International Journal of Accounting Information Systems xxx (xxxx) xxx

Contents lists available at ScienceDirect

International Journal of Accounting Information Systems

journal homepage: www.elsevier.com/locate/accinf

Blockchain architecture: A design that helps CPA firms leverage the technology☆

Nishani Edirisinghe Vincent [a,*], Anthony Skjellum [b], Sai Medury [b]

[a] The University of Tennessee at Chattanooga, 615 McCallie Avenue, Chattanooga, TN 37403, United States of America
[b] SimCenter, University of Tennessee at Chattanooga, 701 East M L King Blvd, Chattanooga, TN 37403, United States of America

ARTICLE INFO

Available online xxxx

Blockchain technology has garnered the interest of the accounting profession in recent years. However, when considering whether to adopt this technology, many business professionals have voiced a lack of a compelling use case as a major challenge. To utilize the technology effectively, first, we need to establish how organizations will connect to the blockchain that will also provide a compelling use-case for CPA firms. In this paper, we design a blockchain architecture for organizations that will facilitate effective connectivity to a blockchain while enabling auditors to leverage this technology to provide audit and assurance services. To design the architecture, we consider two broad questions: first, how do CPA firms gain access to reliable audit evidence and, second, how can client firms maintain confidentiality and security of their data given a decentralized and distributed immutable ledger (i.e., a blockchain). Consequently, the proposed architecture will help auditors gain access to reliable digital audit evidence while incentivizing client firms to adopt blockchain technology by substantially reducing the costs of replacing existing information systems. Given this architecture, auditors could also design continuous audit procedures for their respective clients without having to incur substantial investments in software integration. Further, the architecture can be expanded to include various use cases and supply chain participants, other CPA firms, customers, and regulators.

1. Introduction

Blockchain technology is an important information technology trend that has been closely examined by the accounting profession during recent years. The American Institute of Certified Public Accountants (AICPA) published at least eight press releases about blockchain technology in 2018. The topics of interest included tax reform, implications for audit and assurance, strategic directions, and research opportunities. Further, an AICPA press release mentions that the emergence of blockchain is "widely seen as having significant implications for the evolution of financial audits and other complex processes that require verification and confirmation" (AICPA, 2018b). A global blockchain survey conducted by Deloitte in 2018 indicates that 74% of respondents already participate or would likely participate in a blockchain consortium in the near future (Deloitte, 2018). Further, experts are convinced that firms should at least stay up to date on blockchain development and that doing nothing would be a mistake

☆ This work was performed with partial support from the National Science Foundation under Grants Nos. CCF-1562659, CCF-1562306, CCF-1617690, CCF-1822191, CCF-1821431. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation. We thank the referees and participants at the 2019 UW CISA 11th Biennial Symposium on Information Integrity and Information Systems Assurance for helpful comments, especially the discussants Archana Subramanian and Deniz Appelbaum.

* Corresponding author.
E-mail addresses: surani-vincent@utc.edu, (N.E. Vincent), tony-skjellum@utc.edu, (A. Skjellum), Sai-Medury@mocs.utc.edu. (S. Medury).

https://doi.org/10.1016/j.accinf.2020.100466
1467-0895/

(Deloitte, 2018). Despite such widespread interest, 21% of global respondents and 30% of US respondents say that there is as yet a lack of a compelling use-case to justify blockchain implementation.

Currently, there are supply chain, financial services, distribution, and government use cases for blockchain; however, certified public accounting (CPA) firms are uncertain about how this technology enhances audit and assurance (CPA Canada, 2017). A collaborative whitepaper published by AICPA, CPA Canada, and the University of Waterloo recognizes that blockchain technology will impact audit and assurance and make accessing client information more efficient (CPA Canada, 2017). However, the efficient use of blockchain for CPA firms and other participants will depend heavily on how firms decide to connect to the blockchain. Consequently, like any other system, the design considerations of blockchain architecture at the development stage will impact whether CPA firms can leverage the technology to enhance audit and assurance services provided to their clients. Therefore, in this paper, we provide a blockchain architecture that addresses some major challenges auditors face during an audit. The proposed architecture will not only address client firms' data confidentiality and security issues but will also allow CPA firms to leverage the technology to enhance audit and assurance services. Even though the architecture is presented as a use case for CPA firms, this architecture could also be expanded to provide the means necessary for collaboration, control, and compliance among various processes, supply chains, financial services, and regulatory participants.

When designing a system architecture, the first step is to identify major problems or challenges faced by the particular organization. Once the challenges are well defined, decision-makers can evaluate various alternatives to identify whether a certain technology will be able to provide a solution to the identified challenges. Therefore, from a CPA firm's perspective, the first step is to identify and define a challenge faced by the CPA firm. One of the most important activities in an audit and where the majority of the auditors' time is spent is on collecting sufficient and appropriate audit evidence. Auditors gather evidence to verify the assertions (such as occurrence, completeness, accuracy, cutoff, and classification) embodied in financial statements to meet audit objectives (AICPA, 2006). To form an opinion, the evidence collected should be both relevant and credible. An early study by Beasly et al. (2001) finds that the most common cause of audit deficiencies is the failure to gather sufficient audit evidence. Inability to verify whether the records are complete and accurate, supporting documents gathered are sufficient, supporting documents and account balances have not been altered, proper authorizations were followed in completing a transaction, balances between third parties and the client have been reconciled properly, there are no missing transactions, the CPA firm has access to the required data, and inability to verify whether unauthorized adjustments to accounts have been made comprise some of the challenges auditors face during the evidence-gathering stage.

The Statement of Audit Standard (SAS) No. 106 states that the reliability of audit evidence is influenced by its source and that the internally obtained audit evidence is more reliable when the related controls imposed by the entity are effective (AICPA, 2006). According to SAS No. 106, the reliability of audit evidence increases when the evidence gathered exists in documentary form. In May 2018, a task force comprised of members from the Auditing Standards Board (ASB), Assurances Services Executive Committee (ASEC) and the AICPA's Technical Issues Committee (TIC), came together to discuss the accuracy, completeness, and reliability of audit evidence among other things (AICPA, 2018a). Some items on the committee's agenda were related to the sufficiency of audit evidence gathered and the reliability of the audit evidence. The task force observed that currently most audit evidence originates and is maintained digitally, consequently, audit evidence rarely exists in paper form. Recognizing client firms' dependence on information technology and digital records, the ASB continues to address the reliability of electronic forms of evidence. For example, SAS No. 94 introduced in May 2001 addresses the need to understand the effect of information technology on the auditor's considerations of control mechanisms and risks for account balances and transaction classes in a financial statement audit (Porter and Lasiewicz, n.d.). After reviewing the current environment and the challenges concerning audit evidence, the task force presented several questions for consideration: “Does the inability of testing the completeness and accuracy of the audit evidence preclude the use of that audit evidence? Would the inability to test the completeness and accuracy of audit evidence be considered equally as it relates to both evidence generated internally by management and evidence obtained from sources external to the entity? With respect to the sources of audit evidence, does the ASB believe that all of the considerations to evaluate audit evidence apply in all circumstances regardless of its source?” (AICPA, 2018a).

The task force suggests that audit evidence has many dimensions and thus requires that the auditor evaluate audit evidence from multiple angles. Consequently, the task force identifies several attributes namely, relevance, reliability, authenticity, accuracy, persuasiveness, consistency, precision, completeness, and risk of bias, that affect the consideration of what is sufficient and appropriate audit evidence. Given these challenges in the auditing profession, we consider whether auditors could leverage an emerging technology (i.e., blockchain technology) to provide assurance of reliability, completeness, and accuracy over the digital records and design an architecture that will address some of the challenges and enhance the audit evidence collection process.

The next section briefly discusses the importance of adequate consideration of requirements in the design of IT architecture and explains the basics of blockchain technology. Section 3 introduces the proposed blockchain architecture and discusses its components. Section 4 discusses future work and provides some concluding comments.

2. IT architecture

Systems architecture is a “blueprint for translating business strategy into a plan for information systems (IS)” (Pearlson and Saunders, 2006). Consequently, it is a plan for how all system components, including all the major subsystems, are linked together in a manner that achieves a set of objectives. Therefore, to develop such an architecture, one must consider user requirements, the

Please cite this article as: N.E. Vincent, A. Skjellum and S. Medury, Blockchain architecture: A design that helps CPA firms leverage the technology, International Journal of Accounting Information Systems, https://doi.org/10.1016/j.accinf.2020.100466

business strategy, and/or the problems/challenges that a firm faces.[1] The proper design of the IT components and their connectivity in a system environment are crucial because design and connectivity can either enhance or hinder the flow of information within a firm. Given the current challenge of verifying the reliability of digital audit evidence gathered, the first step in evaluating whether auditors can leverage blockchain technology is to explore the conceptual design of system components and their interaction with the blockchain.

