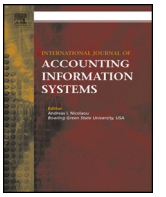
International Journal of Accounting Information Systems 33 (2019) 47–58

Contents lists available at ScienceDirect

International Journal of Accounting Information Systems

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



Establishing the representational faithfulness of financial accounting information using multiparty security, network analysis and a blockchain☆

John McCallig [a,*], Alastair Robb [b], Fiona Rohde [c]

[a] Michael Smurfit Graduate Business School, University College Dublin, Ireland
[b] The University of Queensland Business School, Australia
[c] The University of Queensland Business School and TC Beirne School of Law, Australia

ARTICLE INFO

Article history:
Received 27 October 2017
Received in revised form 26 October 2018
Accepted 11 March 2019
Available online 27 March 2019

Keywords:
Financial reporting
Audit
Faithful representation
Multiparty security
Identity
Public key cryptography
Blockchain
Design science

ABSTRACT

This paper aims to develop a design for an accounting information system that will enhance the representational faithfulness of financial reporting information. One of the functions of financial reporting is to aggregate and report the entity's private data. This paper shows that recognizing that some of the firm's private data is already shared with others allows the methods of multiparty security to be applied to the reporting and audit processes. We contend that using both public key cryptography and network analysis allows the identity of an entity to be modelled as a place on a network. We also develop accounting recordkeeping techniques to balance public access with privacy using a blockchain. Taken together, these three design ideas can enhance the representational faithfulness of financial reporting systems because they use shared data from independent entities, a transparent system, and open-access immutable storage. Faithful representation is enhanced because information from this system can be used by auditors to support their audit opinion or by stakeholders who need credible information about the entity.

1. Introduction

The International Accounting Standards Board's Conceptual Framework for Financial Reporting (IASB) (2018) states that "to be useful, financial information must not only represent relevant phenomena, but it must also faithfully represent the substance of the phenomena that it purports to represent." Both 'relevance' and 'faithful representation' are identified as fundamental qualitative characteristics of the types of information that are likely to be most useful to the users of financial statements (IASB, 2018, p. 15). Relevant financial information is 'capable of making a difference in the decisions made by users,' because it has either predictive or confirmatory value and representationally faithful financial information represents the 'phenomena that it purports to represent' and is 'complete, neutral, and free from error' (IASB, 2018, p. 15).

Christensen (2010) analyses conceptual frameworks from an information perspective and argues that conceptual frameworks' focal point should be accounting's comparative advantage over other information sources. He identifies one of the main characteristics of financial accounting information as being that accounting data are subject to auditing. The objective of this paper is to show that

☆ We thank Gianluca Miscione, Donncha Kavanagh, Sean McGarraghy, Paul Ennis, Eamon Walsh and all the members of the Coding Value Group at UCD for their helpful comments and insights on this paper.

* Corresponding author at: Accountancy Subject Area, UCD Lochlann Quinn School of Business, Belfield, Dublin 4 D04 V1W8, Ireland.
E-mail addresses: John.McCallig@ucd.ie, (J. McCallig), a.robb@business.uq.edu.au, (A. Robb), f.rohde@law.uq.edu.au. (F. Rohde).

https://doi.org/10.1016/j.accinf.2019.03.004
1467-0895/

an accounting information system (AIS) can be developed such that it enhances the representational faithfulness of its accounting data by emulating the audit function.

We use a design science (DS) approach to the development of our proposed AIS. We chose a DS approach as it allows us to use a commonly accepted framework for successfully carrying out research and a model for its presentation (Peffers et al., 2007). DS research, focuses on "how things ought to be in order to attain goals, and to function" (Simon, 1996), "to change existing situations into preferred ones" (Simon, 1996), and making "something created by humans usually for a practical purpose" Geerts (2011). The output of DS research is often referred to as an 'artefact.' Following Peffers et al.'s (2007) framework, we start with the problem identification and motivation, then move to the objective of the solution (Geerts, 2011). Next, we discuss the design and development of our proposed system (Geerts, 2011). As Peffers et al. (2007, p. 55), note "Identified problems do not necessarily translate directly into objectives for the artifact because the process of design is necessarily one of partial and incremental solutions." Consequently, while we evaluate this proposed system in this work, that evaluation is based on alignment with our objectives. Given that many of the ideas in this paper are new we feel they should be fully developed in this paper before moving to a working system.

2. Problem identification and motivation

Stakeholders can find it difficult to establish whether financial reporting information does represent what it purports to because of information asymmetry and agency problems (Jensen and Meckling, 1976). Financial reporting quality and audit quality are often inseparable in terms of observable financial reporting outcomes (Gaynor et al., 2016). For example, Healy and Palepu (2001) identify independent auditors as one mechanism that can increase the credibility of financial disclosures. Auditors access the entity's private information and then report whether this private information faithfully represents the information in the financial statements. Auditors do this in two ways. First, they confirm the entity's private information with outsiders. Second, auditors examine and test the entity's internal controls. Advances in IT systems have allowed auditors to test internal controls on a continuous basis. Continuous testing can improve the quality of estimates and accruals, thus, lowering information risk and potentially mitigating agency problems through increased reliability of the financial statements (Kajüter et al., 2016).

Unfortunately, using auditors to enhance the credibility of financial reporting introduces a new agency problem between the owners of the entity (and other outsiders) and the auditors. This agency problem can arise because auditors may act in the interests of the managers who hire them (Watts and Zimmerman, 1981) and may collude with management in producing reports that do not reflect managers' private information. Stakeholders will find this difficult to detect as audit quality is costly and difficult to assess ex-ante (DeAngelo, 1981). Auditor independence from the managers of the entity mitigates this problem and this issue has been extensively researched in the auditing literature. Church et al. (2015) review this literature and conclude that much experimental evidence suggests that auditors' biases affect their behavior and can negatively affect the audit. Regulatory bodies such as the European Union (European Commission, 2016), the Securities and Exchange Commission (SEC) and the Public Company Accounting Oversight Board (PCAOB) have implemented policies such as the establishment of audit committees, restrictions on non-audit work and auditor rotation to enhance auditors' ability to maintain independence. An audit greatly increases the likelihood that the financial statements will represent what they purport to represent but potentially introduces a new agency problem into financial reporting.

