accountability? What follows is a re-examination of some of the questions raised in Schmidt et al 2016, adopted now in the light of auditing Blockchain in the cloud:
    - o How does Blockchain cloud computing impact the role of the external auditor and audit procedures (traditional attestation)? What robust risk assessment and vendor management processes are in place for management to follow and auditors to verify? Are these different for Blockchain from the traditional cloud computing? Although the role of auditing Blockchain is discussed at length in Dai and Vasarhelyi (2017), blockchain cloud computing is not examined. However, these authors do admit that the complexity of Blockchain applications is a major hindrance to its widespread adoption, and this complexity would be magnified by the cloud.
    - o How does the external auditor approach the structure and planning of an audit involving Blockchain in the cloud? Would the traditional approach change much in an audit of Blockchain data in the cloud? For example, here is a hypothetical approach for an audit of Blockchain data in the cloud, adopted from KPMG's (2013) proposal for auditing CSPs :



Audit Plan

- Develop plan, control objectives and review steps
- Interview IT management to understand client's position on cloud and Blockchain
- Select relevant Blockchain cloud applications for sampling

Fieldwork

- Gather Blockchain evidence in relation to audit objectives
- Interview stakeholders
- Perform Tests of Design and Operational Effectiveness against Audit Review steps

Results

- Document any gaps with Blockchain and cloud controls objectives and risks
- Privide suggestions to address any issues identified in the audit of Blockchain in the Cloud

Figure 1: Suggested audit of Blockchain (BC) transactions in the Cloud, based on proposal by KPMG (2013) for Auditing Cloud Service Providers

- How can the audit standards evolve to provide guidance in auditing Blockchain in the Cloud? According to Dai and Vasarhelyi (2017), regulators are expected to play an essential role in the acceptance of blockchain in the auditing sphere. The auditor's role in this new paradigm of blockchain-based cloud computing may need to be re-defined. For example, would auditors be emphasizing controls more? What standards should be created to enforce audits of smart contracts? Would auditing be needed or even necessary with a cloud-residing blockchain? Which areas of focus should be abandoned and which new audit assertions developed?
- Does the use of Blockchain in the Cloud change the audit client's and auditor's assessment of the third-party cloud provider? Typically, an auditor will attempt to determine the location of the client's data in the cloud, as well as determine if any security breaches occurred, if the data privacy controls are enforced, and if audit rights, integrity, and availability are maintained. Are these features as important with Blockchain in the cloud? Does it matter where the Blockchain is "located"?
- Does the use of Blockchain mitigate the challenge of its location in the Cloud? Some clouds may reside in many other countries where data security rules may differ. Traditionally this has been an issue with cloud computing, but the access controls in place through the smart contracts may greatly reduce this question of maintaining data privacy. The auditor, however, will still need to access the

Blockchain as well as review the smart contract, in order to ascertain that controls and conditions of the contract are operational.

- As cloud service offerings mature, is there a difference with Blockchain regarding the levels of assurance that needs to be provided? Many clouds offer different levels and types of service. Would blockchains require different types of assurance for a Blockchain Cloud as a Software Service (BCSaaS), Blockchain Cloud Platform as a Service (BCPaaS), or Blockchain Cloud Infrastructure as a Service(BCIaaS)?
- In the context of Blockchain, is there a difference between the audit of a private cloud versus a public cloud? Usually the risks are different for private, semi-private, and public Clouds. With Blockchain, there are similar divisions of private, semi-private, and public chains. Are the risks of these chains parallel to their similar clouds, i.e. public Blockchain and public cloud? Or are these audits different?
- How can the external auditor effectively provide audit and assurance of Blockchain transactions in a multi-tiered cloud computing environment? Furthermore, with the assurance that Blockchains are purported to provide, what level of assurance would be necessary? In most cloud environments, there are Identity and Access Management, Financial and Vendor Management, Regulatory, Data, Operational, and Technology risks (KPMG 2013). Are these risks the same with Blockchain in the cloud?

These are but a few of the issues that should be addressed about Blockchain data in the cloud. Also important is the question of feasibility (Dai and Vasarhelyi 2017) – even a modest petabyte cloud generates billions of transactions that would need to be entered in a Blockchains(s) whose hashes would need to be linked but separate and which require updating on a real-time basis. Typically, such a scenario has not been practical for many cloud providers (Appelbaum 2016). With Blockchain these long sequential chains with their dangling hashes would need to be distributed to the edge of the cloud upon auditor demand. It is quite possible that the required costs, implied network, increased storage, and complex compute requirements may make it impossible for cloud providers to offer Blockchain in the cloud with any great scale (Gault 2017).