Blockchain technology is based on a decentralized peer-to-peer network of nodes (computer servers) that electronically maintain a distributed ledger and use some form of consensus mechanism among themselves that is responsible for synchronizing the global state of that ledger.[2] Typically, in a public network like Bitcoin and Ethereum, each so-called "full node" replicates the entire global ledger, therefore, assuring the availability of data and resistance against Denial of Service. The cryptographically linked logs, implemented through the storage of information records (blocks), ensure the immutability of data and enforce nonrepudiation; hence, facilitate the audit trail.[3] The proponents of blockchain emphasize the benefits of transparency (Atzori, 2015), trust or not needing to trust (Zyskind and Nathan, 2015), fault-tolerance because of the distributed ledger (Swan, 2015), ability to self-execute contracts (smart contracts, Cai and Zhu, 2016), supply chain integration, etc.[4] On the other hand, opponents emphasize the lack of inherent confidentiality as a major drawback deriving from the distributed ledger (Stinchcombe, 2018). Therefore, when designing the architecture, we need to leverage the benefits and minimize the drawbacks to achieve the potential for practical and widespread adoption by client firms.

If client firms are to leverage blockchain technology, the architecture should be developed to address business problems that stem from globalization, new and emerging business models, emerging markets, supply chain integration, and international regulatory compliance requirements. Therefore, firms need to address how they connect to and leverage blockchain technology and smart contracts[5] provided on certain platforms, such as Ethereum (Wood, 2014), to enhance transparency and communication among trading partners, customers, regulators, financial institutions, etc. As client firms embrace this technology, the design should also address the concerns of auditors. If the design is not beneficial to the CPA firms, auditors will have to audit around a black box when providing audit and assurance services. Therefore, we focus on a problem auditors face and develop an architecture that benefits CPA firms. Even though we are designing an architecture that CPA firms can leverage, the proposed blockchain architecture can be extended to enhance transparency and communication among other business partners as well. The subsequent discussion focuses on how the client firms would connect to the blockchain and the auditing profession could leverage the technology.

3. The proposed blockchain architecture and design considerations

The proposed architecture addresses two major concerns. First, from the CPA firm's perspective, how do CPA firms gain access to reliable audit evidence? Second, from the client's perspective, how can the client firm maintain confidentiality, privacy, and security of their data given a decentralized and distributed ledger? Apart from these two major concerns, the proposed architecture provides benefits that we discuss in the subsequent sections. The proposed architecture consisting of existing ERP applications, Changelog(s), blockchain and blockchain explorers, is based on a blockchain system developed to enhance the data integrity[6] and nonrepudiation[7]of clinical trial data (Brooks et al., 2018). The next section details each component of the architecture.

3.1. Components of the proposed architecture

In this section, we consider Client Applications and Existing Servers, then Changelogs, and Blockchains, followed by CPA firms.

3.1.1. Client Applications and Existing Servers

Currently, there is a widespread discussion on how to leverage distributed ledgers for accounting (Schmitz and Leoni, 2019; Tan and Low, 2019; Sheldon, 2019). Some suggest (Brandon, 2016; Parikh, 2018) that the blockchain will replace existing

[1] A business strategy outlines how an organization plans to reach a desired position/place/level within a certain timeframe. Therefore, a business strategy will address how the organization plans to achieve certain things and address certain problems to fulfill the vision and mission of the organization. To develop a strategy, an organization identifies goals and objectives that help reach the desired position/place/level. Since IT is an enabler of business strategy—that is, since IT helps organizations achieve goals and objectives and address problems/challenges—these problems/challenges should influence the design of an IT architecture. When IT is developed and implemented so as to help achieve business objectives, we call it business/IT alignment. In this paper, the problem identified—from a CPA firm's perspective—is the problem of gathering sufficient and appropriate audit evidence.

[2] See Kokina et al. (2017) for a review of current developments in blockchain technology.

[3] In public blockchain networks, any form of encryption of the data is up to the application developer who uses the blockchain; it is not included in the most common blockchain technologies. That is, blockchains guarantee availability and integrity in their baseline architectures. These are key aspects of fault tolerance.

[4] See Ølnes et al. (2017) for a discussion on benefits and the promises of blockchain technology.

[5] A so-called smart contract is a series of interactions mediated by the blockchain itself that yields a contractual outcome and often involves the escrow of cryptocurrency and or other assets that change hands through the successful, arms-length completion of this type of online transaction (Buterin, 2014).

[6] Established controls over the integrity, that is, the accuracy and consistency of the data over its lifetime, ensures that that the audit evidence collected has not been tampered with. Therefore, when effective controls are enforce to provide data integrity, auditor can have reasonable assurance that the digital records obtained from internal sources are reliable. However, client firms should establish additional data input controls to assure the accuracy of the data entered into a system.

[7] Non-repudiation refers to a situation where a user responsible for a particular change cannot successfully dispute its ownership or the validity of the change occurred.

Please cite this article as: N.E. Vincent, A. Skjellum and S. Medury, Blockchain architecture: A design that helps CPA firms leverage the technology, International Journal of Accounting Information Systems, https://doi.org/10.1016/j.accinf.2020.100466

enterprise resource planning (ERP) systems and legacy systems maintained in client firms today. However, there are several drawbacks pertaining to this assumption. First, it does not consider the cost of replacing all of the existing systems with blockchain solutions. If client firms have to forego existing complex systems such as ERP systems for blockchain-based applications, client firms will subsequently have to invest significant resources and also absorb the risks associated with the transition to the new technology. Therefore, there is a concern about the economic feasibility of such solutions. Further, given the novelty of decentralized application development, client firms may not be able to reap any benefits of blockchain within a reasonable time frame. Also, these solutions raise the question of willingness from the client firm's perspective to adopt blockchain-based applications and how these should interact with mature IT systems already used by the client firm. Another concern is whether the client firms will be motivated to invest in a blockchain solution given the maturity of existing supply-chain-integration solutions such as electronic-data interchange. Therefore, client firms will have to evaluate critically whether the said benefits of smart contracts, for example, can be addressed using existing technology.

Second, the current blockchain solutions do not address confidentiality and privacy issues. Sharing data over a public ledger raises confidentiality and privacy concerns because most public blockchain networks do not provide support for encryption (Guegan, 2017) and hence, client firms must bear the cost of development for such features. Therefore, encryption and decryption of data may further increase execution overhead and may cause scalability issues when implementing smart contracts. Even though the distributed ledger provides system availability, hence, important aspects of fault tolerance, whether client firms are willing to maintain their data in a distributed ledger where multiple parties have free access to the client firm's data is questionable. Contrary to a public blockchain, a permissioned blockchain network need not require the client firm to encrypt all data being transmitted. Therefore, users can be authorized to access the data and/or participate in the network based on a strictly enforced access control mechanism to mitigate scalability and overhead issues.[8]

Given the computation-resource requirements of certain blockchains to add blocks to the network (in present mining schemes such as proof-of-work on Ethereum) and cost per byte to store data, IT experts question whether the blockchain will provide an operationally feasible solution. Currently, emerging mechanisms to control the cost of creating blocks, the cost of storing each byte of data in the block, and the ability to create blocks much faster at sufficient security are all actively being researched.[9]

Conceptual papers (Deloitte, 2016; Sheldon, 2019; Tan and Low, 2019) mention that it is unlikely that existing systems would be replaced by blockchain technology. However, they do not provide a discussion of how client firms would leverage and connect to a distributed immutable ledger using blockchain technology in the putative presence of their current, operational systems. Given the current challenges, we recommend a more feasible solution: according to the proposed architecture, client firms will maintain their existing systems. Client firms will continue to collect, record, and process transaction data using existing applications and maintain their client-server environments within each client firm. Therefore, the financial burden on each client firm to leverage the blockchain can be substantially reduced; hence, the client firm's willingness to participate in the blockchain and provide the CPA firm access to the data will likely increase.[10]

3.1.2. Changelog

Tan and Low (2019) suggest that blockchain technology will likely be deployed in the database engine tier rather than the application tier. However, they do not make any recommendations as to how the application tier will connect with the database engine. James (2018) provides a proof of concept using Xero, a cloud-based small business accounting software package, on how to create an immutable audit trail. Using an invoice as an example, he explains how Xero can enable the applications to link the data to the blockchain. However, he mentions that the shortcoming in his design is not knowing what was modified in an invoice if the invoice is tampered with after it has been finalized. Therefore, considering the need for confidentiality, privacy, and security of data from a client firm's perspective and the need for reliable audit evidence, a traceable audit trail, and possibly automating audit process from an auditor's perspective, we introduce the Changelog as the means for connecting the application tier with the database engine tier. To provide a traceable and immutable audit trail, we recommend a tight integration of the Changelog with the data objects involved in various steps of a business process.