The contribution of this paper is to describe a system that would both provide auditors with better audit evidence to support their opinion and provide stakeholders with credible information about the entity independently from the auditor. We believe that this system can reduce agency costs between stakeholders and the auditor by providing stakeholders with information on some of the inputs to audit decisions and thus reducing the opportunity for bias. However, in this paper we concentrate on the ability of the system to enhance representational faithfulness as part of the audit.

3. Objectives of a solution

The development of fast computers, digital communication channels and unlimited data storage has completely changed many business and social processes. The accounting and auditing professions, however, have been somewhat slow to adopt these technologies in a central role in their processes (Alles, 2015). The possible uses of such technologies in audit and financial reporting have been the subject of substantial research (e.g., Alles, 2015; Cao et al., 2015; Yoon et al., 2015; Krahel and Titera, 2015). Continuous auditing, where audit procedures are applied a short time after a transaction occurs, does take advantage of the digital storage and processing of business information. However, Alles et al. (2006) find that implementations of continuous auditing seem only to "automate existing audit procedures" and that the audit process must be "reengineered" to fully realize the potential of these systems. Alles et al. (2004) argue that continuous auditing may assist with audits that lack information or analysis, but it is "… no more effective than standard auditing in a setting in which managers and auditors collude to deliberately mislead investors." They suggest using a "black box log file" to keep a third-party record of the audit evidence and processes to improve the credibility of the audit.

While advances in auditing techniques and technology will help to better establish the representational faithfulness of financial accounting information, we go further to consider solutions that address this problem in a more direct way. According to the Conceptual Framework, representationally faithful financial information is 'complete, neutral, and free from error.' We consider how these objectives can be met while preserving the privacy of companies' data using an AIS. To limit the scope of our study, we only consider how these characteristics apply to a part of the financial statements, namely receivables.

3.1. Complete

The IASB Conceptual Framework (2018) states that "a complete depiction includes all information necessary for a user to understand the phenomenon being depicted." The 'completeness' component underpins the notion of having accounting information that permits assessment of management's stewardship and to help users assess future cash inflows to the particular entity. In short, the accounting information should be useful for making assessments of management and for guiding resource allocation decisions. In addition, an AIS system designed to provide such accounting information should be able to facilitate understanding of the system by its users. An AIS system should be transparent in that users can understand how information is collected, processed, and reported.

3.2. Neutral

The IASB Conceptual Framework (2018) states that "a neutral depiction is not slanted, weighted, emphasised, de-emphasised or otherwise manipulated to increase the probability that financial information will be received favourably or unfavourably by users." An AIS system designed to provide representationally faithful information should not introduce any bias into the information reported. As discussed above, auditor's incentives are argued to have a detrimental effect on the representational faithfulness of accounting information. We therefore set the elimination of bias as a major objective in the design of our AIS.

3.3. Free from error

The IASB Conceptual Framework (2018) states that "free from error means there are no errors or omissions in the description of the phenomenon, and the process used to produce the reported information has been selected and applied with no errors in the process." An objective of our AIS system is to provide error free information. Rather than sampling receivables, our proposed AIS system intends to use the populations of receivables from firms being audited. We acknowledge that there may remain erroneous entries in firms' accounting data, however, as our proposed system operates at the population level, such erroneous data should be detected by non-agreement with the reciprocal firms' payables (using a fully developed version of our proposed AIS).

3.4. Privacy

Auditors access entities' private information and then publicly report whether this private information faithfully represents the information in the entities' financial statements. Maintaining the privacy of entities' information is both necessary for reasons such as competitive advantage, and also because auditors act as trusted third parties who keep information confidential. By using multiparty security our AIS seeks to ensure information is kept private by carrying out computations without revealing the inputs.

4. Design and development

Commentators on the internet (Grigg, 2005; Tyra, 2014; Brown, 2015), in the accountancy profession (Deloitte, 2016), and in academia (Dai and Vasarhelyi, 2017; Kokina et al., 2017) suggest that accountancy could make use of blockchain (Ethereum, 2015) technology. Fanning and Centers (2016) suggest that using 'a blockchain the accounting entries between two trading partners can easily be compared while maintaining data privacy.' Dai and Vasarhelyi (2017) argue that an illustration of how this can be achieved is missing from the accounting literature. This paper develops a system based on a combination of blockchain technology, multiparty security, and network analysis that theoretically can achieve a solution that meets our objectives. We investigate the suitability of these theoretically well-developed techniques, from the computer science and statistics fields, for emulating the audit process. Given the early stage of research and practice in this area, this paper is exploratory in nature and seeks to generate design ideas applicable to building an AIS for receivables.

This paper aims to design an AIS that can establish the representational faithfulness of information about an entity's receivables. Technologies will be evaluated, selected and combined in a manner that meets the objectives stated above. The techniques of multiparty security will be evaluated, in Section 4.1, as they can assist in sharing information between entities, while preserving privacy. Information sharing also has the potential to establish that information is error-free in a transparent way. Network analysis is evaluated, in Section 4.2, as a way of establishing an entity's identity as a location on a financial network. This part of the system has the potential to ensure that only valid data is used in the system and that the information is error-free. This use of network analysis also increases the 'completeness' of the information in that users get a better understanding of the nature of receivables as the outcome of the firm's dealing with a network of customers. Distributed storage and blockchain technology are evaluated, in Section 4.3, as a new method of public recordkeeping. This has the potential to increase the transparency of the system. Section 5 provides an evaluation of how these techniques can be integrated to form a complete AIS system and a discussion of the practical problems of implementing such a system.

