Reengineering the Audit with Blockchain and Smart Contracts

Andrea M. Rozario
Ph.D. Student
aochoa@scarletmail.rutgers.edu
Rutgers Business School
Rutgers University
1 Washington Park
Newark, NJ 07102

Chanta Thomas

Assistant Professor of AIS
cthomas@business.rutgers.edu
Rutgers Business School
Rutgers University
1 Washington Park
Newark, NJ 07102

Reengineering the Audit with Blockchain and Smart Contracts

Abstract: Blockchain and smart contracts are evolving business practices by enhancing efficiencies and transparency in the value chain. The fusion of these innovations is also likely to transform auditing by automating workflows but more importantly, by enhancing audit effectiveness and reporting. This paper envisions the future financial statement audit by proposing an external audit blockchain that supports smart audit procedures. The external audit blockchain has the potential to improve audit quality and narrow the expectation gap between auditors, financial statement users and regulatory bodies.

Keywords: Blockchain, Smart Contracts, Audit Evidence, Smart Audit Procedures, PCAOB Inspection Process

INTRODUCTION

Advances in technology have created a ‘real-time’ world in which economic transactions are processed electronically and immediately. Although businesses have adapted to this complex electronic world, the financial auditing paradigm remains in the status quo and continues to reflect a retrospective audit framework. Auditors continue to audit reactively and according to established archetypes, and yet they are still tasked with extending their confidence to the financial statements and protecting the public interest in regards to the financial statements in increasingly complicated and risky environments. It is not surprising that there is an expectation gap between the information auditors provide to financial statement users and the information expected by these users. This gap is the difference between what financial statement users demand, in terms of timely, relevant and reliable information and what they may receive as a result of the audit. Additionally, PCAOB inspection findings illuminate an additional expectation gap between the procedures that auditors actually perform and the procedures they are required to perform in accordance to audit standards and regulations (PCAOB 2016). In both cases, the expectation gap represents a unique opportunity for improvement not only in audit quality, but also in the auditor’s ability to respond to client risks in a rapidly changing technological environment. In response to the challenges facing auditors, this paper proposes an external audit blockchain supported by smart audit procedures aimed at improving audit quality and meeting the information and performance demands of stakeholders.

Blockchain and smart contracts have great potential to improve business process quality. Blockchain is essentially a distributed linear database that protects the integrity of its information with cryptography. Since blockchain provides a tamper-proof audit trail, which can be fused with smart contracts to autonomously execute tasks on behalf of human users (Szabo 1997; Kozlowski 2016), it is increasingly gaining popularity among business entities. Various types of business entities are exploring the numerous blockchain applications that can improve efficiencies across the different components of the value chain. For example, blockchain applications for securing medical records and supply chain provenance are among the many use cases of this technology[1].

Similarly, blockchain is gaining momentum in the public accounting industry. For example, Deloitte was one of the first to successfully audit blockchain protocol[2], whereas PwC and EY have successfully developed auditing tools specifically for auditing blockchain transactions. Notably, PwC recently began to offer continuous auditing software to audit transactions on private business blockchains,[3] and EY developed the EY blockchain analyzer, which is capable of extracting transactions from multiple blockchain ledgers[4].

Despite tremendous technological disruption in the last decade[5], the audit paradigm does not yet parallel the digital business world in adopting the use of new technologies as part of a change to methodology. Alles (2015) suggests that the audit clients' use of advanced technologies is likely to be the driver of adoption of such technologies by auditors. Blockchain and smart contracts technologies can potentially help the current audit framework to evolve by changing the way audit evidence is collected, analyzed and disseminated. By failing to take advantage of blockchain and smart contract technologies, the audit client's digital environment and associated risks will continue to outpace the effectiveness and quality of the auditor's procedures. As a result, it is imperative to examine the extent to which blockchain and smart contracts can disrupt the financial statement auditing paradigm. This paper proposes a conceptual

[1] See: https://medium.com/@matteozago/50-examples-of-how-blockchains-are-taking-over-the-world-4276bf488a4b
[2] See: https://www.ccn.com/big-four-giant-deloitte-completes-successful-blockchain-audit/
[3] See: https://www.pwc.com/us/en/about-us/new-ventures/pwc-blockchain-validation-solution.html
[4] See: https://www.ey.com/en_gl/news/2018/04/ey-announces-blockchain-audit-technology
[5] See: http://usblogs.pwc.com/emerging-technology/rise-robotics-ai-infographic/

framework for an external audit blockchain in which smart contracts, referred to as "smart audit procedures" hereafter, can autonomously execute audit procedures and disclose audit procedures' results to participating users near real-time.

This paper extends the Dai and Vasarhelyi (2017) discussion on the possible applications of blockchain and smart contracts to transform auditing. However, several additional distinctive perspectives are also established. First, in this paper an external audit blockchain, which is supported by smart audit procedures, is proposed. The proposed blockchain can serve as an unified platform to enhance audit effectiveness and audit reporting. Second, this paper maps the characteristics of blockchain that can enhance audit evidence to the requirements of audit evidence described in PCAOB auditing standard 1105 (2010). Furthermore, novel functions for the PCAOB, such as becoming the validators of smart audit procedures [6]and the reviewers of the results of these procedures near real-time, are proposed in an effort to support its evolving initiatives for improving audit quality (PCAOB 2018). Finally, this paper envisions the evolution of the financial audit paradigm by presenting a holistic audit framework that maps assertions to on and off-the-blockchain audit procedures. Taken together, this paper offers useful insights into the potential use of blockchain and smart contracts by auditors to reduce the expectation gap dilemma.

Additionally, this paper uses design science research (DSR) methodology, the science of creating purposeful artifacts (Hevner, March, Park and Ram 2004), as an overall guide for the discussion of the proposed audit methodology. Peffers et al. (2007) propose the following steps for design science research:

[6] By becoming the validators of smart audit procedures, the PCAOB can verify that such audit procedures are designed appropriately and will adequately accomplish the audit objectives prior to the audit inspection process. Doing so will improve the PCAOB audit inspection process and proactively enhance the effectiveness of the financial statement audit.

1) Problem identification and motivation,
2) Define objectives of a solution,
3) Design and development of an artifact,
4) Demonstration of the solution,
5) Evaluation of the solution, and
6) Communication of the results

It is noted that individual DSR studies are not expected to comprise all six activities (Peffers et al. 2007). Likewise, in this paper, the first three activities, comprising problem identification, defining the objectives of a solution and the design of an artifact, are discussed. As research progresses in the blockchain audit domain, it is expected that research papers concerning the development and evaluation of the design will be produced.

The remainder of this paper is organized as follows. The next section identifies the problem and discusses the motivation. The third section describes what a blockchain is, how it operates and its characteristics. The fourth and fifth sections define the objectives of the proposed framework. The conceptual framework is presented in sixth and seventh sections. The last section concludes this paper and discusses limitations and future research.

THE EXPECTATION GAP DILEMMA IN THE DIGITAL ERA

The expectation gap dilemma that exists between both the auditor and the financial statements users and the auditor and the standard setters can be further broken down into an information gap and a performance gap (PCAOB 2016b). The information gap is the result of the information auditors provide to financial statement users versus the information financial statement users expect from auditors. The performance gap, on the other hand, arises from the disconnect between the audit procedures auditors are required to perform per audit standards and the audit procedures that are ultimately performed. Collectively, these gaps call into question the usefulness of auditing, the audit opinion and the usefulness of audited financial statements.

The primary objective for a financial statement auditor is to provide the user of the financial statements with reasonable assurance that an entity's financial statements are free from material misstatement (Louwers et al. 2018). They lend their credibility and confidence to the financial statements and with that, ensure that the public interest regarding that information is protected. Yet, financial statement users are starting to leverage unorthodox sources of information, such as real-time social media postings, to make financial decisions (Stein 2015). In the age of technological disruption and ever-increasing access to large amounts of information, understanding the information gap between what investors and financial statement users need and want from the auditor and what the auditor actually provides needs to be explored.

Moreover, it is the mission of the PCAOB to "oversee the audits of public companies in order to protect the interests of investors and further the public interest in the preparation of informative, accurate, and independent audit reports"[7], improve audit quality and, in some respects, ensure that auditors satisfy the demands of financial statement users. However, their inspection findings suggest that audits are deficient in a variety of areas including the adequacy of substantive procedures performed, identification and testing of controls and the sufficiency of evidence to support the audit opinion (PCAOB 2016; PCAOB 2017). Therefore, a performance gap exists between the procedures auditors are expected to perform and the procedures that are actually performed and reviewed by PCAOB inspectors. Even if on a small scale, this performance gap undoubtedly illuminates the need for audit activities that can lead to higher audit quality.

