JOURNAL OF INFORMATION SYSTEMS
Vol. 31, No. 3
Fall 2017
pp. 5–21

American Accounting Association
DOI: 10.2308/isys-51804

Toward Blockchain-Based Accounting and Assurance

Jun Dai
Rutgers, The State University of New Jersey, Newark
Southwestern University of Finance and Economics

Miklos A. Vasarhelyi
Rutgers, The State University of New Jersey, Newark

ABSTRACT: Since 2009, blockchain has served as a potentially transformative information technology expected to be as revolutionary as the Internet. Originally developed as a methodology to record cryptocurrency transactions, blockchain's functionality has evolved into a large number of applications, such as banking, financial markets, insurance, voting systems, leasing contracts, and government service. Despite such advancements, the application of blockchain to accounting and assurance remains under-explored. This paper aims to provide an initial discussion on how blockchain could enable a real-time, verifiable, and transparent accounting ecosystem. Additionally, blockchain has the potential to transform current auditing practices, resulting in a more precise and timely automatic assurance system.

Keywords: blockchain; smart contract; future accounting; future assurance.

I. INTRODUCTION

Blockchain is one of the most important and innovative technologies developed in recent years (Peters and Panayi 2016; Pilkington 2016; PricewaterhouseCoopers [PwC] 2015; Swan 2015a). Originally used for Bitcoin[1] trading, blockchain establishes a decentralized public ledger that provides a secure infrastructure for transactions among unfamiliar parties without a central authority. This technology is meant to reduce trading costs, increase transaction settlement speed, reduce fraud risk, improve the auditability of transactions, and increase the effectiveness of monitoring (Swan 2015a; Fanning and Centers 2016; Pilkington 2016; Yermack 2017). Blockchain is evolving from a secure monetary transaction system into part of an ecosystem of emerging technologies that includes artificial intelligence, the Internet of Things (IoT), robotics, and crowdsourcing. These technologies together represent the technical foundation of future commerce (Omohundro 2014; Deloitte 2016; Dorri, Kanhere, and Jurdak 2016; Ferrer 2016). Blockchain is obtaining increased attention from the accounting profession. PwC, for example, views blockchain as the "next-generation business process improvement software to structurally alter shared practices between customers, competitors, and suppliers" (PwC 2016). Similarly, Deloitte (2016) expects that blockchain will improve collaboration among businesses and individuals, the transparency of business processes and data, and, ultimately, the productivity and sustainability of the economy.

Recently, blockchain has broadened its technical foundation to support various businesses, such as banking, trading, insurance, data protection, voting, intellectual property, identity authentication, leasing, and government service[2] (Atzori 2015; Cointelegraph 2015; De Meijer 2016; Liebenau and Elaluf-Calderwood 2016; Peters and Panayi 2016; Swan 2015a; Trautman 2016; *Wall Street Journal* [*WSJ*] 2015; Yermack 2017; Zyskind, Nathan, and Pentland 2015). Accounting and assurance could be among the professions to which blockchain would bring great benefits and fundamentally change the current paradigms. Blockchain's functions of protecting data integrity, instant sharing of necessary information, as well as programmable and

We thank J. P. Krahel, Jamie Feiman, Glen Gray, Terry Campbell, two anonymous reviewers, and the participants from the 2nd *Journal of Information Systems* Conference for their helpful comments and suggestions.

Editor's note: Accepted by Robin R. Pennington.

Submitted: May 2016
Accepted: May 2017
Published Online: June 2017

[1] Bitcoin is the most widely used cryptocurrency.
[2] Sample applications include NASDAQ's use of blockchain in private market trading (*WSJ* 2015) and Citibank's creation of three blockchains and issuance of an internal cryptocurrency, the "Citicoin" (Cointelegraph 2015).

automatic controls of processes, could facilitate the development of a new accounting ecosystem. This technology could also serve as a foundation to enable automatic assurance and help the current auditing paradigm become more agile and precise.

However, the potential benefits and challenges that blockchain could bring to the accounting and assurance domains are still under-explored. This paper aims to fill the gap in the literature, and to generate insights for both practitioners and regulators on the acceptance and use of the emerging technology. Specifically, this paper first proposes a blockchain-enabled, real-time, verifiable, and transparent accounting ecosystem. In the ecosystem, blockchain would play the role of the accounting information system, which distributes the power of transaction verification, storage, and management to a group of computers in order to prevent any unauthorized data changes. By incorporating other emerging technologies (e.g., IoT), the system could enable real-time tracking and monitoring of activities of physical objects, and automate the recording and measurement of business performance. This mechanism would facilitate close to real-time reporting of reliable accounting information to interested parties (e.g., managers, auditors, creditors, stakeholders) at various aggregation levels based on their roles and demands. Blockchain is also proposed in this paper as a tool to authenticate any audit-related information. Since blockchain secures the data that are posted on it, auditors could trust the integrity of those data and perform various analyses. Moreover, automatic and agile assurance could be further enabled by "smart controls," which are computer programs that would operate on blockchain to automatically control business processes against pre-determined rules. Since the original design of blockchain is to enable peer-to-peer digital currency trading, how to adapt the existing blockchain mechanisms to the accounting and auditing sphere is worth careful thought.

The main contributions of this paper are threefold. First, it is among the first few studies to introduce blockchain to the accounting and auditing literature. Second, it explores the potential applications and utilization of this technology in the accounting and auditing profession. The discussions and illustrations provide insights to auditors, regulators, and technology vendors, to facilitate the incorporation of blockchain into the existing business procedures, as well as promote the transformation of the current audit model toward the next generation. Third, it provides a discussion on the challenges in the adoption and use of those technologies, as well as potential solutions that could mitigate those concerns.

The remainder of this paper proceeds as follows: Section II provides the background of blockchain, and compares the characteristics of blockchain with existing data management technologies such as database and enterprise resource planning (ERP) systems. Section III illustrates the potential applications of blockchain in re-conceiving corporate accounting. Section IV discusses the utilization of blockchain technology to enable an efficient, effective, and timely assurance system. The challenges facing blockchain adoption and implementation, as well as potential research directions, are discussed in Section V. Section VI concludes and discusses the limitations.

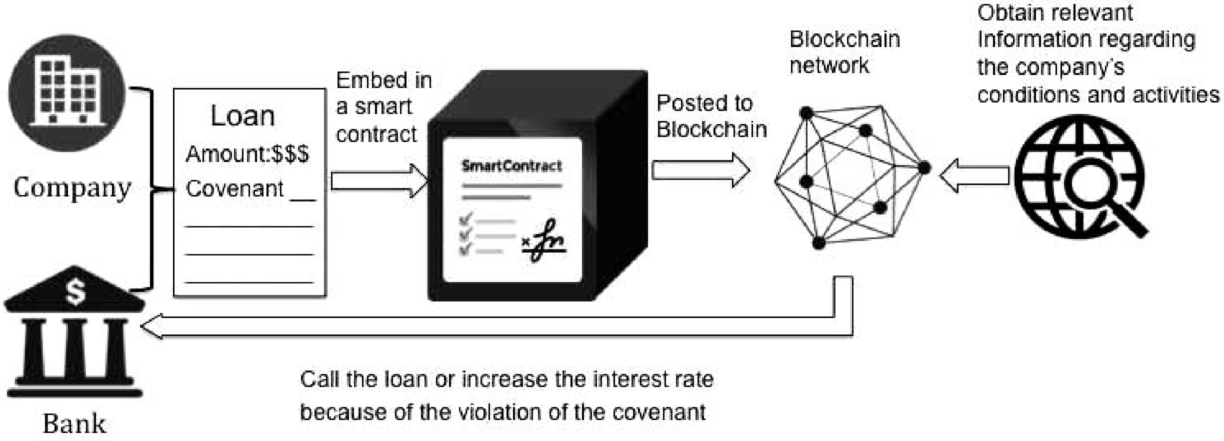
II. BACKGROUND

Blockchain: Background and Applications

Blockchain technology was conceived and initiated by Nakamoto (2008). He used a chain of blocks to create a decentralized, publicly available, and cryptographically secure digital currency system. The system, named Bitcoin, enables peer-to-peer digital currency trading. This eliminates the need for financial intermediaries while maintaining transaction safety. The Bitcoin blockchain can be viewed as a new type of accounting database that records the transactions of the digital currency into blocks. The blocks are arranged in linear chronological order and shared to a network (Fanning and Centers 2016; Peters and Panayi 2016; Swan 2015a; Yermack 2017). The main characteristics of the Bitcoin blockchain include: (1) decentralization, (2) strong authentication, and (3) tamper-resistance. The operation and management of the Bitcoin system are designed to be decentralized. This means that all nodes in the system have access to the entire list of transactions. Such access allows nodes to both verify and publish new transaction records onto blocks, which are then periodically added to the end of the main blockchain with a time stamp (Nakamoto 2008). The system is also able to verify the identity of every payer and payee involved based on a public-key cryptography system (Diffie 1988). It also examines whether the payer possesses enough money for the transaction to occur. Moreover, the process of creating a block on the chain is designed to require costly computational resources. This is to ensure the integrity and irreversibility of published transactions, and makes it almost impossible for a single or a small group of malicious parties to tamper with any blockchain records.