4.1. Information sharing using multiparty security

Information about how much is owed from a customer to a vendor is shared between them. Both parties record this information separately in their own accounting systems. The existence of this shared data allows parallels to be drawn between auditing

and methods of data sharing that have been developed in computer science that aim to replace third parties with computational methods. Secure multiparty computation involves problems where a function is computed from inputs that are scattered amongst different parties, while preserving the privacy of these parties' inputs. The aim of these techniques is to 'emulate' a trusted party that would collect inputs from the parties and compute the function. Goldreich (2013) concludes that "it is possible to construct protocols for securely computing any desired multi-party computation." The difficulty with which these protocols can be developed is dependent on the communication channels used, the extent of adversarial behavior, and the desired level of emulation of the trusted party (Goldreich, 2013).

The techniques of secure multiparty computation are also highly relevant to the problem of establishing the representational faithfulness of financial accounting information. Some financial accounting information is already shared between multiple parties, e.g., a vendor has a list of customers that owe it money for purchases. Each of the customers also stores the information that they owe money to the vendor in their own accounting system. The auditor, who is a trusted third party, takes the vendor's list and confirms a sample of entries with the customers. The auditor then attaches an opinion to a report containing the total of the vendor's list. The use of trusted third party in this way is known as the 'ideal' model (see Fig. 1).

Using the techniques of secure multiparty computation, the vendor could publish the total of what it is owed by customers and have this confirmed by the customers without revealing the individual amounts that are owed, or by using a third party. This method allows the customers to share their data without allowing the other customers to know their balances.

Cramer et al. (2015) explain that this problem can be solved using a tool called secret sharing. Secret sharing provides a way for a party, say customer 1, to spread information on a secret number, in this case their balance, across all the customers such that they together hold full information on the total of the customers' balances, yet no other customer has any information on customer 1's balance. Cramer et al. (2015) go on to explain the mechanics of this procedure as follows. First, a large prime number is chosen by all the customers. In a situation with three customers, customer 1 chooses three random numbers so that the sum of the random numbers modulus the prime number is equal to customer 1's balance. Modular arithmetic is used here so that the total of the random numbers "wrap around" upon reaching the chosen prime number. This means customer 1 could chose very large prime numbers, perhaps 500 digits long, effectively disguising their balance. The random numbers are called the shares of customer 1's balance. Customer 1 sends one random number to customer 2 and the other random number to customer 3 and keeps one random number secret. Fig. 2, below, depicts this process. The customers choose 401 as a prime number and Customer 1 chooses the random number 368 for themselves and 211 for Customer 2 and 318 for Customer 3. The only restriction on choosing these numbers is their sum modulus 401 is customer 1's balance of 95. Customer 1 could have chosen a completely different set of random numbers as long as they meet this restriction. If the prime number and the random numbers are large, then even with knowledge of two out of three of the random numbers and the prime number it is very difficult to work back to Customer 1's balance. This means neither of the other customers can work out customer 1's balance from the random numbers they are assigned, even if they collude with each other.

In step 2 of Fig. 2 each customer repeats customer 1's process and keeps one random number for themselves and sends the others to the other customers. Each customer then adds the random numbers they received from the other customers to their own random number to get a total modulo the prime number. These totals can then be added together to give the total of the customers' balances. In Fig. 2, customer 1 adds their own random number 368, to the random number 90 that was sent to them by customer 2 and to 250 the random number sent by customer 3. The total 708 modulus 401 is equal to 307 which is customer 1's total. Adding this total to the totals for customer 2 and customer 3 gives 1067. Taking 1067 modulus 401 returns the total of the customer's balances 265.

If the customer's totals are published, then anybody with access to the prime number can verify that the total of the list of customers' balances agrees with the customer's records. However, neither the public nor the customers themselves gain any information about the individual customers' balances as long as there are a large number of customers. In this way, multiparty secure computation can emulate the role of a trusted third party like an auditor. However, this procedure would require co-ordination by the vendor so that each customer

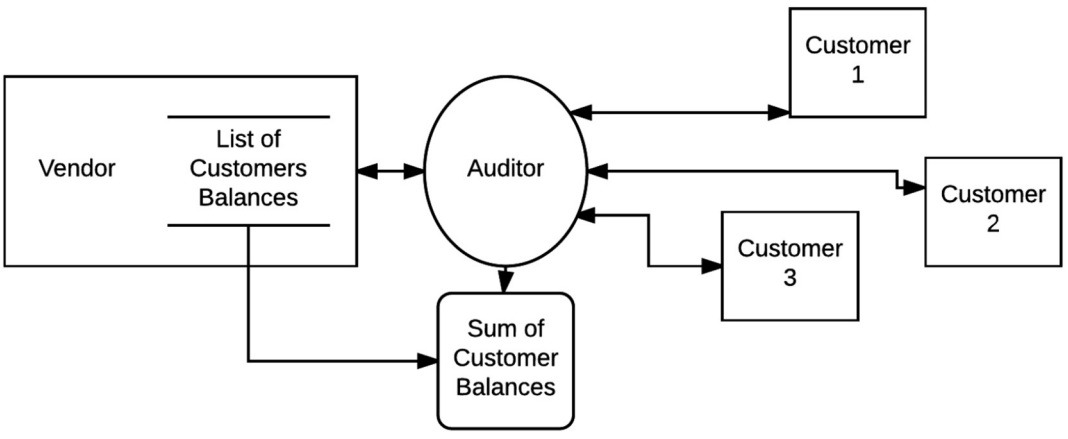


Fig. 1. The ideal model of the audit process for confirmation of customer balances.