The Changelog(s) must be maintained locally by each client firm; therefore, only a given firm will have access to its particular Changelog(s). Business-related events like creating a sales order are captured in the client firm's ERP or legacy

[8] Blockchain networks can be categorized based on their access control. Protocols like Bitcoin, Ethereum and EOS are public networks that do not impose any restrictions on access (Guegan, 2017). Therefore, anyone can participate in mining and/or make transactions on the network. Protocols like Hyperledger, Quorum, and Corda provide frameworks to build custom blockchain networks for required use cases (other than currency). These blockchain frameworks provide the capability to customize access to the network and allow only authorized users to view and/or modify data. Such blockchain networks are often referred to as private/permissioned (Guegan, 2017) networks. The permissioned/private blockchain network may seem to have addressed most of the limitations pertaining to distributed ledger but scalability still remains an outstanding issue. While blockchain networks are attractive for their decentralized nature, the overhead of consensus mechanism continues to be the bottleneck. Proof of Work is highly decentralized and stable but it is extremely slow and computationally expensive. Proof of Stake is expected to be more scalable but it is not yet mature for wide adaptability. Other consensus algorithms like Delegated Proof of Stake attempt to solve scalability issues by delegating the authority to confirm transactions to a subset of miners. This is arguably more centralized than decentralized based on recent incidents.

[9] These future improvements need to be tracked carefully because they will change the landscape of economic feasibility and technological viability of blockchains over the coming months and years.

[10] The client firm's decision to adopt blockchain will be influenced by factors such as pressure from trading partners, need for automation and transparency, connectivity as a result of internet of things, and globalization. Even though this paper approaches the design from a CPA firm and client firm perspective, the motivation for a client to adopt blockchain will come from other sources. The cost savings derived from maintaining existing systems at the client firm is another factor that would positively influence client firms to adopt the technology and the proposed solution. When the client firm embraces the technology, the CPA firm will have to be prepared to leverage the technology for audit and assurance services. If the design is not conducive to the CPA firm's needs, the CPA firms will not be able to leverage the technology.

Please cite this article as: N.E. Vincent, A. Skjellum and S. Medury, Blockchain architecture: A design that helps CPA firms leverage the technology, International Journal of Accounting Information Systems, https://doi.org/10.1016/j.accinf.2020.100466

systems as usual, and when the databases are updated either using a real-time or batch process, all events are simultaneously submitted to the Changelog as well. Each submission should contain metadata related to the given event, such as the user responsible for the change, unique identifier, etc. The Changelog can be perceived as a data store of changes that were made to the client firm's ERP system (the digital record) that provides an audit trail for CPA firms to examine during an audit. Since this Changelog data store is privately maintained by the client firm, it remains susceptible to fraudulent manipulation for any number of reasons. However, the linking of the Changelog(s) to blockchain enables the detection of any manipulations as explained below.

We recommend using the Changelog for two purposes: First, to maintain the hashes of each transaction and, second, to link the steps in a business process to previous steps to ensure the immutability of the business process. Once the client firm creates a digital record of a given business event using the legacy system, the data will be hashed and submitted to the Changelog as indicated in Fig. 1. The transactions are logged with metadata (the unique id of the user responsible for the change, time of occurrence, state of the object before and after the transaction) in the form of hashes. The transactions are digitally signed by the sender's private key, this digital signature can be verified (Goldwasser et al., 1988) using the public key of the sender.[11] Current proof of concepts, such as the one suggested by James (2018), recommend hashing the entire data of the document into one single hash, an approach that does not provide the capability to identify and pinpoint what elements of the document were changed even though it is easy to detect if the document was changed at all. Therefore, in our design, we recommend hashing different segments of the digital document (shown in Fig. 2) and generating a Merkle root (Merkle, 1980) with those hashes, resulting in a unique cryptographic hash for each of the digital documents. As shown in Fig. 2, metadata, master data, transaction terms, and transaction data will be hashed separately before creating a hash for the digital document-sales order.

Further, this architecture can be extended to integrate a client's business processes as well. A Changelog table (called a business process Changelog) can be updated for each business process reflecting the corresponding steps in that particular business process. Once an event is created, apart from hashing the data and entering it the particular event Changelog, each event will be hashed and submitted to the corresponding business process Changelog as shown in Fig. 1. When hashing the data for the business process Changelog, the cryptographic hash of the data object from the previous step in the business process is included as a parent hash. By including the hash of data object from the previous step of the business process, client firms can rest assured that data cannot be modified after the fact. For example, assume a simple business process with three steps: finalizing the sales order, generating the invoice, and collecting the payment. The three steps in the business process are represented by the Sales Order, Invoice, and Payment data objects respectively. Changelog-Sales Order may not have any additional elements since it is the first step in the business process, a record in Changelog-Invoice can include the cryptographic hash of corresponding sales order from the previous step in the business process. Similarly, the Changelog-Payment includes the cryptographic hash of the corresponding invoice. This approach strengthens data integrity across the entire lifecycle of the business process, as opposed to securing a single type of data object. Consequently, the more steps added to the business process the harder it becomes to tamper with digital documents created earlier, thus causing the audit trail to be more robust. It can be especially beneficial for multinational businesses whose operations are spread across a vast geographical area, the offshore branch may regenerate the cryptographic hash of the data received and compare with the hash of record committed to the Distributed Ledger to validate the data without any further communication. Clients may choose to disclose the hashes related to the customer's data objects, by referring to the block number and or the transaction number committed to the immutable distributed ledger, to enhance trust and ensure that the product was delivered according to the agreed-upon terms.

Fig. 3 shows the update process of the Changelog. Once a sales order is entered, the segment hashes and the Merkle root for the sales order is added to the Changelog. Assuming that there are two tiers to a data object (i.e., the table and the transaction) we recommend hashing the data of transaction as mentioned above and maintaining a cryptographic aggregator corresponding to each ERP table, which can be continuously updated with every new transaction's hash. The data related to each transaction must be digitally signed using the preparer's private key.[12] This hash of transaction and digital signature can be simultaneously recorded with related metadata on the Distributed Ledger.

The digital signature together with the provenance of transactions[13] enforces non-repudiation. The timestamp and the incremental change captured can provide further insight into the changes made to transactions, therefore, identify fraudulent transactions if any.[14] Each transaction in the Changelog contains the digital signature generated with the data including the hash of record, list of segment hashes and other related metadata. A transaction is valid only if the digital signature can be verified using the preparer's public key and the data included in the blockchain. Instead of saving the complete file or database on the distributed ledger, a hash of the file or data object can be stored on the Changelog to drastically reduce the storage requirement.

[11] Digital signatures are often used to sign documents electronically, they can establish authenticity (i.e. the document was signed by the sender), and ensure integrity of the document (i.e. the document was not modified after completion of signing). This is achieved by using Asymmetric Encryption techniques where a key-pair consisting of a private key and public key is used for encryption and decryption.

[12] Public Key Infrastructure (PKI) utilizes asymmetric cryptographic encryption techniques involving a keypair consisting of a public key for encryption and private key for decryption (or else a potentially distinct private key for signature and corresponding public key for verification). Digital Certificates are used to validate the identities corresponding to the public keys, these are issued by trusted Certificate Authorities who verify certificate requests.

[13] The chronologically ordered metadata related to transactions is considered as provenance data capturing various states of each data object from the beginning of its creation to its most recent state. This provenance data strengthens accountability of changes to its initiators.

[14] Depending on the requirement and use case, the transaction may or may not contain a link to the data object being referred to. This issue is a design consideration client firms should consider given their specific context.