The blockchain architecture is designed to be a decentralized public database. In this system, every party in the network has the right to read, verify, and update transactions to the chain. In many modern applications, however, this is undesirable. In many cases, such as the use of blockchain within a business or a group of companies, the read and write permissions should be restricted to certain entities. Such systems, known as private blockchains (Pilkington 2016), involve a limited number of participants. The advantage of a private blockchain is that information stored in the chain is only accessible to predetermined entities (e.g., companies only need to share certain accounting records among departments within the organizations or with their suppliers and customers). This design can protect the privacy and confidentiality of business data. Another type of blockchain is

FIGURE 1
A Demonstration of Smart Contracts


Company
Loan
Amount:$$$
Covenant
Embed in a smart contract
SmartContract
Posted to Blockchain
Blockchain network
Obtain relevant Information regarding the company's conditions and activities
Bank
Call the loan or increase the interest rate because of the violation of the covenant

a permissioned blockchain (Peters and Panayi 2016). In a permissioned blockchain, trusted parties are preselected by a central authority and given the authorization to verify transactions. The benefit of a permissioned blockchain is that the role of transaction verification is withheld from irrelevant parties, simplifying the verification process and avoiding unwanted manipulation. In addition, permissioned blockchains are generally more scalable (Peters and Panayi 2016). Since only a limited number of parties can verify transactions, the consensus on validated transactions can be reached much quicker. One potential drawback is that this type of blockchain is based on a highly trusted entity model. Such a model requires that verifying entities do not collude to create false transactions. Since many entities within a business relationship have already established a certain level of trust, this concern is minimized, and permissioned blockchain models may still be more appropriate.

Since 2009, blockchain has evolved through three phases: blockchain 1.0, 2.0, and 3.0 (Swan 2015a). Blockchain 1.0 purely focuses on the trading of cryptocurrency. The functions of digital money transfer, remittance, and payment comprise a new ecosystem: the "Internet of Money" (Peters and Panayi 2016). Blockchain 2.0 involves similar trading, but with a much broader scope of financial applications. Such applications include derivatives, digital asset ownership, smart property, etc. (Fanning and Centers 2016; Swan 2015a). To expand the trading from simply digital currency to a large variety of products, a new type of application called a "smart contract" (Swan 2015a) was introduced in the second generation of blockchain. Blockchain-based smart contracts are computer programs operating on blockchains that autonomously verify, enforce, and execute the terms in contracts (Kiviat 2015; Peters and Panayi 2016; Zhang, Cecchetti, Croman, Juels, and Shi 2016). Smart contracts allow for the encoding of rules and situations that are agreed upon by the various trading parties. These contracts autonomously execute pre-specified tasks, or settle a contract, by examining changing conditions in conjunction with the contract's embedded rules. The concept of a "smart contract" was first proposed by Szabo (1994), who noted that the execution and monitoring of contracts mainly relies on a trusted central authority. The new blockchain-based smart contracts decentralize the enforcement power to each node in the blockchain network. Furthermore, as the trading history is distributed to every entity in the network, repudiation or modification of a trade will be almost impossible. Those functions of blockchain help to dramatically reduce the counterparty risk (Kiviat 2015). Figure 1 illustrates an example where a blockchain-based smart contract is used to monitor and operate a loan covenant. When a company and a bank agree upon a covenant, this conditional term is encoded into a smart contract that is then deployed into a blockchain. The nodes in the blockchain network will monitor the conditions and activities of the company against the requirements outlined in the smart contract. Once a violation of the covenant is detected, the blockchain network will automatically activate the portion of the smart contract pertaining to that violation. This could result in actions such as calling in the loan, increasing the interest rate, or the issuance of a warning, based on what was previously agreed upon by the parties. Auditors and the bank's management could also participate in the mechanism to oversee whether the smart contracts execute in compliance with the predetermined rules.

In addition to trading agreements, smart contracts can also encode other terms and execute tasks following the pre-specified rules. As the complexity and automation of smart contracts increase, their application could be largely expanded. Future applications may range from peer-to-peer ridesharing to self-issuing bonds or crowdfunding with the promise of future dividends (Jacynycz, Calvo, Hassan, and Sánchez-Ruiz 2016; Yuan and Wang 2016). In the long term, smart contracts could facilitate the development of a new type of company called a "Decentralized Autonomous Organization/Corporation (DAO/

DAC)." A DAO/DAC is a company that relies on the blockchain technology to self-organize and operate business. In DAO/DACs, management programs their governance rules and decision-making processes into smart contracts. This creates a structure with decentralized controls on a blockchain network (Jarvenpaa and Teigland 2017). The governance of a DAO/DAC can be achieved by distributing decision-making power to multiple participants within the blockchain network. This would guarantee the execution of an action only when the majority of the participants agree to it (Wright and De Filippi 2015). One of the main considerations of the management of a DAO/DAC is to create a set of appropriate rules that enable effective governance of the specific organizations. A DAO/DAC could collect funds from individuals and pay dividends to crowd-funding investors based on the pre-agreed terms encoded in smart contracts (Swan 2015a). The investors may also participate in decision-making through decentralized voting for approval of future strategies (Wright and De Filippi 2015).

Blockchain 3.0 expands blockchain systems further, beyond financial and business applications. Cloud storage products, voting systems, attestation services, or even government administration could be dramatically transformed toward decentralized self-managing and monitoring models (Swan 2016). Linking the IoT with blockchain technology is another novel application (Atzori 2017; Christidis and Devetsikiotis 2016; Zhang and Wen 2016). IoT is a novel paradigm in which "the pervasive presence around us of a variety of things or objects—such as Radio-Frequency IDentification (RFID) tags, sensors, actuators, mobile phones, etc.—which, through unique addressing schemes, are able to interact with each other and cooperate with their neighbors to reach common goals" (Atzori, Iera, and Morabito 2010). Basically, IoT interconnects physical and virtual things via a global network to enable advanced services (Atzori 2017). Blockchain and smart contracts could be used for the control and trading of the physical objects or services. For example, by using IoT technology embedded in automobiles, drivers could negotiate with other cars to reserve a lane by paying a small compensation (Swan 2015a). In addition, peer-to-peer accommodation rental services can be created when both a service vendor and a customer agree on a smart contract. The vendor can then issue a digital key that is installed in the customer's smartphone to unlock the facility (Hancock and Vaizey 2016). Blockchain and associated smart contract technologies could advance society toward a more automated, flexile, and efficient lifestyle.

Although the literature of many other fields has proposed potential applications of blockchain, there is limited research examining the utilization of this technology within accounting and auditing practice. Yermack (2017) provided a brief discussion on using blockchain to enable real-time accounting. He proposed that with voluntary disclosure of a company's ordinary business transactions via blockchain, interested parties could obtain instant access to accurate financial information. Using the data on blockchain, any information consumer could create his own financial statements, without relying on the judgment of auditors and the integrity of managers. While the detailed mechanisms and paradigms used to support real-time accounting were not designed, the concept is nevertheless noteworthy. Fanning and Centers (2016) suggested that blockchain technology could be of benefit to the auditing profession by making the comparison of corresponding accounting entries, present on the books of each of the trading parties, relatively easy. Explicit illustration on how to achieve such a goal is still missing, but this approach would reduce auditors' efforts relating to financial transaction testing. Kiviat (2015) illustrated the idea of blockchain-enabled "triple-entry accounting" using the example of Bitcoin transactions. It described the mechanism for posting accounting entries of Bitcoin trades to the blockchain in order to prevent transaction tampering. Unfortunately, this "triple-entry accounting" mechanism is specifically designed for the Bitcoin system, and cannot be directly applied to general corporate accounting systems. Peters and Panayi (2016) discussed the utilization of blockchain to facilitate banking ledger processing. While they provide detailed illustration on how the new technology can automate accounting booking processes, the discussion only focuses on the banking context and not broader general accounting systems. Therefore, this paper aims to extend the literature by imagining and proposing the utilization of blockchain in a generic accounting system. Specifically, this paper provides detailed illustration on:

1. How blockchain could create a real-time, verifiable, and transparent accounting ecosystem.
2. How blockchain could be used to develop an automatic assurance system, and help the extant auditing paradigm become more agile and precise.

Database, ERP, and Blockchain

Comparing blockchain with existing approaches could help to understand the advantages of this emerging technology. Databases are the best explored and widespread transaction recording and organizing applications. Specifically, distributed databases are more comparable with blockchain as both systems rely on multiple computers for operation and maintenance procedures. Peters and Panayi (2016) argued that blockchain helps to avoid the conflicts that occur when multiple modifications are made simultaneously by different computers within the distributed database system. They also mention other benefits of incorporating blockchain into such systems. These benefits include the ability to create self-enforcing contracts, as well as to ensure the security, confidentiality, and integrity of the data stored in its ledger.