Customer Balances	
C_1	95
C_2	88
C_3	82
Total	265

Step 1: The Customers jointly choose the prime 401 (p).

Step 2: C_1 Chooses Random Numbers for C_2 and C_3 so that

r_1 for C_1 (self)	+ r_2 for C_2	+ r_3 for C_3	= r_1 + r_2 + r_3		C_1's Balance
368	211	318	897	mod 401 =	95

C_2 and C_3 do the same

	r_1 for C_1	+ r_2 for C_2	+ r_3 for C_3 =	Total	=	Balance
C_1 chooses	368	211	318	897	mod 401 =	95
C_2 chooses	90	278	121	489	mod 401 =	88
C_3 chooses	250	300	334	884	mod 401 =	82
Total	708	789	773	2,270	mod 401 =	265
	mod 401	mod 401	mod 401			
=	307	388	372	1,067	mod 401 =	265

Step 3: Each customer sends their totals modulo 401 to the Blockchain

	C_1	C_2	C_3	p
Sent to blockchain	307	388	372	401

Fig. 2. Illustration of calculating a secure sum of three customer's balances.

knows the other customers with whom they must communicate. This problem will be addressed in the next section on identity. In addition, the procedure also requires two-way communication between each customer and every other customer. Despite these limitations, multiparty secure computation shows great potential to use information that already exists in accounting systems in new and socially useful ways.

4.2. Managing identity and privacy

In the ideal audit model, the trusted third party (auditors) receives information about the identity of the vendor's customers from the vendor. They then contact the customers directly by letter, phone or email and ask them to confirm their balances. The checking of the identity of the customers, however, often does not go beyond receiving replies on headed paper or receiving a reply to a phone call. Auditors should check business addresses and phone numbers via directories or via the internet, but this is not always the case.

One of the most useful innovations of digital currency, e.g. Bitcoin, has been the successful use of public key cryptography to manage identity using public key cryptography (Diffie and Hellman, 1976). In public key cryptography, each entity generates a private key and a mathematically related public key. The public key can be made public and used to send secure messages to the holder of the matching private key, therefore, verifying that messages came from the holder of the matching private key. Nakamoto (2008) argues that

> "… privacy can still be maintained […] by keeping public keys anonymous. The public can see that someone is sending an amount to someone else, but without information linking the transaction to anyone. This is similar to the level of information released by stock exchanges, where the time and size of individual trades, the "tape", is made public, but without telling who the parties were."

On the Bitcoin system (Nakamoto, 2008), identity is established by using a private key to generate a bitcoin address that is like a public key. The holder of the private key that was used to generate that address (Antonopoulos, 2015) can only access Bitcoins sent to that particular address. A similar protocol could be used for business entities. Each entity would generate a private and public key pair. The public key would serve as their identifier. This key would be made known to their customers and suppliers and would most likely be stored with their account information (i.e., as part of their standing data) in an Enterprise Resource Planning (ERP) system. Only the holder of the matching private key could use this public key. However, the real-world identity of this entity is not visible to the public. In this way, information can be made public and can be used for the public audit of accounting aggregates, without disclosing the identities of the business entities involved.

If business entities were to communicate about their obligations as described in Section 4.1 of this paper, it would be possible to reconstruct the topology of the relationships between the entities. Given each customer sends their identifier, the vendor's identifier and a series of random numbers, analysis of this communication could establish which entities were customers of other entities. The physical and social sciences extensively use network theory to model such systems (Strogatz, 2001). Using the terminology of network theory each business entity is a vertex and a customer relationship is an edge (Kolaczyk, 2009). The relationships between entities have a direction whereby one entity is a customer of the other. Fig. 3 shows a network graph of a vendor (vendor 1) who has a relationship with three customers. The vendor and each customer are shown as vertices (circles) and the relationships as edges (lines between vertices).

Broadening the analysis of the relationships of these three customers with their own customers and other vendors shows Fig. 3 can be extended to reflect these vertices and edges. Fig. 4 extends Fig. 3 to reflect the following information. Customer 1 has three customers (C4, C5, and C6). Customer 2 has three customers (C7, C8, and C9). Customer 2 and C8 are also customers of Vendor 2. Customer 3 has three customers (C10, C11, and C12). C12 is also a customer of Vendor 2.

The topology of the network can be used to establish that a particular private key is linked to a real-world entity by using metrics that measure the centrality of a vertex to the network. These measures were developed in the network analysis literature (Kolaczyk, 2009). Closeness centrality measures how 'close' the vertex is to other vertices and is operationalized as the inverse of the total distance of the vertex from all others (Kolaczyk, 2009). Distance is measured as the shortest path between vertices (geodesic distance). For example, in Fig. 4, C4 is relatively distant from all other network nodes compared to Customer 2. Betweenness centrality summarizes the extent to which a vertex is located 'between' other pairs of vertices. Eigenvector centrality measures use the centrality of the neighbors of a vertex to determine that vertex's own centrality. Table 1 shows these measures for the network drawn in Fig. 4. The measures are calculated without considering the direction of the connections, which seems most appropriate for an attempt to establish whether an entity is part of the network. For the example network, the eigenvector measure captures the data that customer 1 is not central to the network and that customer 2 is the most connected of vendor 1's customers.