Please cite this article as: N.E. Vincent, A. Skjellum and S. Medury, Blockchain architecture: A design that helps CPA firms leverage the technology, International Journal of Accounting Information Systems, https://doi.org/10.1016/j.accinf.2020.100466

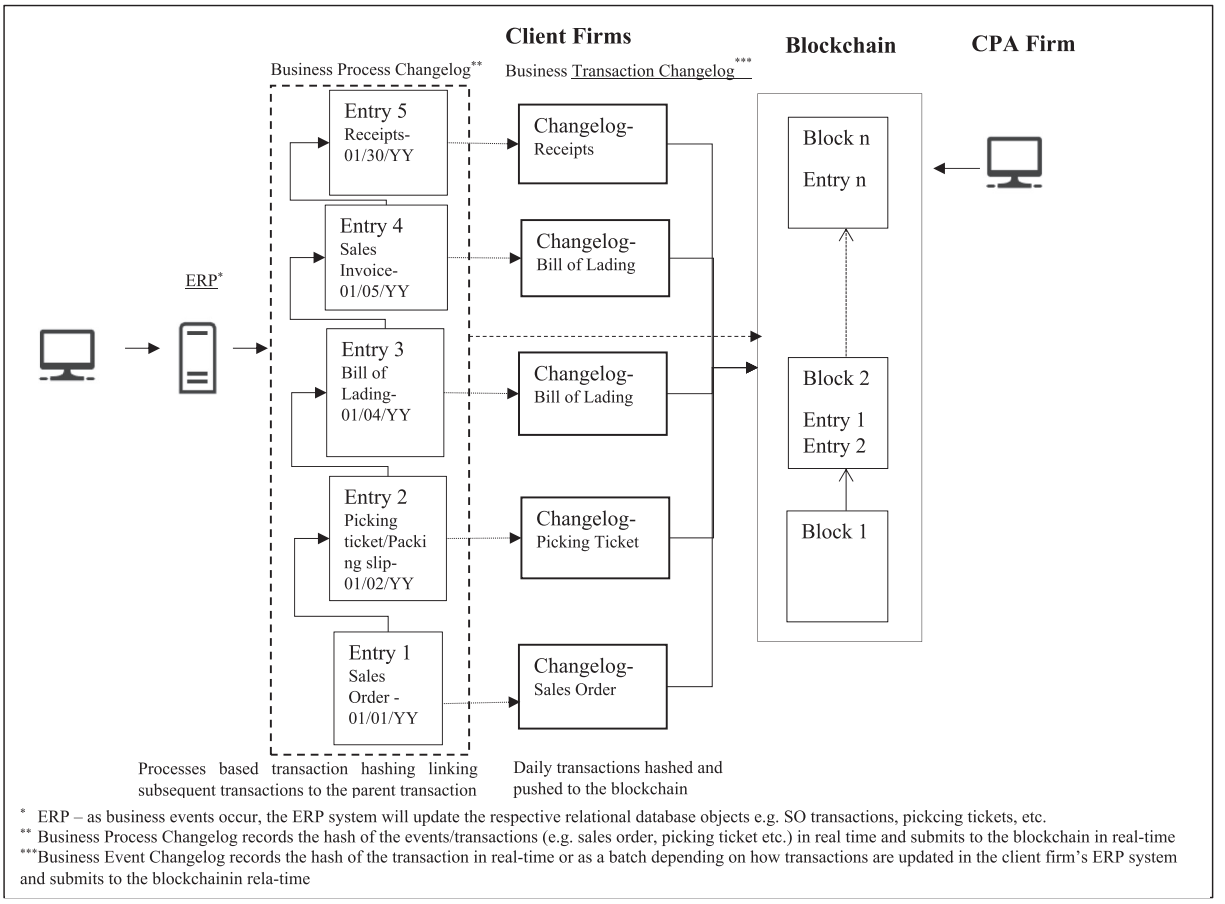


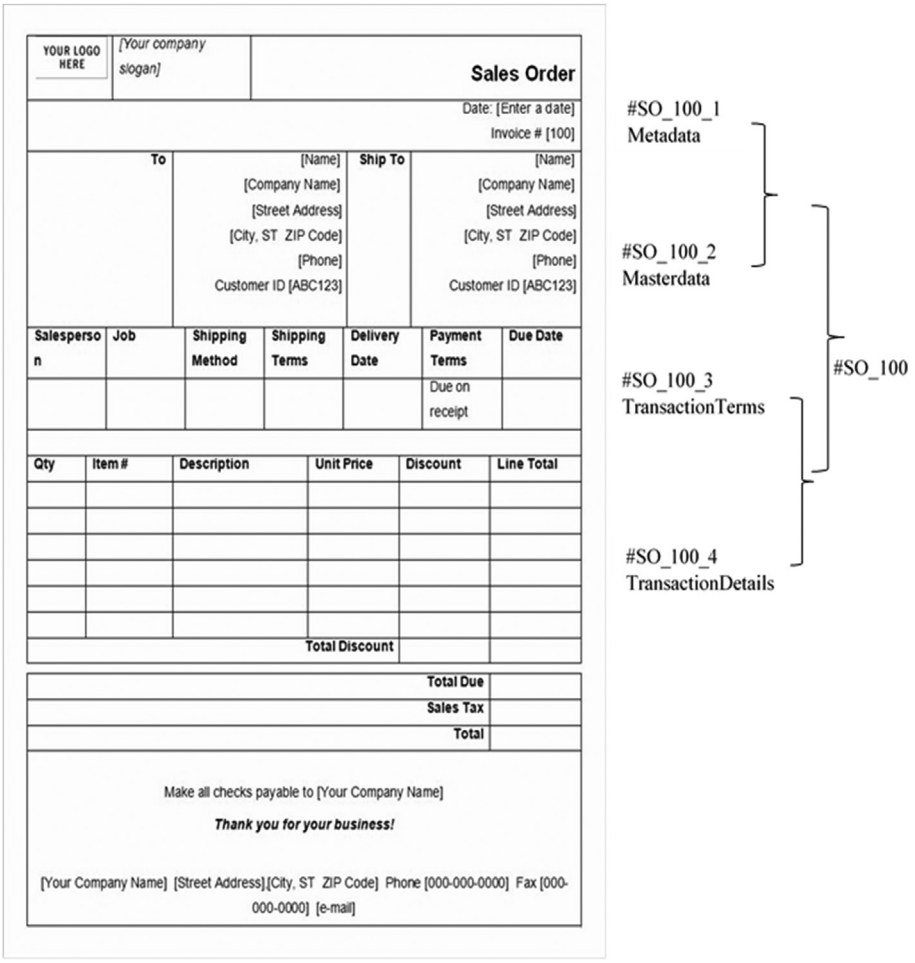
Fig. 1. Blockchain architecture: Linking FIRM'S application tier with blockchain.

With time and increasing size of the distributed ledger, security is enhanced and data integrity is strengthened, thus preventing any subsequent changes to the transactions with an extremely high level of certainty.[15] Additionally, the client firm can protect its sensitive information from leaking to unauthorized users by maintaining the Changelog in-house (and by applying industry-standard data encryption to such data, if desired).

When implementing a Changelog, some design considerations client firms should consider are as follows. First, client firms should consider the type of transaction (sales order, purchase order, asset transfer, etc.) that should be included in the blockchain. Second, given the type of transaction, client firms should consider whether transaction data should be segmented and if so, how to achieve it. The decision to hash separately and/or together (Fig. 2) will be driven by the subsequent use of the hashes. For instance, if transaction data is hashed separately, the effort required to pinpoint discrepancies arising from tampering will be drastically reduced. If the client or the CPA firm suspects fraud, such that shipping addresses in some sales orders are changed after sales orders are approved, recreating hashes for only master data for sales orders and comparing them with segment hashes for master data included in the Changelog can easily identify whether and which digital records have been tampered with after the fact. Third, client firms should consider when a transaction would be considered finalized before hashing and adding it to the Changelog. For example, in the hospitality industry when a reservation is made months in advance and the customers can cancel without a penalty up to 72 h prior to arriving, should the reservation be added as soon as it is confirmed or should the firm wait till 72 h prior to arrival date to finalize the transaction and add it to the Changelog? Fourth, since a company can conceptually maintain any number of Changelogs, client firms should consider the need for different levels or specializations and/or compartmentalization of Changelogs such as including Changelogs for business processes and/or data objects.

[15] We have provided a basic description of the changelog here. However, to increase security and reliability, the hashing mechanisms of the change log should be discussed in detail. Given the scope of the paper, we have limited the discussion to the basic components. Future research should address issues, concerns, security, operational efficiency of the change log, and the hashing mechanism.

Please cite this article as: N.E. Vincent, A. Skjellum and S. Medury, Blockchain architecture: A design that helps CPA firms leverage the technology, International Journal of Accounting Information Systems, https://doi.org/10.1016/j.accinf.2020.100466



Preparer Digital Signature = $\text{Digest}_{\text{private\_key}}$(Invoice# || Timestamp || Hash of Record), where || denotes concatenation

Hash of Record = SHA256(SHA256(#SO_100_1 || #SO_100_2) || SHA256(#SO_100_3 || #SO_100_4)), where || denotes concatenation

Fig. 2. Hashing design consideration for a transaction.