[7] See: https://pcaobus.org/About/History/Pages/default.aspx

It is critical for auditors to be proactive in understanding how disruptive technologies can evolve auditing to satisfy financial statement users demands and aid the PCAOB's continuous initiatives to improve overall audit quality (PCAOB 2017; PCAOB 2018). Some public accounting firms are adapting to business adoption of blockchain technology by exploring how to audit the blockchain protocol or by developing tools to audit the blockchain transactions of their clients[8][9]. Accordingly, this paper proposes a way to enhance audit quality and meet different user demands in near real-time through the use of blockchain and smart contracts to ameliorate the expectation gap dilemma. In doing so, these technologies could evolve the way that financial statement audits are performed and delivered.

BLOCKCHAIN

Blockchain technology became increasingly popular primarily as a result of Bitcoin virtual currency (Nakamoto 2008). Blockchain is an open distributed ledger that enables users to transact directly with each other without the need of a trusted third party (Gruber 2013; Bryans 2014; Singh 2015). Using the Bitcoin network as an example of blockchain functionality, transactions would be sent directly by the payer to the payee and then broadcast on the Bitcoin network. These transactions are combined into blocks and validated by miners[10] about every 10 minutes through cryptography that combines a hash[11] of the transaction and the digital signature of the user. Upon validation of transactions, blocks are posted and time-stamped in the sequential blockchain ledger and are visible by all the nodes[12].

[8] See: https://www.pwc.com/us/en/about-us/new-ventures/pwc-blockchain-validation-solution.html

[9] See: https://www.ey.com/en_gl/news/2018/04/ey-announces-blockchain-audit-technology

[10] Miners are nodes on the Bitcoin network that offer their computational resources to solve the hash function, once the hash function is solved, the transaction is posted to the blockchain ledger and visible by all participating nodes.

[11] Hash functions are used to encrypt and store data efficiently and securely. A hash function takes a string of characters, input x, and produces, a fixed-length, output y consisting of random numbers and characters.

[12] Note that a block is complete when all transactions within the block are validated.

Key characteristics of the blockchain include decentralization, immutability and accountability. Decentralization is achieved by enabling various nodes (computers) to download the blockchain ledger, where every node has a local copy of the blockchain ledger and a universal view of the transactions. Due to the decentralized nature and the fact that each node has its own copy of the ledger, fraud on the blockchain would be unlikely to occur as participating nodes have access to view blockchain transactions as they are posted. In addition, any transactions that may appear fraudulent or in error would be corrected by appending a transaction adjustment to the blockchain.

Due to the cryptographic mechanism employed by the blockchain, immutability is also achieved. Once a block of transactions has been completed and added to the end of the blockchain, they cannot be reversed. This function prevents the problem of double spending coins from a digital wallet since the cryptography essentially prevents retroactive changes to the blockchain ledger. The cryptography and decentralization attributes provide the auditor with a tamper-resistant audit trail. Finally, accountability is achieved on the blockchain as the digital signature of the user binds him or her to the transaction enabling the auditor to verify the originator of the transaction. Collectively, these attributes make this technology appealing for accounting and assurance purposes as it provides a secure set of records, near real-time reporting, a robust audit trail and transparency.

BLOCKCHAIN CAN IMPROVE THE RELIABILITY OF EXTERNAL AND INTERNAL AUDIT EVIDENCE

Ensuring that audit evidence collected for audit procedures is sufficient, relevant and reliable is paramount to auditors (PCAOB AS 1105 2010). Sufficiency is not likely to be a challenge in a blockchain environment since, for the transactions processed on the audit client’s blockchain, auditors would have the ability to extract and test full populations. As a result, auditors would shift their focus to the relevance and reliability requirements of audit evidence. The relevance of blockchain information will likely remain a matter of audit judgment (Brown-Liburd and Vasarhelyi 2015) as auditors would have to determine whether the evidence collected can satisfy audit objectives (e.g. collecting blockchain sales invoices[13] to verify the occurrence of sales transactions can satisfy the audit objective to verify that no fictitious transactions were recorded). With respect to reliability, the blockchain infrastructure has the potential to enhance the integrity of internal and external audit evidence.

When performing traditional audits in the current business environment, which primarily consists of centralized accounting ledgers, external audit evidence is considered more reliable than internal audit evidence as it is less likely for this information to be manipulated by management (PCAOB AS 1105 2010). However, the blockchain characteristics of decentralization, immutability and accountability can enhance the reliability of internal and external audit evidence as financial information, purchase orders[14], invoices and IoT[15] information can be stored on the secure and transparent blockchain ledger.

Since blockchain transactions require reconciliation by participating nodes, before they are posted to the ledger, completeness and accuracy checks are essentially performed proactively. Completeness and accuracy checks are also performed once transactions are posted as participating nodes have access to a universal view of blockchain transactions[16]. In addition,

[13] https://gocardless.com/guides/invoicing/blockchain-and-e-billing/
[14] See: https://www.sofocle.com/procure-pay-process-blockchain-way/
[15] IoT on the blockchain can help overcome security challenges. See: https://www.ibm.com/developerworks/cloud/library/cl-blockchain-for-cognitive-iot-apps-trs/cl-blockchain-for-cognitive-iot-apps-trs-pdf.pdf
[16] The consensus and decentralization infrastructure of the blockchain can help verify the accuracy and completeness of transactions. Validity checks of blockchain transactions is provided by transaction validators on the blockchain, once these validators reach consensus, transactions are posted to the blockchain. In addition, as every node has a

blockchain records are tamper-resistant due to the cryptographic mechanisms that are deployed. These records are protected by code and become irreversible as transaction hashes contain the information of the current transaction and the previous transaction. Finally, the originator of the record can be identified as the hash of the record also contains the user's digital signature. Taken together, blockchain attributes of decentralization, immutability and accountability help improve the integrity of internal and external data. Table 1 summarizes the challenges related to the veracity and variety of audit evidence that are mitigated by the blockchain.

The use of financial and nonfinancial information as audit evidence is known to enhance the accuracy of audit procedures (Brazel, Jones and Zimbelman 2009). However, the costs of preparing audit evidence from different sources has the potential to exceed its expected benefits as auditors may find it cumbersome to combine information from various sources (Appelbaum 2016). Blockchains have the ability to store audit evidence from a variety of sources, therefore helping to overcome the challenge of aggregating financial and nonfinancial information from internal or external sources.

The decentralized infrastructure of the blockchain also promotes the sharing of information in a more structured and similar format across companies or industries. In this manner, heterogeneous data is aggregated in near real-time into the blockchain distributed ledger and visible to participating users. On the blockchain, auditors would have access to all the reconciled financial transactions between, for example, the auditee (revenue) and its respective customers (payments), providing the auditors with one consistent version of economic transactions. Auditors could also benefit from using IoT information, such as locational data from GPS devices, or temperature data, stored on the blockchain to obtain a deeper

local copy of the blockchain ledger they would have the ability to check whether their transactions have been posted and whether they have been posted accurately.

understanding of the client’s business and risk and to improve the accuracy of their estimates and valuations.

Although blockchain information has the potential to be more reliable than information from an ERP system, it is important for auditors to consider the risks that emerge in a blockchain environment. For example, the private keys of digital wallets can be stolen or lost, and there can be errors in smart contract code. Both of these risks could compromise the reliability of blockchain information.

BLOCKCHAIN AUDIT EVIDENCE AND SMART AUDIT PROCEDURES CAN IMPROVE AUDIT QUALITY

Blockchain Smart Contracts as Smart Audit Procedures

Ethereum, a Bitcoin competitor, has become prevalent in debates relating to the future of blockchain technology (Buterin 2013). The Ethereum blockchain network is a more general application of the Bitcoin blockchain network, because it offers users the ability to create and execute a variety of smart contracts. Essentially, a smart contract is a software program that performs actions on behalf of the user based on pre-defined conditions (Szabo 1994). It refers to computer protocol that facilitates the process of engaging in contractual agreements including the enforcement, verification and performance of the terms of a contract (Szabo 1994), and within the blockchain, oversight authority of these contracts is distributed to the participating nodes (Dai and Vasarhelyi 2017). The emergence of blockchain technology has revitalized the concept of smart contracts, thus paving the way for the use of smart contracts as smart audit procedures.

In addition to the variety of external and internal audit evidence from the client’s blockchain having the potential to be a more reliable form of audit evidence, smart audit procedures on a blockchain that is operated by the external auditor and that leverage this audit evidence could also improve audit quality and reporting. Smart contracts on the blockchain are not restricted to legal agreements that become digitized, because they can be valuable in other contexts, such as auditing (Dai and Vasarhelyi 2017). In this way, smart contracts can become smart audit procedures. These smart audit procedures are essentially autonomous software programs that allow auditors to execute audit procedures based on pre-defined parameters. Smart audit procedures have the ability to mimic the function of software agents[17] that have the ability to analyze audit evidence on behalf of the auditor (Koslowski 2016). Rozario and Vasarhelyi (2018) propose that smart audit procedures can be preprogrammed as 'IF-THEN' rules and loaded to the blockchain set up by the external auditor.

