Accounting and Management Information Systems
Vol. 20, No. 4, pp. 646-669, 2021
DOI: http://dx.doi.org/10.24818/jamis.2021.04004

Distributed ledger technology - Addressing the challenges of assurance in accounting systems: A research note

Kishore Singh[1,a] , Amlan Haque[a], Sabi Kaphle[b]
and Janice Joowon Ban[a]

[a] *School of Business and Law, CQ University, Australia*
[b]*School of Health Sciences, CQ University, Australia*

Abstract

Background: With the progressive development of blockchain technology, its potential influence on the accounting and auditing professions is of interest to academia and practitioners. As the technology gains acceptance in businesses such as banking, stock exchanges, insurance, law, government services, and e-voting, business leaders are beginning to recognise its potential to transform their organisations. Despite concerns about how this technology will marginalise the accounting and auditing profession, blockchain continues to lag behind in adoption and there is time for accountants and auditors to reflect on their current practice and update their knowledge and skills to maintain their relevance to the industry.

Motivation: The literature has not fully examined the implications of distributed ledger technology and its implications for the accounting and auditing profession. The intent of this research note is to identify opportunities for research that are of significance to the application of distributed ledger technology to accounting and auditing.

Research Question: To identify possibilities that exist in researching the adoption, implementation and application of a distributed ledger solution in the context of accounting and auditing.

Framework: Based on the literature, the study proposes a framework for a blockchain model of a simplified triple-entry bookkeeping system using smart contracts to automate self-verification and replication of transactions in a public distributed ledger.

Findings: Drawing on the framework the article develops a series of research questions that may significantly reduce barriers and challenges facing organizations that want to implement blockchain technology in their accounting systems.

[1] *Corresponding author*: Dr. Kishore Singh, School of Business and Law, Central Queensland University, 160 Ann Street, Brisbane, Australia, 4001, email: k.h.singh@cqu.edu.au

***Contribution**:* Given the complex nature of blockchain, cross disciplinary research is proposed to bring together information technology, accounting, assurance, economics and psychology resulting in further understanding of the technology as it relates to, and influences the accounting and auditing profession. In doing so, the paper makes several contributions to the literature.

Keywords: Distributed ledger, blockchain, triple-entry bookkeeping, audit and assurance

JEL Codes: M15, M41, M42, O33

1. Introduction

Blockchain is a distributed ledger technology that enables transaction records to be stored in blocks linked together resembling a chain (Williams, 2021). Copies of the distributed ledger are maintained across all computers (nodes) participating in an internet-based peer-to-peer network. Software running on each node verifies and validates transactions. Consensus protocols ensure that no one node or user can unilaterally modify a record as it is stored in multiple locations in the decentralised network. This ensures distributed control as no individual peer controls the ledger, unlike non-distributed ledger approaches where only a single copy of the records exists which may be manipulated for legitimate or malicious purposes.

Blockchain is an innovative technology originally used for Bitcoin. Most recently, blockchain has evolved from a secure cryptocurrency transaction system to encompass technologies that include artificial intelligence, banking, stock trading, voting, and financial services. Accounting and auditing could be the beneficiary of the benefits that blockchain technologies offer. However, applications of blockchain within accounting and auditing requires further research and development (Dai & Vasarhelyi, 2017). Recent reports by the Big 4 audit firms suggest that blockchain will have a significant impact on record keeping, transaction processing and auditing (Schmitz & Leoni, 2019). PwC views blockchain as a technology that will provide “a radically different competitive future in the financial services industry” (PricewaterhouseCoopers, 2016). Similarly Deloitte expects there to be considerable emerging opportunities for organizations in all sectors to adopt blockchain technology to create and deliver compelling services for their customers (Deloitte, 2016b).

A blockchain is a database that does not have any central management authority, however; it can ensure that data is reliably recorded and organised in the database (Tan, 2017). The blockchain is hosted in a peer-to-peer network where one copy of the database is hosted on every node. Given the distributed nature and consensus mechanism of blockchain, it provides a novel approach to control the ledger of recorded transactions. Every new record is added to existing blocks to form a cryptographically linked chain. This arrangement chains the blocks together. Attempts to make changes to previously approved blocks breaks the chain and requires reprocessing of all subsequent blocks. This has to occur at a rate faster than which new blocks are added, making this technically impossible. As a result, the blockchain is considered immutable and may be resistant to fraudulent transactions (Schmitz & Leoni, 2019). It needs to be noted, however, that blockchain technology does not guarantee security. Adopters need to understand the fundamental differences between public and private blockchains and adopt a suitable model for their context.

Although blockchain applications are appearing in several businesses, will the accounting and auditing profession be such a beneficiary? The potential benefits and challenges require additional study. Despite concerns about how this technology will marginalise the profession, blockchain continues to lag behind in adoption and adequate time remains for accountants and auditors to reflect on their current practice and update their knowledge and skills to maintain their relevance to the industry. While it is not feasible to predict the future impact of blockchain, this paper reviews existing studies and offers several themes for future research and practice within the accounting and audit profession.

This paper makes the following contributions: i) it offers an overview of blockchain in relation to the accounting and auditing profession; ii) it proposes ideas for integrating existing accounting information systems with blockchain technology; iii) it discusses challenges that limit the adoption of blockchain technology within accounting; and iv) it proposes future research opportunities that may provide academics and practitioners with valuable information about the impact that adoption, implementation and application will have on the profession. Findings from future research may provide further insights into the practice of accounting and assurance that facilitates the incorporation of blockchain into existing business models.

The remainder of this paper proceeds as follows. Section 2 provides a background on distributed ledger technology, section 3 discusses the Byzantine Generals Problem and a conceptual model for blockchain-based triple-entry bookkeeping is proposed in section 4. Section 5 discusses the use of blockchain in audit and assurance followed by a discussion on the challenges faced in adopting distributed ledger technologies in section 6. In section 7, suggestions for further research are provided, and we offer concluding remarks in section 8.

2. Distributed ledger technology and blockchain

A distributed ledger is a data structure that resides across multiple computer devices, generally geographically dispersed. Distributed ledger technology (DLT) includes blockchain technologies and smart contracts. While distributed ledgers existed prior to Bitcoin, the Bitcoin blockchain is a convergence of several technologies, including timestamped transactions, peer-to-peer (P2P) networks, cryptography, shared computational power, and a specialized consensus algorithm. DLT consists of three components; a data model that captures the current state of the ledger, a language of transactions that changes the ledger state and, a protocol used to obtain consensus among participants regarding which transactions to accept, and in what order (Hyperledger.org, 2020 ; Tan & Low, 2019 ; Williams, 2021). .

