TİDE Academia Research
Sayı 3 / 103-140 (2021)

Research Article/ Araştırma Makalesi

THE EXTERNAL FINANCIAL STATEMENT AUDIT PROCESS AND BLOCKCHAIN TECHNOLOGY

Graham GAL[1]
Matthew SHERWOOD[2]

Submitted/Başvuru: 15.06.2021
Last Revised/Son Düzeltme: 29.07.2021
Accepted/Kabul: 30.07.2021

Abstract

This study examines the relationship between the financial statement audit process and blockchains. While clients' use of blockchain technology might provide some benefits to external auditors' substantive testing procedures, those benefits appear very limited, and an increase in controls testing effort is likely to offset any reduction in substantive audit effort. This is due to blockchain technology's inability to provide assurance regarding most of the financial statement assertions external auditors test. The study notes that many of the purported benefits of blockchain technology to the auditing profession, such as the ability to test a full set of transactions and the potential for real-time auditing, existed before the development of blockchain. Thus, while blockchain is likely to have some effect on the auditing profession, it is hard to say to what extent that impact might be.

Keywords: Blockchains, Independent Audit, Internal Controls

JEL Classification: M15, M42, 033

[1] Associate Professor Dr., Department of Accounting, Isenberg School of Management, University of Massachusetts, Amherst, MA 01003 USA gfgal@isenberg.umass.edu, ORCID ID:0000-0001-6526-9367

[2] Assistant Professor Dr., Department of Accounting Isenberg School of Management, University of Massachusetts, Amherst, MA 01003 USA msherwood@isenberg.umass.edu, ORCID ID:0000-0001-5856-5003

To cite this article: Gal, G., & Sherwood, M. (2021). The External Financial Statement Audit Process and Blockchain Technology. *TİDE AcademIA Research*, 3(1), 105-142

FİNANSAL TABLOLARIN BAĞIMSIZ DENETİM SÜRECİ VE BLOKZİNCİR TEKNOLOJİSİ

Öz

Bu çalışma finansal tabloların denetim prosedürü ile blokzincirler arasındaki ilişkiyi incelemektedir. Müşterilerin blokzincir teknolojileri dış denetçilerin maddi doğruluk testi yöntemlerine bazı faydalar sağlayabilirken bu faydalar çok sınırlı kalabilir ve iç kontrol testlerindeki artışla maddi doğruluk denetimlerindeki azalış dengelenebilir. Bunun sebebi, blokzincir teknolojisinin dış denetçilerin test ettiği mali tablo iddialarının çoğuna ilişkin güvence sağlayamamasıdır. Bu çalışma blok zinciri teknolojisinin denetim mesleğine sağladığı söylenen, tam bir işlem setini test etme yeteneği ve gerçek zamanlı denetim potansiyelinin bulunması gibi bazı faydalarının çoğunun blok zincirinin geliştirilmesinden önce de var olduğuna dikkat çekiyor. Bu bağlamda, blokzincirin denetim mesleği üzerinde bir miktar etkisinin olması ihtimal dahilinde olsa da bu etkinin ne ölçüde olabileceğini söylemek zor.

Anahtar kelimeler: Blokzincirler, Bağımsız Denetim, İç Kontroller

JEL Sınıflandırması: M15, M42, 033

1. Introduction

Advancements in technology have led to fundamental changes in the way businesses process their transactions, and report results. For instance, developments in computing hardware and software allow firms to capture and process increasingly large sets of transaction-level data, in relatively less time. While this makes it easier for management access and analyze the firm's transactions, the lack of a tangible record of each transaction makes its validation more difficult. Despite this challenge, the likelihood of organizations reverting to the use of more hard copy transactions is remote, which in turn makes the data quality assurance of firms' transactions, and subsequent performance disclosures, increasingly important and challenging. Obtaining an external financial statement audit, is one-way firms attempt to provide outsiders with assurance regarding the validity of their disclosed transactions. At the same time auditors also face challenges stemming from changes in technology. Auditors have to adjust their processes to account for the fact that clients' information can be captured and stored in multiple settings and locations, exist in multiple computer systems, be processed by software created by different vendors, and can be accessed by multiple users at multiple locations (Rittenberg & Schwieger, 2001). Further, to continue to be able to provide relevant assurance services, auditors need to adapt to how technology alters the way their clients conduct and record their business activities.

In addition to general complexity increases in clients' information systems, the audit process has been affected by regulatory change and advances in auditor-developed technologies. Section 404(b) of the Sarbanes Oxley Act requires financial statement auditors to assess their clients' internal control procedures, which are to create, process, allow access, and generally influence the quality of the data used in financial disclosures (United States Congress, 2002).[3] While audits always included some review of internal controls, Sarbanes-Oxley mandates auditor review and opine on the Internal Controls over Financial Reporting (ICFR) of their external audit clients. In 2002, the SEC issued rule changes to accelerate the filing of quarterly and annual reports, which resulted in an acceleration of the audit completion date. Auditors, in part, used new technologies to cope with the

[3] This increased recognition of the importance of reviewing financial reporting processes has also been shown in the review of cybersecurity (Steinbart, Raschke, Gal, & Dilla, 2016; 2018)

reduced audit timeline. These included advances in electronic working paper software, automating roll forward and leads sheet generation, expanded use of Computer Assisted Auditing Techniques (CAATs) and development of Continuous Controls Monitoring (CCM) systems.[4] Certainly, these technologies have significantly increased the reliability of the audit process (Rittenberg & Schwieger, 2001). However, auditors still face concerns about reviewing the quality of the increasingly large and complex sets of transaction-related data clients use to produce financial statements and disclosures. While clients' adoptions of some recent technologies, such as cloud computing, seem to make data quality assessment harder for the external auditor, enterprise blockchain platforms are being perceived by some as a solution to auditors' data quality assessment issues within financial reporting procedures.

Enterprise blockchain platform (EBP) technology has several unique qualities, some of which might be able to address certain data quality concerns companies face with regards to their financial reporting procedures. For instance, once a block of transactional data is added to the blockchain, users with access to the blockchain, can readily identify any alterations to its block's contents. The locking of data within a chain of blocks often referred to as an "immutable ledger," is a core aspect of all blockchain technologies, and ensures no subsequent changes to details including the transaction's values and date. While some of the properties of blockchains provide some assurance on certain measures of data quality there are other assertions made by management concerning their financial statements that could also me impacted by the use of blockchains. Thus, accounting and reporting concerns, such as ensuring the accuracy of a product's historical purchase price, or the period in which a transaction occurs, become known with certainty. The idea, that recording transactions using an EBP can result in an immutable ledger, has led to claims that inherent accounting assurances blockchain offers, will end the need for other external assurance mechanisms, such as independent financial statement audits. Certainly, features such as those described above and in the subsequent section, make EBP technology amenable to address specific accounting and reporting risks. However, are they a panacea that will solve

[4] While the suggestion to use software to continuously review transactions, or add in audit work is not new (Vasarhelyi & Halper, 1991) the use of CAATs and CCM within the external audit setting has become more prevalent (Kogan, Alles, Vasarhelyi, & Wu, 2014).

all accounting and reporting related assurance concerns and remove the need for external assurance of the financial statements? If not, what financial reporting procedures and external audit areas, might an EBP affect or not affect? The purpose of this manuscript is to address the changes that might ensue to the financial reporting process and to the auditing of financial statements as a result of the adoption of EBP. Specifically, the paper will. discuss the potential effects of EBP adoption on the quality of companies' transactional data, and accounting processes and how this might affect external auditors' procedures, and testing, with regards to their assessments of management's assertions over their financial statements.

The remainder of this paper is organized as follows. Section 2 looks at blockchains in more detail and discusses the characteristics, which could impact companies' data quality, accounting procedures, and financial statement preparation. Section 3 highlights the financial reporting process, describes management's assertions over the firm's financial statements, and briefly discusses typical external financial statement audit procedures. Section 4 presents a set of comprehensive examples that examine how adopting a distributed transaction repository EBP or a smart contract EBP might affect data quality and accounting procedures, as well as how each might affect how auditors validate managements' assertions. Section 5 discusses how EBPs might influence public accounting firms, and Section 6 presents a summary, conclusions, and implications.

2. Blockchain Technology

As the name implies, a blockchain is a series of information "blocks" that are connected. The chaining of the blocks creates a time sequence in which order is preserved in such a way as to make reordering of events difficult if not impossible. The core components of each block are a set of transactions sent by participants to the chain during a short period of time. While other types of transactions, such as smart contracts, are being considered for blockchains, at this time exchanges of cryptocurrencies predominate on blockchains.