Figure 1 describes an example of a smart analytical procedure to address the risk of material misstatement in sales. In the example, audit logic is translated to computer logic, which is the smart audit procedure and loaded to the external audit blockchain that the audit firm has set up. The results of the smart audit procedures can then be verified by any blockchain users the audit firm has provided access to. Then, one of two methods could be employed to manage the processing of notable items that are identified by smart audit procedures. The auditor could either manually investigate the notable items or, a follow-up smart audit procedure that prioritizes records that require further investigation could be pre-programmed.

The aforementioned example describes a smart analytical procedure. However, simpler ones can be performed. For example, a smart control procedure can be described as a simplistic rules-based system that checks that the sales order, shipping documents and sales invoice match and take place in the correct order. If there are differences, like with traditional audit procedures, auditors would have to inquire with management and perform additional testing to ensure these

[17] Intelligent agents are computer programs that autonomously perform specific tasks on behalf of the human user (Nelson, Kogan, Srivastava, Vasarhelyi and Lu 2000; Vasarhelyi and Hoitash 2005).

differences do not indicate a material misstatement. In addition, follow-up smart audit procedures could also be pre-programmed to handle the notable items that are identified by other smart audit procedures.

Blockchain Audit Evidence and Smart Audit Procedures Can Improve Audit Quality

Merged with blockchain technology, smart audit procedures have the potential to transform auditing. As discussed in the preceding section, blockchain mitigates challenges associated with gathering audit evidence and potentially improves the reliability of both internal and external audit evidence. For example, if a smart audit procedure processes unreliable information from the client's ERP system, the results could be misleading and potentially cause auditors to over or under estimate audit risk (Appelbaum 2016). However, the infrastructure of the blockchain, including decentralization, immutability and accountability characteristics, has the potential to substantially improve the reliability of financial and nonfinancial data. Therefore, the variety of more reliable data on the blockchain has the potential to enhance the effectiveness of smart audit procedures by more accurately capturing the real risk of material misstatement.

In addition, blockchain audit evidence may enhance auditor judgment in a way that was not possible before. Now, auditors could have access to a variety of immutable data that enhances their ability to assess risk in new and innovative ways. For example, a variety of nonfinancial data that is typically not stored in a linear database (e.g. locational data from GPS devices, temperature sensors, weather data, etc.) can be connected to the blockchain, and new and reliable datasets can be generated. These datasets can enhance the accuracy of smart audit tests and auditors' understanding of the client's business environment. For example, for audit client's that deliver perishable food items to a customer's designated location, GPS locational data and temperature data on the blockchain can capture the exact time, date, place and temperature of these items providing the auditor with more visibility of the revenue process, including reasonableness of some of the client's estimates regarding spoilage, returns, etc. Incorporating these less traditional, nonfinancial predictors into a smart analytical model for sales could substantially improve the predictive power of the model (Yoon 2016) and provide new insights as to potential risks that may arise as a result of the client's business environment. For instance, temperature data on the blockchain can directly capture whether food items that are in transit are damaged. In this manner, nonfinancial information on the blockchain enables auditors to obtain deeper insights into risks that may lead to misstatements in revenue and other significant accounts such as inventory, accounts receivable and accounts payable.

Smart audit procedures that can automate manual and repetitive audit tasks that do not require audit judgment offer auditors the opportunity to focus resources on higher risk areas and thus improve audit quality. These high risks areas could include, but are not limited to, the analysis of notable items that are generated by smart audit procedures or the analysis of management's fair value assumptions.

Blockchain Audit Evidence and Smart Audit Procedures Can Improve Audit Reporting

The traditional audit paradigm is backward-looking and reflects a retrospective assurance model (Chan and Vasarhelyi 2011), because an opinion on the audited financial statements is issued at a point in time, several weeks after the occurrence of financial events. Therefore, the usefulness of annually audited financial statements in a modern world where financial statement users base their decisions on information that is available near real-time is questionable (Vasarhelyi and No 2017; IAASB 2016; Rozario and Vasarhelyi 2018).

With smart audit procedures, audits naturally transition to a proactive audit model. Proactive audits have the potential to improve audit quality by detecting material misstatements at different points in time and by providing timelier and more transparent information to financial statement users (AICPA 2015). In addition, by executing smart audit procedures that use client blockchain information on the external audit blockchain, which is discussed in the following section, the reliability of audit evidence is preserved since management does not need to provide data to the auditor as they would directly extract information from the client's blockchain. This is important as audit procedures generally incorporate extracted information from the client's ERP system which could be subject to management manipulation[18].

Equally important, blockchain-based smart audit procedures can support the PCAOB's evolving initiatives in promoting audit quality (PCAOB 2017; PCAOB 2018) by enabling close monitoring of the audit firm's process near real-time. This idea of leveraging technology to "guard the guards" (i.e. auditing the auditors) is not a new concept. Alles, Kogan and Vasarhelyi (2004) proposed a "black box log file" that enables third party monitoring. This paper expands on this concept by proposing that blockchain and smart contract technologies could be implemented to securely store audit procedures that could be visible by relevant external parties that oversee financial statement audits, such as the PCAOB.

By closely monitoring the audit firms' process to address the risk of material misstatement and ultimately opine on financial statements, blockchain-based smart audit procedures offer the ability to perform more proactive audit inspections and potentially prevent audit failures. As suggested by Rozario and Vasarhelyi (2018) "with blockchain based smart audit procedures, both auditors and regulators have the opportunity to proactively address areas

[18] Although, external auditors generally engage IT auditors to test IT controls in order to ensure access to change management controls is restricted and ensure changes in the ERP system are valid, the risk of management making inappropriate changes still exists. Compared to an ERP system, this risk is lower on the blockchain since the ledger is distributed and relevant nodes would insure the data on the ledger is correct.

where audit firms have been deficient." Consequently, regulators can leverage blockchain-based smart audit procedures to improve the audit inspection process (PCAOB 2017).

In the following sections, interlinked blockchain ecosystems and the audit approach on the external audit blockchain ecosystem are described. The interlinked ecosystems consist of a business blockchain and a proposed external audit blockchain. Subsequently, the audit approach on the external audit blockchain ecosystem is proposed by describing a series of risks that relate to the revenue process and the potential smart audit procedures that could be used to address those risks.

INTERLINKED BLOCKCHAIN ECOSYSTEMS

A business ecosystem is defined as "an economic community supported by a foundation of interacting organizations and individuals" (Moore 1996). Therefore, the byproduct of businesses shifting portions of their activities to the blockchain would be a blockchain ecosystem in which several business entities, such as Walmart and its suppliers [19], exploit the benefits of this technology. Similarly, as blockchain and smart contracts provide a unified and secure platform for the collection, analysis and dissemination of audit evidence, it is plausible for auditing to evolve to be more closely aligned with external users' expectations.

The evolving blockchain ecosystem is likely to be a multitude of interlinked blockchain ecosystems such as the ones described above. In this type of ecosystem, proactive audits are advantageous, because within it the auditor has the capability to view and extract a variety of reliable information from the client's blockchain without the need for laborious data standardization and then feed this data to pre-defined smart audit procedures that have been

[19] Walmart and its suppliers share relevant and reliable information about the quality of food items near real-time See: https://www.nytimes.com/2018/09/24/business/walmart-blockchain-lettuce.html

vetted by the PCAOB. Interlinked blockchain ecosystems are depicted in Figure 2. These ecosystems facilitate the seamless sharing of relevant and reliable information that is transmitted across active participants on numerous private and permissioned blockchains.

Permissioned Business Blockchain Ecosystem

Private and permissioned blockchains may be more appropriate in business and audit settings as they limit the amount of participants (Pilkington 2016). In addition, the responsibilities of these participants are defined in advance by the blockchain network administrator (Peters and Panayi 2015). This type of blockchain is useful as it helps preserve the confidentiality and security of information, and only a restricted amount of participants would have access to information and the access would be pre-determined. Certain participants may have the permission to send and/or receive transactions, others may have permission to only validate and post transactions, while others may have read-only access.

In the PBC (Private/Permissioned Blockchain) Business Ecosystem, the network administrator, which could be an employee of the audit client, would provide access to the client's blockchain. Accordingly, read and write access to customers A and B, supplier A and the bank can be restricted by the network administrator. The access[20] that is granted to these participants would depend on the agreement between the client and these external parties.