2.1 Blockchain basics

A blockchain is a public database that is updated and shared across many computers in a network. It is an instantiation of a distributed ledger, enabled by consensus, combined with a system for "smart ontracts" and other technologies. Together these can be used to build transactional applications that establishes trust, accountability, and transparency (Hyperledger.org, 2020). "Block" refers to the fact that data and state are stored in sequential batches or "blocks". "Chain" refers to the fact that each block cryptographically references its parent. A block's data cannot be changed without changing all subsequent blocks, which would require the consensus of the entire network. Each new block and the chain as a whole must be agreed upon by every computer in the network. This is to ensure that everyone has the same data. To accomplish this distributed agreement, blockchains need a consensus mechanism (Ethereum.org, 2021).

2.2 Smart contracts and consensus

Smart contracts are computer programs that execute predefined actions when certain conditions within the system are met. They facilitate the exchange and transfer of something of value (for example, monetary transactions, shares or property) and allow the ledger state to be modified (Hyperledger.org, 2020 ; Konstantinidis *et al*., 2018). Consensus in the network refers to the process of achieving agreement among the network participants as to the correct state of data on the system. This results in all nodes sharing exactly the same data. A consensus algorithm does two things: i) it ensures that the data on the ledger is the same for all the nodes in the network, and ii) it prevents malicious users from manipulating the data. There are several types of consensus algorithms which vary by blockchain implementation, for example Proof of Work, Proof of Stake and Proof of Burn (Bonsón & Bednárová, 2019 ; Dai & Vasarhelyi, 2017 ; Hyperledger.org, 2020).

2.3 Public and private blockchains

There are different categories of blockchain types. These are defined according to whether authorization is required for network nodes and whether access to the blockchain data is public or private. A permissionless blockchain is also known as a *public* blockchain, because anyone can join the network to be a verifier without obtaining permission to perform network tasks. Participation is encouraged because verifiers are a vital component of the network (Peters & Panayi, 2016). A permissioned blockchain, or *private* blockchain, requires pre-verification of participating parties within the network, and these parties are trusted or known to each other. Additional verifiers may be added with agreement of the current members or a central authority. Permissioned blockchains are purpose built and therefore can be integrated with an organisations existing systems (such as an accounting information system). The participants on the network are named and are legally accountable for their activity (Peters & Panayi, 2016).

The choice between permissionless and permissioned blockchains is driven by the type of application. Most enterprise use cases involve extensive screening before parties agree to conduct business with each other. Only trusted parties participate in the network. Each participant that is involved in the business requires permissions to execute transactions on the blockchain. Conversely, when trust is implicit, parties transact without having to verify each other's identity, for example the Bitcoin blockchain. In this instance a permissionless blockchain is suitable (Hyperledger.org, 2020).

2.4 Blockchains, ERP Systems and databases

A blockchain is a write-only data structure. New entries get appended to the end of the ledger. Every new block gets appended to the blockchain by linking to the previous block's fingerprint or *hash* (a *hash function* is a type of mathematical function which turns *data* into a fingerprint or *hash)* (Lewis, 2016). There are no permissions within a blockchain that allow editing or deleting of data (Tan & Low, 2019).

ERP systems are pre-packaged business applications built upon Relational Database Management Systems (RDBMS). They are used to process and distribute business information across the organisation in a timely manner to provide support for management decision making (Kuhn Jr & Sutton, 2010). Organisations are able to integrate data from multiple disparate systems enterprise-wide (Dai & Vasarhelyi, 2017). In a relational database, data can be easily modified or deleted. Database administrators have permissions to make changes to the data and/or its structure. Relational databases are generally designed for centralized applications, where a single entity controls the data.

Blockchain may be considered a new type of database that has the potential to replace the accounting functions in an ERP system or be used in conjunction with the existing accounting information system. Unlike the centralized nature of an ERP system, blockchain is decentralized and distributes the power of transaction verification, storage, and organization to a collection of computers. In addition to reducing the risk of a single point of failure it also becomes more difficult for management to override the internal control system with the potential to reduce incidence of fraudulent transactions (Dai & Vasarhelyi, 2017 ; Peters & Panayi, 2016).

2.5 Transactions

Blockchain records are electronically signed using keys (a long string of characters unique to an individual). A transaction record has two matched signatures from the participating parties to prove that the transaction originated from them. These signatures are used to generate a fingerprint or hash. The records in the blockchain are organized into blocks with two fingerprints added in the sequence; fingerprint of block, fingerprint of the previous block, and transaction records (Tan, 2017). The blocks are chained using the fingerprints as shown in Figure 1.

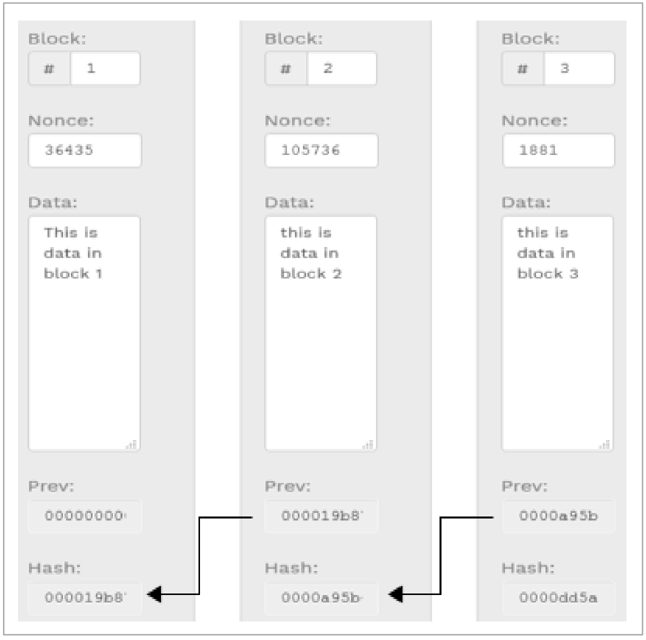
2.6 Immutability of Data

Immutability of data residing on the blockchain is a key driver to deploy blockchain-based solutions. This *unchanging over time* feature makes the blockchain useful for accounting and financial transactions. Once a transaction is written onto the blockchain it cannot be changed easily (Hyperledger.org, 2020 ; Lewis, 2016).

"When people say that blockchains are immutable, they don't mean that the data can't be changed, they mean it is extremely hard to change without collusion, and if you try, it's extremely easy to detect the attempt" (Lewis, 2016).

It is difficult to change or tamper with transactions in a blockchain, because each block is linked to the previous block by including the previous block's hash (Ethereum.org, 2021). This hash includes the root hash of all the transactions in the previous block. If a single transaction were to change, not only would the root hash change, but so would the hash contained in the changed block. Therefore, each subsequent block would need to be updated to reflect this change. The amount of resources required to perform this recalculation for the changed block and each subsequent block would be prohibitive. If someone modified a transaction in a block without going through the necessary steps to update the subsequent blocks, it becomes a trivial task to recalculate the hashes in the blocks and determine that data has been modified (Peters & Panayi, 2016).