Participates on the blockchain are assigned a key or wallet. Much like a traditional bank account, the wallet contains an amount of cryptocurrency exchanged on the particular blockchain. The wallet has a public key which is used to locate the wallet on the chain, and a private key which is the owner's link to the wallet. Depending on the type of blockchain the owner of the wallet may be anonymous.[5] Each participant can add or accept transactions sent to the chain, and after a transaction is included in a block each participant will get an updated copy of the entire set of blocks. For a transaction to be added to a block, it must be verified, and accepted by a simple majority (51%) of the chain's participants.[6] There are a couple of steps in the verification process, and the finalization of an exchange transaction. First, the user digitally signs the transaction, indicating the recipient's wallet id, includes an amount of coin that is to be exchanged on the particular chain, and an amount of the coin to run the transaction.[7] Different chains exchange different types of coin. It is envisaged that it would be easy to have exchange transactions across multiple chains, and therefore transactions which have multiple types of coins or resources. To accomplish these multiple resource exchanges, a number of issues need to be addresses (Back, et al., 2014). Wang & Kogan (2018) provide an example of the interaction of sidechains where different types of coins, representing different assets, are exchanged. The Accounting Blockchain Coalition (ABC) has also looked at different types of digital assets, including asset tokens which embody a claim against the issuer, utility tokens which allow the wallet holding them to access an application or service, payment tokens can be used to acquire goods or services, and hybrid tokens which have some characteristics of the others. These classifications are critical as different jurisdictions consider certain types of digital assets as securities while others do not (Accounting Blockchain Coalition Internal Controls Working Group, 2019). For example, the International Monetary Fund faces the problem of determining which digital assets, particularly if it is issued by a country, should be viewed as financial reserves (He, 2018). As a second step in the verification process, the exchange transaction is timestamped. This timestamping preserves the order of transactions. While timestamping of transaction is necessary to prevent double-spending, it is not sufficient. One potential threat to double spending is in fast payment implementations (Karame, Androulaki, Roeschlin, Gervais, & Capkun, 2012). Because final

[5] In permissionless blockchains the owners of wallets are usually anonymous while in permissioned blockchains the parties are usually known to other participants (Vukolić, 2017). However, even in permissioned blockchains there are techniques which can be used to reduce anonymity (Meiklejohn, et al., 2016; Ron & Shamir, 2013) .

[6] A blockchain is made up of nodes each of which contain a complete set of blocks. This ensures that no one node can alter either the order of the blocks or the information on transactions without the knowledge of all other participants.

[7] On the Ethereum blockchain the payment to run the transaction is called "gas".

verification occurs when the exchange transaction is added to a block on the blockchain, and this may not occur for a few minutes, it is possible to use a coin in two fast payment transactions, where multiple exchanges occur in that time frame; such as for a cup of coffee (Karame, Androulaki, & Capkun, 2012). Another potential threat to double spending attacks occurs when there is a fork in the blockchain; an alternative chain is introduced at a particular block (Wirachantika, Barmawi, & Wahyudi, 2019). While, not quite the same as a traditional double spending attack, a user can alter the order of exchanges as they appear on the blockchain, by attaching a higher processing fee to a transaction. This fee provides a financial incentive to the miners which will finalize the inclusion of a transaction in a block. Therefore, by attaching a higher fee to one transaction an owner of a wallet can cause one transaction to appear to have occurred prior to what was actually an earlier transaction. Because of scalability issues with bitcoin type blockchains, the delay in propagation of transactions to the other participants, can allow modification of the information (Gervais, Ritzdorf, Karame, & Capkun, 2015).

The process of creating an immutable block of transactions is done through "mining". Mining is the process of accepting a set of transaction into a block, and propagating this new block to all chain participants. The key to the immutability of both the blocks in the chain and to the information contained in each block is a set of hashes. Hashing algorithms are mathematical functions which take a string as input and produce a digital representation (Ali Orumiehchiha, Pieprzyk, & Steinfeld, 2012; Bellaire, Jaeger, & Len, 2017; Hamer, 2002; National Institute of Standards and Technology, 2015). There are many classifications of these algorithms, but they have two essential attributes (Chi & Zhu, 2017). First, the digital representation, the hash, should change if there are any changes to the input string. Second, there should be few if any collisions. The first attribute implies that a hash can provide evidence that a set of information, the string, has been altered. However, to actually find any change depends on the length of the string; a change in a six-word sentence would be easier to find than a change in a 6 trillion record database. The hash of a set of transactions in a block should detect a change in any of the characters which make up the contents of the block. The second attribute is a measure of the probability that two different strings will yield the same hash; their hashes collide. This attribute is similar to the first but has a slightly different implication. The first implies a quick test to see if a set of information, a string of any length, has changed. The second determines how easy it is to change the string and keep the same hash. Regardless of the hashing algorithm there is a non-zero probability of a collision; two different strings yield the same hash. For blockchain implementations, changing the original transaction's wallets to a different receiving or sending wallet that is sending the cryptocurrency would be a significant change. The probability of finding the exact alteration that could make such a change undetectable used to be quite remote. However, with the advent of quantum computers this is no longer a remote possibility (Bryanov, 2019).

For the bitcoin blockchain, the hash for a block is based on the content of the transactions included in the block, the date, and a number called a nonce (Cryptoticker, 2019). The transactions to be included in the block are hashed in a hierarchical tree structure called a Merkle Tree (Merkle, 1980; USA Patent No. US4309569, 1982). The top node of the tree contains a hash of the top branches, these branches contain the hash of the branches at the next level, and so on with the hash of individual transactions at the lowest level. The hash for a block on the bitcoin chain must meet certain structural constraints. Through the process of "mining" the hash of the Merkle Tree, and the other information in the block is converted into the block's hash. Each blockchain can choose a particular algorithm to arrive at a consensus on way in which this mining is to take place (Chi & Zhu, 2017; Tan, Hu, & Wang, 2019). In the bitcoin blockchain the information in each transaction (and so the hash at the top of the Merkle Tree) and the date are fixed, so to meet the constraints on the address or hash of the block the miner iterates through possible values for the nonce until a solution is reached. The miner that solves the problem of identifying a hash which satisfies bitcoin's Proof-of-Work (PoW) consensus requirement receives a set number of bitcoins in payment. It is estimated that in 2018 miners were required to iterate through 25.0 million tera hashes per second to solve bitcoin's PoW.[8] The required computing power to find a nonce has resulted in pools of miners that collaborate on the work provided (Sheehan, et al., 2017).

These requirements, to have an encrypted wallet, to create a hash of the information in

[8] A tera hash is 1x1012 hashes. Thus, to compete for bitcoin's mining prize requires the computing ability to iterate through 25x1012 hashes per second (Yang, 2018).