3.1.3. Blockchain

The blockchain consists of blocks of data records that are linked to the previous blocks. The parent hashes included in each block to link the chain makes the blockchain immutable. The process of adding blocks to the blockchain is called mining. Mining and consensus are carried out by participating nodes (servers) on a decentralized network (this is the most significant cost of time and energy, and therefore the cost for adding blocks in current blockchain technology). Mining nodes aggregate the transactions, calculate and place a Merkle root in each of the block headers. The Merkle root helps other miners to verify the transactions (Merkle, 1980) and the block before adding it to the distributed ledger maintained at each node.

In the proposed architecture, the next step is to connect the Changelog to the blockchain. This link is established by digitally signing using the preparer's private key and submitting a hash of the Record maintained in the Changelog and related metadata such as sales order number, timestamp and preparer's unique identification number to the blockchain.[16] Once the block is mined, the block ID can be attached to the respective Changelog.

Public/permissionless blockchain networks provide the advantage of advanced decentralization.[17] However, using a cryptocurrency-based blockchain solution like Ethereum, EOS, or NEO, requires a choose-two tradeoff between scalability, degree of decentralization,[18] and security.

[16] The proposed architecture suggests that only a cryptographic hash of the latest Changelog entry be added to the blockchain, as opposed to the actual data.

[17] Decentralization refers to the peer-to-peer network paradigm where the all participating nodes have the authority to validate and store new transactions, as opposed to a client-server system where the server reserves the authority and client must trust server's response. Public blockchain networks like Ethereum allow any participating node to compete and achieve the authority to propose new blocks therefore providing advanced decentralization.

[18] The extent of decentralization is based on the proportion of total participating nodes with authority to validate transactions at any given moment. This may vary from a few elected representative nodes (DPoS) to the entire network (Bitcoin).

Please cite this article as: N.E. Vincent, A. Skjellum and S. Medury, Blockchain architecture: A design that helps CPA firms leverage the technology, International Journal of Accounting Information Systems, https://doi.org/10.1016/j.accinf.2020.100466

A: Changelog

Changelog										
SOrder_No	Date	SO_Seg1_#	SO_Seg2_#	SO_Seg3_#	Hash_Of_Record	Preparer_ID	TimeStamp	Cryptographic aggregator of SO table	Preparer Digital Signature	Block_ID
100	08/01				#SO_100			0000Hdw24		
101	08/01				#SO_101			0000Dt4586		
102	08/02				#SO_102			0000PS578d		
:								:		
110	08/06				#SO_110			:		
111	08/06				#SO_111			000ufH0044		

B: Records on Distributed Ledger

Blockchain			
TimeStamp	Preparer ID number	Transaction_ No	Hash of Record
08/Aug/2019:06:36:15 -0700		#SO_100	
08/Aug/2019:06:47:29 -0700		#SO_101	
:			
:			
08/Aug/2019:18:24:15 -0700		#CR_620	
08/Aug/2019:19:36:75 -0700		#PO_005	

Fig. 3. Changelog for sales orders. Panel A: Changelog. Panel B: Records on distributed ledger.

Established and widely known cryptocurrencies like Bitcoin and Ethereum are known to be slow (Zheng et al., 2017) as a result of their Proof-of-Work consensus algorithm. EOS (Block.one, 2018), considered a potential alternative to Ethereum, is comparatively more scalable[19] since it implements the Delegated Proof of Stake (DPoS) consensus algorithm,[20] which allows a subset (21 nodes) of participating entities to validate the transactions as opposed to all entities participating in the validation process. These 21 major entities, termed Block Producers, are repeatedly voted by the rest of the participating nodes in the network. Recently proposed, Facebook's Libra project seeks to implement a version of Practical Byzantine Fault Tolerance (Castro and Liskov, 1999) called LibraBFT (Baudet et al., 2019) and, according to their whitepaper, claims to meet the present industry standards of scalability achieved by electronic payment services like Visa, Mastercard, and PayPal. The Libra solution is preparing to go live in 2020 (Taskinsoy, 2019), it may prove to be the first public Digital Ledger Technology (DLT)[21] with unprecedented performance.

Decentralization is perhaps the major limiting factor to scalability but it is the most desirable aspect of utilizing a DLT. Proof-of-Work consensus algorithms facilitate true decentralization, but the Bitcoin network has experienced the formation of pools to increase the odds of achieving incentives. Lately, around 11 active pools are majorly responsible for validating all transactions (Blockchain.com, 2019) in the network, which is somewhat similar to the Delegated Proof of Stake (DPoS) consensus algorithm where a fixed number of Block Producers carry the mining responsibility. DPoS, in comparison to PoW, is far more scalable

[19] Scalability, in the context of blockchain technology, is measured as the number of transactions per unit time committed to a block and successfully added to the blockchain. Transactions per second (tps) is commonly used to compare scalability of blockchain solutions.

[20] In a peer-to-peer decentralized computing environment of blockchain network, the consensus algorithm helps synchronize each node to resolve disparities in state of the global ledger and eventually achieve a common global state. This is not required in monolithic client-server system because a single entity is responsible for state transitions and the server can carry this out without conflict.

[21] Distributed Ledger Technology (DLT) is the storage system of replicated, shared, and synchronized digital data geographically spread across multiple sites, countries, or institutions. It is an umbrella term enveloping all components involved with a blockchain based data storage system. The term blockchain is specifically referred to the underlying data structure of cryptographically linked blocks used for storing data as transactions, it's an alternative to Relational Database where data is stored in rows of tables linked with relationship constraints.

Please cite this article as: N.E. Vincent, A. Skjellum and S. Medury, Blockchain architecture: A design that helps CPA firms leverage the technology, International Journal of Accounting Information Systems, https://doi.org/10.1016/j.accinf.2020.100466

according to industry standards. However, EOS is currently facing a controversy: the users of EOS demand for more transparency in the initial selection process to reduce chances for nepotism and/or corruption. Facebook's Libra, on the other hand, provides organizations the opportunity to join the Libra Association for an entry fee of $10 million. The members of the Libra Association are empowered to decide the future development of the Libra coin but are not necessarily validators in the DLT network.

3.1.3.1. Security (true immutability). High profile cryptocurrencies like Bitcoin and Ethereum are susceptible to attacks because of the large amount of money involved and given the fact that they are publicly accessible. As a result, incidents leading to Hard Forks, where the underlying logic is altered and the blockchain history is rewritten, is not unknown to the public. In such cases, one must trust the core developer community to act with integrity.

To avoid this choose-two tradeoff, we recommend initially using a permissioned distributed ledger network with smart-contract capability.[22] The solution should be facilitated via a smart contract that also includes user-account management. Enterprise blockchain networks with scalable consensus algorithms like Practical Byzantine Fault Tolerance (PBFT) or Federated Byzantine Fault Tolerance (FBFT) are preferable for implementing the Changelog. The cost for development, integration, and operation may be shared by client firms that are part of a blockchain coalition and an appointed CPA firm; any one of them may choose to participate in the distributed ledger technology (DLT) network as a validating node. Consequently, both the client firm and the auditor will maintain a copy of the ledger and have access to the data at all times.

Depending on the context, client firms should consider whether the transactions entered in the Changelog should be simultaneously pushed to the blockchain or whether it should be done as a batch process in time intervals ranging between 30 s to 15 min. Batch submission must be encouraged solely for scalability optimization[23] and the system design must consider the time interval as a window of vulnerability when fraudulent manipulation goes undetected, hence avoiding batch submission at all costs in time-sensitive high-risk businesses. The batch submission may also be carried out in sync with the business process lifecycle.[24] Since this design is scalable to multiple firms, the blockchain will contain hashes of the Changelogs for as many firms as needed in a decentralized, distributed ledger. Hence, for example, block two can include transactions related to client one as well as client two thereby providing a single view of the truth in an ecosystem.