Using figure 2 for illustration, customer A could pay for purchased goods with digital currency and, along with the client, track the shipment of the goods with GPS and temperature sensors to verify the location, quality and time of shipment of the goods. Once the goods are

[20] While this type of blockchain can be useful in settings where confidentiality of the information is important, its major drawback is that it would be less decentralized than a public and permissionless blockchain, which would enable trust in a trustless environment. Therefore, this infrastructure is more beneficial when it is applied to a context where there is some trust amongst parties, yet trust needs to be enhanced (Glaser 2015; Gockel et al. 2018).

delivered and payment has been satisfied, the audit client may use these funds to satisfy loan covenants with their bank and purchase raw materials from supplier A to manufacture more inventory. In the blockchain, the aforementioned business events are visible by the audit client and its relevant participants in near real-time, as soon as transactions become posted to the blockchain. Additionally, the auditor can be a read-only node on the blockchain (PwC 2017) and have access to timely and reliable information as they are independent assurors of the audit client and do not directly engage in client business operations.

Permissioned External Audit Blockchain Ecosystem

There are benefits to having the external auditor be a node on the audit client's blockchain. The auditor, acting as an independent node on the client's blockchain, would have read-only access to the complete population of internal and external blockchain information, such as sales transactions, legal smart contracts, GPS data, various logs, etc. In addition, the client and auditor could reach the consensus to add the auditor as a node on the client's blockchain as sharing information on this platform would be less disruptive to the client than data extraction in a traditional auditing paradigm since less information would have to be extracted by management. Secondly, the auditor would benefit from being a node on the blockchain as the reliability of potential audit evidence is ensured by blockchain architecture.

There are a few reasons that should be considered in justifying the read-only access the auditor would have on the client's blockchain and why the smart audit procedures should take place on the external audit blockchain and not on the client's blockchain. First, the auditor is not an active participant engaging in transactions with the client's blockchain related participants; they are the independent verifiers of the client's assertions concerning financial statements (Louwers et al. 2018). Second, to preserve auditor independence on the blockchain, it would not be feasible for the auditor to perform smart audit procedures on the auditee's blockchain as it could be perceived as impairment of independence in appearance (Alles, Kogan and Vasarhelyi 2002). Finally, read-only access is appropriate as it helps maintain the scalability of the private and permissioned blockchain by limiting the auditor to only have access to view and extract information.

Figure 2 also depicts the proposed independent external audit blockchain. Since the auditor is a node on the client's blockchain, they can extract audit relevant information, such as sales transactions, load it to their own blockchain and smart audit procedures could autonomously execute predetermined audit tests. The external audit blockchain ecosystem would consist of smart internal control tests, smart test of details and smart analytics that could enhance audit quality. These smart audit procedures could help detect material misstatements at different time intervals. After setting up their blockchain, the audit firm's IT team, in conjunction with the auditors, can design smart audit procedures and load those procedures to the external auditor blockchain. The PCAOB, as one of the active nodes on the auditor's blockchain, could vet these procedures as this is part of the consensus architecture of a blockchain. Auditors would then load smart audit procedures to the blockchain, but a different node on the blockchain, the PCAOB, could validate the smart audit procedures before they are activated.

One of the objectives of the PCAOB is to ensure audits are conducted in accordance with GAAS (generally accepted auditing standards). By including the PCAOB as a participating node on the auditor's blockchain, these regulators are able to provide oversight of the auditing firms prior to the firm's subsequent quality inspection. This can help improve the PCAOB's inspection process and communication between PCAOB inspectors and audit firms. Currently, the PCAOB inspects large audit firms (firms that audit more than 100 public companies) on an annual basis and small audit firms on a triennial basis. These quality inspections occur after all audit testing has been concluded and the audit opinion has been issued. Hence, blockchain and smart contracts provide a way for the PCAOB to to enhance the effectiveness their inspection process by shifting it from a reactive to a more proactive inspection process that could detect potential audit deficiencies near real-time. We propose that the PCAOB would be appropriately qualified to verify the basic requirements of smart audit procedures, which could include verifying that smart audit procedures are designed to test significant financial statement accounts and specific assertions. Accordingly, the PCAOB would have the ability to validate the smart audit procedures that auditors post to their blockchain, view the results of smart audit procedures and also send inspection related information to auditors about their procedures. Therefore, issues previously discussed, like failure to appropriately test aspects of the audit or performing inadequate procedures, would be mitigated, as the PCAOB would be able to vet the appropriateness of the auditor's procedures prior to their execution. Potentially, to expedite this process, the PCAOB may develop its own smart audit procedures to determine the appropriateness of the auditor's procedures.

Secondary users of the external audit blockchain could also include other audit stakeholders like key investors, the SEC and the audit committee. The external audit blockchain would grant the auditors the ability to send relevant information to the appropriate parties. For example, analyses for revenue including checks that match the sales invoice, shipping and sales order details and regression analysis that predicts future revenue or future customer churn could be executed by smart audit procedures on the external audit blockchain and sent to users of the financial statements to influence their investing decisions. The deployment of smart audit procedures on the blockchain can help improve audit quality by offering timelier information to financial statement users and assisting with the regulator's quality assessment process.

Smart audit procedures and their results would be visible by participating parties based on the following hierarchical structure.

PCAOB

Smart audit procedures would be visible to the PCAOB for vetting and approval prior to execution of the procedures by the auditor. In addition, the results of the smart audit procedures would also subsequently be visible by PCAOB inspectors. The PCAOB could be given read and write access within the external audit blockchain to allow inspectors to view, comment on and make suggestions to the auditor's proposed smart audit procedures. However, it would not be feasible for the entire audit process to go on the blockchain. Since complex audit procedures such as the evaluation of the tax provision and fair value level 3 investments require a high degree of auditor judgment, they are likely to remain off-the-blockchain[22]. Thus, the PCAOB would likely adopt a hybrid approach to inspecting audit procedures for quality and collect documentation for audit procedures on and off-the-blockchain for their inspection process. Nevertheless, the visibility of smart audit procedures and their results on the tamper-proof external audit blockchain can facilitate the auditor's compliance with the PCAOB's requirements by preventing the use of inadequate audit procedures and thus help prevent audit failures.

SEC, Audit Committee, Financial Statement Users

The SEC can also be a node on the external audit blockchain and given read-only access to the results of smart audit procedures that have flagged for potential fraud or restatement

[22] The term off-the-blockchain refers to audit procedures that are not recorded on the decentralized audit blockchain depicted above. An example of on and off blockchain procedures is presented in Table 2.

indicators. This type of information would be highly beneficial to SEC regulators as they perform risk assessment procedures to select potential companies for inspection. Also, having the audit committee as a node on the external audit blockchain would facilitate a more direct and timely method of communication from the auditors to the audit committee. Lastly, the general public, including key investors, lenders and key suppliers, would have read-only access to view the results of smart audit procedures at the transactional level and to view the results of testing of the operating effectiveness of internal controls. This will provide them with access to more useful information than that provided by the aggregated nature of the traditional financial statements. Smart audit procedures have great potential to enhance the informational value that is provided by auditors. While a traditional audit opinion for financial statements may not yet be possible on the external audit blockchain, auditor certifications at the transaction and internal control level may provide timely and relevant information to various stakeholders (AICPA, 2015).

CONTINOUS AUDIT AND THE AUDIT APPROACH ON THE EXTERNAL AUDIT BLOCKCHAIN ECOSYSTEM FOR REVENUE

Vasarhelyi and Halper (1991) developed a Continuous Auditing Process System (CPAS) at AT&T Bell Labs that executed automated analyses, near real-time, on a complete population of records. The automated analyses comprised pre-defined benchmarks, based on auditor defined rules. Each time records exceeded the benchmarks they were flagged by the system and investigated by auditors. Since then, more Continuous Auditing (CA) applications have been developed and implemented by business entities (Kuenkaikaew and Vasarhelyi 2013).

Despite the progressive adoption of this methodology by business organizations, adoption of CA by external auditors is practically non-existent. The major hurdle of CA adoption by external auditors resides within statutory requirements that mandate the auditor to be independent in appearance, which presents a conflict with CA methodologies that must be impounded on the client's computer system (Alles et al. 2002; Bumgarner and Vasarhelyi 2015). A viable solution to the independence problem for CA could be an audit data warehouse (Sigvaldason and Warren 2004). However, the aggregation of various sources of endogenous and exogenous data would remain a challenge. Moreover, for CA to become a reality in financial statement audits, a platform to securely execute automated audit procedures and to disseminate the results of those procedures would be required.