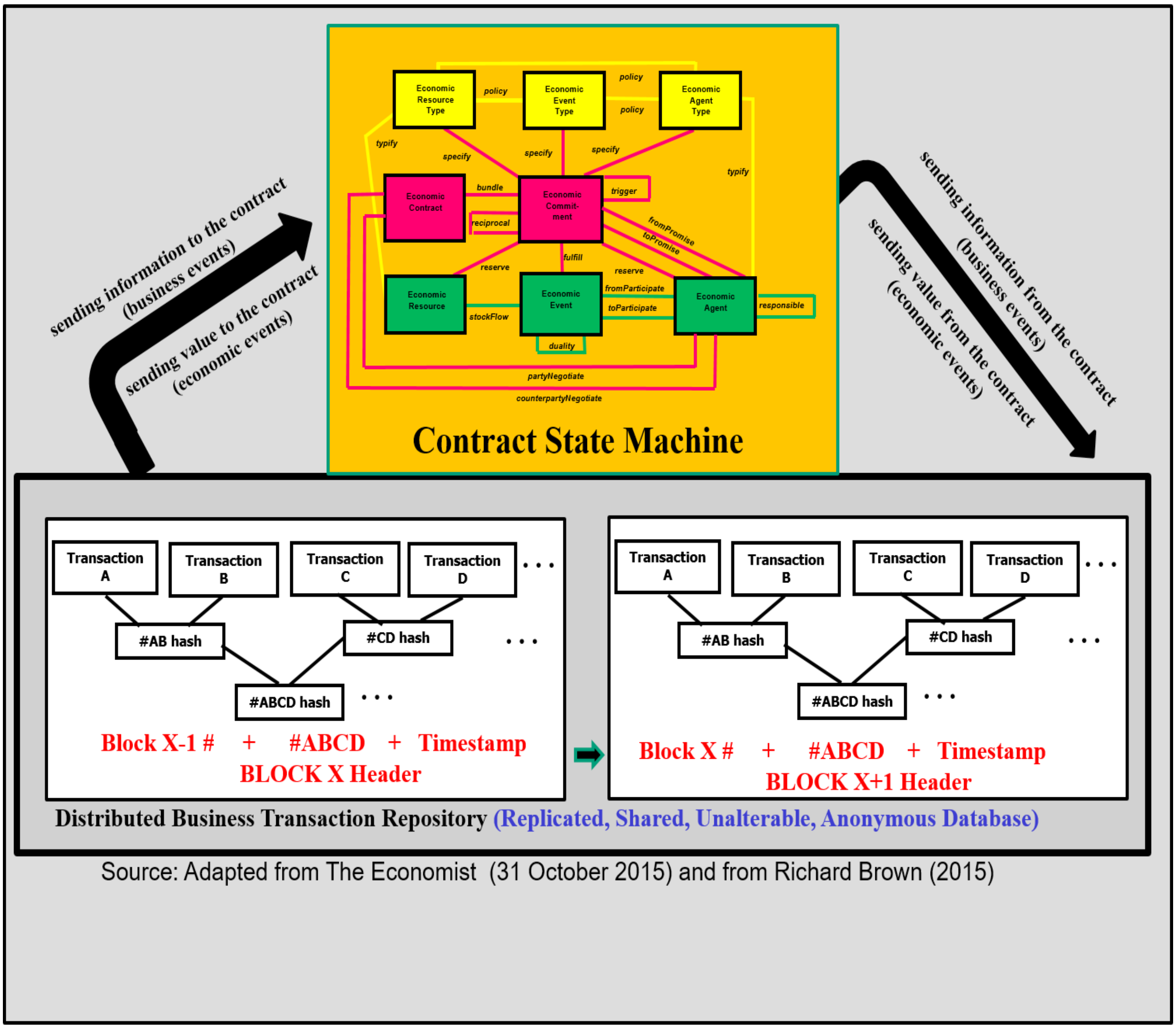
the block, and the mining supports a level of assurance on the integrity of the information in a specific block. The creation of links to previous blocks preserves the temporal order of blocks. So, the hashing of information in a block, and the linking of the blocks in a chain preserves both some level of assurance on the integrity and the potential to ascertain when transactions occurred. However, it is not necessary that the information on the blockchain is correct. First, even if a wallet sends an exchange transaction to the chain it is not verified immediately, and so there is a period of time between sending and confirming the exchange. This period may not be critical unless there is some need to use the results of an exchange in a subsequent exchange – the oil was received and the gas was produced and subsequently delivered. While some have argued that a ledger on the blockchain can include the accounting for both sides of the transaction (Dai & Vasarhelyi, 2017), there are some difficulties with this approach. The blockchain is a set of transactions in "Collaboration Space" (International Organization for Standardization and the International Electrotechnical Commission , 2007). The blockchain works because no single party determines what a particular exchange means; one parties cash receipt is another parties cash disbursement. In more complex transactions, forcing the blockchain to one party's view of the transaction, limits its applicability; one party's raw material is another party's finished good. In addition, if the exchange is for a particular cryptocurrency, it is difficult to determine whether the other side of the exchange has taken place. For instance, if an amount of cryptocurrency is sent to a wallet with the expectation of delivery of some other asset, such as inventory, the actual delivery is off-chain.[9] Therefore, for complete information in a supply chain it would be necessary to include access to off chain sensors (Hussain, 2017). To support audit of information on the blockchain, another issue that must be considered is the precise timing of the exchange.

The time used for blockchain exchanges is UnixEpoch time (Epoch Converter, 2019). This is based on seconds from a specified time (January 1, 1970 00:00:00) at Coordinated Universal Time.[10] As exchanges are mined into a block, the time of the block will be different than the time the transaction was executed and may also be different than the

[9] It has been suggested that the Internet of Things (IoT) can bring movement of all assets to the blockchain (Christidis & Devetsikiotis, 2016; Dai & Vasarhelyi, 2017). This move of transactions to "collaboration space" requires a different type of contract and a view of contracted resources as types and delivery as instances (McCarthy, Geerts, & Gal, 2021)

[10] In some countries this is referred to as Greenwich Mean Time.

time it was sent to the block. This difference could be small; however, there is a potential issue with the time. As blockchains deal with exchanges on a global scale the block's times can change some recognition issues. The time assigned to an exchange could differ from the time at the actual location of the exchange. This difference could potentially differ by a day, two minutes before midnight versus one minute after midnight, which could make a payment late according to the terms of a contract. Additionally, an exchange could also be mined in a different year which would change amounts in a firm's financial statement.



Source: Adapted from The Economist (31 October 2015) and from Richard Brown (2015)

Figure 1 A Distributed Business Transaction Repository State Machine

(Source The REA Ontology, McCarthy, Geerts, and Gal 2021)

While smart contracts (Luu, Chu, Olickel, Saxena, & Hobor, 2016) are not currently a pervasive part of blockchains they certainly are part of its future. A smart contract is computer code containing statements which look for actions which meet conditions of an agreed upon exchange. The processes which complete these actions are off chain and in most cases are the result of firm's business processes.[11] Figure 1 depicts the relationship between a firm's information system and blockchains. Figure 1 shows a representation of the REA classes and associations (McCarthy, Geerts, & Gal, 2021) that are related to data in the chain's blocks. When smart contracts are designed, there is a relationship to states in the firm's information system. The economic events are those that are mined into the blocks while contracts are based on type images and indicate a control structure within the firm. For instance, before authorizing transfer a cryptocurrency payment, the state "received merchandise" must occur. Therefore, the firm's information system must recognize the state, and send a message to the smart contract that the state has been completed. So, controls in the organization must include both a determination of state changes, and authorization for the transfer messaging. The mechanics of state machines can enforce the requisite controls over the states in the organization to execute a smart contract (Haugen, 2002; Horiuchi & McCarthy, 2011; Horiuchi & Shimizu, 2016). However, other organizational controls are necessary to ensure the proper execution of the business events which result in the addition of exchanges to the blockchain (Accounting Blockchain Coalition Internal Controls Working Group, 2019).

This section has examined some of the features of blockchains that can ensure the integrity of the information; once mined into the blockchain it cannot be easily changed. However, blockchains cannot provide complete assurance of the veracity of the data; information on the chain indicates that inventory was delivered, but this does not mean that inventory was of the correct quantity and quality. Therefore, an audit over the financial information contained in the chain is necessary to provide reasonable assurance of the financial statements. The next section examines the audit process as it relates to the blockchain.

[11] There are some events which become part of smart contract conditions, such as a date at which payment must be received or the contract becomes void.

3. The Financial Reporting Process and Blockchain

3.1Financial Statement Preparation

The previous section presented some of the important issues that must be considered when a company uses blockchains to perform exchanges of resources. While blockchains can ensure that the data has not been altered, it cannot ensure that the data matches the information concerning the exchange of resources not actually contained in the chain. This section looks at financial reporting and audits of this information when blockchains keep some of the company's information.

Figure 2 presents a high-level overview of the general financial reporting process that firms use to generate the financial statements regulators, investors, and other outside stakeholders require. In the most basic of terms, the financial reporting process consists of three steps. First, the firm engages in and records business transactions. The firm groups and summarized like-kind business transactions, netting the inflows and outflows within balances against one another. Finally, assigning the net transaction amounts to financial statement lines. To allow for comparability of financial statements among firms, financial statement line items are consolidated and presented based on regulatory guidelines.[12] Firms then close their books for the period, and the process begins anew.

[12] In the United States the financial reporting guidelines are established by the Financial Accounting Standards Board. Financial reporting in other countries is regulated by the International Accounting Standards Board.

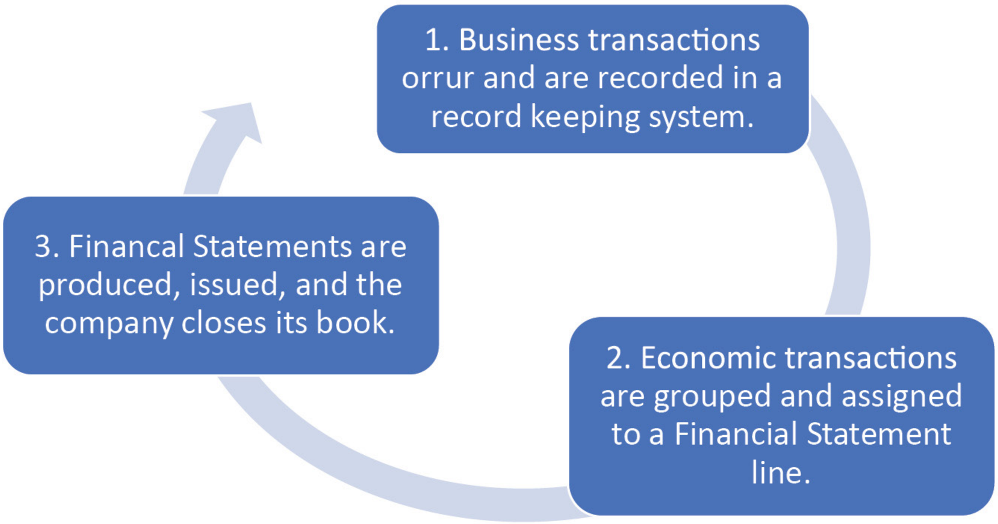

1. Business transactions orrur and are recorded in a record keeping system.
2. Economic transactions are grouped and assigned to a Financial Statement line.
3. Financal Statements are produced, issued, and the company closes its book.