Figure 1. Simplified blockchain architecture



Block: # 1
Nonce: 36435
Data: This is data in block 1
Prev: 00000000
Hash: 000019b8

Block: # 2
Nonce: 105736
Data: this is data in block 2
Prev: 000019b8
Hash: 0000a95b

Block: # 3
Nonce: 1881
Data: this is data in block 3
Prev: 0000a95b
Hash: 0000dd5a

(Adapted from: Blockchaintrainingalliance.com, 2021)

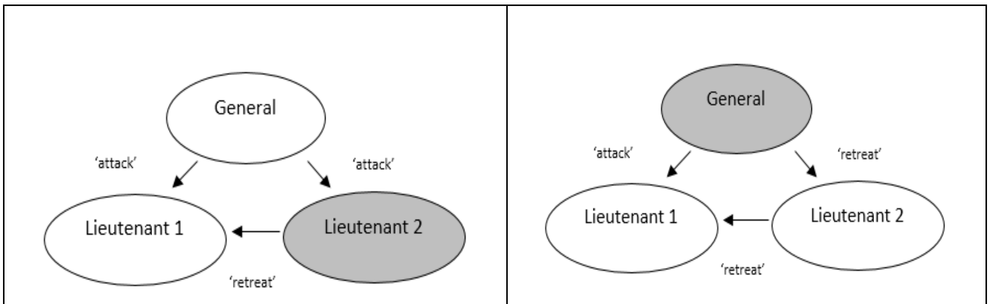
3. The Byzantine Generals Problem and the accounting ecosystem

The Byzantine Generals Problem describes the difficulty of corrupt communications in a decentralized network (Lamport, Shostak & Pease, 1982). In this problem a fictitious commanding General makes a decision to attack or retreat. This decision needs to be communicated to multiple lieutenants. A given number of these lieutenants, possibly including the General, may be traitors that cannot be relied upon to either properly communicate these orders or they may actively alter them. Within the context of computer applications the generals and lieutenants are collectively referred to as *processes*. The General initiating the order is the *source* process and the orders are *messages*.

Generals and Lieutenants that are traitors are *faulty processes*, and loyal Generals and Lieutenants are *correct processes*. The order to retreat or attack is a binary message namely, attack or retreat. An interesting problem is that if the source process is faulty, all other processes have to still agree on the same value, regardless that it is faulty. For example, the source process may tell some processes that the order is attack, and others that the order is retreat. After receiving the order, source processes can poll each other to determine whether there is a conflict or not. However, given different values between two peers, reaching consensus regarding which one is correct is not a trivial activity, as either the source or peer may potentially be faulty (Lamport *et al*., 1982 ; Mark, 2008) (Figure 2). The conclusion that someone is lying is easily reached but identifying the faulty process is not.

Within an accounting context the commanding General may be a module in an ERP system (for example, FI module in SAP) and the Lieutenants may be clients connected to the system. Clients may wish to determine total expenditure for a given vendor for the current period. A reliable FI module would report the same values to all clients, but a corrupted one may report different values to each client, causing the clients to disagree about the true value of total expenditure. Alternatively the Byzantine Generals Problem may also occur due to fraudulent behaviour in humans. For example, a loyal vendor sends an invoice for services rendered and a traitorous customer withholds payment to the vendor, or a traitorous vendor sends a fake invoice for services rendered and a loyal customer pays the vendor. Centralized ERP systems are therefore vulnerable to corruption and are unable to solve the Byzantine Generals problem, which requires that truth be established without trust (River.com, 2021).

Figure 2. Faulty Byzantine processes



Lieutant 2 is a traitor

General is a traitor

3.1 Double entry bookkeeping

Throughout history ledgers have been used to record accounting transactions. These ledgers were initially recorded on stone, parchment, wood and gradually moved towards paper in the 13th and 14th centuries as good quality paper became available (Sangster, 2016). The primitive mechanism of recording business transactions was single-entry bookkeeping where each transaction was recorded only once. Double entry bookkeeping transformed the recording and maintaining of accounting transactions and is the basis for the modern financial system. In the double entry system each transaction requires two accounting entries, a debit and a credit. This helps to preserve an audit trail as amounts are recorded twice and debits must equal credits. Although it is an improvement on the single entry system particularly with regards to errors, fraud detection and financial reality, it is susceptible to manipulation. Even if debits equal credits transactions can be manipulated and fabricated to appear as such. To confirm integrity of accounting transactions auditing is required, which is a time consuming process. Auditors may select a small sample from the entire population of transactions to perform their audit, which may result in errors and fraud being overlooked (Cai, 2021 ; Singh & Best, 2016). Consequently a major problem with the double-entry system is trusting the human and fallible bookkeeper, accountant or auditor.

3.2 Proof-of-work (PoW)

The Byzantine Generals Problem may be solved by using a Proof-of-Work (PoW) consensus mechanism that establishes a set of objective rules for the blockchain (River.com 2021). All networked nodes work to produce a unified transaction history through distributed consensus. Transactions are recorded in a chain of blocks. Every node seeks to produce the next block in the chain using a PoW process. In order to achieve this, the node must publish proof that they invested considerable work into creating the block. The proof is attached in the block header. New blocks are distributed throughout the network and all nodes reach consensus by selecting only one block. As long as the majority of computing power is controlled by loyal nodes (Lieutenants), members can agree on the state of the blockchain and all transactions therein. Each node verifies for itself whether blocks and transactions are valid. If any node attempts to broadcast false information, all nodes on the network will immediately recognize it as invalid and ignore it. Additionally, once a block has been added to the blockchain, it is extremely difficult to remove, making the blockchain virtually immutable (Nakamoto, 2008 ; Xiao *et al*., 2020).

3.3 Triple entry bookkeeping

Ijiri (1986) introduced a triple-entry bookkeeping system to account for wealth, momentum, and force, where the conventional identity debits = credits is extended and a new accounting identity is introduced to link measurements using a rate of change of momentum relationship. The concept of ‘the rate at which income is being earned’ was defined as momentum, measured in monetary units per period, such as dollars per month. A further third-level entry was defined to record the changes of momentum. Grigg (2005) proposed a completely different meaning for the term triple-entry bookkeeping where in addition to traditional double-entry, a third entry is recorded for the same transaction between entities. At the time there was no solution to Grigg’s method as it was unclear who would act as a trusted, neutral third party to control the shared ledger. The triple-entry accounting discussed to in this paper uses Grigg’s method of recording accounting entries in a distributed ledger or with a third party.