Blockchain has the potential to be an important facilitator for CA adoption by external auditors. By collecting a myriad of more reliable data from the client's blockchain and feeding such data to the independent external audit blockchain, where smart audit procedures execute audit tests, auditors insure the integrity of audit evidence and maintain independence while having the ability to provide near real-time assurance and reporting in a real time economy. It is important to highlight that the blockchain provides a unique platform for both near real-time assurance and reporting, because it would facilitate the autonomous deployment of smart audit procedures.

Responding to Revenue Risks with Blockchain Smart Audit Procedures

Figure 3 provides an example of how smart audit procedures can work seamlessly to address multiple phases of the audit for the revenue cycle. This example illustrates how through the use of smart audit procedures executed on an external audit blockchain, the auditor's response to risk can become more proactive. As a result, the external audit blockchain ecosystem for revenue in Figure 3 depicts a variety of smart audit procedures that can be deployed to ensure that the risk of fictitious or erroneous revenue transactions is addressed and that the auditor's detection risk is reduced. The auditor would extract audit evidence from the client's blockchain and send this information to the hash of the smart audit procedure on the external audit blockchain. The smart audit procedure can then automatically perform the pre-defined audit test.

To address the risk of fictitious or erroneous revenue transactions, four smart audit procedures could be applied: 1) a smart analytical procedure that matches the code of the legal smart contracts of the client could be set-up on the external audit blockchain; this procedure can be pre-programmed to match the code of the client's legal smart contracts in the current period under audit to the code of client's legal smart contracts from the prior audit period. By performing this procedure, the auditor can verify that the legal contracts of the client have not changed and if they have, the smart internal control test would flag any contract amendments. In addition, this procedure could also assist auditors in identifying new legal smart contracts that need to be audited. The described test could also serve as a triple-purpose audit procedure as it could assist with risk assessments, provide audit evidence for the existence and rights and obligations assertions over sales revenue and provide evidence of the operating effectiveness of internal controls.

The other smart audit procedures could be applied include: 2) a smart analytic that could execute a regression model based on pre-defined parameters including previous weeks' sales and IoT data that provides the location and temperature of the goods. This smart analytic can facilitate risk assessments and provide audit evidence about management's assertions of the revenue account balance; 3) in conjunction with this smart analytic, a smart internal control test could be automatically configured to use IoT data to match the location and temperature of the goods that are in transit to the expected location and temperature of the goods, as per the contract terms, thus providing audit evidence about the effectiveness of internal controls; and 4) finally, a three-way match smart internal control test could compare sales orders, sales invoices and shipment amounts, this control can serve as a triple-purpose audit procedure.

Collectively, these smart audit procedures would enable the auditor to assess the risk of material misstatement more accurately and timely manner. Therefore, as smart audit procedures increase audit efficiency, auditors would be able allocate more time to higher risk audit areas and areas requiring more complex auditor judgment while increasing the informational value they provide to various stakeholders.

Holistic Audit Framework for Revenue

Going forward, auditing with blockchain is likely to consist of both smart audit procedures on the blockchain and audit procedures off-the-blockchain. Both are needed to effectively conduct audits.

Even though an external audit blockchain ecosystem for revenue supports the automation and reporting of audit procedures, audit judgment will still remain salient. As a result, audit procedures that are unstructured due to a high level of subjectivity and complex judgments would remain outside of the blockchain. When testing using the blockchain, auditors will have to address notable items that smart audit procedures flag as not meeting pre-defined conditions. These items may require further investigation and perhaps paper-based audit evidence that would need additional documentation. The verification of legal paper-based company contracts and complex revenue estimates, such as when revenue is earned on a percentage of completion approach, are examples of additional procedures that may have to be manually verified and documented outside of the external auditor blockchain.

In addition, some accounting information will need to be verified outside of the blockchain environment due to the nature of the information. Information such as month-end adjusting journal entries, for example, would remain off-the-blockchain as these entries are generally related to company specific events (e.g. intercompany inventory transfers or consolidation adjustments). These type of entries do not pertain to routine business operations, and consequently may not satisfy the transaction validation criteria. Therefore, if accounting information exists outside of the blockchain it should be also be verified outside of it, since this technology can provide more reliable information only when there is a single version of transactions (O' Leary 2018).

Even though it may not be reasonable to program smart audit procedures on the blockchain for highly subjective audit procedures and for information that exists outside of it, it is still very clear that an external audit blockchain ecosystem has great potential to enhance audit quality and audit reporting. Table 2 provides a holistic representation of an audit approach for revenue, which takes the above considerations into account. Particularly, significant audit risks that are generally important for manufacturing clients and those that carry inventory. Each risk described in the Table 2 is aligned with respective assertions (occurrence, completeness, cut-off) and relevant audit procedures for risk assessment, substantive testing and/or tests of controls. The last column in the table indicates whether the audit procedures would be executed on the external audit blockchain (i.e. smart audit procedures) or if they would remain in the traditional environment, off the external audit blockchain.

For example, using Table 2, to address the risk of fictitious or erroneous revenue transactions, auditors would perform eight audit procedures, two of which would need to be performed off the external audit blockchain. Four of these procedures, which were described in Figure 2, could function as smart audit procedures on the blockchain. Moreover, two additional smart internal control tests could be designed to ensure that customers of the client maintain active digital wallets and have appropriate levels of access (e.g. access to send payment information but not to validate and post this information). For the risk that revenue transactions are not recorded in the correct period related to the cut-off assertion, additional audit procedures would not be necessary since, due to the inherent nature of blockchain technology, revenue is recorded at the same time the transaction occurs. Similarly, as reconciliations occur in near real-time by the auditee and its customer on the blockchain, ensuring the completeness of revenue transactions would also not be necessary. However, the three-way match that checks sales orders, sales invoices and shipping details can serve as a secondary test to verify cut-off and completeness. Finally, the evaluation of management revenue return estimates would be an audit procedure that remains off-the-blockchain. The smart audit procedures and off the blockchain audit procedures described within Table 2 are not all inclusive of a potential future hybrid audit approach. However instead, this table illustrates some of the significant risks and relevant audit procedures to describe the evolution of audit as audit clients and external auditors shift their business practices to the blockchain.

CONCLUSION

Limitations and Future Research

The external audit blockchain proposed in this paper was supported by smart audit procedures that leveraged the benefits of blockchain technology under the assumption that blockchain would be widely but selectively adopted by businesses. Overall adoption of blockchain technology would in turn generate a higher demand for audit services on the blockchain (Alles 2015).

However, the blockchain technology itself has limitations, in addition to some inherent issues with incorporating the technology into audit methodology. Those limitations include the computational power, storage capabilities, cybersecurity risk, litigation risk, vulnerability of smart contracts and regulatory acceptance of the use of blockchain.

To ensure the integrity of the data, many blockchains such as Bitcoin and Ethereum, rely on cryptographic mechanisms that demand significant computational power. Blockchain by design is not equipped to be more efficient than traditional centralized databases or to store substantial volumes of data, which is of paramount importance as the frequency of IoT data that is placed on the blockchain increases[23]. Novel methods for solving the problem of data storage on blockchain including "decentralized storage" [24] and "blockweave" [25] have been proposed. However, the effectiveness of these methods in solving the storage issue is yet to be determined. Therefore, there is a need for research to examine both the extent to which a private and permissioned blockchain is more beneficial than a traditional centralized database and whether blockchain technology could be utilized to store big data.

[23] IoT data on the blokchain. See: https://www.ibm.com/developerworks/cloud/library/cl-blockchain-for-cognitive-iot-apps-trs/cl-blockchain-for-cognitive-iot-apps-trs-pdf.pdf

[24] Decentralized storage combines the characteristics of blockchain with techniques of sharding and swarming to meet the demand for the storage of massive amounts of information. See: https://dataconomy.com/2018/01/blockchain-data-storage-decentralized-future/.

[25] Blockweave offers low-cost storage on the blockchain. See: https://www.forbes.com/sites/shermanlee/2018/06/08/blockchain-is-critical-to-the-future-of-data-storage-heres-why/#3a423bea33e9 .

Although the blockchain can be considered hack proof because it is a decentralized and immutable database, the risks of collusion and of private keys of digital wallets being stolen or lost emerge as cybersecurity threats. Collusion could occur when the majority of blockchain nodes control the blockchain network and retroactively alter transactions. In addition, blockchain users must be cognizant of securing access to the private keys of their digital wallets as they can be stolen or lost (Gruber 2013). Future research should be conducted to explore the effects of collusion among blockchain users and the possibility of stealing private keys.

Since the users of the financial statements are more informed about the audit from having read-only access to the results of the smart audit procedures, they will be able to more accurately align their expectations with the reality of what auditors actually do thereby reducing the expectation gap between auditors and the users of the financial statements. However, it still may be possible for auditor litigation risk to increase. Research is needed to explore whether auditors and audit firms may have increased exposure as a result of the increasing audit coverage, being a node on the client’s blockchain, and to determine the optimal balance between meeting financial statement users’ demands while maintaining an acceptable level of audit litigation risk. This research on liability and exposure should include exploring erroneous code in smart audit procedures that could lead to inappropriate assessments about the risk of material misstatement as auditors would be relying on the output that is produced by these procedures.