Figure 2 The Financial Reporting Process

The Financial Reporting Process	
1.	Business transactions occur during the firm's normal course operations. They include things such as acquiring raw materials, producing a service or product, making sales, paying employees, and paying taxes, just to name a few. Companies typically record transactions in their order of occurrence (i.e., chronologically) in their company database. Economic transactions are then recorded as journal entries. Each entry debits at least one account and credits at least one account. The journal entries are transferred from their cycle-specific sub-ledgers to the general ledger. The journal entries are sorted based on the account receiving the debt or the credit.
2.	The general ledger accounts are summed to produce a listing of each account's balance, known as the trial balance. The firm records any necessary adjusting entries, which are summed with the trial balance, to create an adjusted trial balance. The adjusted trial balance accounts are assigned to a financial statement line item based on the firm's chart of accounts.
3.	The financial statement produced and made available to management and to shareholders. The company then closes its books for the fiscal year and begins the process anew in the subsequent fiscal year.

A nuanced description of the financial reporting process is beyond the scope of this manuscript. However, a few specific details about the typical financial reporting process will aid our subsequent discussion. First, firms can, and do, use a variety of technologies, ranging from simple spreadsheets to complex Enterprise Resource Planning systems (ERP), to record business transactions. Second, when business transactions are captured they are assigned a unique identifier – a primary key, and then when they are converted to accounting records they are assigned a unique journal entry number. The journal entry number is essential as it allows users of the accounting system (e.g., firm employees and the external auditors), to identify the specific components of each economic transaction or event. Many aspects of an external financial statement audit rely on transaction-level data. However, while regulators govern the presentation of financial statements and disclosures, there are no regulations on internal record-keeping methodologies. Thus, there is no basis for comparison of data across companies at the transaction-level.

Blockchain technologies seem the most poised to impact the creation and recording of transactions steps in the financial reporting process that. As discussed in the prior section, blockchain technology is conceptually broad, and its role still somewhat undefined. However, there are currently two technologies within the enterprise blockchain space that are at the forefront; smart contracts, and disturbed transaction repositories.[13] While both use the same basic blockchain concepts, and there is some overlap between them, their primary focuses differ. A detailed discussion of similarities and differences of these technologies, as well as the companies, platforms, features, and programming languages used to develop specific blockchain technologies, is beyond the scope of this paper.[14] However, it is necessary to touch upon both of these technologies as their role within the financial statement audit process will be examined in the following section of this paper.

One of the many players in the smart contract space is Ethereum, which is an open-source distributed public blockchain network.[15] It allows for the building of decentralized appli-

[13] Blockchains have sometimes been referred to as distributed transaction repository, however, a better term is the distributed transaction repository as this indicates a record of transactions as opposed to a record of accounting entries (International Organization for Standardization and the International Electrotechnical Commission, 2019)

[14] For more information on these topics as well as academic articles regarding these topics please see: Dai, J., & Vasarhelyi, M. A. (2017).

[15] Other smart contract firms include EOS, Cardano, and RSK..

cations (DAPP), which can incorporate smart contract functionality. One such example of a smart contract DAPP built on Ethereum is Quorum, which was developed by J.P. Morgan. Quorum allows for high speed and high throughput processing of private transactions among a group of known, and allowed participants; this is an example of a permissioned blockchain. A noted advantage of Quorum is the use of partial state databases, which creates a network that is partly public and partly private. When the conditions trigger the execution of a contract, the transaction recorded within the blockchain will be hashed and available to anyone with permission to view the block. However, the specific details of the transactions will be encrypted and visible only to users who receive a decryption key from the transaction manager.

In the distributed transaction repository space several companies are working with the Linux Foundation's opensource Hyperledger project.[16] Hyperledger is neither a tool nor a platform like Ethereum, but rather an umbrella strategy with multiple platforms for developing enterprise solutions. Whereas the focus of smart contracts, at least for the moment, is primarily on financial and insurance industries, Hyperledger's focus is on allowing firms to personalize blockchains to address the specific needs of their firm. Hyperledger blockchains are private and permissioned networks that can allow for smart contract transactions (known as chain code) to occur. Channels within Hyperledeger, provide a private a subnet of communication and allow transactions between premised members, that are accessible only to permissioned network members.

The ultimate role that blockchain technology might play in the financial reporting process is still unknown. However, based on the current iteration of the technology, it appears that the most significant role is likely to be on recording and storing transactions. At its core, the current blockchain technology is a shared data warehouse, the contents of which are verifiable by any member with access to the chain. The fact that multiple members of a chain have a copy of the transactional history makes it difficult, if not impossible, for firms or individuals to change or alter past transactions without the other members of the chain knowing. Distributed transaction repositories' potential to generate immutable records of

[16] Key member firms of Hyperledege include IBM, SAP, Intel, Oracle, and Microsoft. For a full list of Hyperledge members see https://www.hyperledger.org/members.

transactions will create a single shared record of transactions. Under traditional systems both parties would create a record of an exchange transaction, but under a distributed transaction repository only one record is needed. Therefore, each party has a record of the transaction that can be used in the production of their financial statements. Smart contracts can reduce human intervention in the recognition of the terms of exchanges. Together these technologies will likely influence not only the production of financial statements, but also the process of providing financial statement assurance.

4. Independent Financial Statements Assurance

4.1. Financial Statement Audit Process

The term audit refers to inspection or examination performed by someone other than the preparer or performer. More specific to this setting Rittenberg and Schweiger's (2001, p. 13), definition of an audit as a, "…systematic process of objectively obtaining and evaluating evidence regarding assertions about economic actions and events …" Accounting standards, such as US GAAP and IFRS, represent the established criteria to which auditors are to compare the financial statements. While the framework issued by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) (2013), provides the criteria for testing the internal controls over financial reporting (ICFR).

The external auditor is typically engaged to assess three aspects of the auditee's financial reporting process. First, did the auditee follow the accounting standards when recording their business activities? Subsequent to the passage of the Sarbanes-Oxley legislation (United States Congress, 2002) a second assessment includes an evaluation of the effectiveness of ICFR. Third, are the amounts reported within the auditee's financial statements materially correct? During an audit, the external audit team performs procedures to obtain evidence allowing them to form an opinion on the reasonableness of the auditee's claim that the financial statements are materially accurate and ICFR are effective.[17] The auditor then issues a report expressing their opinion on the financial statements and effectiveness of the ICFR. Figure 3 presents a summarized overview of the financial statement auditing process.

[17] While their discussion in detail is beyond the scope of this paper, two keys aspects of a financial statement audit are independence, and materiality. Generally, independence in this setting means, not both not having a financial interest in an audit client, as well as maintaining an appearance of independence from the client's management. Materiality refers to the fact that auditors are to provide "reasonable" not "absolute" assurance regarding the accuracy of the financial statements.

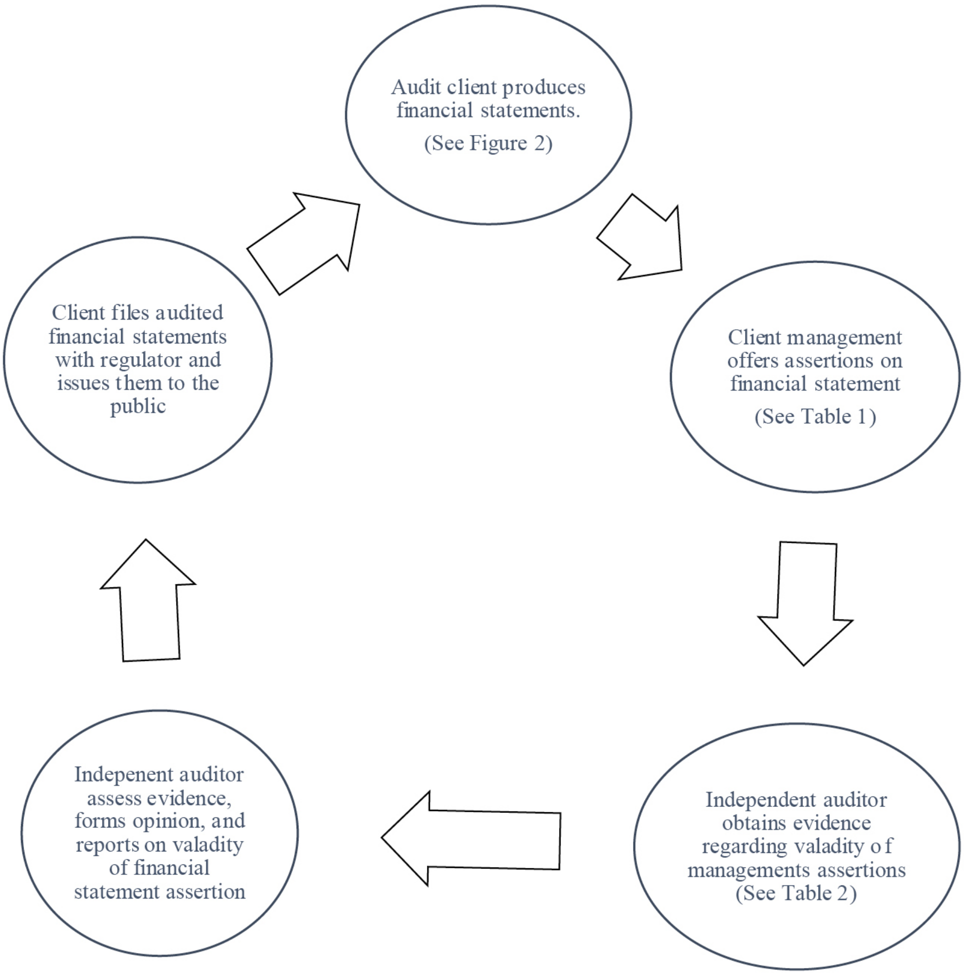

Audit client produces financial statements.
(See Figure 2)
Client management offers assertions on financial statement
(See Table 1)
Independent auditor obtains evidence regarding valadity of managements assertions
(See Table 2)
Indepenent auditor assess evidence, forms opinion, and reports on valadity of financial statement assertion
Client files audited financial statements with regulator and issues them to the public