ERP systems are among the most important innovations in corporate database usage (Davenport 1998). An ERP system is prepackaged business software that provides an integrated solution for the organization's information processing needs (Nah,

TABLE 1

Differences between ERP and Blockchain

ERP	Blockchain
Centralized	Decentralized and distributed
High tampering risk	Low tampering risk
Many data operations	Append only
Relational database	Linear transactional database
Human labor-intensive	Non labor-intensive
Currently do not have self-enforcing contracts	Easier to create self-enforcing smart contracts
Controls are specially designed and in place	Controls could be set through smart contracts-smart controls
Accounting-specific modules	Currently no accounting-specific modules

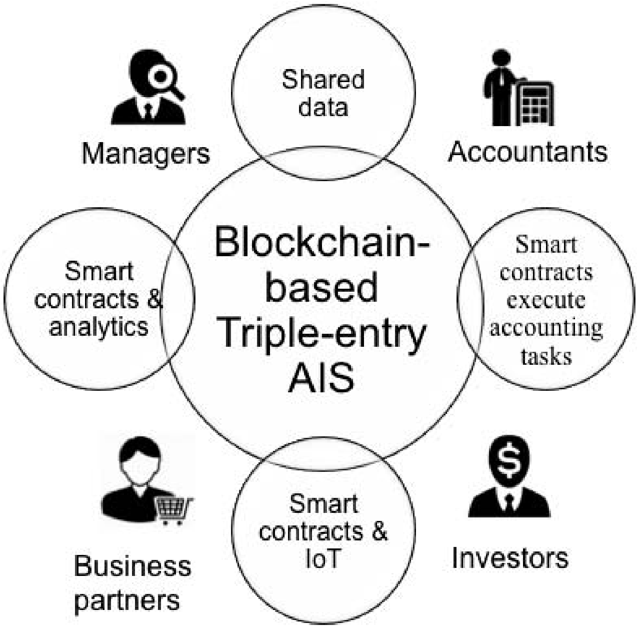
Lau, and Kuang 2001). ERPs are usually built upon core Relational Database Management Systems (RDBMS) to automatically process various business transactions (Kuhn and Sutton 2010). Besides process automation, ERP systems also distribute timely and accurate data, which provides the basis for information analysis and management decision support (Hitt, Wu, and Zhou 2002). Using ERP systems, firms can integrate data from different business segments, reengineer business processes, improve financial controls, and increase information transparency and visibility (Grabski, Leech, and Schmidt 2011; Morris and Laksmana 2010; O'Leary 2004; Robey, Ross, and Boudreau 2002).

Blockchain is considered a new type of database that has the potential to either play the role of the accounting module in an ERP or be used in conjunction with the existing accounting information system. Unlike a regular ERP that is usually organized in a centralized architecture, blockchain distributes the power of transaction verification, storage, and organization to a group of computers. This mechanism can largely reduce the risk of a single point of failure (Peters and Panayi 2016), and make it more difficult for management to override the system. Blockchain is able to prevent any unauthorized data changes, protecting companies' data from cyber-attacks. Generally, blockchain is an append-only linear transactional database. It has a relatively simple data organizing scheme as compared to an ERP, which is usually based on a relational database and allows many data operations (e.g., insertion, update, and deletion). With such efficient structure, blockchain can facilitate the tracing of tokenized objects (e.g., inventory items, accounting documents). Unlike an ERP system that requires intensive human efforts, blockchain is designed to operate automatously with little human intervention (Peters and Panayi 2016; Swan 2015b). The ability to create smart contracts allows accountants to design and deploy various controls on blockchain systems. Also, the decentralization nature of blockchain can help to prevent the manipulation of the control mechanism. Current blockchain systems do not have the accounting-specific modules present in ERP systems; therefore, this study proposes ideas for incorporating ERP and blockchain technologies. It also provides insights into using this technology for the accounting purpose. The comparison between ERP and blockchain systems is summarized in Table 1.

III. A BLOCKCHAIN-BASED ACCOUNTING ECOSYSTEM

As mentioned in Section I, the accounting profession could largely benefit from blockchain, and its current paradigm may be eventually changed thanks to this emerging technology. Blockchain, as well as associated smart contracts, can be leveraged to securely store accounting data, to instantly share relevant information with interested parties, and to increase the verifiability of business data. Using blockchain technology, companies are able to generate new accounting information systems that record validated transactions on secure ledgers. Those transactions will include not only monetary exchanges between two parties, such as payments collected from clients, cash deposited to banks, etc., but also the accounting data flow within a company. Such systems would enable close to real-time reporting by instantly broadcasting accounting information to interested parties, such as managers, auditors, creditors, and stakeholders. Because of the dramatic decrease in the unit cost of processing, memory, and storage, as well as the emergence of distributed public ledgers like blockchain, external participants can access companies' real-time accounting information at low cost. Smart contracts could serve as automatic controls that monitor accounting processes based on predetermined rules. In addition, with the advancement and popularization of IoT, controls could be embedded into the blockchain. These IoT-based controls could be incorporated into various physical objects in order to monitor and enact business processes in real time. Moreover, data analytics can also be used in conjunction with blockchain to discover anomalies and other useful information. In this system, managers, accountants, business partners, and investors could actively collaborate to verify transactions, as well as provide reliable evidence for cross-validation. These components should come together and comprise a real-time, verifiable, and transparent accounting ecosystem. Figure 2 provides an overview of the blockchain accounting ecosystem.

FIGURE 2
An Overview of Blockchain-Based Accounting Ecosystem


Shared data
Managers
Accountants
Blockchain-based Triple-entry AIS
Smart contracts & analytics
Smart contracts execute accounting tasks
Smart contracts & IoT
Business partners
Investors

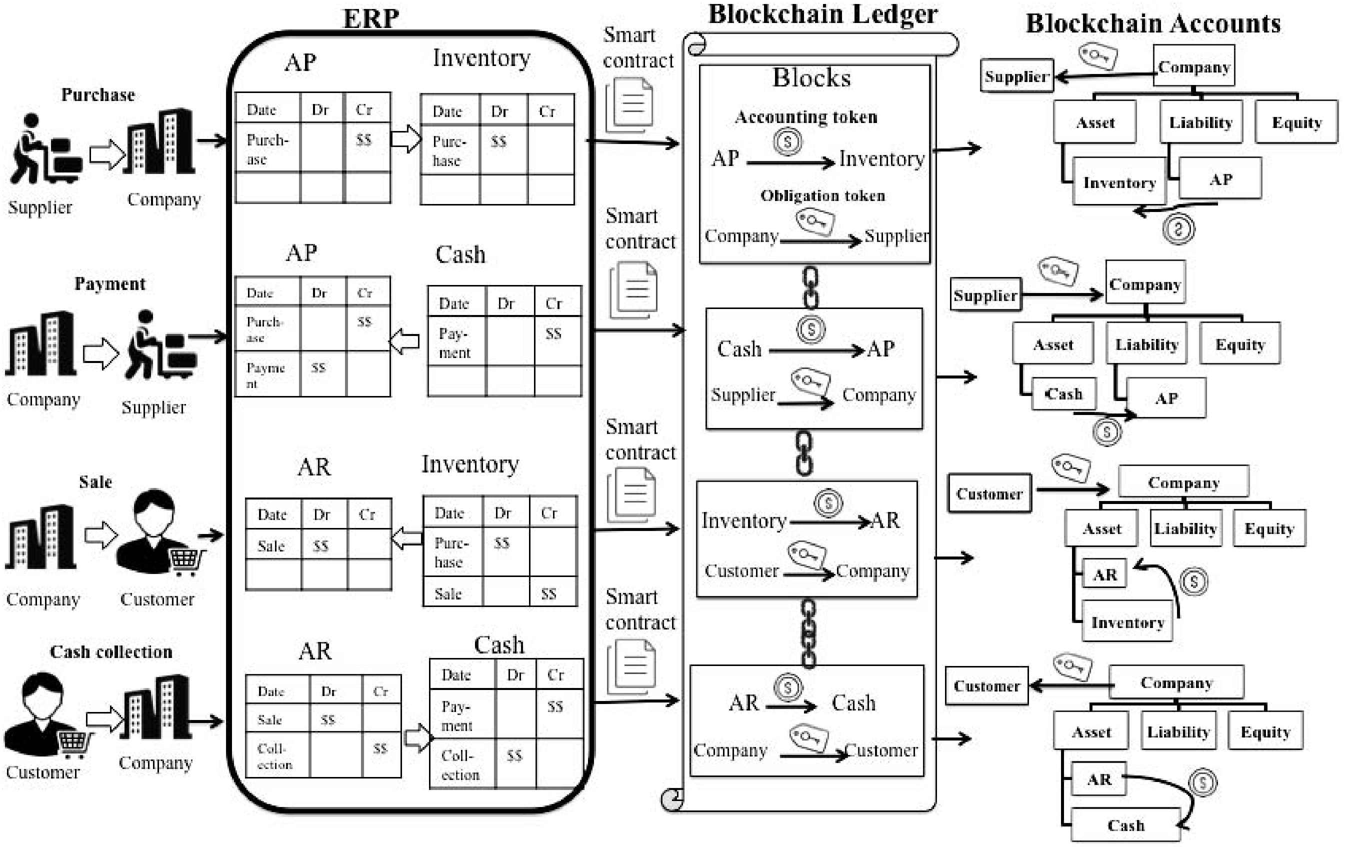
Triple-Entry Accounting

Triple-entry accounting[3] has been discussed for years by both academics and professionals (Grigg 2005, 2011; Elias 2011; Tyra 2014; Kiviat 2015; Lazanis 2015). The primitive mechanism of transaction and business activity recording is single-entry bookkeeping, in which each transaction is only recorded in one account (Sangster 2016). Although such a mechanism is simple and efficient, it is fraught with a high risk of errors and fraud, since such issues are difficult to track and repair. To improve the accuracy of the bookkeeping system, traditional financial accounting is based on a double-entry system (Pacioli 1514). This system enables rapid confirmation that the transaction has been correctly entered (Sangster 2016). The double-entry system can reduce the risk of human documentation error, such as accidental deletion of transactions, but it does not provide comprehensive assurance for companies' financial statements. Although auditors serve as third-party examiners who perform a series of tests on companies' accounting records and provide their opinions on the accuracy of the financial statements, improvements on the existing reporting and assurance system are still needed.