The audit profession is also currently experiencing a paradigm shift as a result of rapid technological advancements, and regulators and standard-setters are taking notice. Based on the drafts for comment that the IAASB and the PCAOB have issued with relation to revising or creating new audit standards that recommend the use of more sophisticated audit analytics (IAASB 2016; PCAOB 2018), there is uncertainty around how audit standards should be updated or changed. As a result, the automated execution of audit analytics on the blockchain could create an entirely new set of challenges to regulators and standard-setters. These challenges lead to the need for research that helps to illuminate exactly how the oversight model of financial statement audits be disrupted (including the effect on audit quality) and how smart audit procedures on blockchain should be regulated.

In their latest strategic plan, the PCAOB stated that they are open to exploring the use of technology to automate their processes (PCAOB 2018). This paper proposed novel functions for the PCAOB, which would offer inspectors the ability to leverage blockchain and smart contract technologies to improve their inspection process and potentially prevent future audit failures. However, the feasibility of incorporating the PCAOB's inspection process into a blockchain environment should be empirically validated.

Summary

As blockchain and smart contracts are rapidly evolving business practices, the potential of these emerging technologies in the external audit domain should not be neglected. This paper envisions the evolution of the financial statement audit paradigm by proposing an external audit blockchain supported by smart audit procedures in an attempt to foresee the benefits of this technology to auditing. The external audit blockchain benefits from the auditee's blockchain financial and nonfinancial information and has the potential to improve audit quality through the autonomous execution of audit procedures. Importantly, as smart audit procedures can autonomously disclose the results of audit procedures near real-time on the tamper-proof blockchain ledger, it is possible that these technologies could reduce the expectation gap between auditors, financial statement users and regulators (Rozario and Vasarhelyi 2018).

Although blockchain and smart audit procedures are important facilitators for evolving from a retroactive audit framework to a proactive audit framework to parallel a digital and near-the-event business environment, it is important to emphasize that the future audit framework is likely to comprise of on and off-the-blockchain audit procedures. Hence, while blockchain and smart audit procedures may radically evolve the way financial statement audits are performed and delivered, audit judgment is expected to remain a salient component of financial statement audits. Finally, while the benefits of blockchain and smart contracts to auditing were the primary focus of this paper, several issues and challenges to the adoption of these technologies, which lead to future research opportunities, were presented.

REFERENCES

Alles, M. G., Kogan, A., & Vasarhelyi, M. A. 2002. Feasibility and Economics of Continuous Assurance 1. In *Continuous Auditing: Theory and Application* (pp. 149-167). Emerald Publishing Limited.

Alles, M. G. 2015. Drivers of the use and facilitators and obstacles of the evolution of Big Data by the audit profession. *Accounting Horizons* 29 (2): 439-449.

American Institute of Certified Professional Accountants (AICPA). 2015. *Audit Analytics and Continuous Audit: Looking Toward the Future,* New York, NY

Appelbaum, D. 2016. Securing Big Data Provenance for Auditors: The Big Data Provenance Black Box as Reliable Evidence. *Journal of Emerging Technologies in Accounting, 13*(1), 17-36.

Bell, T., Marrs, F., Solomon, I., & Thomas, H. 1997. Auditing Organizations through a Strategic Lens: The KPMG business measurement process. *Montvale, NJ: KPMG Peat Marwick, LLP*.

Brown-Liburd, H., & Vasarhelyi, M. A. 2015. Big Data and audit evidence. *Journal of Emerging Technologies in Accounting*, *12*(1), 1-16.

Bryans, D. 2014. Bitcoin and money laundering: mining for an effective solution. *Ind. LJ*, *89*, 441.

Bumgarner, A., and Vasarhelyi, M. A. 2015. Continuous Auditing—A New View, Chapter 1 in AICPA, Audit Analytics and Continuous Audit: Looking Toward the Future, *American Institute Of Certified Public Accountants.* New York, NY 2015

Buterin, V. 2013. Ethereum white paper.

Chan, D. Y., & Vasarhelyi, M. A. 2011. Innovation and practice of continuous auditing. *International Journal of Accounting Information Systems*, *12*(2), 152-160.

Curtis, M. B., and E. A. Payne. 2008. An examination of contextual factors and individual characteristics affecting technology implementation decisions in auditing. International Journal of Accounting Information Systems 9(2): 104-121.

Dai, J., & Vasarhelyi, M. A. 2017. Towards Blockchain-based Accounting and Assurance. *Journal of Information Systems*.

Gockel, B., Acar, T., and Forster, M. 2018. Blockchain in Logistics. *DHL Trend Research.*

Gruber, S. 2013. Trust, Identity and Disclosure: Are Bitcoin Exchanges the Next Virtual Havens for Money Laundering and Tax Evasion. *Quinnipiac L. Rev.*, *32*, 135.

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

International Auditing and Assurance Standards Board (IAASB). 2016. Exploring the Growing Use of Technology in the Audit, with a Focus on Data Analytics. New York, NY: IFAC.

Kozlowski, S. 2016. A Vision of an ENHanced ANalytic Constituent Environment: ENHANCE. Doctoral dissertation, Rutgers, The State University of New Jersey.

Kuenkaikaew, S., & Vasarhelyi, M. A. 2013. The Predictive Audit Framework. *International Journal of Digital Accounting Research.* Vol. 13: 37-71.

Louwers, T. J., Ramsay, R. J., Sinason, D. H., Strawser, J. R., & Thibodeau, J. C. 2018. *Auditing and assurance services*. New York, NY: McGraw-Hill/Irwin.

Mainelli, M., & Smith, M. 2015. Sharing ledgers for sharing economies: an exploration of mutual distributed ledgers (aka blockchain technology). *The Journal of Financial Perspectives*, *3*(3), 38-69.

Moffit, K., Rozario, A. M., Vasarhelyi, M. A. 2018. Robotic Process Automation for Auditing. Forthcoming in "Journal of Emerging Technologies in Accounting".

Moore, J. 1996. The Death of Competition: Leadership & Strategy. *The Age of Business Ecosystems, HarperCollins, New York*.

Nakamoto, S. 2008. *Bitcoin: A peer-to-peer electronic cash system*. Working paper.

Nelson, K. M., Kogan, A., Srivastava, R. P., Vasarhelyi, M. A., & Lu, H. 2000. Virtual auditing agents: the EDGAR Agent challenge. Decision Support Systems, 28(3), 241-253.

No, W. G., & Vasarhelyi, M. A. 2017. Cybersecurity and Continuous Assurance. *Journal of Emerging Technologies in Accounting*, *14*(1), 1-12.

Peffers, K., Tuunanen, T., Rothenberger, M.A. and Chatterjee, S., 2007. A design science research methodology for information systems research. *Journal of management information systems*, *24*(3), pp.45-77.

Peters, G. W., and E. Panayi. 2015. Understanding Modern Banking Ledgers through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money. Working paper. Cornell University.

Pilkington, M. 2016. Blockchain Technology: Principles and Applications. Research Handbook on Digital Transformations, edited by F. Xavier Olleros and Majlinda Zhegu. Edward Elgar.

Pricewaterhousecoopers. (PwC). 2017. PwC Blockchain Validation Solution. Retrieved from: https://www.pwc.com/us/en/about-us/new-ventures/pwc-blockchain-validation-solution.html

Public Company Accounting Oversight Board (PCAOB). 2010. Audit Evidence. PCAOB Auditing Standard No. 1105. Washington, DC: PCAOB.

Public Company Accounting Oversight Board (PCAOB). 2016. Audit Expectations Gap: A Framework for Regulatory Analysis. Washington, D.C: PCAOB. Retrieved from: https://pcaobus.org/News/Speech/Pages/Franzel-speech-Institute-12-13-16.aspx

Public Company Accounting Oversight Board (PCAOB). 2017. The State of Audit Quality and Regulatory Approaches to Achieving High Quality Audits. Retrieved from: https://pcaobus.org/News/Speech/Pages/Franzel-state-audit-quality-regulatory-approaches-achieving-high-quality-audits-12-7-17.aspx

Rozario, A. M., & Vasarhelyi, M. A. 2018. Auditing with smart contracts. International Journal of Digital Accounting Research.

Sigvaldason, T., and Warren, J.D., 2004. *Solving the Software Architecture Riddle to Deliver Enterprise-wide Continuous Financial Process Monitoring and "Auditing."* Financial Market Solutions, LLC.