Figure 3 Life Cycle of a Financial Statement Audit

Note: The above diagram outlines the general lifecycle of the annual financial statement audit. The process begins with the client engaging in and recording business activities. The business activities are summarized to form the client's financial statements. The client makes assertions about the financial statements, and the external auditor performs audit tests to obtain evidence regarding the validity of those assertions. Based on the results of the audit tests, the external auditor forms an opinion about the degree to which the financial statements conform to reporting standards (e.g., U.S. GAAP, IFRS, or any local standards) and issue an audit report presenting the auditor's opinion. The client includes the auditor's report when filing their financial statements with the appropriate regulatory body.

Note:
process

The use of blockchains can impact this process in a few ways. First, some of the events which are related to the financial statements may now be executed by smart contracts. Thus, the code actually plays a role in recording of economic transactions. This means that the auditor must have a way to inspect the smart contract's code, to have assurance that the terms of the contract are appropriate, and then perform relevant tests to verify the contract executes (and creates the requisite transactions) as designed. As some of the firm's assets are contained in a blockchain wallet, the auditor must confirm that controls over the access to the wallet are sufficient (Accounting Blockchain Coalition Internal Controls Working Group, 2019).

4.2 Management Assertions

When a company issues financial statements, its management explicitly or implicitly makes assertions (i.e., claims) regarding the financial statement's adherence to accounting standards, the operating effectiveness of the ICFR, and the accuracy of the values reported. It is the auditor's job to perform procedures so they can assess the validity of management's assertions. In many ways, management's assertions are technology agnostic, as it does not matter if the firm records its transactions using paper and pencil, a spreadsheet, or an ERP. Regardless of the mechanism by which firms store their transactional data, they must process and present the data following reporting criteria. While a client's choice in technology might influence the tools an auditor uses to assess the validity of management's assertions, the technology cannot replace the need to perform the procedures. Table 1, presents management's assertions as defined by both the PCAOB and the AICPA.[18]

[18] As this manuscript focuses on the external financial statement audits required by the SEC for publicly traded firms our discussion centers on the PCAOB's defined management assertions. However, due to the significant similarities between PCABO and AICPA assertions, the conclusion drawn can be applied to both sets of assertions.

Table 1 Management's Financial Statement Assertions

Panel A: PCAOB Financial Statement Assertions - per Auditing Standard 1105.11

- *Existence* or *occurrence*—Assets or liabilities of the company exist at a given date, and recorded transactions have occurred during a given period.
- *Completeness*—All transactions and accounts that should be presented in the financial statements are so included.
- *Valuation* or *allocation*—Asset, liability, equity, revenue, and expense components have been included in the financial statements at appropriate amounts.
- *Rights* and o*bligations*—The company, holds or controls rights to the assets, and liabilities are obligations of the company at a given date.
- *Presentation* and *disclosure*—The components of the financial statements are properly classified, described, and disclosed.

Panel B: AICPA Financial Statement Assertions - per AU §326.15

Note: This table presents management's assertions regarding the company's financial statements as defined by the PCAOB and the AICPA. Please see https://pcaobus.org/Standards/Auditing/Pages/default.aspx and https://www.aicpa.org/research/standards/auditattest/sas.html, for the complete set of PCAOB and AICPA auditing standards, respectively.

Certainly, the state of enterprise blockchain technology within the financial reporting and financial statement auditing arenas is not very mature. Firms can choose among the various enterprise blockchain technologies to pursue, and to what degree they want to incorporate that technology into their financial reporting process. Different levels of implementation and adoption of differing blockchain technologies will impact the way in which transaction data is capture and maintained by the firm's information system. However, as noted above, smart contracts and distributed transaction repositories are currently at the forefront of enterprise blockchain solutions. Within the realm of those two blockchain technologies, the aspects of the financial reporting process whose change is likely to be affected the most are the quality and storage of clients' data and the clients' accounting processes. Despite the level of implementation of these technologies, auditors still have a set of evidence gathering procedures as outlined in Table 2. These procedures are technology independent and therefore it is critical to consider how blockchains might impact evidence gathering. As a result, in the following pages, we provide a set of comprehensive examples that examine the potential impact on the external audit of changes to clients' data quality and accounting procedures in relation to clients' adopting distributed transaction repositories, or smart contract blockchain technologies.

Table 2 Audit Evidence Gathering Procedures per PCAOB AS 1105

AS 1105 paragraph	**Evidence Type**	**Description**
.15	*Inspection*	Inspection involves examining records or documents, whether internal or external, in paper form, electronic form, or other media, or physically examining an asset. Inspection of records and documents provides audit evidence of varying degrees of reliability, depending on their nature and source and, in the case of internal records and documents, on the effectiveness of the controls over their production. An example of inspection used as a test of controls is inspecting records for evidence of authorization.
.16	*Observation*	Observation consists of looking at a process or procedure being performed by others, e.g., the auditor's observation of inventory counting by the company's personnel or the performance of control activities. Observation can provide audit evidence about the performance of a process or procedure, but the evidence is limited to the point in time at which the observation takes place and also is limited by the fact that the act of being observed may affect how the process or procedure is performed.

.17	*Inquiry*	Inquiry consists of seeking information from knowledgeable persons in financial or nonfinancial roles within the company or outside the company. Inquiry may be performed throughout the audit in addition to other audit procedures. Inquiries may range from formal written inquiries to informal oral inquiries. Evaluating responses to inquiries is an integral part of the inquiry process. Note: Inquiry of company personnel, by itself, does not provide sufficient audit evidence to reduce audit risk to an appropriately low level for a relevant assertion or to support a conclusion about the effectiveness of a control.
.18	*Confirmation*	A confirmation response represents a particular form of audit evidence obtained by the auditor from a third party in accordance with PCAOB standards.
.19	*Recalculation*	Recalculation consists of checking the mathematical accuracy of documents or records. Recalculation may be performed manually or electronically.
.21	*Analytical Procedures*	Analytical procedures consist of evaluations of financial information made by a study of plausible relationships among both financial and nonfinancial data. Analytical procedures also encompass the investigation of significant differences from expected amounts.

Note: The table describes specific audit procedures per AS 1105 of the PCAOB's auditing standards. The purpose of an audit procedure can be a risk assessment procedure, a test of controls, or a substantive procedure.

third column outlines why the enterprise blockchain technology (a distributed transaction repository in Table 3, a smart contract in Table 4) might provide validity to the financial statement assertion(s). The fourth column outlines why the enterprise blockchain technology (a distributed transaction repository in Table 3, a smart contract in Table 4), might not provide validity to the financial statement assertion(s). The final column presents what, if anything, the procedure from Table 2 auditor might consider doing to gain sufficient validation of management's particular financial statement assertion(s).

For the sake of simplicity, we provide a short description of the assertion here. However, we refrain from reporting the fictious financial statement values, or how blockchain technology might or might not validate the assertion, as well as from describing what additional procedures the auditor might perform, as that information is contained below within Tables 3 and 4.

As shown in the first column, the first set of assertions shown in each panel of Tables 3 and 4 is that of existence or occurrence. The existence assertion, is primarily applicable to balance sheet line items, and relates to whether the assets or liabilities claimed by the company, via its financial statements, exist as of the financial statement date. Occurrence is the counter-part of existence and deals with the validity that the recorded transactions included in the financial statements, truly represent the events that occurred during a given period and is primarily applicable to the income statement. For exchanges captured in DTR the information about the exchange is immutable, it cannot be changed, and therefore there is a high level of assurance in the occurrence of the transaction. For transactions coded in smart contracts, there is also a high level of assurance on the existence of exchanges. Thus, both block chain technologies provide a high level of assurance on the existence or occurrence assertation.