The "triple-entry system" was recently proposed to be utilized as an independent and secure paradigm in order to improve the reliability of companies' financial statements. The triple-entry system originally required transaction processing authorization from a neutral intermediary, with each party (the two parties involved in the transaction and the intermediary) creating a record for the transaction, resulting in three entries total (Grigg 2005). However, this mechanism requires an independent and reliable intermediary to verify each individual transaction. In addition, entries stored by the intermediary are also exposed to the risk of loss or unauthorized changes due to cyber-attacks. Blockchain technology has the potential to improve this mechanism and mitigate these problems. It could play the role of the intermediary by distributing and automating the storage and verification process, providing a secure foundation that prevents tampering and irregular accounting entries. Because of the nature of blockchain, once an accounting entry is confirmed and added to the chain, it can hardly be altered or destroyed. Moreover, smart contract technology could enable rapid verification of transaction records following accounting standards or pre-specified business rules. By encoding the third accounting entry into blockchain, a transparent, cryptographically secure, and self-verifying accounting information system can be generated, which could facilitate reliable data sharing between business parties and continuous reporting for shareholders.

[3] Ijiri (1986) proposed a "triple-entry bookkeeping" system to measure "momentum accounting" that reflects how fast income or assets are changing. However, the triple-entry accounting in this paper refers to documenting accounting entries in blockchain or with a third party.

FIGURE 3
A Triple-Entry Accounting Information System



One potential design of the simplified triple-entry accounting information system is shown in Figure 3. This system would record information regarding both transactions between business parties and data flows within an organization. In the system, every transaction would create a record stored in the blockchain ledger, in addition to the entries that have been included in the traditional double-entry system. To reflect data flows within an organization, the entries in the blockchain ledger would be recorded in the form of token transfers between accounts, which together comprise an interlocking system of enduring accounting records. Accounts in the blockchain ledger would be organized in a hierarchical structure to aggregate data at various levels, which enables both instant balancing of the accounting equation and different views of information for different users. Tokens in the blockchain ledger would also be used as certificates to attest to obligation or ownership of assets among business parties. Blockchain technology allows for timely examination of potential errors or fraud within accounting entries (e.g., duplicate payments), as well as automation of transaction verification using data from business partners. Moreover, smart contracts encoded with accounting and business rules could enable efficient control of the recording process.

Figure 3 displays the working process of the system, using a simple purchase-sale business cycle as an example. When a company purchases goods from its supplier by credit, it will record Accounts Payable and Inventory in its ERP system. It will simultaneously submit this event in the form of a transfer of a digital token (which is the "accounting token") between two blockchain accounts, to the blockchain ledger. An accounting token in the blockchain ledger can be simply viewed as a symbol for recording and tracking purposes. Each account in the modern double-booking system would have a corresponding blockchain account. A blockchain account is equivalent to a Bitcoin wallet,[4] which contains an account's unique identifier,[5]

[4] A Bitcoin wallet is a software package that allows users to make transactions on the Bitcoin network.
[5] Rather than creating a Bitcoin-like random wallet identifier, the account's unique identifier could be assigned by a trusted third party, such as the Securities and Exchange Commission (SEC), in order to prevent abuse.

related transactions, current balance, and cryptographical keys[6] for verification. Blockchain accounts would be formed in a hierarchical structure that aggregates accounting records at three levels: individual accounts at the bottom; total assets, liabilities, and equity in the middle; and the company as a whole at the top. This structure can automatically confirm the balance sheet equation using smart contracts. For example, if the balance in the company account is set as the balance in the assets account less the total balance of the liabilities and equities account, then a smart contract could be created to monitor the balance of the company account, which issues alerts when the balance does not equal to zero. Another benefit of the hierarchical structure of accounts is that it allows data views at various levels. Various consumers of information have different demands and restrictions on accounting data acquisition; thus, different data views should be granted based on user roles.

As on-credit inventory purchases involve an obligation to an outside party, an "obligation token" would be used to record such an event. This token is a certificate that attests to the obligation and ownership of an asset, as well as its amount and timing, and is undeletable and undeniable once issued. The obligation token mechanism can facilitate the implementation of automatic confirmation (Dai and Vasarhelyi 2016) by automatically matching the total token value with the supplier's account receivable balance. The obligation token could also be embedded in a smart contract that encodes the interparty relationship and can execute payment once certain conditions are realized (e.g., due date arrives). Other business rules, such as issuing discounts for early payments, could also be easily encoded into the smart contract, which allows autonomous execution of pre-specified terms based on future conditions and activities.

After a token transaction is submitted to the blockchain network, the computers in the network would perform several procedures to verify the transaction, including the verification of:

1. recording by the company's ERP system;
2. posting of the transaction;
3. asset transfer;
4. correct amounts and accounts; and
5. posting party validity (e.g., the company's ERP system or AP clerks).

Although the verification process will be automated by blockchain technology, this process should be restricted to certain parties, such as accountants, management, auditors, etc. Therefore, the blockchain ledger in this scenario falls into the permissioned blockchain category. In addition, each party would have a specific role in the verification process, and their actions and concerns might be addressed differently. For example, if an auditor doubts a transaction, then it might be paused for confirmation by accountants, while the CFO could decide to cancel it entirely. These rules could also be executed by smart contracts. Valid transactions would be grouped into blocks and appended to the main chain, and then users who have authorizations can view and explore them. Due to the nature of blockchain, confirmed and uploaded transactions cannot be manipulated. To protect the privacy of a company's sensitive data, the transactions could be encrypted before being uploaded to the blockchain ledger, and only users who have the decryption key should be able to view the content of transactions.

Following the same procedure, the company would record accounting data generated in the procurement, sale, and cash collection business processes into the blockchain ledger. Accounting tokens would be transferred from the cash account to the payable account when the company processes a payment. Meanwhile, the supplier would send the obligation token back to the company to attest the clearance of obligation. Similarly, the company could collect an obligation token when its customer makes a purchase by credit, and clear the token as long as payment is received. As discussed earlier, all the processes operate automatically, and since the entries are cryptographically assured by blockchain technology, falsifying or destroying them to conceal fraud is practically impossible.

With the increasing automation of accounting information in the modern business world, most accounting standards should be embedded into the software and systems that implement and execute the recording process (Krahel 2012). Smart contracts could play an important role in the encoding of accounting rules and the autonomous recording of transactions that are in compliance with certain accounting standards. For example, after programming the rule of "sales should be recorded after shipment of goods" into smart contracts, such programs could examine the shipment date before inserting a sales record into the blockchain ledger, and pause transaction updates until goods are shipped. Smart contracts that have accounting rules encoded could effectively control the recording of accounting activities and, therefore, provide automatic assurance on processes such as posting, classification, and cutoff. For this reason, it is imperative for companies, auditors, and standard setters to collaborate in the design and implementation of smart contracts, as this can facilitate the execution, automation, and self-monitoring of such contracts. Libraries of the templates of these smart contracts would progressively be developed and

[6] Cryptographical keys are a pair of public and private keys used in the public-key cryptography system (Diffie 1988). They aim to verify the authenticity of the sender of a transaction, and ensure that the sender cannot repudiate a transaction after its occurrence.

contribute to decreasing the cost of their creation. Furthermore, independent certification authorities could vouch for their validity and integrity.

Enabling the Accounting Ecosystem

The functions of automatic information verification, processing, storing, and reporting in the blockchain-based triple-entry accounting information system could together form a self-sufficient accounting ecosystem. In such an ecosystem, smart contracts would operate as autonomous software agents[7] on blockchain technology for verification, control, fraud prevention, etc. Many accounting processes could be automated by encoding business rules or agreements into smart contracts. Examples include automatically processing and recording payments using invoicing through self-enforcing smart contracts, and monitoring employees' performance and paying dynamic salaries using smart employment (Peters and Panayi 2016). Automation of tax filings in the form of smart contracts could provide continuous updates to government agencies. By programming tax rules into smart contracts, the tax system could become substantially simpler and less controversial (Allison 2015).[8] Smart contracts could also be combined with IoT technologies, which can capture the actual conditions and activities of physical objects, in order to automate the bookkeeping process. For example, smart contracts can execute to post a sales record to the blockchain ledger if an inventory item is known to be departing the company based on its geographic information transmitted via the IoT. Furthermore, as future devices will be equipped with sensors, intelligent chips, and accessible to networks (Dai and Vasarhelyi 2016), they may be able to self-report any inventory damage, non-delivery, or delays. These reports could trigger smart contracts to adjust the corresponding accounting measurements in time. Besides automation, smart contracts could add intelligence to the accounting process by integrating Big Data and predictive analysis. For example, a smart contract encoded with a default- or a credit rating-prediction model could monitor debtors' default risks based on their financial status and purchase behaviors and, therefore, adjust bad debt estimations accordingly.

Ideally, blockchain-based financial information could be made visible immediately to shareholders, creditors, business partners, government agencies, or other interested parties (Yermack 2017). Each information consumer has unique interests and objectives that lead to different needs of accounting data; e.g., CFO and auditors require full access to all accounting data, AP clerks need to review accounts payable entries, and investors only use highly aggregated information. Therefore, specialized access authorizations should be granted to each type of information consumer based on their role and demands. As discussed in the previous section, the blockchain-based accounting information system could allow users to view data at various aggregation levels based on predetermined roles. Such an increase in transparency, coupled with the verifiable nature of the blockchain, has the potential to increase shareholder trust by reducing opportunities for management earnings manipulation (Yermack 2017). Since the recording and presentation process is shifting from manual operation to progressive automation, the accountant's role is changing from collector and aggregator to interpreter and analyst.