Singh, K. 2015. The New Wild West: Preventing Money Laundering in the Bitcoin Network. *Nw. J. Tech. & Intell. Prop.*, *13*, iii.

Szabo, N. 1994. Smart contracts. *Retrieved from: http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html*

Tapscott, D. and Tapscott, A. 2016. *Blockchain revolution*. 1st ed. New York: Portfolio-Penguin.

Titera, W. R. 2013. Updating audit standard—Enabling audit data analysis. *Journal of Information Systems*, *27*(1), 325-331.

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

Vasarhelyi, M. A., & Hoitash, R. 2005. Intelligent Software Agents In Accounting: an evolving scenario. *M. Vasarhelyi, A. Kogan (a cura di), The Evolving Paradigms of Artificial Intelligence and Expert Systems: An International View, 6*.

Vaziri, A. 2016. Smart BoL – Reducing Contractual Enforcement Costs. Retrieved from: https://www.chainofthings.com/news/2016/11/23/smart-bol-reducing-contractual-enforcement-costs

Yoon, K. 2016. “Big Data as Audit Evidence: Utilizing Weather Indicators.” Chapter 3 of the dissertation titled *Three Essays on Unorthodox Audit Evidence*, Rutgers University, Newark N.J.

Table 1: Challenges of Gathering Audit Evidence that are Mitigated by the Blockchain

Challenges	Blockchain Attributes	Blockchain Benefits
Traceable origins of sources (veracity)	Decentralization Immutability	Data Integrity to improve the **reliability of audit evidence**

	Accountability	
Disaggregated data sources (variety)	Decentralization	One distributed depository for financial and nonfinancial data to improve the accuracy and timeliness of audit procedures and provide deeper client insights

Figure 1: Smart audit procedure for sales (Adapted from Rozario and Vasarhelyi 2018)

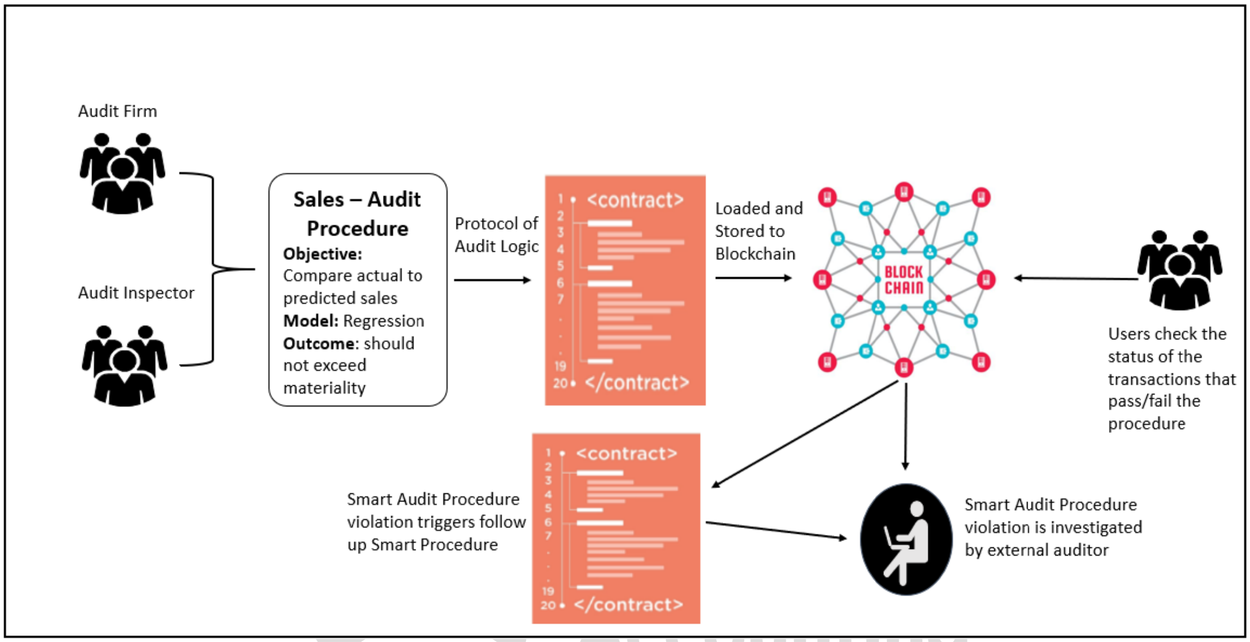

Audit Firm
Audit Inspector
Sales – Audit Procedure
Objective: Compare actual to predicted sales
Model: Regression
Outcome: should not exceed materiality
Protocol of Audit Logic
<contract>
</contract>
Loaded and Stored to Blockchain
BLOCK CHAIN
Users check the status of the transactions that pass/fail the procedure
Smart Audit Procedure violation triggers follow up Smart Procedure
Smart Audit Procedure violation is investigated by external auditor