The second row of the first column of both panels of Tables 3 and 4 contains the completeness management assertion. The completeness assertion addresses whether all of the transactions that should be included and represented within the financial statements are, and that only the transactions which should be include have been. Both technologies, distributed transaction repository and smart contracts, provide assurance for this assertion. However, the auditor would need to verify the controls over DTR while with smart contracts the auditor would need to reconcile the transaction activity.

The third row of the first column of both panels of Tables 3 and 4 contains the rights and obligations financial statement assertion within our example. This assertion indicates that the company holds or controls the rights to the assets and is responsible for the liabilities and other obligations, as indicated on the financial statement, as of the financial statement date. With each of these technologies the information is cannot be changed without a significant effort, which probably cannot occur in a timely fashion. Therefore, each of the technologies provides a high level of assurance that this assertion is supported.

The fourth row of the first column of both panels of Tables 3 and 4 contains the management assertions of valuation or allocation. This assertion relates to whether the financial statements report asset, liability, equity, revenue, and expense components at their appropriate amounts. This might include the recording of valuation adjustments to present assets at their fair or net realizable values. This assertion is problematic for each of the technologies. In each case there are actions which are outside of the blockchain that have a significant impact on valuation. For example, if a transaction represents an exchange with an outside supplier for inventory, with the result in a payable, the auditor must still perform additional procedures to verify that the inventory was received and that it has the appropriate value. This implies that blockchain technologies do not replace the need to observe physical inventories.

The fifth and final row of the first column of both panels of Tables 3 and 4 contains the management assertion of presentation and disclosure. As the term suggests, this assertion relates to whether the components of the financial statements are correctly classified, described, and disclosed. It also includes making sure that the financial statements include all of the required disclosures and the accompanying footnotes. Unfortunately, neither of the blockchain technologies can be relied upon for proper presentation. An auditor must rely on other controls to ensure that information is presented correctly.

Table 3 Panel A

Fun Toys, Inc. Example

Enterprise Blockchain Technology Type: Distributed transaction repository Financial Reporting Process: *Data Quality*

Assertion	***Fun Toys, Inc.***	***How might an Enterprise Blockchain Distributed transaction repository validate the assertion?***	***How might a Distributed transaction repository not validate the assertion?***	***What additional procedures might the auditor consider?***
Existence or Occurrence	The financial statements (F/S) of Fun Toys indicate an inventory balance of $5.42 million, and costs of sales of $27.1 million.	The use of a Distributed transaction repository Enterprise Blockchain Platform (DTR-EBP), allows both Fun Toys and their business partners to record the shared activity once. This results in a verifiable, third-party record the auditor might rely upon regarding the occurrence of transactions. Presuming that Fun Toys would not pay for items not received, the ledger also verifies that at one point, the inventory purchased did exist.	While the use of a DTR-EBP can provide assurance around transaction occurrence, it cannot assure that assets physically exist as of the F/S date. Thus, despite the DTR-EBP indicating the acquisition of real assets (e.g., inventory), it does not provide validation that those assets continue to exist. Also, the DTR-EBP can only provide assurance regarding the transaction recorded using it. Any activity that Fun Toys records outside of the DTR-EBP will receive no assurance.	The auditor will need to perform audit procedures (e.g., physical inspection) to ensure the assets, which Fun Toys claims are real, and still in their position, are, in fact, real and still in their position. The auditor will also need to perform audit procedures on any activity that Fun Toys records outside of the DTR-EBP.
Completeness	The F/S of Fun Toys indicate a cash and equivalents balance of $5.97 million and an advertising expense of $5.24 million.	If Fun Toys records all of their activity using a DTR-EBP, the auditor can verify each transaction and the date of its occurrence. If the auditor can reconcile the net transaction activity per Fun Toys DTR-EBP with the balances per the F/S, the auditor can determine if only the transactions, as well as all of the transactions occurring within the fiscal period, are reported, in the F/S.	Even if the transactions per the DTR-EBP are reconciled to the F/S, the auditor will need to determine if all of the transactions that should be reflected in the F/S are. Otherwise, the auditor runs the risk of Fun Toys engaging in activity outside of the DTR-EBP and failing to consolidate it with the activity per the DTR-EBP.	The use of a DTR-EBP allows for a reduction in human intervention. However, the auditors will need to reconcile the balances per the DTR-EBP with the F/S and perform audit procedures on reconciling items. The auditor will also need to test for transactions that should be included in the F/S but are not.

Table 3 Panel A Continued

Assertion	***Fun Toys, Inc.***	***How might an Enterprise Blockchain Distributed transaction repository validate the assertion?***	***How might a Distributed transaction repository not validate the assertion?***	***What additional procedures might the auditor consider?***
Rights and Obligations	The F/S of Fun Toys, indicate the company's accounts receivable balance is $9.7 million and accounting payable balance is $4.22 million.	Fun Toys can track their exchanges of goods using a DTR-EBP. Given the distributed nature, both Fun Toys and their business partners record the transaction separately, resulting in a verifiable, third-party record, the auditor might rely upon regarding the rights of ownership and obligation, as the parties provide validation of the transactions with one another. Fun Toys can be either a buyer or seller, depending on the transaction. Thus, if all of Fun Toys purchases or sales occur via a DTR-EBP the auditor can verify, summarize, and compare all of the DTR_EBP balances, to the balances per the F/S.	Fun Toys will not be able to conduct all of its sales and purchases via a DTR-EBP. As a result, Fun Toys will need to maintain a separate set of records to account for sales and purchases occurring outside the DTR-EBP, which it will need to summary and use it to reconcile the DTR-EBP balances with the F/S. Obviously, the DTR_EBP will not provide the auditor assurance with regards to the transactions recorded outside of the DTR-EBP.	The auditor will need to obtain details of the transactions occurring outside of the DTR-EBP and will need to perform sufficient audit procedures and gather evidence, as to the rights and obligations pertaining to this activity. The auditor will also need to reconcile the combined DTR-EBP and non-DTR-EBP activity with the F/S and perform audit procedures over the reconciling activity.

Table 3 Panel A Continued

Valuation or Allocation	The F/S of Fun Toys, indicate the company's accounts receivable balance is $9.7 million and accounting payable balance is $4.22 million.	Similar to the rights and obligation assertion, if a DTR-EPB is used, then the known transaction values can be obtained via the multi-party immutable ledgers, which can lend validity to the amounts per the F/S.	Similar to rights and obligations, it is unlikely all transactions will occur via a DTR-EBP. Unlikely rights and obligations, valuation and allocation, include significant management estimates, of items such as the allowance for doubtful accounts, and fixed asset depreciation It is unclear how management would record estimates via a DTR-EBP. Further, as these entries only affect Fun Toys there will be no third-parties to validate the DTR-EBP.	As Fun Toys is the only affected party, it is unlikely that the adjusting transactions would be recorded using a DTR-EBP. Thus, to test these assertions, the auditor will need to perform significant procedures to determine if management's assumptions are reasonable. The auditor will also need to perform audit procedures around any transactions recorded outside of the DTR-EBP.
Presentation and Disclosure	Management asserts the F/S and disclosures comply with US-GAAP.	The use of a DTR-EBP might allow the auditor to confirm the accuracy of the values within the F/S.	The use of a DTR-EBP will not provide any comfort on if the F/S comply with US-GAAP.	The auditor will need to review the F/S and test any deviations between reporting requirements and how the F/S are presented.

Panel B

Enterprise Blockchain Technology Type: Distributed transaction repository

The aspect of the Financial Reporting Process: Accounting Procedures

Assertion	***How an Enterprise Blockchain Distributed transaction repository might not validate the assertion?***	***What additional procedures might the auditor consider?***
Existence or Occurrence	Despite Fun Toys' ability to auto-order and make and receive payments via a DTR-EBP, their auditor will still need to perform validation testing to ensure that the items Fun Toys paid for were the actual items that were received. Further, the auditor will need to review the relevant policies to understand and test which transactions should be occurring within the DTR-EBP.	After understanding which transactions, the DTR-EBP should be processing, the auditor needs to test both the DTR-EPB controls and its activity. The controls testing is to ensure that authorized activity is occurring. The activity testing is to assess if accounting policies are being followed.
Completeness	While the use of a DTR-EBP might be able to ensure that all of the transactions within the DTR-EBP are represented in the F/S, it cannot ensure that Fun Toys has engaged in all required transactions. Thus, the auditor will need to ensure that any required transactions have taken place within the proper period.	The auditor of Fun Toys will need to review and be familiar with all relevant accounting and regulatory policies. The auditor will then need to review the transactions of Fun Toys either within or outside of the DTR-EBP to ensure that all necessary transactions, have occurred.