Vendor 1 could possibly attempt to mislead this measure of identity by establishing fake customers on the network who would then confirm a fake balance, which could be included in the vendor's list of customer balances. It would be very difficult for vendor 1 to organize other independent entities with established identities on the network to establish connections with this fake customer. The fake customer can be detected by performing a network cut, that is, excluding vendor 1 from the analysis and

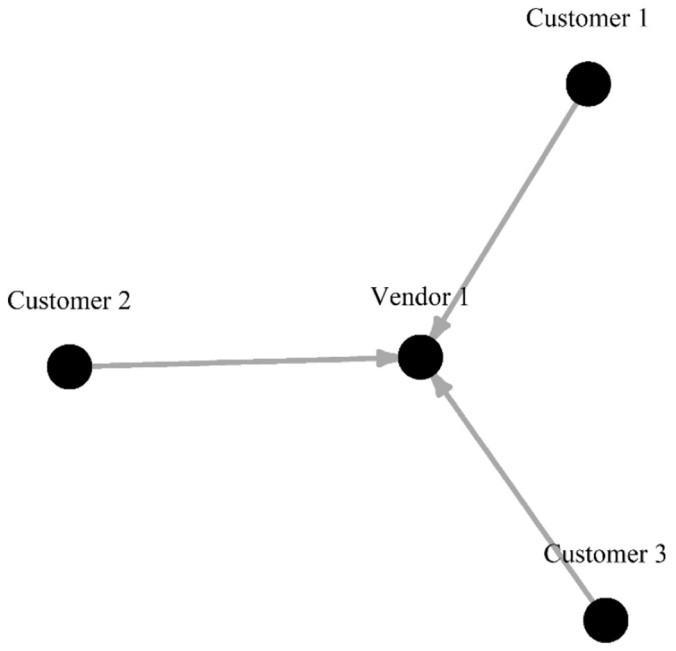


Fig. 3. A network graph of the vendor customer relationship.

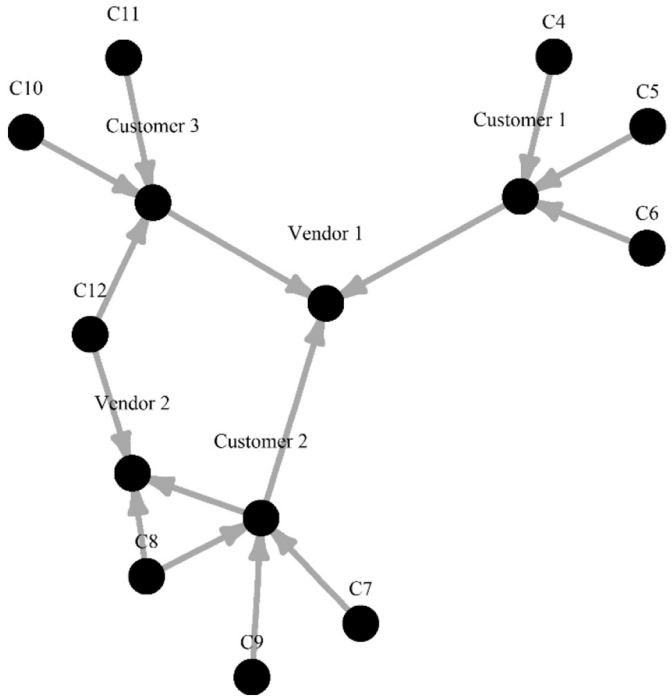


Fig. 4. A network graph of vendor customer relationships with 2 vendors.

examining the network to see whether there are any independent subnetworks. Fig. 5 shows a network graph that excludes vendor 1 indicating that customer 1 is in a subnetwork that may be a creation of vendor 1.

The design decision to model an entity's identity as their place on a network allows us to consider new ways of managing an entity's public and private identity. Financial transactions require that each party to a transaction know the real-world identity of the other parties. The public only need to know that these entities have a real-world existence, and this can be established by locating them on the topology of a financial network. Public key cryptography and the network analysis of financial relationships can help establish the representational faithfulness of financial information by increasing the transparency of the financial network that supports the entity's assertions that they have claims on that network.

4.3. Public recording of accounting information

Accounting record-keeping was revolutionized in the 1970s and 1980s with the introduction of computers to business. Codd (1970) proposed keeping large data banks in a relational database. The translation process from manual double-entry records to relational databases was straightforward and all businesses have adopted this technology as the cost of computer processing power and storage has fallen. These accounting databases evolved into Enterprise Resource Planning (ERP) systems that now

Table 1
Centrality measures for the example network.

	Centrality measure			
	Degree	Closeness	Betweenness	Eigenvector
Vendor 1	3	0.04	46.50	0.71
Customer 1	4	0.03	33.00	0.41
Customer 2	5	0.04	34.50	1.00
Customer 3	4	0.04	28.00	0.57
C4	1	0.02	0.00	0.15
C5	1	0.02	0.00	0.15
C6	1	0.02	0.00	0.15
C7	1	0.03	0.00	0.36
C8	2	0.03	0.00	0.63
C9	1	0.03	0.00	0.36
C10	1	0.03	0.00	0.20
C11	1	0.03	0.00	0.20
C12	2	0.03	4.50	0.47
Vendor 2	3	0.03	5.50	0.75

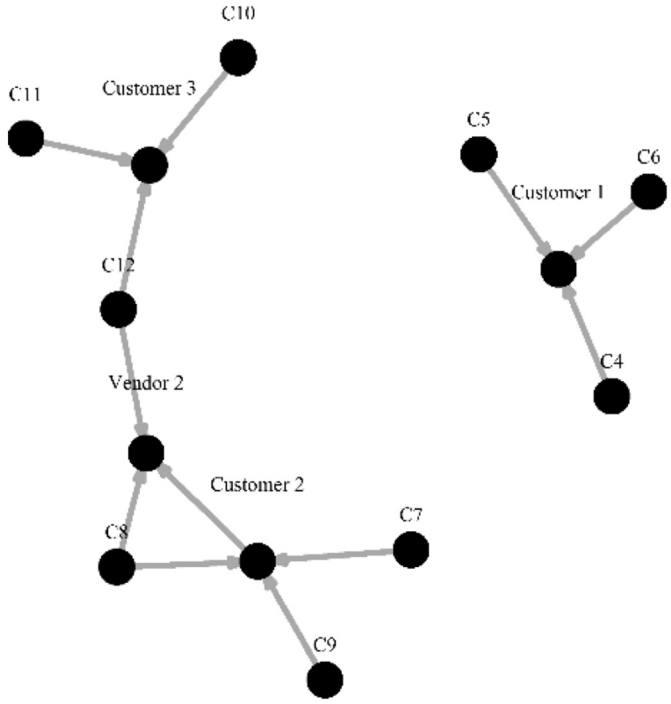


Fig. 5. A network graph excluding vendor 1.

store a wide range of information including accounting records. These systems integrate accounting information with other information such as inventory flows and personnel records that would have been stored separately in the past. The development of relational databases and ERP systems has slowly increased interest in using more advanced data analysis techniques (Vasarhelyi et al., 2015), and continuous auditing (Alles, 2015) with accounting data.