One important issue that is worth careful consideration is the scope of participants in the blockchain-based accounting ecosystem. This is especially the case with regard to the processes of transaction verification as well as smart contract creation and validation. The blockchain-based accounting system is proposed as a permissioned blockchain in which only entities inside a company (e.g., its ERP system or accountants) can submit a transaction record to the blockchain ledger, with the verification function being restricted to accountants, management, and auditors. The design and performance of smart contracts may involve a large range of participants, such as management, representatives from business partners, creditors, auditors, service vendors (such as Big Data analysis firms), etc., as long as they can devote their competencies to create effective and efficient smart contracts. However, the validation of smart contracts' compliance with regulations and legislations should be performed by relevant professionals, such as auditors, lawyers, and regulators.

IV. APPLYING BLOCKCHAIN TO CONTINUOUS ASSURANCE

As blockchain technology and associated smart contracts become increasingly adopted for use in creating a verifiable and tamper-proof system, the current assurance paradigm may be fundamentally changed. A blockchain ledger could be leveraged as a reliable medium to store any audit-related documents. As those information and documents are continuously shared with relevant parties, the role of providing assurance can be expanded from primarily auditors to a much broader scope of participants, like business partners, creditors, government bodies, etc. In addition, many analytical tools can then be applied to

[7] A software agent is a software component that acts autonomously to meet preset objectives (Briscoe and De Wilde 2009; Vasarhelyi and Hoitash 2005).

[8] It must be noted that the laws and regulations to be automated must be clearly "rule-based" in current technology, with very clear comprehensive contingencies. "Principle-based" rules are difficult to automate (Krahel 2012). Many rules will not be uniform, but rather diverse according to companies' special situations. Smart contract designers (management, auditors, lawyers, or regulators) can determine the terms or rules that are most suitable for their firms.

the accounting records within the blockchain in order to discover patterns, identify anomalies, and extract other audit evidence. Moreover, as more and more physical objects (e.g., machines, production lines, and inventory items) become equipped with digital capabilities and have access to the Internet, real-time business process monitoring could be embedded into the blockchain technology and executed by these physical objects.

Using Blockchain to Increase Information Auditability

One essential benefit of the blockchain infrastructure is the increased auditability of information. Since a blockchain ledger secures the data that are posted on it, it could also lend veracity to many audit-related documents. For example, if each individual inventory item is registered in the blockchain upon its arrival at the company's warehouse, and its location and condition are continuously updated, then a complete track and history of inventory items could be generated. This would enable remote, real-time inventory examination. Even audit trails could be documented on blockchain to facilitate tracing and review in the future. Similarly, information in electronic invoices, bills of lading, letters of credit, receipts, etc., could also be documented in the blockchain (Ernst & Young [EY] 2015), on which all documents are traceable and unchangeable, allowing auditors to test the completeness of financial information. Those documents could also be shared among related parties for cross-validation. For example, missing invoices at the customer side may indicate a fictitious sale. To enable this mechanism, new standards might be implemented that enforce the incorporation of blockchain technology into the documentation of accounting information. Requiring certain types of documents to be filed on blockchain would mean that the absence of any records might indicate false transactions or fraud. Placing blockchain technology in the hands of managers, auditors, business partners, and creditors can achieve a new level of assurance. These parties may participate in the transaction verification process by providing reliable and independent information used for attesting to obligations and ownership. The collaboration of these individuals could provide trusted real-time assurance through the "proof of transaction" mechanism.

Smart Controls

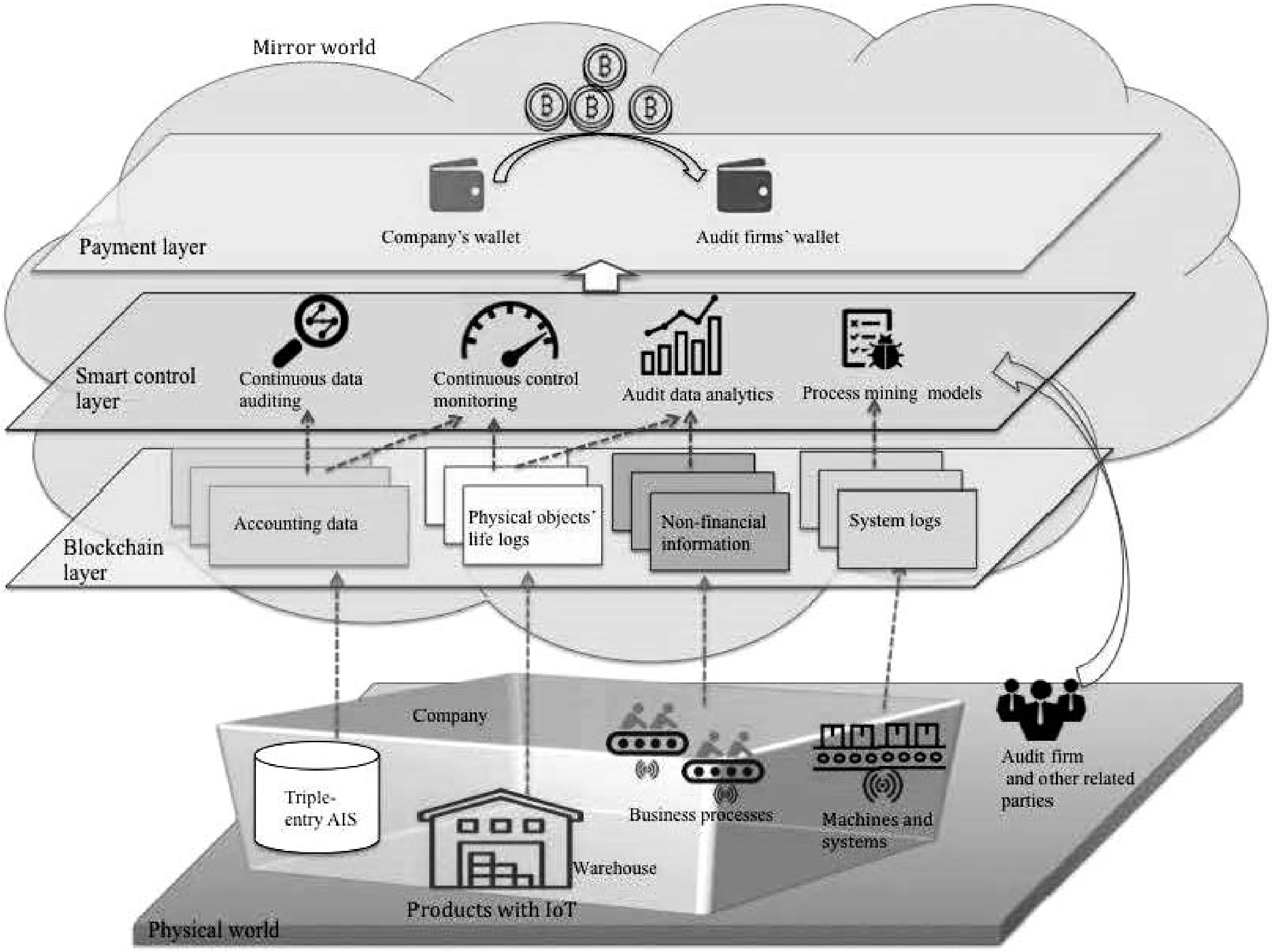
While traditional auditing is centered around the audit of paper-based income statements on an annual or quarterly basis, this is no longer the world in which businesses operate. Increases in the speed and scope of business activity mean that any advancement enabling auditors to provide assurance closer to the transaction date would be meaningful. The traditional audit cannot provide near-real-time assurance due to the manual nature of its procedures and the lack of tools to effectively analyze and monitor large amounts of transactional data (Alles, Kogan, and Vasarhelyi 2002; Vasarhelyi and Halper 1991). Since the 1990s, there have been discussions on how paper-based auditing techniques would be dramatically augmented by, and eventually integrated into, smart contracts (Szabo 1997). With the integration of blockchain technology, smart contracts can operate with the supervision of multiple parties. A smart contract-enabled, control-based assurance paradigm could play an essential role in the new business world. Managers and auditors would program the firm-specific control protocols into smart contracts, which, in turn, could monitor accounting records or business processes. The protocols could implement not only general accounting rules, but also more intelligent controls, especially when combined with other state-of-the-art techniques, such as Big Data, data analytics, and continuous auditing/monitoring models. For example, smart controls could revoke a transaction if the company's process mining model (Jans, Alles, and Vasarhelyi 2014) detects that its underlying processes are disobeying certain internal business rules. One of the advantages of smart controls is their ability to self-adjust based on environmental changes (Szabo 1997). Therefore, smart contracts could execute complex controls to support an intelligent, flexible, and timely assurance paradigm.

The assignment of authority to change the accounting and business rules pertaining to smart controls could be critically important, as companies may manipulate these rules to gain illicit benefits. Ultimately, smart controls must rely on a governance process[9] through which users agree to certain requirements for changing underlying code, as well as provisions for dispute resolution (Yermack 2017). Since the mechanism of blockchain technology ensures the integrity of posted data, it would also be utilized for protecting the code embedded in smart contracts. By posting (and probably encrypting) codes of smart controls on blockchain, managers and auditors could continuously verify the integrity of those programs.