Conclusion

In this paper, we derived that the requirements which are necessary for a system to be a DLT using Nakamoto as the guide. The requirements are that the system must be peer-to-peer (no trusted third party), transactions are publicly announced, there is a single history of the order of the transactions, there is a time-stamp server, and there needs to be a system of proof-of-work. We then took these design requirements and using Design Science Research (DSR), we discussed accounting systems which match those requirements. We then mapped the audit issues of data reliability, data security and transaction transparency in those classes of accounting systems which lend themselves to a blockchain or distributed ledger solution approach, using DSR as our criteria (Hevner et al 2004, Peffers et al 2008).

After this, we discussed how auditors should go about providing assurance on systems which have these characteristics. We considered how DLT technologies pertain to the evidence standards of both internal and external auditors. We also consider how such systems would affect confirmations. Then we developed a proof of concept application of a DLT in a cloud computing environment. Finally, we consider the challenges that DLTs pose for both accounting and auditing in the cloud and suggest some avenues for future research.

Businesses and governments, which are audited by public accounting firms, are beginning to adopt DLT technologies for some components and processes. Soon the audit profession will be forced to examine blockchain in an engagement, and even blockchain events in a cloud. This paper combines and extends the research started with Schmidt et al 2016 and Dai and Vasarhelyi 2017, in that it discusses the condition of DLT within the cloud. We call attention to those issues that are prevalent in both domains and consider them in this new light. It is conceivable that many challenges to auditors in the traditional cloud environment may disappear with DLT; however, new issues may emerge. This paper draws attention to the fact that current business IT and data collection/storage systems are complex and may be cloud based, and that the potential for DLT and its audit should be regarded in these circumstances.

Furthermore, the audit profession will need to adjust itself to the phenomenon of Blockchain based on its current practice and evolve incrementally. Alles et al (2008) discuss these steps of adjustment – many steps of evolution are intertwined with business needs, management support, process adjustments, efficiency monitoring, and regulatory adjustments. These stages of technology adoption and regulatory changes could take years to process. The big fear is that the audit profession may adapt too slowly in comparison to the pace of its clients, thereby becoming increasingly irrelevant and ineffective in an audit.

Finally, there may be a conflict between the essential philosophies of blockchain and auditing. Blockchain is a de-centralized technique with minimal regulation, structure, and authority, where all participants have an equal vote. Within the DLT domain there is little guidance about the structure of chains and their conventions. Within DLT there is not a central regulatory authority or a trusted third-party verifier. In fact, DLT is considered by some to be perfect example of a libertarian, decentralized democracy (Warncke 2017).

Auditing, however, is a regulation driven profession. It is highly structured and its practices are dictated by the PCAOB and SEC. Is a marriage of this conservative auditing profession possible with the liberal unstructured domain of DLT? The answer to this query will drive and help formulate the answers to the questions posed in the previous section and in other research. Both practices are on opposite ends of the spectrum – can both domains compromise and adjust to meet in the middle? This paper focuses attention on the issues facing the audit profession as it regards the possibility of auditing blockchain transactions, particularly in cloud domains. Risk assessments and governance policies of clients must be considered in this new format of DLT cloud computing. It is hoped that the aforementioned complexities of Blockchain and Cloud Computing are not marginalized by the audit profession as it conducts its affairs with clients who are rushing to adopt DLT, and DLT in the cloud.

References

Alles, M.G., Kogan, A., and Vasarhelyi, M.A. 2008. Audit Automation for Implementing Continuous Auditing: Principles and Problems. Working paper, Rutgers, the State University of New Jersey.

American Institute of Certified Public Accountants (AICPA), 2006. *Audit Evidence: Statement on Auditing Standards No. 106. AU Section 326*. New York, NY: AICPA.

Appelbaum, D. 2016. Securing Big Data Provenance for Auditors: The Big Data Provenance Black Box as Reliable Evidence. *Journal of Emerging Technologies in Accounting,* Vol. 13, No. 1 Spring 2016, pp. 17-36

Appelbaum, D. and Nehmer, R. 2017. Using Drones in Internal and External Audits: An Exploratory Framework. *Journal of Emerging Technologies in Accounting*, Volume 14, Number 1, 2017.

Armbrust, M., Fox, A., Griffith, R., Joseph, A.D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I. and Zaharia, M., 2010. A view of cloud computing. *Communications of the ACM*, *53*(4), pp.50-58.