3.1.4. CPA firms

Given the proposed architecture, CPA firms can access the distributed ledger and retrieve Changelog hashes in addition to gathering evidence for an audit for each of their clients. The final cryptographic aggregators corresponding to ERP tables can be matched to the Changelog(s) to ensure that transactions have not been modified in the ERP system and/or modified without authorization. See Appendix A for a step-by-step guide for the audit procedure. In case of discrepancy, the Changelog facilitates an audit trail to identify the event and the person sending the transaction that may have caused the discrepancy. For example, the auditor can extract all transactions for that specific client using the public key of the preparer. If the auditor wants to focus on a specific set of transactions such as sales orders or invoices, he/she can use the public key of the preparer of a Changelog to extract all transactions related to a specific event. Then the auditor can first compare the sales order hash to the hashes obtained from the blockchain. Further, the auditor may generate the cryptographic aggregator associated with those transactions and compare it with the latest version of this cryptographic aggregator in Changelog. If there are indeed no discrepancies, then there is reasonable assurance that no modification has taken place after the sales orders were finalized.

If the hashes don't match, then auditors can identify the sales order that was manipulated including the specific elements of the Sales Order that were manipulated. Regenerating the Merkle root hashes of each Sales Order and comparing them with the corresponding Merkle root hash mentioned on the blockchain will help pinpoint the specific Sales Order resulting in discrepancy. There may be multiple Sales Orders causing the mismatch in the cryptographic aggregator, each of these can be identified for further investigation. Regenerating segment hashes using the latest version of the data from the ERP system and comparing these with the corresponding list of hashes in the Changelog record will help uncover the exact segment of Sales Order that was modified. Further, because the hash of a digital document is segmented, auditors can focus their attention on what is relevant to the assertion being tested. For example, auditors testing the financial assertion related to authorization may focus on changes in the segment hashes of metadata whereas auditors testing the financial assertion related to accuracy of transactions may focus on segment hash discrepancies in transaction data.

CPA firms will need to update their knowledge and skill set to able to perform cryptographic operations like computing Merkle Root and cryptographic aggregators to be able to take advantage of Changelog architecture independently. They may also rely on open-source or third-party developer implementations for this purpose. However, it is essential to ensure that these implementations meet the National Institute of Standards and Technology (NIST) Cryptographic Standards and Guidelines.

The proposed architecture also facilitates continuous auditing by allowing periodic regeneration and comparison of the cryptographic hash of the corresponding data object from the previous step of the business process before finalizing the data object in the current step. Further, by periodically regenerating the cryptographic aggregator associated with an RDB table, or collection of data objects like Sales Orders, and comparing with the cryptographic hash committed to the blockchain, suspicious/problematic

[22] Given that the technology is in the early stages of development and adoption, we recommend a permissioned distributed ledger network. However, when blockchain technology use among corporations becomes widespread, this design can be extended readily into a public blockchain as well.

[23] The blockchain networks produce blocks of transactions with a block period ranging between 15 s to 10 min and businesses can gain speed in transaction commitment to the blockchain by following a batch process with time intervals similar to that of the block periods of their chosen blockchain solution.

[24] We have limited the discussion of mining in this paper as it needs further consideration. Instead of a proof-of-work algorithm, Brooks et al. proposes a lightweight mining algorithm. This is an area that needs further discussion and will be based on whether we use a permissioned, permissionless, or a hybrid blockchain. Therefore, we focus on the basics of the architecture in this paper. Other lightweight mining schemes are also being developed and discussed in the literature at present.

Please cite this article as: N.E. Vincent, A. Skjellum and S. Medury, Blockchain architecture: A design that helps CPA firms leverage the technology, International Journal of Accounting Information Systems, https://doi.org/10.1016/j.accinf.2020.100466

Table 1
How the components of the proposed architecture address attributes of sufficient and appropriate digital audit evidence identified by the Task Force.

	Attributes	How the proposed architecture addresses the attributes
Sufficiency (quantity) and appropriateness (quality)	Relevance	Maintaining separate Changelogs for different business events and business process enables the auditor to focus on a specific type of transaction such as sales, or the revenue cycle. Therefore, the auditor can focus on transactions that are relevant to a specific assertion and or audit objective.
	Reliability	When a majority of audit clients in various industries start using the blockchain, auditors may be able to easily cross-reference transaction details of one client firm with other organizations without destructing the confidentiality, privacy, and security of other organizations' transactions by comparing hashes maintained in the blockchain.
	Authenticity	When a digital record is changed in a relational database, the current field is updated. When the transactions are hashed and recorded in the changelog, in case a transaction is modified, the segment hash will change enabling the auditor to detect the change by comparing the Changelog hash and the blockchain hash for a particular record(s). Further, since transactions are hashed with metadata, auditors can observe the metadata for accuracy without having to depend on a client firm's IT or IT specialist at the CPA firm by simply comparing hashes. Because of business process Changelogs, auditors can verify the authenticity of subsequent business transactions as well.
	Accuracy	Auditors can recreate hashes using transaction data maintained in the client firm's ERP system and compare the resulting hashes with the hashes recorded in the Changelog and blockchain and accurately identify which transactions, at which point have been tampered with if necessary. Therefore, auditors can confirm the accuracy of digital records with reasonable assurance. Given other technology tools available, such as big data analytics, these comparisons can be automated saving the auditor time and effort.
	Persuasive	Sufficiency a measure of quantity, suggests that auditors obtain enough evidence to support a given assertion. Changelogs enable the auditor to inspect the population of transaction data for a given period rather than a sample.
	Consistency	Auditors can verify whether there are digital records that circumvent any internal controls or management policies by comparing hashes on the Changelog and recreating the hashes for the database object in the ERP system. Since hashing and recording transactions in the Changelog is conducted without the knowledge of the end-user, it can be applied consistently to all transactions. Further, the auditor will be able to depend on audit evidence collected using the same method year after year.
	Precision	Segmenting and hashing transactions enable auditors to detect not only whether a transaction was tampered with but also to pinpoint what elements were modified.
	Completeness	The Changelog enables the auditor to observe the whole business process and the population of transactions for a given period. Comparing the hashes of the business process level Changelog with hashes provided in the blockchain ensures that the entire business process has or has not been tampered with.
	Risk of bias	One bias that is important during evidence collection is availability bias. Complexity in ERP systems, not understanding which data objects to combine, and incorporative IT staff can hinder auditors and create availability bias. The proposed architecture and the components simplify the retrieval process by recommending applications developed for CPA firms that enable easy access to hash records and inbuilt analytics tools.

transactions can be detected on a timely basis. Since compatibility with software is not an issue with hashes retrieved from the blockchain, auditors can easily develop automated processes to conduct continuous audit procedures.

The proposed blockchain architecture addresses the challenge of obtaining reliable digital audit evidence. Further, the task force related to AU-C section 500, audit evidence identified several attributes that would lead to higher quality audit evidence (AICPA, 2018a). In Table 1, we provide a brief description of how the proposed architecture consisting of existing ERP systems and the Changelog(s) maintained at the client firms, and the blockchain addresses the relevance, reliability, authenticity, accuracy, persuasiveness, consistency, precision, completeness and risk of bias in the digital records.

CPA firms should focus on developing decentralized applications that will enable the CPA firm to retrieve the hashes maintained in the blockchain and audit transactions for each individual client. Another challenge auditors have with continuous auditing is the incompatibility of tools with all client systems. The proposed architecture provides individual firms the choice to use a system that meets the firm's requirement and provides CPA firms the capability to access client data to conduct audits without having to invest in different tools for each individual client.

3.2. Benefits of the proposed architecture

There are some noteworthy benefits to the proposed architecture. First, there is a significant reduction in the level of investment required both by the client firms and by CPA firms. Given that the clients can maintain the existing transaction servers, the required investment is substantially reduced. CPA firms benefit from cost savings by being able to use consistent applications across clients. Second, the benefit relates to data integrity and reliability. The Changelog maintained in-house provides an additional layer of protection. The Changelog links subsequent transactions of a particular event increasing reliability of the data available to the CPA firms. If a transaction is altered, the Changelog will be able to detect tampering and the point of tampering of the transaction. Further, digital signatures at the point of creating the Changelog and adding to the blockchain will also assure the reliability of the data. Third, the ability to maintain sensitive information in-house and only include a hash of the hash in the blockchain provides an additional layer of security. Fourth, the given architecture can be easily expanded to include as many clients as needed (Fig. 4). Fifth, the proposed architecture eliminates the maintenance of many different versions of the truth. Consequently, the reconciliation of third-party transactions would be simplified. Sixth, the architecture also provides auditors the

Please cite this article as: N.E. Vincent, A. Skjellum and S. Medury, Blockchain architecture: A design that helps CPA firms leverage the technology, International Journal of Accounting Information Systems, https://doi.org/10.1016/j.accinf.2020.100466