When a distributed ledger is shared among several parties it is subject to the Byzantine Generals Problem. This is due to the failure of a distributed system in determining trustworthiness of individual elements. A solution to the problem was released by Nakamoto (2008) where the Byzantine dilemma was resolved. Nakamoto (2008) provided a practical solution to the theory that Grigg (2005) had previously proposed and it did not involve trust. The approach was to cryptographically validate all accounting entries by a third entry by hashing and a nonce. A nonce is an arbitrary number that is used one time when the message is concealed in plain text. Whilst digital signatures are part of the solution, a key component is the removal of the requirement to have a trusted third party. In addition to transaction entries in the ledger remaining consistent, the infrastructure adds a third entry into the ledger's validation process, which is cryptographically signed (Nakamoto, 2008). DLT plays the role of the intermediary by distributing and automating storage and verification and prevents tampering and falsified accounting entries. Due of the nature of blockchain, once an accounting entry is confirmed and added to the chain, it is near impossible to modify or delete the entry (Dai & Vasarhelyi, 2017).

In this paper we discuss the use of smart contracts and a decentralized ledger to implement triple-entry accounting. By maintaining the third accounting entry in the blockchain, a cryptographically secure accounting system becomes possible, and may enable reliable data sharing among various stakeholders (for example, vendors, customers, banks and shareholders).

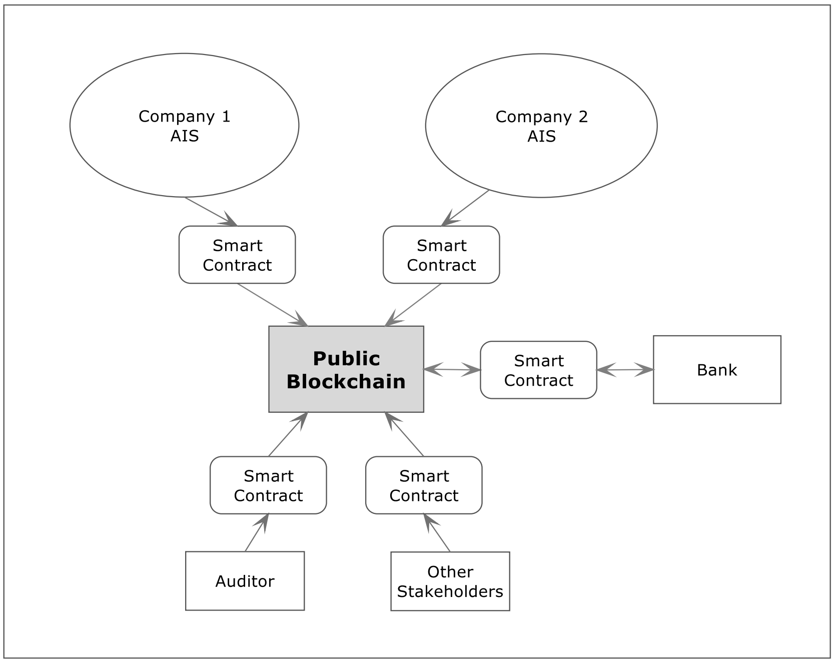
4. Conceptual model for blockchain based triple-entry booking

One possible model of a simplified triple-entry bookkeeping system is shown in Figure 3, based on (Grigg, 2005). In such a system, companies would record transactions in their accounting information systems (AIS) in the standard double-entry format, and smart contracts would replicate these transactions in a public distributed ledger or blockchain. The use of smart contracts adds an additional level of automation within the blockchain, enabling the ledger to self-execute instructions to perform verifications, detect potential fraudulent transactions and enforce agreements between the transacting organizations (Cai, 2021). Furthermore, given blockchains immutable nature the third entry will become the trusted source of truth.

Assume Company 1 (vendor) sells products or provides or services to Company 2 (customer). Both Company 1 and Company 2 predetermine the rules of the transaction on a self-executing smart contract. Company 1 creates an invoice in its AIS. A timestamped version of this transaction together with terms and details of payment are recorded in the blockchain. To ensure privacy of the transaction it will be encrypted with Company 2's public key. Once Company 2 verifies and approves the transaction, the blockchain is updated. A smart contract will confirm the transaction with the bank. The bank transfers the payment and the smart contract updates the public ledger to reflect that payment has been made. Auditors can access the public ledger and verify authenticity through the transaction hash. Digitally signing and timestamping the transactions prevent them from being altered and will provide reliable audit trail evidence leading to trustworthy financial information. Public transactions will be visible to all participants. Private transactions will be restricted to those participants whose public keys are specified in the transaction. In this way, although transactions are executing in a public blockchain, participants that are not party to the transactions will not have access. Participants with appropriate access would have the ability to aggregate the firm's transactions to produce income statements or balance sheets on an ad hoc basis, thus removing the need to rely on quarterly financial statements prepared by the firm.

Using the same procedure, a company may record accounting data generated by other business processes, for example, sales, purchases, inventory management and cash collections. Recording of these processes will each require a customized smart contract. All the processes are automated and transaction entries are cryptographically secured by the blockchain which renders falsification or modification to conceal fraud virtually impossible. Whilst the scope of participant access to the blockchain may be broad, submission of transactions to the distributed ledger and its subsequent verification may be restricted to the participating companies, accountants, auditors and management, namely those with specialized authorizations.

Figure 3. Conceptual model for blockchain-based triple-entry bookkeeping



In Figure 3, by applying the Byzantine Generals Problem to accounting, Company 1 would play the role of the General, company 2, the auditor and other stakeholders would be the Lieutenants. Participating companies would be prevented from manipulating accounting transactions as their traditional entries are mirrored with a reliable third entry that cannot be retroactively altered. Consequently, triple-entry accounting enabled by smart contracts and blockchain technology may resolve the trust and transparency concerns associated with double-entry accounting systems. This may require fraudsters to increase their efforts to perpetrate fraud, rather than simple falsification of transaction records, leading to a subsequent decline in such activities. Although one needs to be cognisant of the fact that the source of the data initially recorded in the AIS and, ultimately the blockchain needs to be valid in the first instance. Therefore, this approach may still be fallible to collusion and off-book frauds.

Many firms may be hesitant to move their entire accounting records onto the blockchain. It is not necessary to begin by moving all accounting transactions to the blockchain. The blockchain as a source of trust can be very helpful in existing accounting structures. It may be gradually integrated with typical accounting procedures; commencing with securing the integrity of records, to completely traceable audit trails. The technology has the potential to change current accounting practices and to provide a method of automating accounting processes in compliance with the regulatory requirements. With globalization of markets, difficulties in compliance with cross-border transactions, and the volume and velocity of financial transactions, audit professionals face increasing challenges as traditional audit procedures are unable to provide near-real time assurance (Alles, Kogan & Vasarhelyi, 2002 ; Rezaee *et al*., 2002).