Assunção, M.D., Calheiros, R.N., Bianchi, S., Netto, M.A. and Buyya, R., 2015. Big Data computing and clouds: Trends and future directions. *Journal of Parallel and Distributed Computing*, *79*, pp.3-15.

Bacani, C. 2017. "The Death of Accounting and Auditing and What to do About It." *CFO Innovation,* Tuesday March 21, 2017. https://www.cfoinnovation.com/story/12767/death-accounting-and-auditing-and-what-do-about-it

Back, A. 2002. Hashcash – A Denial of Service Counter-Measure. http://www.hashcash.org/papers/hashcash.pdf.

Committee of Sponsoring Organizations of the Treadway Commission (COSO) (2012). Enterprise Risk Management for Cloud Computing. https://www.coso.org/Documents/Cloud-Computing-Thought-Paper.pdf.

Dai, J, and Vasarhelyi, M.A. (2017) Towards Blockchain-based Accounting and Assurance. , In-Press. https://doi.org/10.2308/isys-51804

Deloitte. 2017. “Blockchain Technology: A game-changer in accounting?” www. Deloitte.com/de/blockchain

Elifoglu, I.H., Guzey, Y., and Tasseven, O. 2014. Cloud Computing and the Cloud User’s Auditor. Review of Business; Jamaica 35.1 (Summer/Fall 2014): 76-83.

Gault, M. 2017. “BlockCloud: Re-inventing Cloud with Blockchains.” May 13, 2017: https://guardtime.com/blog/blockcloud-re-inventing-cloud-with-blockchains

Geerts, G. L. 2011. A Design Science Research Methodology and its Application to Accounting Information Systems Research. *International Journal of Accounting Information Systems*, 12(2), 142 – 151.

Hevner, A., March, S. T., Park, J. & Ram, S. 2004. Design Science in Information Systems Research. *MIS Quarterly*, 28(1), 75 – 105.

KPMG. 2013. “Cloud Computing: Risks and Auditing.” Presented at the IIA Chicago 53rd Annual Seminar, April 15, 2013. https://chapters.theiia.org/chicago/Annual%20Seminar%20Presentations/E3%20-%20Cloud%20Computing%20Risks%20and%20Auditing.pdf

Louwers, T., Blay, A., Sinason, D., Strawser, J., and Thibodeau, J. 2017 Auditing & Assurance Services 7e, McGraw Hill Education, New York: NY

Nakamoto, S. 2008. Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf.

Muniswamy-Reddy, K. K., D. A. Holland, U. Braun, and M. I. Seltzer. 2006. "Provenance-Aware Storage Systems." In *USENIX Annual Technical Conference, General Track*, pp. 43-56.

Nehmer, R. A. and Srivastava, R. 2016. Using Belief Functions in Software Agents to Test the Strength of Application Controls: A Software Agent Framework. *International Journal of Intelligent Information Technologies*, 12(3), pp.

O’Driscoll, A., Daugelaite, J. and Sleator, R.D., 2013. ‘Big data’, Hadoop and cloud computing in genomics. *Journal of biomedical informatics*, *46*(5), pp.774-781.

Peffers, K., Tuunanen, T., Rothenberger, M. A. & Chatterjee, S. 2007. A Design Science Research Methodology for Information Systems Research. *Journal of Management Information Systems*, 24(3), 45 – 77.

Public Compnay Accounting Oversight Board (PCAOB). 2010. *Audit Evidence. PCAOB Auditing Standards No. 15.* Washington, DC: PCAOB.

Sakka, M.A., Defude, B. and Tellez, J., 2010. Document provenance in the cloud: constraints and challenges. In *Networked Services and Applications- Engineering, Control and Management* (pp. 107-117). Springer Berlin Heidelberg.

Schmidt, P. J., Wood, J. T. and Grabski, S. V., 2016. Business in the Cloud: Research Questions on Governance, Audit, and Assurance. *Journal of Information Systems* 20(3), 173 – 189.

Teeter, R.A. and Vasarhelyi, M.A., 2010. Remote Audit: A Review of Audit-Enhancing Information and Communication Technology Literature. *Journal of emerging technologies in accounting*.

Vasarhelyi, M.A. and Halper, F.B., 1991. The continuous audit of online systems. In *Auditing: A Journal of Practice and Theory*.

Warncke, E. 2017. "Beyond Bitcoin-Decentralized Banking." Published online June 30, 2017: https://hackernoon.com/beyond-bitcoin-truly-decentralized-banking-d7793edc7d99

Wilken, C. L. and Chenhall, R. H., 2010. A Review of IT Governance: A taxonomy to inform accounting information systems. *Journal of Information Systems* 24(2), 107 – 146.