Figure 2: Interlinked Blockchain Ecosystems

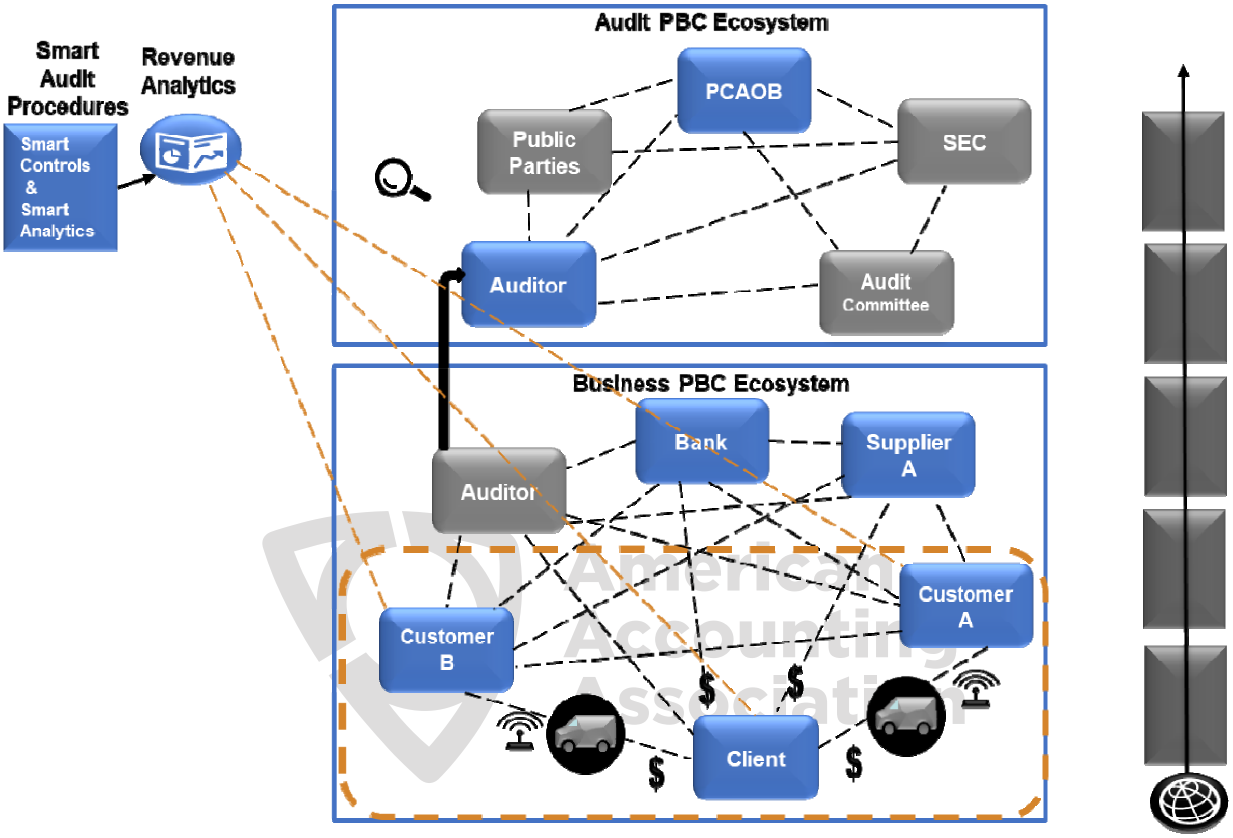


Figure 3: Blockchain Smart Audit Procedures for Revenue

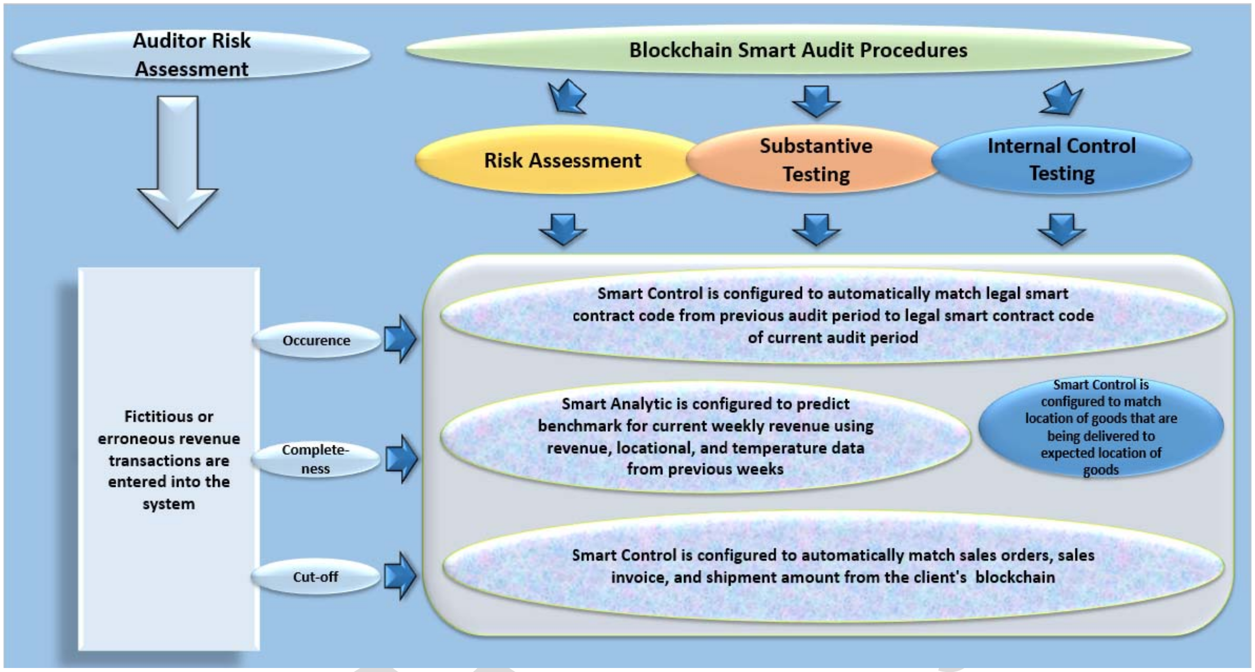
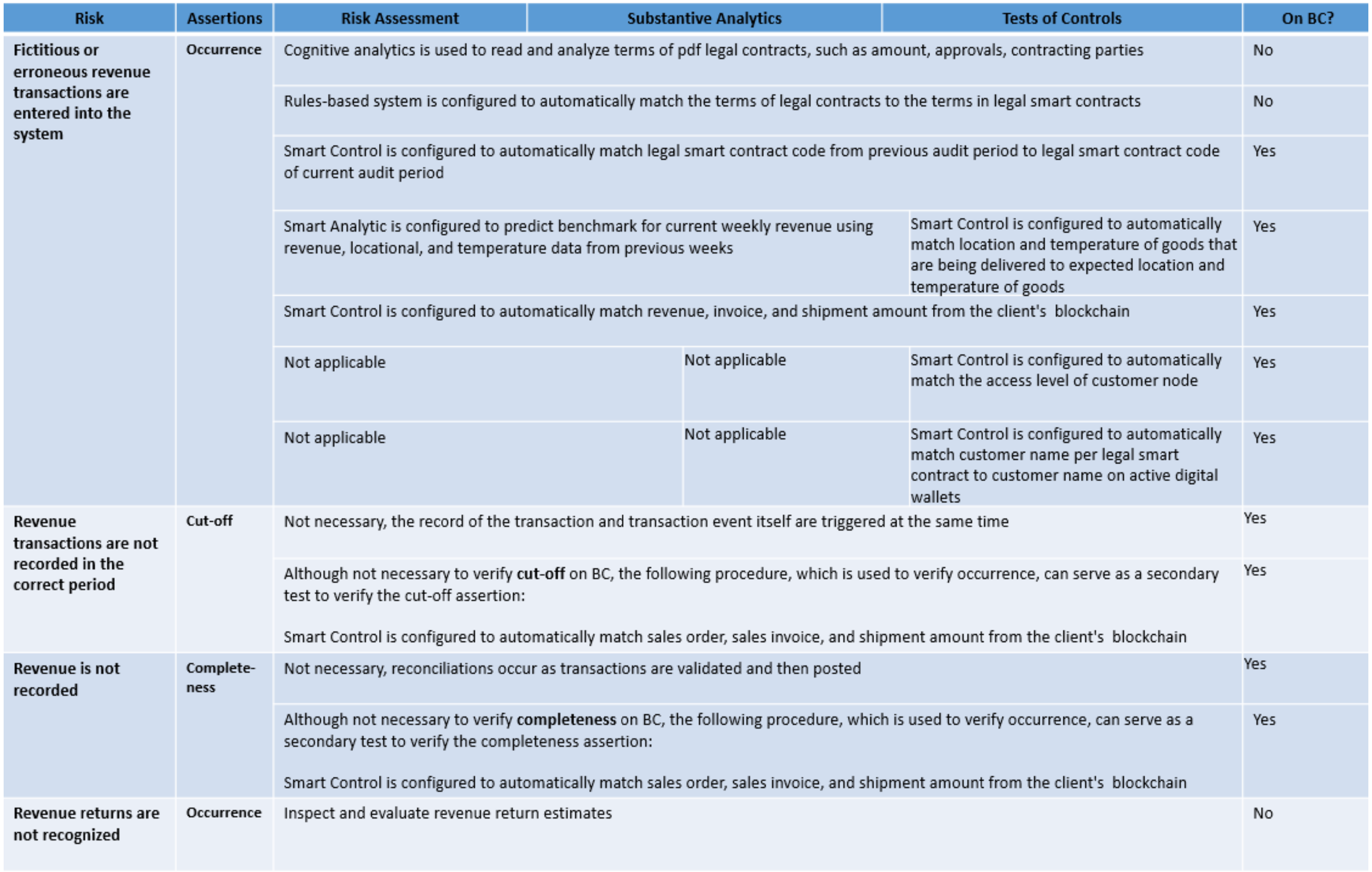

Auditor Risk Assessment
Blockchain Smart Audit Procedures
Risk Assessment
Substantive Testing
Internal Control Testing
Fictitious or erroneous revenue transactions are entered into the system
Occurence
Complete-ness
Cut-off
Smart Control is configured to automatically match legal smart contract code from previous audit period to legal smart contract code of current audit period
Smart Analytic is configured to predict benchmark for current weekly revenue using revenue, locational, and temperature data from previous weeks
Smart Control is configured to match location of goods that are being delivered to expected location of goods
Smart Control is configured to automatically match sales orders, sales invoice, and shipment amount from the client's blockchain

Table 2: Example of Holistic Audit Approach for Revenue Adapted and Modified from Louwers et al. 2018



Risk	Assertions	Risk Assessment	Substantive Analytics	Tests of Controls	On BC?
Fictitious or erroneous revenue transactions are entered into the system	**Occurrence**	Cognitive analytics is used to read and analyze terms of pdf legal contracts, such as amount, approvals, contracting parties			No
		Rules-based system is configured to automatically match the terms of legal contracts to the terms in legal smart contracts			No
		Smart Control is configured to automatically match legal smart contract code from previous audit period to legal smart contract code of current audit period			Yes
		Smart Analytic is configured to predict benchmark for current weekly revenue using revenue, locational, and temperature data from previous weeks		Smart Control is configured to automatically match location and temperature of goods that are being delivered to expected location and temperature of goods	Yes
		Smart Control is configured to automatically match revenue, invoice, and shipment amount from the client's blockchain			Yes
		Not applicable	Not applicable	Smart Control is configured to automatically match the access level of customer node	Yes
		Not applicable	Not applicable	Smart Control is configured to automatically match customer name per legal smart contract to customer name on active digital wallets	Yes
Revenue transactions are not recorded in the correct period	**Cut-off**	Not necessary, the record of the transaction and transaction event itself are triggered at the same time			Yes
		Although not necessary to verify **cut-off** on BC, the following procedure, which is used to verify occurrence, can serve as a secondary test to verify the cut-off assertion: Smart Control is configured to automatically match sales order, sales invoice, and shipment amount from the client's blockchain			Yes
Revenue is not recorded	**Complete-ness**	Not necessary, reconciliations occur as transactions are validated and then posted			Yes
		Although not necessary to verify **completeness** on BC, the following procedure, which is used to verify occurrence, can serve as a secondary test to verify the completeness assertion: Smart Control is configured to automatically match sales order, sales invoice, and shipment amount from the client's blockchain			Yes
Revenue returns are not recognized	**Occurrence**	Inspect and evaluate revenue return estimates			No