Blockchain-based continuous assurance has been associated with the debate on the role of the auditing profession in this autonomous self-regulating paradigm (Peters and Panayi 2016; Yermack 2017). Although auditors' accuracy verification roles may be diminished, their judgment, oversight, and insight should become even more necessary. The focus of auditing would change from record tracing and verification to more complex analysis, such as systemic evaluation, risk assessment, predictive audits, and fraud detection. Another essential role that auditors would play is that of an evaluator and examiner over the design,

[9] Today's legal and regulatory system is a governance system of this type for extant data and processes. However, rules and regulations will have to be rewritten to reduce the ambiguity in their interpretation.

FIGURE 4
The Vision of Blockchain-Based Assurance World



creation, and execution of smart controls. Auditors should understand the codes in smart controls, and investigate the accuracy of program operation. To be qualified to perform such roles, auditors should be technically trained and have the assistance systems that are designed for auditors to understand, operate, and analyze blockchain and associated technologies (Tschakert, Kokina, Kozlowski, and Vasarhelyi 2016).

The Change of Assurance Paradigm

Blockchain, along with other emerging technologies (e.g. IoT, continuous auditing and control monitoring mechanisms, process mining models, etc.), could dramatically change the current audit paradigm, and therefore promote a new generation of auditing (Dai and Vasarhelyi 2016). In the new paradigm, blockchain technology can serve as a foundation that stores and secures any audit-related data. Auditors and other service providers could create smart contracts running on top of blockchains that perform effective controls and advanced analyses. The vision of the blockchain-enabled audit paradigm is shown in Figure 4.

The new audit paradigm would consist of two components: (1) a physical world, and (2) a mirror world, which is a virtual model that reflects business activities and conditions of objects in the physical world. Each physical object would have a virtual representation in the mirror world, with the conditions, locations, surrounding environment, history, and activities continuously transmitted via IoT or other information and communication technology. The mirror world is comprised of three layers: blockchain, smart control, and payment.

The blockchain layer is an ecosystem of blockchains, each of which would record a type of data that is needed for audits. Examples of such data include:

1. companies' financial data from the triple-entry accounting information system;
2. life-logs of physical objects (such as inventory, machines, buildings) recorded and transmitted by IoT;
3. nonfinancial information from various business processes or from outside information resources (such as news, social media); and
4. system logs that record real business processes as used in process mining (Jans et al. 2014).

Since the integrity of those data is protected by blockchain, the audit could rely on those data when performing advanced analyses.

The smart control layer allows auditors or other experts to provide digitized controls using smart contracts. Many audit services, such as continuous data auditing (Vasarhelyi and Halper 1991; Vasarhelyi, Alles, and Williams 2010), continuous controls monitoring (CCM) (Alles, Brennan, Kogan, and Vasarhelyi 2006), audit data analytics (American Institution of Certified Public Accountants [AICPA] 2015), etc., have been digitized and could be offered remotely. Besides, associating blockchain data integrity with process logs in ERPs (e.g., through process mining and real-time exception analysis) could substantially improve the integrity and reliability of business systems. Those services could be quantified into small tests or analytical apps (Dai 2017) and sealed into smart contracts. Those smart contracts would autonomously operate on top of the blockchain ecosystem and analyze the data to preemptively identify significant risks, prevent frauds, and support decisions.

The top layer is an automatic payment system that will send a payment to auditors once the pre-agreed audit services are provided. Smart contracts could monitor the progress of service providing, and initiate payments once the services have been accomplished. As the use of cryptocurrencies increases in the real business world, companies might use such cryptocurrency to make payments. Consequently, smart contracts can directly control the digital wallet of a company and send pre-agreed cryptocurrency amounts to its audit firm's wallet. With cryptocurrency and smart contract controls, the payment process can become completely automated. Such a system could protect and benefit both companies and audit firms, as payments would be issued only if services are completed.

V. CHALLENGES AND RESEARCH OPPORTUNITIES

Although this paper proposes potential applications of blockchain, the challenges of acceptance and full utilization of this technology in the accounting and auditing sphere cannot be neglected. In the past decades, many disruptive technologies, such as ERP and EDI (Electronic Data Interchange), have generated great contributions toward improving a firm's productivity and reducing operational costs. However, the technical complexity of the solutions, the requirement of substantial investments of financial and time resources, the difficulty to expand the technologies to business partners, and the demand for business and process changes could all hinder the adoption of such technologies (Davenport 1998; Iacovou, Benbasat, and Dexter 1995; Kuan and Chau 2001; Law and Ngai 2007; Pan and Jang 2008). Since blockchain shares many of these challenges with ERP or EDI, lessons learned from their implementations could serve as object lessons in this context.

The acceptance of ERP and EDI technologies has been well studied in the literature. The Technology-Organization-Environment (TOE) framework (Tornatzky, Fleischer, and Chakrabarti 1990) has been used to examine the factors that have significant influence on ERP or EDI adoption (Kuan and Chau 2001; Pan and Jang 2008; Schniederjans and Yadav 2013). This framework examines the three aspects that drive or impede the adoption and use of technological innovations at the firm level: the technological context, the organizational context, and the environmental context. The following sections provide a comparative discussion on the challenges in the adoption and implementation of blockchain for accounting purposes with those of ERP or EDI from the three perspectives in the TOE framework. Future research opportunities that resolve or alleviate the challenges are also identified.

Technological Context

Many studies have identified the significant impacts of technology readiness and capability in EDI or ERP adoption (Kuan and Chau 2001; Kuhn and Sutton 2010; Pan and Jang 2008; Schniederjans and Yadav 2013). Similar challenges could be faced by blockchain pioneers. Many mainstream blockchain mechanisms, such as Bitcoin, are highly demanding of storage and computational power in order to ensure the security of data, even though the data stream of transactions may not be terribly large. Therefore, the adoption of blockchain technology in large corporate systems will depend on the projected development of larger storage systems, wider bandwidth for data transmission, and substantial expansion of computational power. Meanwhile, management needs to consider the scope of accounting data and other information necessary to post to a blockchain system in order to provide sufficient transparency and accurate assurance, while preventing the system from becoming overwhelmingly demanding for resources. In addition, sensitive information should be protected from irrelevant parties (Gal 2008). This discussion leads to future research opportunities such as:

- Would corporate blockchain streams quickly expand to an unmanageable size?
- What accounting data should be recorded in blockchain? What other information (such as IoT data) should be loaded to blockchain in order to provide better assurance?

Similar to EDI (Iacovou et al. 1995), blockchain can only maximize the benefit to enterprises through the wide adoption of the technology, since sufficient participants are required to ensure the security of the ledger, provide reliable verification of transactions, and prevent illicit collusions. In addition, a large variety of reliable audit evidence could be provided through information shared by separate organizations (third-party confirmation). Unfortunately, however, the operation of blockchain usually needs substantial storage and computation resources. Placing volumes of corporate data into such a system would be extremely demanding and potentially expensive for current commercial computing. Such requirements of substantive resources could impede the popularization of this technology, especially among small and medium enterprises (SMEs). Even large corporations may refuse to use blockchain applications if they have significantly adverse effects on the efficiency of current systems and related performance issues (Kuhn and Sutton 2010). Solutions for alleviating such overhead costs include using permissioned blockchain, creating less costly algorithms, etc. Although some light and scalable blockchains have been piloted (such as Ripple[10] and Litecoin[11]), the security models on which those mechanisms rely may not be suitable for accounting applications. Therefore, a special blockchain scheme is still needed to provide reliable and accurate accounting information at reasonable storage and computational cost. In addition to technical advancement, blockchain practitioners may learn lessons from the adoption of EDI. When this occurred, large organizations, industry associations, and governments promoted the popularization of the technology through partner expansion plans (Iacovou et al. 1995). This idea leads to future research opportunities such as:

- How can existing blockchain mechanisms be changed to be more applicable for accounting applications?
- Should large enterprise and governments play the role of the main promoters in the acceptance phase? How could they help SMEs to adopt and use this emerging technology?

The impact of IT complexity has been well discussed in the adoption of ERP or EDI (Premkumar, Ramamurthy, and Crum 1997; Bradford and Florin 2003). Lack of awareness and understanding of the technology is also a major challenge for blockchain popularization (Deloitte 2016). Blockchain's algorithms and operating paradigms require substantial system and security knowledge. As such, managers, accountants, and auditors should obtain necessary training and cooperation from IT professionals in using this technology correctly and efficiently. These parties also need special training in order to participate in the design and implementation of smart contracts. Moreover, the audit of smart contracts is an even more complex issue that requires solid understanding of this technology. This leads to future research opportunities such as:

- What knowledge should managers, accountants, and auditors acquire to be ready to use the blockchain-based accounting information system?
- What training should be provided to managers, accountants, and auditors, respectively, in order to help them understand, design, and audit smart contracts?