Table 3 Panel B Continued

Assertion		***What additional procedures might the auditor consider?***
Rights and Obligations		The auditor will need to test the details of all transactions occurring outside the DTR-EBP to ensure they are accurately reflected within the F/S. The auditor will also need to test if the DTR-EBP activity is in accordance with Fun Toys accounting policies
Valuation or Allocation		The auditor will need to gain a detailed understanding of key valuation policies (e.g., allowance for bad debts, fixed asset depreciation). The auditor will need to test the activity around these items, to ensure accounting policies are being followed.
Presentation and Disclosure		The auditor will need to test the F/S to ensure reporting requirements are being followed.

Table 4 Panel A

Enterprise Blockchain Technology Type: *Smart Contracts*

Mass-York Bank Corp. *Example*

Assertion	***Mass-York Bank Corp.***	***How an Enterprise Blockchain Smart Contract might validate the assertion?***	***How an Enterprise Blockchain Smart Contract might not validate the assertion?***	***What additional procedures might the auditor consider?***
Existence or Occurrence	The Mass-York financial statements (F/S) claim that as of the end of the fiscal year, the institution has cash holdings of $573 million and engaged in hedge position swaps resulting in revenue of $181 million.	The use of a decentralized application (DAPP) built on an enterprise blockchain platform (EBP) will allow the auditor to track and confirm the value of transactions conducted with a third party also using the DAPP. This will create an immutable ledger based on these transactions and will provide the auditor comfort over the occurrences of the transactions, and the existence of account balances equal to the transactions net ending balance.	The auditors will only be able to obtain comfort on these assertions with regards to the transactions, and the net ending account balances, that are recorded using the smart contract EBP.	At a minimum, the auditor will need to reconcile the transaction activity and the net ending balances per the EBP and the F/S to ensure that the balances and activity per the F/S agree to the activity recorded via the EBP. The auditor will need to thoroughly investigate and test any differences between the F/S and the EBP, as well as activity occurring outside of the EBP.
Completeness	The Mass-York F/S indicate general operating expenses of $3.24 million.	If Mass-York records all transactional activity using a smart contract EBP, the auditor can use the beginning account balances, the net activity, and the ending accounting balances to verify that all expected transactions have been recorded.	Even if the auditor is able to confirm that all the transactions recorded in the F/S should have been, EBP is unable to provide validation to the auditor that all transactions which should have been recorded within the EBP, actually were recorded.	The auditor will need to test any activity recorded outside of the EBP. Further, the auditor will need to perform audit procedures to look for and examine any activity that should have been included within the F/S and was not.

Table 4 Panel A Continued

Assertion	***Mass-York Bank***	***How an Enterprise Blockchain Smart Contract might validate the assertion?***	***How an Enterprise Blockchain Smart Contract might not validate the assertion?***	***What additional procedures might the auditor consider?***
Rights and Obligations	The F/S of Mass-York indicate the company's mortgage receivable balance is $179 million, and the long-term debt payable balance of $526 million.	Mass-York can track their exchanges of goods using an EBP. Given DAPP's nature, both parties in the transaction, can record the transaction separately, which can lend validity to rights of ownership after the exchange. Mass-York can be either the buyer or seller, Thus, if all of Mass-York's activities occur via EBP, the auditor could verify Mass-York's EBP activity, summarize it, and reconcile it to the F/S.	It is unlikely that Mass-York will have the ability to conduct all of its activity via a smart contract EBP. As a result, Mass-York will need to maintain a separate set of records that account for the activity that occurs outside of the EBP. Obviously, the EBP will not be able to provide any support to the validity of the transactions or net account balances of the activity recorded outside of the EBP.	The auditor will need to obtain the details of all activity that occurs outside of the EBP. The auditor will need to reconcile the balances and activity per the EBP with the F/S, using the activity recorded outside of the system. The auditor will then need to perform sufficient audit procedures to gather evidence as to the rights and obligations pertaining to the reconciling activity.
Valuation or Allocation	The F/S of Mass-York indicate the company's mortgage receivable balance is $179 million, and the long-term debt payable balance of $526 million.	Similar to the rights and obligation assertion, if Mass-York uses a smart contract EBP, then the known transaction values can be obtained, and the immutable ledgers can lend validity to the amounts per the F/S.	It is unlikely all activity will occur via a EBP. Thus, activity outside of the EBP will not be validated by a trading partner. Additionally, valuation and allocation include management estimates, for items such as the realizable value. It is unclear to what extend management would record estimates via an EBP, as estimates are internal operational decisions.	The auditor will need to obtain the summarized EBP values and reconcile them to the F/S. These reconciling items are likely to include both activities occurring outside of the EBP and internal estimates. The auditor will then need to test the assertions on the activity and internal estimates.
Presentation and Disclosure	Management asserts the F/S and disclosures comply with US-GAAP.	The use of an EBP might allow the auditor to confirm the accuracy of the values within the F/S.	The use of an EBP will not provide comfort as to if the F/S presentation and disclosures comply with US-GAAP.	The auditor will need to test the F/S to ensure reporting requirements are being followed.

Panel B
Enterprise Blockchain Technology Type: *Smart Contracts*
The aspect of the Financial Reporting Process: *Accounting Procedures*

Assertion	***Mass-York Bank Corp.***	***How an Enterprise Blockchain Smart Contract might validate the assertion?***	***How an Enterprise Blockchain Smart Contract might not validate the assertion?***	***What additional procedures might the auditor consider?***
Existence or Occurrence	The financial statements (F/S) of Mass-York claim that as of the end of the fiscal year, the institution has cash holdings of $573 million and engaged in hedge position swaps resulting in revenue of $181 million.	The use of a decentralized application (DAPP) built on an enterprise blockchain platform (EBP) will allow the auditor to investigate the consistency with which the transactions conducted with a third party are recorded. The immutable ledger based on the multi-party transactions and will provide the auditor comfort that transaction did occur and are not fictitious entries.	The auditor will only be able to obtain comfort with the validity of these assertions with regards to the transactions, and the net ending account balances, that are recorded using the smart contract EBP. For example, if the accounting policy calls for an activity to occur automatically when a condition is met, the smart contract EBP does not provide evidence that a sale occurred every time that the condition is met.	At a minimum, the auditor will need to reconcile each EBP with the appropriate Mass-York accounting policy. The auditor will need to review and then investigate, any differences between the operation of the EBP and company policy.
Completeness	The Mass-York F/S indicate general operating expenses of $3.24 million.	If Mass-York records all transactional activity using a smart contract EBP, the auditor will be able to validate the volume and dates of occurrence of the transactions.	While the smart contract EBP will provide details such as the date of the transactional activity, it will not provide evidence with regards to if the smart contracts execute transactions in-line with the associated accounting policies or regulatory guidance.	At a minimum, the auditor will need to reconcile each EBP with the appropriate Mass-York accounting policy. The auditor will also need to ensure that any changes made to the EBP are done so in a time manner to ensure all transactions are occur in line with company expectations.

Table 4 Panel B Continued

Assertion	*Mass-York Bank Corp.*	*How an Enterprise Blockchain Smart Contract might validate the assertion?*	*How an Enterprise Blockchain Smart Contract might not validate the assertion?*	*What additional procedures might the auditor consider?*
Rights and Obligations	The F/S of Mass-York indicate the company's mortgage receivable balance is $179 million, and the long-term debt payable balance of $526 million.	If Mass-York tracks their exchanges of goods using smart contracts within an EBP, the auditor will be able to validate the ownership rights and performance obligations of the transactions recorded via the smart contract EBP.	While the smart contract EBP will provide details of the transactions recorded within it, the EBP will not provide evidence with regards to if the firm continues to retain the rights and the obligations that have been recorded within the smart contract EBP.	The auditor will need to reconcile each EBP with the appropriate Mass-York accounting policy. The auditor will want to ensure that the smart contracts are performing as expected, and in accordance with Mass-York's policies. The auditor will also need to test the design of new or revised EBPs.
Valuation or Allocation	The F/S of Mass-York indicate the company's mortgage receivable balance is $179 million, and the long-term debt payable balance of $526 million.	The use of a smart contract EBP by Mass-York will provide validation of the historical costs of their transactions. The fact that the other party within each transaction has agreed to the terms of the transaction and recorded them via the immutable ledger, validates the value of the transactions.	Simply because the other party agrees with the price or allows the transaction to occur does not ensure that the internal policies of Mass-York are being followed. As a result, the auditor will be unable to determine if internal policies are being followed, as well as if Mass-York is complying with regulatory policies.	At a minimum, the auditor will need to reconcile each EBPs with the appropriate Mass-York accounting policy. The auditor will need to test if the smart contracts follow Mass-York's accounting policies. The auditor will need to thoroughly review and test any differences between how the EBP is operating, and the accounting policies.
Presentation and Disclosure	Management asserts that the presentation of the F/S and disclosures comply with US-GAAP.	The use of an EBP might allow the auditor to confirm the accuracy of the values within the F/S.	The use of an EBP will not provide comfort as to if the F/S presentation and disclosures comply with US-GAAP.	The auditor will need to test the F/S to ensure reporting requirements are being followed.