5. Blockchain in audit and assurance

Blockchain technologies are creating new opportunities and challenges for audit and assurance. Audit is prescribed by regulations in many countries for selected companies. The purpose of the audit is to provide an opinion on whether financial statements are true and fair (Tan & Low, 2019). Current audit practice is labour intensive. The process commences with auditors being provided with journal entries, spreadsheet files and other documents both in electronic and manual formats. Before commencing the audit, the data needs to be prepared and the audit planned. This is a time consuming and lengthy process (Schmitz & Leoni, 2019). As awareness of blockchain-based systems increases there may be significant implications for accounting and auditing functions within organizations. Blockchains potential for providing reliable accounting information is appealing to accountants, auditors and investors. By using blockchain technology to record transaction data in real-time, auditors and audit systems can conduct substantive testing in a continuous manner. The immutability and irreversibility of transaction data would ensure its integrity thereby preventing fraud (Wang & Kogan, 2017).

Despite current auditing controls, accounting frauds continue to occur (ACFE 2020). Poor accounting practice, centralization of accounting and globalization of markets continue to pose challenges across transnational regimes. Accounting transactions recorded in a blockchain, however, may not automatically be true and accurate as errors of off-book frauds may still occur and go unrecognized. However, the likelihood of such occurrences is small. The increasing number of transactions and the speed at which they occur are the main weakness that characterizes accounting, particularly as auditors cannot audit all transactions and they only sample a selection based on the risk level (Alles *et al*., 2002; Rezaee *et al*., 2002). Furthermore, there is limited cross checking of transactions recorded in the accounts of participating companies (Faccia & Mosteanu, 2019)

Within auditing many areas (e.g., cash payments, accounts payable, and so on) are audited through the collection of confirmations from third parties of a company's balances. In a blockchain based distributed ledger many of these transactions are already verified by the participating companies and are therefore already verified. Multi-party verification may assist in the collection of reliable audit evidence for transactional information, thereby enhancing the quality of such evidence (Fuller & Markelevich, 2020). In Figure 3, participating company’s replicate their accounting transactions in a blockchain. Smart contracts verify transactions which improve the quality of data available to auditors compared to internal company documents that lack third party verification (the approach currently used to collect audit evidence). Accountants and auditors would be able to efficiently examine historical and current transactions and spend less time verifying these transactions, saving resources for more subjective areas of the audit (Deloitte, 2016a).

Accounting information systems produce detailed log files of activities and transactions performed. For example, Singh and Best (2015) describe a type of fraud referred to as “flipping” where a vendor’s banking details are temporarily changed, payment is processed (to the fraudsters bank account) and banking details are changed back to the original values. In a blockchain environment, two approaches may be used to prevent such an event from occurring. In the first instance, both the vendor and customer need to approve the requested change, or secondly, if companies replicate only log files onto the blockchain, then an immutable record of the “flipping” is available on the blockchain for investigation by auditors. By recording audit logs on the blockchain, tracing and review of entries would be enhanced as all entries are unchangeable. Such continuous auditing will make it simpler for auditors to investigate fraud since this real-time multi-party verification approach will highlight anomalies at the time of occurrence allowing for timely investigations (Schmitz & Leoni, 2019). Similarly, electronic copies of purchase orders, invoices, bills of lading, goods receipts, credit memos, and so on can be recorded in the blockchain enabling auditors to test the completeness of financial information (Dai & Vasarhelyi, 2017). Sharing these documents among related parties provides for cross-validation. For example, missing invoices at the customer side may indicate a fictitious sale. Therefore, the absence of particular records may indicate fraudulent transactions.

By using a blockchain based distributed ledger, stakeholders do not need to rely on the judgment of auditors and the integrity of accountants and company executives. They participate in transaction verification and provide real-time assurance of the data. Therefore they can rely on the trustworthiness of data on the blockchain and impose their own accounting judgment to make their own adjustments such as depreciation or inventory revaluation (Yermack, 2017). Instead of relying on auditors whom may be subject to moral hazard and agency problems (Ronen, 2010) each stakeholder has the ability to create their own financial statements from the blockchain data, for any time period of their choosing. This radical change in accounting and financial reporting does require making proprietary information available to outsiders, however the benefits are the increased trust in the company's data by shareholders and the changed role of auditors who would no longer be needed to assure the accuracy of the company's books and records.

As organizations increasingly adopt blockchain technology for creating verifiable accounting systems, the current assurance paradigm will change. Blockchain enabled auditing may enhance an auditors understanding of the clients business as the engagement is on a continuous versus annual basis. However, this assumes that the company records all its business transactions on the blockchain. By using the blockchain as a reliable storage medium any audit-related documents will be stored immutably. This information and documents are available for sharing with stakeholders thus potentially expanding the role of providing assurance from auditors to business partners, creditors, government bodies, etc., creating a new level of assurance.

6. Challenges in adopting distributed ledger technologies

Integrating blockchain technologies into existing accounting ecosystems may offer opportunities to transform the audit by providing auditors with more efficient and effective ways to verify accounting data by using smart contracts and trust-less multi-party verification of transactions. However, integration in the accounting and auditing disciplines faces a number of challenges (Fuller & Markelevich, 2020). Key among them are challenges regarding the lack of standards, regulatory challenges, and the lack of knowledge about blockchain and distributed ledger technologies. Other challenges include: resistance to change, interoperability with existing accounting information systems, complexity, scalability and cost (Blockchaintrainingalliance.com, 2021).

Coyne and McMickle (2017) determined that blockchain accounting is infeasible for several reasons. They identify the following three hurdles: the need for confidentiality that renders public blockchains undesirable, the ability for firms to retroactively manipulate private blockchains, and the limited transaction verification that the blockchain provides. The need for confidentiality is a key factor as data such as customer and vendor lists, unit prices and transactions stored in ledgers would need open publication in a public blockchain. A private blockchain may resolve the issue however, by restricting access the network may revert to two-party verification and this fails to create a solution to the Byzantine Generals Problem. Additionally, all companies that participate in the network would need to adopt the same blockchain technology. This may force companies to adopt multiple blockchain implementations, depending on whom they are transacting with.

Consensus protocols in the blockchain ensure that all participants comply with agreed rules, transactions from a legitimate source, and every participant consents to the state of the distributed ledger (Sayeed & Marco-Gisbert, 2019). Proof of Work consensus prevents retroactive modification of the blockchain due to the manipulator requiring significant computing resources and energy requirements. However, if the manipulator were a group with 51% of the computing power, then revisions could be made and the firms blockchain would be at risk. By maintaining a private blockchain 100% of control would remain with the company but it will have the ability to modify the blockchain. An alternative approach would be to actively require an external auditor to participate in the verification process. With the work distributed among various participants, transaction verification may still be ineffective as the validity of these transactions may be questionable. This is a result of participants being unaware of the true nature of the transaction (Coyne & McMickle, 2017), for example, collusion between a purchasing manager and an accomplice vendor may result in a company being overcharged for goods or services provided (Singh & Best, 2015). Thus it is not clear whether blockchain technology will increase the reliability of the accounting numbers.