Many distributed systems are used by trusted parties who rely on each other not to record incorrect information or not to maliciously alter the distributed information. Developments in digital currencies, such as Bitcoin, have demonstrated the use of distributed systems that do not rely on trust between the parties. Using a data structure called a blockchain, upon which Bitcoin is based, the distributed system can be made public and opened to any parties whether trusted or not. A blockchain is "an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed" (Nakamoto, 2008). It is innovative in that it relies on a public mechanism that involves expending computing power on solving a tough mathematical problem to establish the integrity of the information. The Bitcoin blockchain relies on economic incentives rather than fiat or trust to keep it operational and functional.

A blockchain is a data structure that contains a chain of blocks of transactions that are linked together in sequence. When a block is added to the blockchain it is linked to the most recently added block (parent block). This means that the sequence of blocks can be established right back to the first block (genesis block) (Antonopoulos, 2015). Blocks are only added to the chain when a consensus is reached amongst the participants. The Bitcoin blockchain operates over a peer-to-peer network where the entire chain of blocks (the blockchain) is transmitted to all the nodes on the Bitcoin network. Allowing many nodes to access this information provides an alternative to the traditional model of a central authority or regulator who controls record-keeping themselves or provides rules as to how it should be carried out. Blocks can only be added to the Bitcoin blockchain using a mechanism based on expending computing power to earn fees and mine new Bitcoins. The system is designed so that it is very difficult for dishonest nodes on the network to gather enough computing power to corrupt the network. The Bitcoin system also provides incentives for honest nodes to keep the system going and to make an adequate return from their efforts. Permissioned blockchains such as Hyperledger Fabric use identity to secure the blockchain in situations where there is more trust between the participants.

The potential of the blockchain to change how business records are stored and interact with each other has been widely recognized. This technology can also be called a 'Distributed Ledger' and the Bank of England has argued that this distributed approach to record keeping is not limited to payment systems like Bitcoin (Bank of England, 2014). For example, the R3 Corda project (Brown, 2016) is an alliance of the world's largest financial institutions that aims to realize the benefits of distributed ledger technology in the financial services industry. Deloitte (2016) have also identified blockchain technology as viable for storing accounting transactions. Ethereum (2015) have developed open access software that provides public access to a blockchain. Coyne and McMickle (2017) argue that the Blockchain is not suitable for accounting as "economic transactions exist outside of accounting records." However, our use of the blockchain is different from theirs in that we use it for recording and verifying aggregate financial reporting information rather than processing and verifying individual transactions.

The design of our AIS recognizes that it is useful to store some accounting records in a distributed system such as a blockchain as this will address some of the problems of managing public and private accounting information. Multiparty computations of accounting aggregates can be stored on a distributed system using public keys as an identifier. This would allow public access to enough information to verify the aggregates without compromising the identities and financial dealings of the entities involved. Fig. 6 illustrates this procedure. Each customer would store their totals from Fig. 2, the public key of the vendor and a signature with their own private key on a blockchain. The auditor or any stakeholder could search the blockchain for information relating to the vendor's balances and assemble the aggregate of the vendor's customer list without gaining any information on the real-world identity of the customers or their individual balances. Network analysis could be used to establish that the customers had a real-world existence using their position on the wider financial network. Using a distributed system like a blockchain will enhance the representational faithfulness of financial reporting by providing transparent, open access and immutable storage of the evidence supporting an entity's assertion that they have claims on other entities.

5. Evaluation

In this section we discuss how our AIS could be implemented and how integrating the three technologies could provide representationally faithful financial information, while ensuring its privacy.

The system could be implemented as follows. At the end of each reporting period the vendor would analyze their list of receivables and contact each one to confirm balances. This process should already be part of the internal controls of the organization. The vendor would have chosen a public key and communicated it to each of its customers. This could be stored in an ERP with the rest of the vendor's information. Likewise, each customer would have chosen a public key and communicated this with the vendor. The vendor would then communicate a list of all its customers' public keys to each customer. Each customer would use the techniques of multi-party security to share its balance amongst all the other customers. This process could be entirely automated within the ERP and be as transparent to the user as the SSL transactions that enable a secure http connection. Using smart contracts on the blockchain is another alternative for this information exchange but is beyond the scope of this paper. Each customer then computes the totals of the shares that have been sent to them and send this number with their own public keys and the public key of the vendor to the blockchain. Again, this process can be automated within an ERP. The auditor could use the information on the blockchain, network analysis and their knowledge of the entity's customer balances as audit evidence. Any interested stakeholder can also analyze the information that has been recorded on the blockchain to confirm the total of receivables that appears in the financial statements.

Table 2 and the discussion below summarizes how the technologies discussed in the design section integrate to achieve the three objectives of the system.