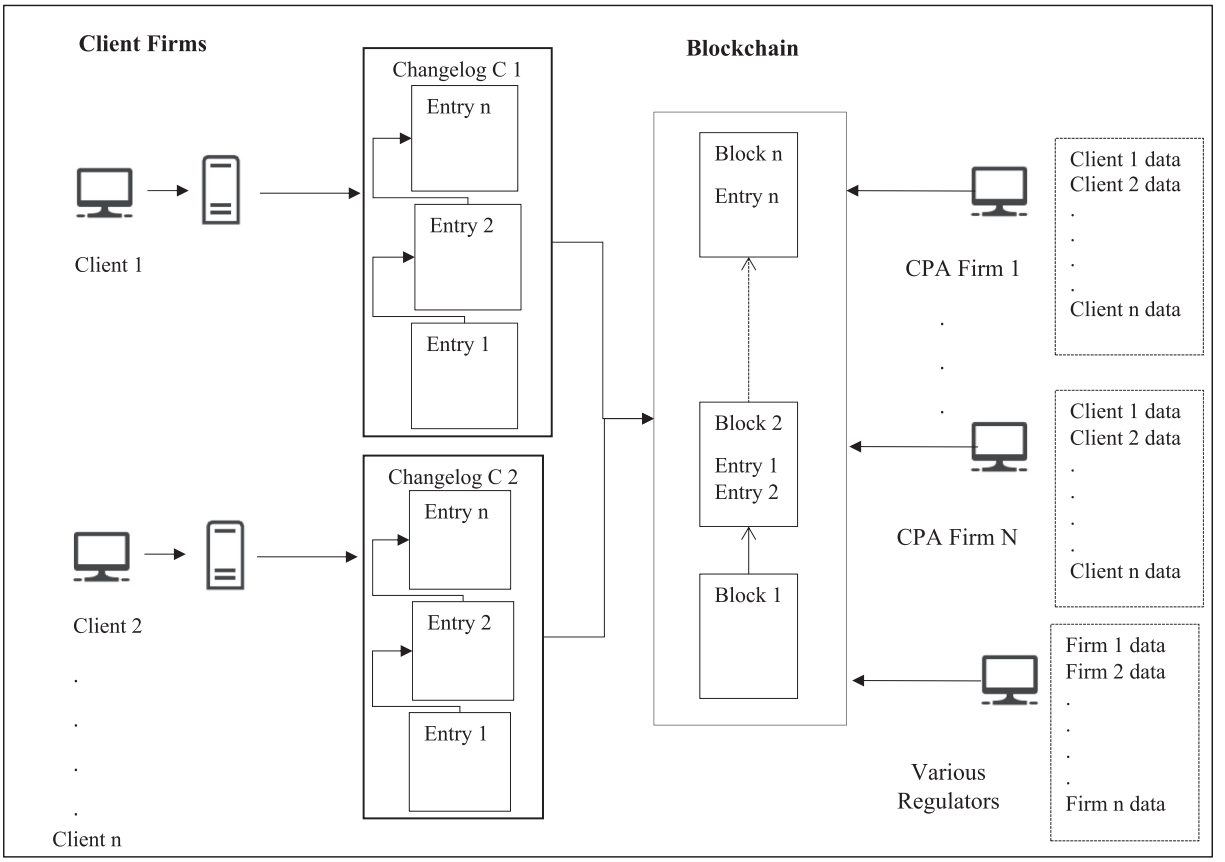


Fig. 4. Expanded blockchain architecture.

means, if necessary, to access the transaction server of a given client to obtain evidence to verify the assertions.[25] Seventh, having a common decentralized and distributed ledger enables and can positively influence the use of smart contracts. Therefore, the external blockchain helps assure that internal threats are reduced (i.e., tampering with the in-house data will be detectable through the blockchain hashes).

4. Conclusion

Experts argue that blockchain technology has considerable potential. However, blockchain technology is in the early stages of development. Therefore, many interested parties are exploring ways to leverage blockchain technology. In this paper, we identified a pressing problem in the accounting profession and have provided a candidate blockchain architecture that would address the problem of collecting reliable digital audit evidence. The proposed architecture not only addresses the necessity to ensure that the audit evidence is reliable but it also can address issues of investment costs, access to data, privacy, and security. Further, the proposed architecture can be expanded to include as many clients as needed. Fig. 4 presents how the proposed architecture can be expanded to include multiple CPA firms and regulators. We anticipate these developments to take place in various stages. First, Blockchain coalitions may start implementing blockchain solutions to automate and manage the supply chain. A CPA firm, such as one of the big four, may start leveraging blockchain for audit and assurance for a particular client in the coalition during this phase. This phase may involve a permissioned/private blockchain in which case it would not need heavy consensus algorithms. In the next phase, the CPA firm will be able to expand the blockchain solution to incorporate other clients who may be a part of the same blockchain coalition. As more client firms start to use blockchain and smart contracts, we anticipate blockchain coalitions integrating with each other and CPA firms and clients moving to a public blockchain. Client firms will be more likely to invest in a platform that gives them the flexibility to partner with many vendors, customers, regulatory bodies, etc. Hence, the proposed architecture provides flexibility for growth and expansion.

Current technical limitations of scalability, transaction speed, decentralization, and energy consumption are being researched in computer sciences and engineering. As technical specifications improve and more smart devices are added to the network, firms will increasingly consider the benefits of smart contracts and blockchain for automating business processes and

[25] Given the scope of the paper, we have not provided a detailed discussion here.

Please cite this article as: N.E. Vincent, A. Skjellum and S. Medury, Blockchain architecture: A design that helps CPA firms leverage the technology, International Journal of Accounting Information Systems, https://doi.org/10.1016/j.accinf.2020.100466

communicating among trading partners. Since the technology is still developing, we limit the discussion of such technical details in this paper and emphasize how client firms would connect to the blockchain in such a manner that CPA firms could leverage the technology for audit and assurance services.

As a next step, we plan to evaluate various enterprise DLT frameworks and develop a prototype of the proposed solution. The prototype will contain smart contracts and will enforce standard ERP system access controls. This solution will be evaluated for scalability, confidentiality, privacy, and security in terms of network latency, throughput, and threat models consisting of various fraudulent manipulation scenarios. Future research needs to explore whether advanced data visualization features and flexibility offered in a Graph database system (Exonum, 2019) have an advantage over a Relational Database for storing the data itself while storing metadata of changes on the distributed ledger. Further, research should investigate potential tradeoffs that arise with implementing graph databases (Vicknair et al., 2010) in terms of transaction speed and required development efforts. Further, future research should address additional controls that should be designed over the entire business process for recording business-level changes to the changelog, hashing algorithms, and data structures used and stored in the blockchain. Moreover, there are research opportunities to investigate design considerations of transaction data segmentation in different transactions in various industries.

This paper contributes to the IT governance and blockchain literature by developing and introducing a blockchain architecture that could be expanded to address the information needs of various stakeholders. However, this is only a preliminary effort at describing a vision for blockchain technology as it relates to the accounting profession. There are still other challenges that need to be addressed before full implementation, such as scalability, methods of granting permission to CPA firms to access the transaction servers through the blockchain platform, how to establish seamless switching of CPA firms without major implementations, the type of blockchain (whether it should be a permissioned, permissionless or hybrid blockchain), and establishing a feasible mining algorithm that meets security requirements without costing immense computing resources for the distributed servers and systems hosting the blockchain. We also contribute to the profession by emphasizing the importance of communicating audit and assurance needs of the CPA firms to guide the development of blockchain-based business solutions. Lastly, this paper also makes some suggestions to CPA firms to start planning for required technical skills in providing audit and assurance services.

Appendix A

Step by step guide on how client ERP/legacy systems may connect to the blockchain

1. The sales order is entered into the system and the relational database tables are updated for the sales order
2. Subsequent to finalizing the Sales Order, a set of cryptographic hashes and their Merkle Root are generated for each segment of the Sales Order. Altogether, this data is digitally signed using the preparer's private key.
3. The list of hashes, its Merkle root and preparer's digital signature is recorded on Changelog including metadata like the Sales Order number, timestamp and preparer's unique identification number.
4. A cryptographic aggregator representing all of the data in the Sales Order relational database table may be updated with the cryptographic hash of the new record and added as part of the record.
5. Concurrently, the Merkle root and the Digital Signature is recorded on the Distributed Ledger, including related metadata like preparer's unique id and timestamp.
6. The validating servers on the Distributed Ledger network can verify the digital signature of the data by using the preparer's public key. Upon validation, the selected server can commit this transaction to the blockchain.
7. Once the block is mined the client will be notified of the blockchain block ID. The blockchain block ID can be attached to all the corresponding records in the Changelog. Developing a dedicated and shared smart contract can be another way of communicating these hashes; it may also help with user account management and preparer's public key lookup.