Scalability is a key reason preventing wide-scale adoption of triple-entry accounting on the blockchain. Since transacting parties are required to maintain a common distributed ledger, all verifiers need to participate and cooperate. This technically limits the number of transactions that can be performed per second (Cai, 2021). Decentralisation and the many distributed copies of a blockchain limit the number of transactions per second. For example, the Bitcoin network can process a maximum of 7 transactions per second (Blockchain-council.org, 2020). Visa on the other hand processes approximately 1700 transactions per second with over 150 million transactions per day. Improving scalability may require increasing the transactions per second or reducing the block size. When leveraging a public blockchain, for example Bitcoin or Ethereum, these parameters are hard coded and it may not be possible to adjust them (Kenny, 2019). While a single company may not exceed the performance limit of the blockchain, the distributed ledger only reaches its potential when there are many companies using it.

Companies considering implementation of blockchain technology need to justify its use over traditional accounting information systems or even lower cost alternatives. Alternative technologies currently exist that would deliver similar outcomes to blockchain for accounting purposes, such as distributed databases or ERP systems (Peters & Panayi, 2016). Furthermore, there is no substantial business case for integration of blockchain with traditional accounting systems at present (Fuller & Markelevich, 2020). Companies that have invested heavily in their ERP systems are reluctant to invest further in emerging technologies. Additionally, as blockchain integration is a significant technological transformation that may require accountants, auditors and other users to change their work practices, there may be resistance to such change. To reap the benefits of blockchain, acceptance by all stakeholders is needed (Davis, 1989).

7. Suggestions for further research

Blockchain may be seen as a new technology that offers a solution to triple-entry bookkeeping (Grigg, 2005). This distributed ledger system may enable a significant change in the approach companies use to exchange information (Deloitte, 2016a). However, as with any new technology there are significant barriers and challenges facing companies that want to implement blockchain in their accounting systems. Given the complex nature of blockchain it is prudent that further research is conducted to examine multi-dimensional aspects of the technology. Cross disciplinary studies that bring together information technology, accounting, assurance, economics and psychology may assist in providing support for blockchain. While the body of academic and professional knowledge is continually developing, it is still equally limited. Accountants and auditors need to develop appropriate knowledge in collaboration with academics and professionals across a multitude of disciplines to better understand the technology, its application and benefits to their clients.

7.1 Standards and Privacy Issues

As blockchain systems evolve and the impetus for adoption in organisational accounting system increases, there will be significant implications for accountants, auditors, corporate stakeholders and regulators. Advances in accounting systems towards blockchain technology and smart contracts will enable automated verification based on accounting standards and pre-specified business rules (Dai & Vasarhelyi, 2017). While standards may be embedded within smart contracts, it is imperative that all stakeholders participate and collaborate in the design and implementation of such standards. Research is required to determine the adequacy of existing standards and to propose changes that consider blockchain and triple-entry accounting.

Another area for research is to determine the practicality of embedding all the rules of financial accounting within smart contracts. Would it even be possible to automate all these rules? Future research may investigate changes to accounting practice to take advantage of blockchain technology. In the current regulatory environment, external stakeholders are unable to verify accounting records personally due to lack of access. However, if companies make their accounting information publicly available, these stakeholders could be asked to verify transactions recorded by the company. Future research can further investigate the feasibility of this option.

The auditor's role will evolve to focus on more valuable activities, such as strategy advice, in-depth analyses and data mining and the current audit paradigm may need to change. Research is needed to determine; how these audit standards may need to change, what standards should be embedded in smart contracts and whether blockchain consensus is a sufficient audit mechanism. Furthermore, while blockchain increases trust, there is no agreement on who is accountable for fraud, errors, or anomalies within the transaction data. Research is therefore required to determine, who is responsible for governance of the blockchain, and what is the role of accounting and audit professionals in this process.

Privacy concerns regarding a company's accounting records on a distributed ledger are significant. While several approaches exist to ensure privacy in the distributed ledger, for example: using hashes of transactions on the ledger, using trusted third parties to independently verify transactions, or by using cryptographic schemes to obscure transaction contents, these do not support public verifiability and this eliminates the benefits of a distributed ledger (Cai, 2021 ; Narula, Vasquez & Virza, 2018). The second approach is to use a public blockchain which reveals transaction contents and may discourage implementation. Future research may investigate development of an accounting specific blockchain model that offers a hybrid solution.

7.2 Lack of knowledge

Blockchain technologies are disrupting the accounting and auditing profession. These developments have implications that may alter the role of professional accountants and auditors. They need the knowledge and skills to maintain their relevance to industry or risk being replaced by IT professionals and technology. Research is required to identify gaps in the knowledge areas of professional accountants and auditors associated with blockchain technologies and propose strategies to address these gaps. It is key that accountants and auditors have a solid understanding of the current state of blockchain technologies. This will help them understand and determine the implications for the profession. While it is not feasible to fully understand the impacts of blockchain technology on accounting and auditing, practitioners are facing business clients currently adopting the technology. Hence accountants and auditors must broaden their skill set and knowledge to be able to anticipate and meet the demands of their clients. Research is required to identify implications for the accounting and auditing practice. While traditional accounting and auditing services will remain important in the future, the spectrum of tasks that accountants and auditors are required to provide will change, as will the skills they need to develop. Research should aim to answer questions such as what knowledge do accountants and auditors need in a blockchain environment, and how will the job role of accountants and auditors change. Research findings may foster changes to audit standards, education and university curricula.

7.3 Resistance to change

Why do people accept or reject new technology? Research suggests that there are two primary determinants. First, people will use a system if they perceive that it will help them improve their job performance. This is referred to as *perceived usefulness*. Second, is their perception about the ease of use of the system. If they believe that it is too hard to use the system then the performance benefits are outweighed by the effort needed to use it. This is referred to as *perceived ease of use*. Both factors determine acceptance of a new system (Davis, 1989). Thus, even if blockchain improves performance, if it is not perceived as useful, it may unlikely be used due to resistance or unwillingness by individuals to use it (Walsh *et al*., 2021). Researchers may need to address issues relating to psychological factors that cause resistance prior to and after adoption of blockchain. Accountants and auditors may have a bias towards current technology and prefer to continue using these. There is a perception of a knowledge gap in their understanding of the technology. Research is required to assess the relative costs and benefits of blockchain over current systems and development of appropriate training and education to address these concerns. Adoption of blockchain accounting systems may require a change in culture of the organisation as a whole. Switching from existing stable accounting information systems to emerging technologies requires a change in the perception of all users. Traditional systems are closed and private, whereas distributed ledger technology requires an open ecosystem which may be considered inferior. Research that provides an organisational perspective on blockchain to illustrate its performance characteristics in relation to existing systems is needed. Users may be motivated to adopt blockchain technologies if they believe that failure to do so would result in a significant impact to the organisation and its participation in the digital economy. Uncertainty among users continue to prevail due to limited understanding of the technology and why it may be introduced in their organisations. Additional research is needed to reduce these uncertainties.