Organizational Context

Perceived benefits and costs have been considered one of the main predictors for the initial use of EDI and ERP (Kuan and Chau 2001; Premkumar, Ramamurthy, and Nilakanta 1994; Schniederjans and Yadav 2013). Large established companies have difficulty adopting disruptive technologies (such as blockchain) until their traditional business model is seriously threatened (Christensen 2013). In general, the development and operation of blockchain require very large computational resources, and the blockchain ledger should be distributed to avoid collusion and corruption, which may create a heavy overhead for companies. If blockchain technology is to be widely adopted, then its beginning will be in the areas where security and data integrity are of paramount concern and the volume of data is not overwhelming, such as ecommerce businesses. Startups that intend to sell blockchain-related products could provide a fertile testing ground. Corporate processes would have to be changed dramatically, with a large initial investment in smart contracts,[12] making firms rebalance their workforces, placing and trusting

[10] See: https://ripple.com

[11] See: https://litecoin.org

[12] As in many modern computer processes, smart contracts will entail large initial investment in development and validation, but very small incremental costs in their usage. This will apply also in the progressive layering of smart contracts with increasing degrees of interaction and aggregate complexity.

their data in the public domain (even if encrypted), and convincing business partners to participate in an open-share environment. All of this should be implemented while conducting business in parallel with their traditional systems, like ERPs. However, similar to other add-on modules, large organizations operating multiple ERPs may have to invest valuable resources in order to integrate blockchain applications with each individual system (Kuhn and Sutton 2010). Consequently, questions arise such as:

- How could a multi-entry system work and interface with evolving traditional systems?
- What markets could receive the most benefits from the adoption of the blockchain-based accounting information system?
- How can the original blockchain model be adjusted for real-time reporting and assurance purposes?

Environmental Context

The acceptance and use of ERP and EDI have proven to be significantly influenced by regulator pressure (Iacovou et al. 1995; Kuan and Chau 2001; Schniederjans and Yadav 2013). Therefore, regulators are expected to play an essential role in the adoption stage of blockchain within the accounting sphere. Regulators should have a deep understanding of the technology and its impact on businesses, and provide appropriate guidance and supervision to prevent misuse and abuse of blockchain and smart contracts. They should also think about how the existing accounting standards can be adapted to the increasingly verifiable and transparent accounting ecosystem. Moreover, the auditors' role in the new accounting system should be rethought, and the current audit paradigm may need reengineering. Consequently, questions arise such as:

- How should accounting standards be changed? Should there be parallel standards created for this transformation?
- What standards should be created to enforce the audit of smart contracts?
- Would auditing be needed/necessary with a secure blockchain data stream? In which areas? Which areas should be abandoned, and what new audit assertions must be created?

VI. CONCLUSIONS

This paper proposes a radically different measurement and assurance paradigm utilizing modern blockchain and associated smart contract technologies. Although the technological world has provided business with computers, Internet, and advanced analytic methods, the essence of the accounting measurement model has remained the late medieval model of double-entry (Pacioli 1514). Furthermore, auditing's basic approach (Montgomery 1919) has been very slowly evolving for a century, making the use of technologies limited, at best. The fear is that basing modern accounting and auditing in these old technologies will make the processes redundant, non-flexible, defenseless against modern cyber-attacks, and dependent on anachronistic rules.

Consequently, after drawing on multiple disciplines and thought pieces from the accounting profession, this paper argues for a blockchain-based accounting and assurance methodology that would provide real-time, verifiable information disclosure and progressively automated assurance. However, the difficulties of both the development and implementation of such a radically different technology cannot be ignored.

While the goal of this paper is to discuss and provide insights on how blockchain technology could impact the accounting and assurance profession, our study has many limitations. We point out three important ones. First, blockchain technology is emerging and rapidly developing. As new algorithms and approaches are introduced, its accounting and assurance applications may need to be expanded and reconsidered. Second, this paper only provides a general discussion of the role that blockchain technology could play in the accounting and assurance environment. Blockchain's applications and challenges in specific areas, such as government auditing, need further thoughts. Third, concepts like triple-entry accounting may be just an adaptation to the extant world, which may not be advanced enough to use going forward in a rapidly changing world.

REFERENCES

Alles, M. G., A. Kogan, and M. A. Vasarhelyi. 2002. Feasibility and economics of continuous assurance. *Auditing: A Journal of Practice & Theory* 21 (1): 125–138. doi:10.2308/aud.2002.21.1.125

Alles, M. G., G. Brennan, A. Kogan, and M. A. Vasarhelyi. 2006. Continuous monitoring of business process controls: A pilot implementation of a continuous auditing system at Siemens. *International Journal of Accounting Information Systems* 7 (2): 137–161. doi:10.1016/j.accinf.2005.10.004

Allison, I. 2015. *Deloitte, Libra, Accenture: The Work of Auditors in the Age of Bitcoin 2.0 Technology*. Available at: http://www.ibtimes.co.uk/deloitte-libra-accenture-work-auditors-age-bitcoin-2-0-technology-1515932

American Institution of Certified Public Accountants (AICPA). 2015. *Audit Analytics and Continuous Audit: Looking Toward the Future*. Available at: https://www.aicpa.org/InterestAreas/FRC/AssuranceAdvisoryServices/DownloadableDocuments/AuditAnalytics_LookingTowardFuture.pdf

Atzori, M. 2015. *Blockchain Technology and Decentralized Governance: Is the State Still Necessary?* Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2709713

Atzori, M. 2017. *Blockchain-Based Architectures for the Internet of Things: A Survey*. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2846810

Atzori, L., A. Iera, and G. Morabito. 2010. The Internet of Things: A survey. *Computer Networks* 54 (15): 2787–2805. doi:10.1016/j.comnet.2010.05.010

Bradford, M., and J. Florin. 2003. Examining the role of innovation diffusion factors on the implementation success of enterprise resource planning systems. *International Journal of Accounting Information Systems* 4 (3): 205–225. doi:10.1016/S1467-0895(03)00026-5

Briscoe, G., and P. De Wilde. 2009. Computing of applied digital ecosystems. In *Proceedings of the International Conference on Management of Emergent Digital EcoSystems,* Article 5, ACM. Available at: http://dl.acm.org/citation.cfm?id=1643823.1643830

Christensen, C. 2013. *The Innovator's Dilemma: When New Technologies Cause Great Firms to Fail*. Boston, MA: Harvard Business Review Press.

Christidis, K., and M. Devetsikiotis. 2016. Blockchains and smart contracts for the Internet of Things. *IEEE Access: Practical Innovations, Open Solutions* 4: 2292–2303. doi:10.1109/ACCESS.2016.2566339

Cointelegraph. 2015. *Citi Develops 3 Blockchains with Own "Citicoin" Token*. Available at: http://cointelegraph.com/news/114717/citi-develops-3-blockchains-with-own-citicoin-token

Dai, J. 2017. *Towards App-Based Auditing*. Unpublished Dissertation, Chapter 4, Rutgers, The State University of New Jersey.

Dai, J., and M. A. Vasarhelyi. 2016. Imagineering audit 4.0. *Journal of Emerging Technologies in Accounting* 13 (1): 1–15.

Davenport, T. H. 1998. Putting the enterprise into the enterprise system. *Harvard Business Review* 76 (July/August): 121–131.

De Meijer, C. R. 2016. The U.K. and Blockchain technology: A balanced approach. *Journal of Payments Strategy and Systems* 9 (4): 220–229.

Deloitte. 2016. *Blockchain: Enigma, Paradox, Opportunity*. Available at: https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/financial-services/deloitte-nl-fsi-blockchain-enigma-paradox-opportunity-report.pdf

Diffie, W. 1988. The first ten years of public-key cryptography. *Proceedings of the IEEE* 76 (5): 560–577. doi:10.1109/5.4442

Dorri, A., S. S. Kanhere, and R. Jurdak. 2016. *Blockchain in Internet of Things: Challenges and Solutions*. Available at: https://arxiv.org/ftp/arxiv/papers/1608/1608.05187.pdf

Elias, M. 2011. *Bitcoin: Tempering the Digital Ring of Gyges or Implausible Pecuniary Privacy*. Available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1937769

Ernst & Young (EY). 2015. *Sharing Ledgers for Sharing Economies: An Exploration of Mutual Distributed Ledgers* (*aka Blockchain Technology*). Available at: http://www.the-blockchain.com/docs/Journal%20of%20Financial%20Perspectives%20-%20Sharing%20Ledgers%20for%20Sharing%20Economies.pdf

Fanning, K., and D. P. Centers. 2016. Blockchain and its coming impact on financial services. *Journal of Corporate Accounting and Finance* 27 (5): 53–57. doi:10.1002/jcaf.22179

Ferrer, E. C. 2016. *The Blockchain: A New Framework for Robotic Swarm Systems*. Available at: https://arxiv.org/pdf/1608.00695v1.pdf

Gal, G. 2008. Query issues in continuous reporting systems. *Journal of Emerging Technologies in Accounting* 5 (1): 81–97. doi:10.2308/jeta.2008.5.1.81

Grabski, S. V., S. A. Leech, and P. J. Schmidt. 2011. A review of ERP research: A future agenda for accounting information systems. *Journal of Information Systems* 25 (1): 37–78. doi:10.2308/jis.2011.25.1.37

Grigg, I. 2005. *Triple Entry Accounting*. Systemics, Inc. Available at: http://iang.org/papers/triple_entry.html

Grigg, I. 2011. *Is Bitcoin a Triple Entry System?* Available at: http://financialcryptography.com/mt/archives/001325.html

Hancock, M. and E. Vaizey. 2016. *Distributed Ledger Technology: Beyond Block Chain*. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf

Hitt, L. M., D. J. Wu, and X. Zhou. 2002. Investment in enterprise resource planning: Business impact and productivity measures. *Journal of Management Information Systems* 19 (Summer): 71–98.

Iacovou, C. L., I. Benbasat, and A. S. Dexter. 1995. Electronic data interchange and small organizations: Adoption and impact of technology. *Management Information Systems Quarterly* 19 (4): 465–485. doi:10.2307/249629

Ijiri, Y. 1986. A framework for triple-entry bookkeeping. *The Accounting Review* 61 (4): 745–759.