Step by step guide on how the auditor can leverage the blockchain for continuous auditing and assurance services

1. The auditor can use a blockchain explorer to extract all the blockchain block IDs for a specific client using the public key for that specific client.
2. The auditor can compare the Merkle roots mentioned in the transactions of the blockchain, to the Merkle root of the corresponding Sales Order included in the Changelog.
3. If there are no modifications or changes, matching Merkle roots in step number 2 should provide reasonable assurance that the Changelog was not modified.
4. Then the cryptographic aggregator is regenerated using the data in the Sales Order table, matching this with the latest version of the cryptographic aggregator present in the Changelog should provide reasonable assurance that the data in the entire Sales Order table was not modified after the fact.
5. In case of a mismatch in the cryptographic aggregator, the auditor may identify the Sales Order with mismatching Merkle Root.
6. Next, the auditor can recreate the segment hashes for the specific Sales Order with an unmatched hash of record and compare with segment hashes included in the Changelog to identify exactly which elements of the Sales Order were indeed modified.

Please cite this article as: N.E. Vincent, A. Skjellum and S. Medury, Blockchain architecture: A design that helps CPA firms leverage the technology, International Journal of Accounting Information Systems, https://doi.org/10.1016/j.accinf.2020.100466

References

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

American Institute of Certified Public Accountants (AICPA), 2018a. ASB Meeting. Agenda item 5. May 14–17. Scottsdale, AZ. Retrieved from https://www.aicpa.org/research/standards/auditattest/asb/20180515-asb-meeting-agenda-materials.html.

American Institute of Certified Public Accountants (AICPA), 2018b. Accounting firm leaders and innovators gather for strategic discussions on blockchain technology. Press release, May 8, 2018. Retrieved from https://www.aicpa.org/press/pressreleases/2018/firm-leaders-innovators-gather-for-discussions-on-blockchain.html.

Atzori, M., 2015. Blockchain technology and decentralized governance: is the state still necessary?. Retrieved from. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2709713

Baudet, M., Ching, A., Chursin, A., Danezis, G., Garillot, F., Li, Z., Malkhi, D., Naor, O., Perelman, D., Sonnino, A., 2019. State Machine Replication in the Libra Blockchain.

Beasly, M., Carcello, J., Hermanson, D., 2001. 10 audit deficiencies. J. Account., 63–66 Retrieved from http://www.journalofaccountancy.com/Issues/2001/Apr/Top10AuditDeficiencies.htm.

Block.one, 2018. EOS.IO technical whitepaper v2. Retrieved from https://github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md.

Blockchain.com, 2019. Hash rate distribution: an estimation of hash rate distribution amongst the largest mining pools. Retrieved from. https://www.blockchain.com/en/pools.

Brandon, D., 2016. The blockchain: the future of business information systems? Int. J. Acad. Bus. World 10 (3), 33–40.

Brooks, R., Wang, K.C., Yu, L., Oakley, J., Skjellum, A., Obeid, J., Lenert, L., Worley, C., 2018. Scrybe: a blockchain ledger for clinical trials. IEEE Blockchain in Clinical Trials Forum: Whiteboard Challenge Winner (2018).

Buterin, V., 2014. A next-generation smart contract and decentralized application platform. White Paper. vol. 3, p. 37.

Cai, Y., Zhu, D., 2016. Fraud detections for online businesses: a perspective from blockchain technology. Financ. Innov. 2 (1), 20.

Castro, M., Liskov, B., 1999. Practical byzantine fault tolerance. OSDI 99 (February), 173–186.

CPA Canada, 2017. Blockchain technology and its potential impact on the audit and assurance profession. Retrieved from https://www2.deloitte.com/content/dam/Deloitte/us/Documents/audit/us-audit-blockchain-technology-and-its-potential-impact-on-the-audit-and-assurance-profession.pdf.

Deloitte, 2016. Blockchain technology: a game-changer in accounting?. Retrieved from https://www2.deloitte.com/content/dam/Deloitte/de/Documents/Innovation/Blockchain_A%20game-changer%20in%20accounting.pdf

Deloitte, 2018. Breaking block https://www2.deloitte.com/us/en/pages/consulting/articles/innovation-blockchain-survey.html?id=us:2ps:3gl:confidence:eng:cons:32019:nonem:na:0WyqNxkn:1141606379:339149875841:b:Brand_Blockchain:Brand_Blockchain_Survey_BMM:br.

Exonum, 2019. Incorruptible auditing: exonum-powered graph database management. Retrieved from https://medium.com/meetbitfury/incorruptible-auditing-exonum-powered-graph-database-management-c4ed422c4ba7.

Goldwasser, S., Micali, S., Rivest, R.L., 1988. A digital signature scheme secure against adaptive chosen-message attacks. SIAM J. Comput. 17 (2), 281–308.

Guegan, D., 2017. Public blockchain versus private blockhain. Documents de travail du Centred'Economie de la Sorbonne 2017.20 (ISSN: 1955-611X. 2017,).

James, R., 2018. Creating an immutable audit trail on the blockchain with Xero & Tierion. Retrieved fr https://devblog.xero.com/creating-an-immutable-audit-trail-on-the-blockchain-with-xero-tierion-be423d39380b.

Kokina, J., Mancha, R., Pachamanova, D., 2017. Blockchain: emergent industry adoption and implications for accounting. J. Emerg. Technol. Account. 14 (2), 91–100.

Merkle, R.C., 1980. Protocols for public key cryptosystems. 1980 IEEE Symposium on Security and Privacy. IEEE, pp. 122–134 (April).

Ølnes, S., Ubacht, J., Janssen, M., 2017. Blockchain in government: benefits and implications of distributed ledger technology for information sharing. Gov. Inf. Q. 34, 355–364.

Parikh, T., 2018. The ERP of the future: blockchain of things. Int. J. Sci. Res. Sci. Eng. Technol. 4 (1), 1341–1348.

Pearlson, K., Saunders, C., 2006. Managing and Using Information Systems: A Strategic Approach. Wiley & Sons, Hoboken, NJ.

Porter and Lasiewicz CPAs, d. N.A. SAS No. 94: new standards on technology and internal control. Retrieved from https://www.garyportercpa.com/books/audit-articles/127-sas-no-94-new-standards-on-technology-and-internal-control.

Schmitz, J., Leoni, G., 2019. Accounting and auditing at the time of blockchain technology: a research agenda. Aust. Account. Rev. 89 (29), 331–342.

Sheldon, M., 2019. A primer for information technology general control considerations on a private and permissioned blockchain audit. Curr. Issues Audit. 13 (1), A15–A29.

Stinchcombe, K., 2018. Blockchain is not only crappy technology but a bad vision for the future. Retrieved fr https://medium.com/@kaistinchcombe/decentralized-and-trustless-crypto-paradise-is-actually-a-medieval-hellhole-c1ca122efdec.

Swan, M., 2015. Blockchain: Blueprint for a New Economy. O'Reilly Media, Inc.

Tan, B.S., Low, K.Y., 2019. Blockchain as the database engine in the accounting system. AAR 29 (2), 312–318.

Taskinsoy, J., 2019. Facebook's Project Libra: Will Libra Sputter Out or Spur Central Banks to Introduce Their Own Unique cryptocurrency Projects? (Available at SSRN 3423453)

Vicknair, C., Macias, M., Zhao, Z., Nan, X., Chen, Y., Wilkins, D., 2010. A comparison of a graph database and a relational database: a data provenance perspective. Proceedings of the 48th Annual Southeast Regional Conference. ACM, p. 42 (April).

Wood, G., 2014. Ethereum: a secure decentralized generalized transaction ledger. Ethereum Proj. Yellow Pap. 151 (2014), 1–32.

Zheng, Z., Xie, S., Dai, H., Chen, X., Wang, H., 2017. An overview of blockchain technology: architecture, consensus, and future trends. 2017 IEEE International Congress on Big Data (BigData Congress), Honolulu, HI, pp. 557–564 https://doi.org/10.1109/BigDataCongress.2017.85.

Zyskind, G., Nathan, O., 2015. Decentralizing privacy: using blockchain to protect personal data. IEEE Security and Privacy Workshops. SPW2015, pp. 180–184.

Please cite this article as: N.E. Vincent, A. Skjellum and S. Medury, Blockchain architecture: A design that helps CPA firms leverage the technology, International Journal of Accounting Information Systems, https://doi.org/10.1016/j.accinf.2020.100466