7.4 Interoperability

Blockchain has the potential to disrupt current accounting systems and models. It has made the concept of triple-entry booking possible in practice with the use of distributed ledgers (Deloitte, 2016a ; Nakamoto, 2008). Therefore, it has the potential to revolutionise the sector. Transforming existing accounting systems to incorporate blockchain is still in the early stages. Building an entire new accounting system from the ground up may be currently impractical due to regulatory requirements, complex control systems and other checks and balances that are required to maintain integrity and reduce opportunities for fraud and errors to occur. Organisations, however, are seeking opportunities to incorporate blockchain technologies with their existing accounting systems.

Research is required to investigate how organisations may leverage and integrate their existing investments in ERP systems with blockchain technologies. Dai and Vasarhelyi (2017) propose a theoretical design where transactions are recorded in an organisations ERP system and a token is transferred to the blockchain ledger representing the third immutable entry. Nevertheless, there are several challenges associated with their model. From a technological perspective, blockchain is complex and resource intensive and finding business partners willing to co-operate with a decentralized architecture may be problematic. The model relies on a private blockchain implementation which is not consistent with the triple-entry framework proposed by Grigg (2005). It functions within a closed ecosystem, which is not publicly accessible, so it has limited application. Additional academic research regarding implementations within the accounting discipline is scarce (Schmitz & Leoni, 2019).

The Big 4 audit firms (PwC, Deloitte, Ernst & Young and KPMG) continue to conduct their own research and development relating to blockchain accounting systems. Further research and development in blockchain based accounting systems are needed to demonstrate real-world implementations of triple-entry accounting that are of practical value to organizations. Another area of research is the smart contracts that are needed to be the intermediary between the accounting information system and the blockchain. For accountants and auditors an area of concern is ensuring that standards and regulations are maintained in the development of smart contracts. Another issue is determining what rules and controls that are to be embedded within smart contracts. More research is needed to address these development issues and to guide the application of smart contracts within audits, that may make the audit process more effective and efficient. Research methods may include experiments, surveys, interviews, and case studies.

7.5 Scalability, complexity and cost

Several challenges determine the appropriateness of a blockchain for an accounting system. Notably scalability is of concern (Dai & Vasarhelyi, 2017; Fuller & Markelevich, 2020). In an existing regular double-entry database, two copies of a transaction record exist, one in the customers database and one in the vendors. Transactions in a distributed ledger are replicated on each participants computer. Depending on the number of participants this could be hundreds or thousands of copies, with associated infrastructure and storage costs. Another potential scalability concern is transaction velocity. The Bitcoin blockchain processes a maximum of 7 transactions per second (Blockchain-council.org, 2020). Visa on the other hand processes approximately 1700 transactions per second. Research is therefore required to determine the implications of scalability and extensive computational requirements for large organisations with many customers and vendors, for example, would such blockchains become unmanageable over time. Further research could investigate development of blockchain systems for accounting specific applications.

Within a double-entry accounting system, auditors regularly make changes or revisions to previously reported numbers. These occur because of changes in estimates, rules or accounting errors. In existing systems auditors can make changes to previously reported numbers, however, with the immutable nature of blockchain, this may be an issue. Research is needed to determine how blockchain systems will support revisions to previously reported numbers and whether the technical complexity of such systems will limit or prevent adoption.

Blockchain accounting systems differ from cryptocurrency ones. Participants is a cryptocurrency blockchain are rewarded with monetary payments. The same is not the case in an accounting blockchain as participants are not reimbursed. Instead they participate to obtain benefits such as data reliability, resilience, and potential cost reduction for accounting and auditing functions in the long term. These potential benefits may serve as an incentive for companies to adopt the platform, however, research is required to determine the extent to which companies are willing to change their internal systems, absorb the cost of adoption and invest in education and training of their users. Additionally, each company may adopt a different type of blockchain which implies that participants would need investments in a multitude of blockchain systems. Will this be feasible? Further research is needed in this regard as the difficulty of making a compelling cost/benefit case is likely to a challenge widespread adoption.

8. Concluding remarks

Blockchain technology is gaining acceptance in many businesses such as banking, stock exchanges, insurance, law, government services, voting and more industries continue to be identified regularly as business leaders recognise its potential to transform their organisations. The accounting and audit profession may benefit from this disruptive technology. While it is not feasible to predict the future impact of blockchain, this paper offers several areas of research to investigate this disruptive technology and its potential to transform the accounting and audit profession. Accounting transactions and ledgers presently reside in ERP systems within a company's centralised database. A blockchain solution enables the creation of a distributed ledger that is hosted on multiple decentralised databases. The element of trust located with a single authority in the centralized approach is removed as trust is *democratised* among each participant. The use of smart contracts enables automated verification based on accounting standards and pre-specified business rules. Consequently the role of accountants and auditors may evolve to focus on more valuable activities, such as strategy advice, in-depth analyses and data mining and the current audit paradigm may need to change. However, they will continue to play an important role in the organisation by offering advice on policy decisions related to blockchain. Furthermore, while blockchain technology may resolve the trust and transparency concerns associated with double-entry accounting systems it continues to remain fallible to collusion and off-book frauds. Therefore, it does not guarantee that financial reports will be true and fair. Organisations at present are unwilling to forgo their investments in current ERP systems and feel the need to control their private accounting data. However, it is anticipated that traditional accounting information systems may selectively integrate blockchain technology into some of their applications. Therefore, while blockchain-based accounting systems will benefit the profession, it is unlikely to be transformative. It is therefore the authors' opinion that blockchain-based accounting is not a silver bullet for the profession at present?

This research note aimed to provide some additional perspectives on blockchain research. Contemporary research focuses on blockchain technology as it applies to other disciplines. There is limited research on its application to the accounting and audit profession. Given the complex nature of blockchain, it is prudent that further research is conducted to examine multi-dimensional aspects of the technology. Cross disciplinary studies that bring together information technology, accounting, assurance, economics and psychology may assist in providing support for blockchain. Additionally, a holistic focus on the links between blockchain, triple-entry accounting and existing accounting systems may provide academics and practitioners with valuable information about the impact on adoption, implementation and application on the profession. While the body of academic and professional knowledge is continually developing, it is still equally limited.

Finally, adopting blockchain based accounting systems are not just about implementing new technology alone. It transforms the way organizations manage their accounting, assurance, risk and compliance practices. It takes time and attention, and a variety of challenges may be expected during the transformation process. Research should enable academics and managers alike to understand the extent to which blockchain technology can transform their processes, risks and controls, technology, and people to achieve their business objectives.

References

ACFE (2020) Report to the nation on occupational fraud and abuse, https://www.acfe.com/report-to-the-nations/2020/. *Accessed:* 7/10/2021

Alles, M. G., Kogan, A. & Vasarhelyi, M. A. (2002) "Feasibility and economics of continuous assurance", *Auditing: A Journal of Practice & Theory*, vol. 21 (1): 125-138.