Jacynycz, V., A. Calvo, S. Hassan, and A. A. Sánchez-Ruiz. 2016. Betfunding: A distributed bounty-based crowdfunding platform over ethereum. In *Distributed Computing and Artificial Intelligence, 13th International Conference,* 403–411. Available at: https://link.springer.com/chapter/10.1007/978-3-319-40162-1_44?no-access=true

Jans, M., M. G. Alles, and M. A. Vasarhelyi. 2014. A field study on the use of process mining of event logs as an analytical procedure in auditing. *The Accounting Review* 89 (5): 1751–1773. doi:10.2308/accr-50807

Jarvenpaa, S., and R. Teigland. 2017. Introduction to trust, identity, and trusted systems in digital environments minitrack. In *Proceedings of the 50th Hawaii International Conference on System Sciences*. Available at: https://www.researchgate.net/publication/317396207_Introduction_to_Trust_Identity_and_Trusted_Systems_in_Digital_Environments_Minitrack

Kiviat, T. I. 2015. Beyond Bitcoin: Issues in regulating blockchain transactions. *Duke Law Journal* 65: 569–608.

Krahel, J. P. 2012. *On The Formalization of Accounting Standards*. Ph.D. Dissertation, Rutgers, The State University of New Jersey.

Kuan, K. K., and P. Y. Chau. 2001. A perception-based model for EDI adoption in small businesses using a technology-organization-environment framework. *Information and Management* 38 (8): 507–521. doi:10.1016/S0378-7206(01)00073-8

Kuhn, J. R., Jr., and S. G. Sutton. 2010. Continuous auditing in ERP system environments: The current state and future directions. *Journal of Information Systems* 24 (1): 91–112. doi:10.2308/jis.2010.24.1.91

Law, C. C., and E. W. Ngai. 2007. ERP systems adoption: An exploratory study of the organizational factors and impacts of ERP success. *Information and Management* 44 (4): 418–432. doi:10.1016/j.im.2007.03.004

Lazanis, R. 2015. *How Technology Behind Bitcoin Could Transform Accounting as We Know It*. Available at: http://www.techvibes.com/blog/how-technology-behind-bitcoin-could-transform-accounting-as-we-know-it-2015-01-22

Liebenau, J., and S. M. Elaluf-Calderwood. 2016. *Blockchain Innovation beyond Bitcoin and Banking*. Working paper. Available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2749890

Montgomery, R. H. 1919. *Auditing Theory and Practice*. 2nd edition. New York, NY: The Ronald Press.

Morris, J. J., and I. Laksmana. 2010. Measuring the impact of enterprise resource planning (ERP) systems on earnings management. *Journal of Emerging Technologies in Accounting* 7 (1): 47–71. doi:10.2308/jeta.2010.7.1.47

Nah, F., J. Lau, and J. Kuang. 2001. Critical factors for successful implementation of enterprise systems. *Business Process Management* 7 (3): 285–296. doi:10.1108/14637150110392782

Nakamoto, S. 2008. *Bitcoin: A Peer-To-Peer Electronic Cash System*. Available at: https://bitcoin.org/bitcoin.pdf

O'Leary, D. E. 2004. Enterprise Resource Planning (ERP) Systems: An empirical analysis of benefits. *Journal of Emerging Technologies in Accounting* 1 (1): 63–72. doi:10.2308/jeta.2004.1.1.63

Omohundro, S. 2014. Cryptocurrencies, smart contracts, and artificial intelligence. *AI Matters* 1 (2): 19–21. doi:10.1145/2685328.2685334

Pacioli, L. 1514. *Paciolo on Accounting* (*Summa de Arithmetica, Geometria, Proportioni e Proportionalita: Distintio Nona—Tractatus XI, Particularis de Computis et Scripturis*), translated by Brown, R. G., and K. S. Johnson. New York, NY: McGraw-Hill.

Pan, M. J., and W. Y. Jang. 2008. Determinants of the adoption of enterprise resource planning within the technology-organization-environment framework: Taiwan's communications industry. *Journal of Computer Information Systems* 48 (3): 94–102.

Peters, G. W., and E. Panayi. 2016. Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the Internet of Money. In *Banking Beyond Banks and Money,* 239–278. New York, NY: Springer International Publishing.

Pilkington, M. 2016. *Blockchain Technology: Principles and Applications*. Available at: https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=2662660

Premkumar, G., K. Ramamurthy, and S. Nilakanta. 1994. Implementation of electronic data interchange: An innovation diffusion perspective. *Journal of Management Information Systems* 11 (2): 157–186.

Premkumar, G., K. Ramamurthy, and M. Crum. 1997. Determinants of EDI adoption in the transportation industry. *European Journal of Information Systems* 6 (2): 107–121. doi:10.1057/palgrave.ejis.3000260

PricewaterhouseCoopers (PwC). 2015. *Money Is No Object: Understanding the Evolving Cryptocurrency Market*. Available at: https://www.pwc.com/us/en/financial-services/publications/assets/pwc-cryptocurrency-evolution.pdf

PricewaterhouseCoopers (PwC). 2016. *What's Next for Blockchain in 2016?* Available at: https://www.pwc.com/us/en/financial-services/publications/viewpoints/assets/pwc-qa-whats-next-for-blockchain.pdf

Robey, D., J. W. Ross, and M. C. Boudreau. 2002. Learning to implement enterprise systems: An exploratory study of the dialectics of change. *Journal of Management Information Systems* 19 (1): 17–46. doi:10.1080/07421222.2002.11045713

Sangster, A. 2016. The genesis of double entry bookkeeping. *The Accounting Review* 91 (1): 299–315. doi:10.2308/accr-51115

Schniederjans, D., and S. Yadav. 2013. Successful ERP implementation: An integrative model. *Business Process Management Journal* 19 (2): 364–398. doi:10.1108/14637151311308358

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

Swan, M. 2015b. *Blockchain Thinking: The Brain as a DAC* (*Decentralized Autonomous Organization*). Presented at the Texas Bitcoin Conference (March 27–29). Available at: http://www.the-blockchain.com/docs/Blockchain%20Thinking%20-%20The%20Brain%20as%20a%20DAC%20-%20Decentralized%20Autonomous%20Organization.pdf

Swan, M. 2016. Blockchain temporality: Smart contract time specifiability with blocktime. In *International Symposium on Rules and Rule Markup Languages for the Semantic Web,* 184–196. New York, NY: Springer International Publishing.

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

Szabo, N. 1997. Formalizing and securing relationships on public networks. *First Monday* 2 (9). doi:10.5210/fm.v2i9.548

Tornatzky, L. G., M. Fleischer, and A. K. Chakrabarti. 1990. *Processes of Technological Innovation*. New York, NY: Lexington Books.

Trautman, L. J. 2016. *Is Disruptive Blockchain Technology the Future of Financial Services?* Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2786186

Tschakert, N., J. Kokina, S. Kozlowski, and M. A. Vasarhelyi. 2016. Why CPAs and organizations need to learn to use advanced technology to predict and achieve outcomes. *Journal of Accountancy*. Available at: http://www.journalofaccountancy.com/issues/2016/aug/data-analytics-skills.html

Tyra, J. M. 2014. *Triple Entry Bookkeeping with Bitcoin*. Available at: https://bitcoinmagazine.com/articles/triple-entry-bookkeeping-bitcoin-1392069656

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

Vasarhelyi, M., and R. Hoitash. 2005. Intelligent software agents in accounting: An evolving scenario. In *The Evolving Paradigms of Artificial Intelligence and Expert Systems: An International View*. Volume 6, edited by Vasarhelyi, M., and A. Kogan. Princeton, NJ: Markus Wiener Publishers.

Vasarhelyi, M. A., M. Alles, and K. T. Williams. 2010. *Continuous Assurance for the Now Economy. A Thought Leadership Paper for the Institute of Chartered Accountants in Australia*. Queensland, Australia: Institute of Chartered Accountants.

Wall Street Journal (*WSJ*). 2015. A Bitcoin technology gets NASDAQ test. Available at: http://www.wsj.com/article_email/a-bitcoin-technology-gets-nasdaq-test-1431296886-lMyQjAxMTE1MzEyMDQxNzAwWj

Wright, A., and P. De Filippi. 2015. *Decentralized Blockchain Technology and the Rise of Lex Cryptographia*. Working paper. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664

Yermack, D. 2017. Corporate governance and blockchains. *Review of Finance* (forthcoming). doi:10.1093/rof/rfw074

Yuan, Y., and F. Y. Wang. 2016. Towards blockchain-based intelligent transportation systems. In *Proceedings of the IEEE 19th International Conference on Intelligent Transportation Systems (ITSC),* 2663–2668. Available at: http://ieeexplore.ieee.org/abstract/document/7795984/

Zhang, Y., and J. Wen. 2016. The IoT electric business model: Using blockchain technology for the Internet of Things. *Peer-to-Peer Networking and Applications* 10 (4): 983–994.

Zhang, F., E. Cecchetti, K. Croman, A. Juels, and E. Shi. 2016. Town crier: An authenticated data feed for smart contracts. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security,* 270–282. Available at: https://www.researchgate.net/publication/308691770_Town_Crier_An_Authenticated_Data_Feed_for_Smart_Contracts

Zyskind, G., O. Nathan, and A. Pentland. 2015. Decentralizing privacy: Using blockchain to protect personal data. In *Proceedings of the 2015 IEEE Security and Privacy Workshops* (*SPW*), 180–184. Available at: http://dl.acm.org/citation.cfm?id=2867781