5.1. Free from error

Many different parties who are independent from the firm's management must co-operate to compute the aggregate of the information. This approach removes the need to only examine a sample of customer balances and thus ensure the total is a more faithful representation of the amount presented in the financial statements. Further, by using the AIS's network capabilities,

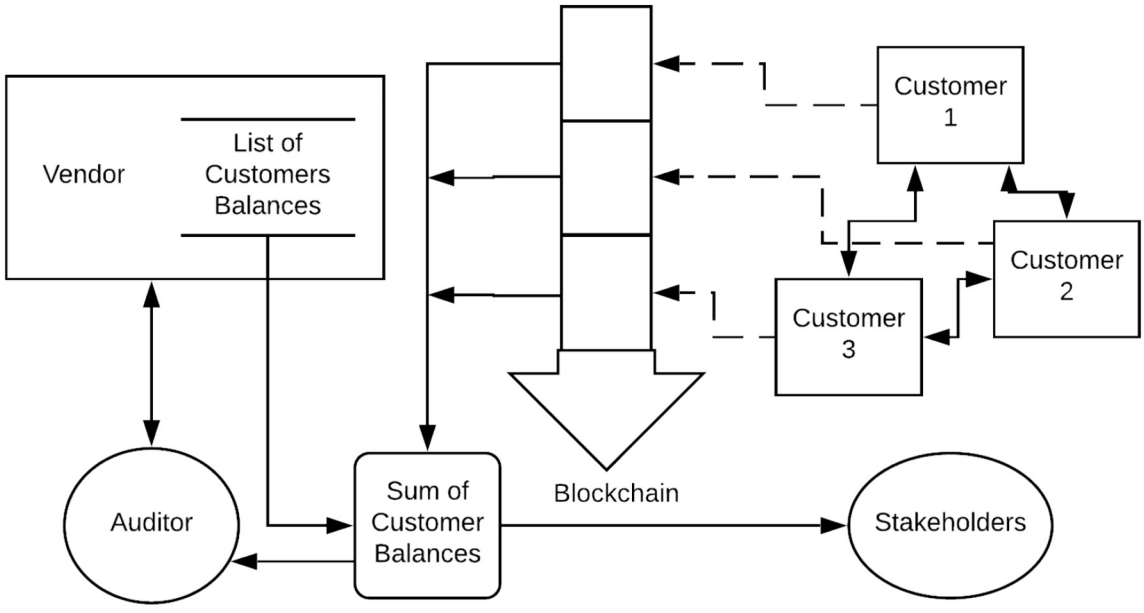


Fig. 6. The real model of a secure audit process with data stored on a blockchain.

Table 2
Achieving the design goals of a receivables AIS.

Design goal: Information should be:	Technology		
	Multiparty security	Public key cryptography and network analysis	Blockchain
Free from error	All account balances can be confirmed All customers must use the system or receivables will not be confirmed.	Fake receivables can be detected by examining their connections on the network	Blockchain is immutable so data cannot be added later
Complete	The system is transparent to the user. The nature of the information and how is has been processed is disclosed by opening the system itself.		
Neutral	The system is neutral in its operation. There is no trusted third party who can use the system for their own benefit and present biased information		

phantom or fraudulent participants can be uncovered, reducing the likelihood of errors in the aggregate of receivables. Finally, by using blockchain technology and its distinctive tamper-evident characteristic, any attempts to alter or add data to that already received will be apparent.

5.2. Complete

A complete depiction includes "all information necessary for a user to understand the phenomenon being depicted" (IASB, 2018). However, the audit is an 'obscure' process (Power, 1997) which is difficult to explain or understand. The techniques described above may be technically complex, but they are deterministic, and the process is transparent. Users can observe the flow of information onto the blockchain and verify the receivables balances themselves. This means that sophisticated users can evaluate the validity of the information produced by the system by observing and participating in the system themselves.

5.3. Neutral

The process described, above, removes the risk of the auditor not carrying out their work or colluding with management in suppressing their findings, thus enhancing the credibility of the audit and the audited financial information. Rather than relying on samples of data produced by the entities being audited, or merely phoning those concerned to verify receivables, the nature of this proposed AIS is such that human involvement is eliminated. By eliminating human involvement, as far as possible, audit reports should be free from possible bias.

5.4. Privacy

We have made much of the privacy benefits of the proposed AIS via the process of accessing entities' private information and reporting whether this private information faithfully represents the information in the financial statements. Privacy, while a desirable component of any audit related activity is, however, not an explicit component of representational faithfulness, therefore, we have not included it as a design goal. While not a design goal, our proposed AIS does offer, at least, the following three privacy related benefits. First, multiparty security computations can be carried out without revealing the inputs therefore maintaining the privacy of financial information. Second, individual account balances can be kept private while providing public access to total balances. Third, customer identities are private with data on the blockchain only able to be used to establish totals of receivables.

6. Conclusion

This paper aims to design an information system that would enhance the representational faithfulness of financial reporting information. It reviews advances in the management of public and private information that have been developed, and applied to problems in other disciplines, and adapts them to the financial reporting environment. These techniques provide alternative models that can address the information asymmetry and agency problems inherent in financial reporting and audit.

First, this paper shows that recognizing that some of the firm's private data is already shared with others allows the application of the methods of multiparty security to establish the representational faithfulness of financial reporting information. Second, using public key cryptography and network analysis, an identity for an entity is developed. Drawing on ideas from social network analysis, identity is established using location on a network rather than legal status. Using public key cryptography, the privacy of the real-world identity of counterparties to transactions can be concealed while still publicly disclosing their location on the financial network. Finally, the existing concepts of accounting recordkeeping are developed to balance public access with privacy using a blockchain.

Bringing together developments in distributed storage with multiparty computation and network analysis allows us to start to consider the financial reporting systems of the future. These systems will enhance the representational faithfulness of financial reporting in three main ways. First, the information will be provided by many entities, independent from the reporting entity, that together hold the necessary information to confirm the entity's claims. Second, the financial network and accounting process that supports the entity's claims will be more transparent to the users of the information. Third, the information will be stored on a blockchain that uses a transparent and public method of recording and cannot be altered. Together, these concepts will reduce

the agency costs inherent in financial reporting and audit and enhance the credibility and transparency of the financial reporting system.