Blockchain-council.org (2020) Blockchain: Underlying technology behind cryptocurrency and why does its transaction speed matter?, https://www.blockchain-council.org/cryptocurrency/top-cryptocurrencies-with-their-high-transaction-speeds. Accessed*:* 11 August 2021

Blockchaintrainingalliance.com (2021) Blockchain overview: Business foundations on demand, *Blockchain Training Alliance,* https://blockchaintraining alliance.com/pages/lab-distributed. Accessed*:* 27 July 2021

Bonsón, E. & Bednárová, M. (2019) "Blockchain and its implications for accounting and auditing", *Meditari Accountancy Research,* In press

Cai, C. W. (2021) "Triple entry accounting with blockchain: How far have we come?", *Accounting & Finance*, vol. 61 (1): 71-93.

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

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

Davis, F. D. (1989) "Perceived usefulness, perceived ease of use, and user acceptance of information technology", *MIS Quarterly,* Management Information Systems Research Center, University of Minnesota, 13 (3): 319-340.

Deloitte (2016a) "Blockchain technology. A game-changerin accounting?", *Deloitte & Touche GmbH Wirtschaftsprüfungsgesellschaft,* https://www2.deloitte.com/content/dam/Deloitte/de/Documents/Innovation/Blockchain_A game-changer in accounting.pdf. Accessed*:* 28 July 2021

Deloitte (2016b) Blockchain. Enigma. Paradox. Opportunity, https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/financial-services/deloitte-nl-fsi-blockchain-enigma-paradox-opportunity-report.pdf. Accessed*:* 13 July 2021

Ethereum.org (2021) Ethereum developer resources, https://ethereum.org/en/developers/docs/intro-to-ethereum/. Accessed*:* 13 July 2021

Faccia, A. & Mosteanu, N. R. (2019) "Accounting and blockchain technology: from double-entry to triple-entry", *The Business & Management Review*, vol. 10 (2): 108-116.

Fuller, S. H. & Markelevich, A. (2020) "Should accountants care about blockchain?", *The Journal of Corporate Accounting & Finance,* vol. 31 (2): 34-46.

Grigg, I. (2005) "Triple entry accounting", working paper, pp. 1-10.

Hyperledger.org (2020) About hyperledger, https://www.hyperledger.org/about. Accessed*:* 13 July 2021

Ijiri, Y. (1986) "A framework for triple-entry bookkeeping", *Accounting Review,* vol. 61: 745-759.

Kenny, L. (2019) "The blockchain scalability problem & the race for visa-like transaction speed", https://towardsdatascience.com/the-blockchain-scalability-problem-the-race-for-visa-like-transaction-speed-5cce48f9d44. Accessed*:* 11 August 2021

Konstantinidis, I., Siaminos, G., Timplalexis, C., Zervas, P., Peristeras, V. & Decker, S. (2018) “Blockchain for business applications: A systematic literature review”, In *Business Information Systems*, Springer.

Kuhn Jr, J. R. & Sutton, S. G. (2010) “Continuous auditing in ERP system environments: The current state and future directions”, *Journal of Information Systems*, vol. 24 (1): 91-112.

Lamport, L., Shostak, R. & Pease, M. (1982) “The byzantine generals problem”, *Transactions on Programming Languages and Systems*, ACM, 4 (3), 382-401.

Lewis, A. (2016) “A gentle introduction to immutability of blockchains”, LinkedIn.

Mark, N. (2008) The Byzantine Generals Problem, Dr. Dobb's Journal (1989), San Mateo: MultiMedia Healthcare Inc, 33 (4): 30.

Nakamoto, S. (2008) Bitcoin: A peer-to-peer electronic cash system, https://bitcoin.org/bitcoin.pdf. Accessed*:* 28 July 2021

Narula, N., Vasquez, W. & Virza, M. (2018) zkledger: Privacy-preserving auditing for distributed ledgers, *15th USENIX Symposium on Networked Systems Design and Implementation (NSDI 18).*

Peters, G. W. & Panayi, E. (2016) “Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money”, *Banking Beyond Banks and Money*, Springer.

PricewaterhouseCoopers (2016) What’s next for blockchain in 2016?, https://www.pwc.com/us/en/financial-services/publications/viewpoints/assets/pwc-qa-whats-next-for-blockchain.pdf. Accessed*:* 13 July 2021

Rezaee, Z., Sharbatoghlie, A., Elam, R. & McMickle, P. L. (2002) Continuous auditing: building automated auditing capability. *Auditing*, 21 (1), 147-163.

River.com (2021) “What is the byzantine generals problem?”, *River Financial*, https://river.com/learn/what-is-the-byzantine-generals-problem/. *Accessed:* 28 July 2021

Ronen, J. (2010) “Corporate audits and how to fix them”, *Journal of Economic Perspectives*, vol. 24 (2): 189-210.

Sangster, A. (2016) “The genesis of double entry bookkeeping”, *The Accounting Review*, vol. 91 (1): 299-315.

Sayeed, S. & Marco-Gisbert, H. (2019) “Assessing blockchain consensus and security mechanisms against the 51% attack”, *Applied Sciences*, vol. 9 (9): 1788.

Schmitz, J. & Leoni, G. (2019) “Accounting and auditing at the time of blockchain technology: a research agenda”, *Australian Accounting Review*, vol. 29 (2): 331-342.

Singh, K. & Best, P. (2016) “Interactive visual analysis of anomalous accounts payable transactions in SAP enterprise systems”, *Managerial Auditing Journal*, vol. 31 (1): 35-63.

Singh, K. & Best, P. J. (2015) “Design and implementation of continuous monitoring and auditing in SAP enterprise resource planning”, *International Journal of Auditing*, vol. 19 (3): 307-317.

Tan, B. S. (2017) “Blockchain - A database with a twist”, https://ssrn.com/abstract=2958565 *Accessed:* 13 July 2021

Tan, B. S. & Low, K. Y. (2019) “Blockchain as the database engine in the accounting system”, *Australian Accounting Review*, vol. 29 (2): 312-318.

Walsh, C., O’Reilly, P., Gleasure, R., McAvoy, J. & O’Leary, K. (2021) “Understanding manager resistance to blockchain systems”, *European Management Journal*, vol. 39 (3): 353-365.

Wang, Y. & Kogan, A. (2017) “Designing privacy-preserving blockchain based accounting information systems”, *SSRN Electronic Journal*.

Williams, R. (2021) “What is blockchain?”, *The Blockchain Academy*, https://theblockchainacademy.com/. Accessed*:* 09/04/2021

Xiao, Y., Zhang, N., Lou, W. & Hou, Y. T. (2020) “Modeling the impact of network connectivity on consensus security of proof-of-work blockchain”, IEEE.

Yermack, D. (2017) “Corporate governance and blockchains”, *Review of Finance*, vol. 21 (1): 7-31.