6. Conclusion

Since its introduction in 2008, the concept of blockchain technology has undergone rapid advances. This has led to an expansion of the technology from the world of crypto-currencies into mainstream applications, such as smart contracts and distributed transaction repositories. While the processing of data via blockchain technology is typically automated, the quality and accuracy of the recorded transactions remain limited to the accuracy and correctness of the transaction parameters established within the blockchain source code. The use of blockchain technology might reduce the potential for error due to human intervention during the processing phase of the accounting cycle. However, this reduction in risk will be offset by an increase in the risk of error within the transaction processing source code of any blockchain tool.

The identification of this transfer of risk is important, as it highlights the continued necessity for external assurance of firms' financial reports even within the realm of blockchain-based accounting systems. While the recording of activity via a blockchain might occur outside the control of the management, the ability to provide accurate and reliable data to external stakeholders is reliant on the processes and procedures put in place by management. Thus, while the adoption of blockchain might alter the manner in which an independent accountant obtains assurance over a client's financial statements, it does not reduce or remove the need of an external assurance provider.

By using both a distributed transaction repository and smart control example, this manuscript presents the potential relation between blockchain technology and the external audit process. In particular, it examines the following three questions. How might an Enterprise Blockchain Distributed transaction repository validate the assertion? How might a Distributed transaction repository not validate the assertion? What additional procedures might the auditor consider? This manuscript presents the relationship between management assertation concerning information contained in financial statements and the implications that the use of blockchains have on these assertations. This manuscript differs from studies on the effects of blockchain on accounting and auditing as it does not co-mingle blockchain with other emerging technologies, nor does it present a prototype of how the technology might be applied within a new accounting ecosystem. Rather this manuscript strips away other new technologies to focus solely on the potential relation between blockchain technologies and the external audit of the financial statements by an independent accountant.

Author Contribution

The authors have equal contribution to the paper.

Conflict of Interest

There is no conflict of interest among the authors.

Financial Support

The authors have not received any financial support for this study.

Peer-Review

Externally peer-reviewed

References

Accounting Blockchain Coalition Internal Controls Working Group. (2019). Digital token classification and definitions. New York: Accounting Blockchain Coalition.

Accounting Blockchain Coalition Internal Controls Working Group. (2019). Possible threats and vulnerabilities of assets related to digital assets and blockchain transactions and possible internal control activities and actions to address them. New York: Accounting Blockchain Coalition.

Ali Orumiehchiha, M., Pieprzyk, J., & Steinfeld, R. (2012). Cryptanalysis of RC4-Based hash function. Proceedings of the Tenth Australasian Information Security Conference (pp. 33-38). Melbourne, VIC: Association for Computing Machinery.

Back, A., Corallo, M., Dashjr, L., Friedenbach, M., Maxwell, G., Miller, A., Wuille, P. (2014, October 22). Enabling blockchain innovations with pegged sidechains. Retrieved from https://blockstream.com/sidechains.pdf

Bellaire, M., Jaeger, J., & Len, J. (2017). Better than advertised: Improved collision-resistance guarantees for md-based hash functions. ACM SIGSAC Conference on Computer and Communications Security, (pp. 891-906). Dallas, TX.

Bryanov, K. (2019, June 30). Quantum computing vs. blockchain: Impact on cryptography. Retrieved from CoinTelegraph - The Future of Money: https://cointelegraph.com/news/quantum-computing-vs-blockchain-impact-on-cryptography

Chi, L., & Zhu, X. (2017). Hashing techniques: A survey and taxonomy. ACM Computing Surveys, 50(1), 11:1-11:36.

Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the internet of things. IEEE Access, 4, 2292 - 2303.

Committee of Sponsoring Organizations of the Treadway Commission. (2013). COSO internal control - integrated framework: Internal control over external financial reporting. NY: COSO.

Cryptoticker. (2019, April 8). What is the blockchain data structure? Retrieved from Cryptoticker: https://cryptoticker.io/en/blockchain-data-structure/

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

Epoch Converter. (2019, April 8). EpochConverter. Retrieved from https://www.epochconverter.com/

Gervais, A., Ritzdorf, H., Karame, G. O., & Capkun, S. (2015). Tampering with the delivery of blocks and transactions in bitcoin. Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security (pp. 692-705). Denver: Association for Computing Machinery.

Hamer, J. (2002). Hashing revisited. Proceedings of the 7th Annual Conference on Innovation and Technology in Computer Science Education (pp. 80-83). Aarhus, DK: Association for Computing Machinery.

Haugen, R. (2002). The commitment oriented orchestration layer -- managing your business commitments. UN/CEFACT Quarterly Meeting. Seattle, WA.

He, D. (2018). Monetary policy in the digital age. Finance & Development, 55(2). Retrieved from International Monetary Fund.

Horiuchi, S., & McCarthy, W. E. (2011). An ontology-based state machine for catalog orders. Value Modeling and Business Ontologies Workshop. Ghent, BE.

Horiuchi, S., & Shimizu, X. (2016). Rethinking the development of a business process state machine. Shogaku Ronsan, 593-657.

Hussain, F. (2017). Internet of things: Building blocks and business models. Springer International Publishing.

International Organization for Standardization and the International Electrotechnical Commission . (2007). ISO/IEC 15944-4 - Information technology - business operational view - part 4: business transaction scenarios - accounting and economic ontology. Geneva, CH: International Standards Organization.

International Organization for Standardization and the International Electrotechnical Commission. (2019). ISO/IEC 15944-21 Information technology - business operational view - part 21: guidance on the application of the open-edi business transaction ontology in distributed business transaction repositories (committee specification working draft). Geneva, CH: International Standards Organization.

Karame, G. O., Androulaki, E., & Capkun, S. (2012). Double-spending fast payments in bitcoin. ACM conference on Computer and Communications Security (pp. 906-). Raleigh: Association of Computing Machinery.

Karame, G. O., Androulaki, E., Roeschlin, M., Gervais, A., & Capkun, S. (2012). Misbehavior in bitcoin: A study of double-spending. ACM Transactions on Information and System Security, 18(1), 2:1-2:32.

Kogan, A., Alles, M. G., Vasarhelyi, M. A., & Wu, J. (2014). Design and evaluation of a continuous data level auditing system. Auditing: A Journal of Practice & Theory, 33(4), 221-245.

Luu, L., Chu, D.-H., Olickel, H., Saxena, P., & Hobor, A. (2016). Making Smart contracts smarter. Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (pp. 254-269). Vienna: Association for Computing Machinery.

McCarthy, W. E., Geerts, G. L., & Gal, G. (2021). The REA ontology. Sarasota: American Accounting Association.

Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G. M., & Savage, S. (2016). A fistful of bitcoins: characterizing payments among men with no names. Communications of the ACM, 59(4), 86-93.

Merkle, R. C. (1980). Protocols for public key cryptosystems. IEEE Symposium on Security and Privacy (pp. 132-145). Oakland, CA USA: IEEE.

Merkle, R. C. (1982). USA Patent No. US4309569.

National Institute of Standards and Technology. (2015). FIPS PUB 180-4 Secure hash standard (SHS). Gaithersburg, MD: National Institute of Standards and Technology.

Rittenberg, L. E., & Schwieger, B. (2001). Auditing concepts for a changing environment (Third ed.). New York: Harcourt, Inc.

Ron, D., & Shamir, A. (2013). Quantitative analysis of the full bitcoin transaction. International Conference on Financial Cryptography and Data Security (pp. 6-24). Okinawa: Springer.

Sheehan, D., Gleasure, R., Feller, J., O'Reilly, P., Li, S., & Cristiforo, J. (2017). Does miner pooling impact bitcoin's ability to stay decentralized? Proceedings of the 13th International Symposium on Open Collaboration. Galway,IR: Association for Computing Machinery.

Tan, D., Hu, J., & Wang, J. (2019). VBBFT-Raft: An understandable blockchain consensus protocol with high performance. 7th International Conference on Computer Science and Network Technology (pp. 111-115). Dalian: IEEE.

United States Congress. (2002). Sarbanes-Oxley act. Washington, DC: United States Congress.

Vasarhelyi, M. A., & Halper, F. B. (1991). The continuous audit of online systems. Auditing: A Journal of Practice & Theory, 10(1), 110-125.

Vukolić, M. (2017). Rethinking permissioned blockchains. Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts (pp. 3-7). New York: Association for Computing Machinery.

Wang, Y., & Kogan, A. (2018). Designing confidentiality-preserving blockchain-based transaction processing systems. International Journal of Accounting Information Systems, 30, 1-18.

Wirachantika, W., Barmawi, A. M., & Wahyudi, B. A. (2019). Strengthening fawkescoin against double spending attack using merkle tree. Proceedings of the 3rd International Conference on Cryptography, Security and Privacy (pp. 49-54). Kuala Lumpor: Association for Computing Machinery.

Yang, S. (2018, February 21). The rise of bitcoin factories: Mining for the masses. Wall Street Journal.