This paper is limited in several ways. First, it only considers one part of the auditing process namely receivables. Although this implies that companies using this system could also use it for their payables. Second, it does not consider the many practical challenges in implementing such a system. As described above, the system involves communication between all of the firm's customers which would involve considerable digital co-ordination. Third, it is not clear who would run the blockchain necessary for this design. Fourth, there are many regulatory challenges of developing such a system. Nevertheless, this paper provides a high-level design that can enable further research to focus on these practical issues and design improvements.

Further research is required on developing these designs further, building more elaborate models and building a working system. Such further research could explore the applicability of the proposed system to other areas that, as a part of an audit, require confirmation, e.g., accounts payable. The next research goal should, perhaps, be to explore various implementation methods for the design in this paper, e.g., an Ethereum blockchain using simulated data. This would allow research to explore the practical requirements of the system and to identify its advantages. Further research is also required on how the AIS system described in this paper could provide better information for society. Credit flow within the economy depends on good quality information and this system may be able to provide such information at low cost. A system that focuses on public information needs would undoubtedly require Government, political, and professional association support which would require further research on the social value of such a system.

This paper contributes to the academic literature and industry discussion on how new technologies can enhance the representational faithfulness of financial accounting information. It does this by considering how theoretically well-developed techniques, from the computer science and statistics fields, could emulate and strengthen the audit process. It is essential that accounting academics and industry inform this discussion given that ubiquitous computing power, fast communications and powerful analysis capabilities are exerting great pressure to re-examine financial reporting processes and the accountancy profession.

References

Alles, M., 2015. The drivers of the adoption and facilitators of the evolution of Big Data by the audit profession. Account. Horiz. 29 (2). https://doi.org/10.2308/acch-51067.

Alles, M., Kogan, A., Vasarhelyi, M., 2004. Restoring auditor credibility: tertiary monitoring and logging of continuous assurance systems. Int. J. Account. Inf. Syst. 5 (1), 183–202. https://doi.org/10.1016/j.accinf.2004.01.010.

Alles, M., Brennan, G., Kogan, A., Vasarhelyi, M., 2006. Continuous monitoring of business process controls: a pilot implementation of a continuous auditing system at Siemens. Int. J. Account. Inf. Syst. 7 (2), 137–161. https://doi.org/10.1016/j.accinf.2005.10.004.

Antonopoulos, A., 2015. Mastering Bitcoin. O'Reilly Books, Sebastopol, CA.

Bank of England, 2014. Quarterly Bulletin. Q3.

Brown, R.G., 2015. Cost? Trust? Something Else? What's the Killer App for Block Chain Technology?. Available at. https://gendal.me/2015/01/15/cost-trust-something-else-whats-the-killer-app-for-block-chain-technology/

Brown, R.G., 2016. Introducing RC Corda™: A Distributed Ledger Designed for Financial Services. Available at:. http://r3cev.com/blog/2016/4/4/introducing-r3-corda-a-distributed-ledger-designed-for-financial-services.

Cao, M., Chychyla, R., Stewart, T., 2015. Big Data analytics in financial statement audits. Account. Horiz. 29 (2). https://doi.org/10.2308/acch-51068.

Christensen, J., 2010. Conceptual frameworks of accounting from an information perspective. Account. Bus. Res. 40 (3), 287–299. https://doi.org/10.1080/00014788.2010.9663403.

Church, B.K., Jenkins, J., McCracken, S., Roush, P., Stanley, J., 2015. Auditor independence in fact: research, regulatory, and practice implications drawn from experimental and archival research. Account. Horiz. 29 (1). https://doi.org/10.2308/acch-50966.

Codd, E.F., 1970. A relational model of data for large shared data banks. Commun. ACM 13 (6). https://doi.org/10.1145/362384.362685.

Coyne, J., McMickle, P., 2017. Can blockchains serve an accounting purpose? J. Emerging Technol. Account. https://doi.org/10.2308/jeta-51910 In-Press.

Cramer, R., Damgård, B., Nielsen, J., 2015. Secure Multiparty Computation and Secret Sharing. Cambridge University Press, Cambridge, U.K.

Dai, J., Vasarhelyi, M., 2017. Towards blockchain-based accounting and assurance. J. Inf. Syst. https://doi.org/10.2308/isys-51804 In-Press.

DeAngelo, L., 1981. Auditor size and audit quality. J. Account. Econ. 3 (3), 183–199.

Deloitte, 2016. Blockchain Technology: A game-changer in accounting? Available at https://www2.deloitte.com/content/dam/Deloitte/de/Documents/Innovation/Blockchain_A%20game-changer%20in%20accounting.pdf

Diffie, W., Hellman, M., 1976. New directions in cryptography. IEEE Trans. Inf. Theory 22 (6), 644–654. https://doi.org/10.1109/TIT.1976.1055638.

Ethereum, 2015. A Next Generation Smart Contract and Decentralized Application Platform, Ethereum White Paper. Available at:. https://github.com/ethereum/wiki/wiki/White-Paper.

European Commission, 2016. Reform of the EU Statutory Audit Market - Frequently Asked Questions. Available at. http://europa.eu/rapid/press-release_MEMO-16-2244_en.htm.

Fanning, K., Centers, D., 2016. Blockchain and its coming impact on financial services. J. Corp. Acc. Financ. 27 (5), 53–57. https://doi.org/10.1002/jcaf.22179.

Gaynor, L., Kelton, A., Mercer, M., Yohn, T., 2016. Understanding the relation between financial reporting quality and audit quality. Audit. J. Pract. Theory 35, 1–22. https://doi.org/10.2308/ajpt-51453.

Geerts, G., 2011. A design science research methodology and its application to accounting information systems research. Int. J. Account. Inf. Syst. 12, 142–151.

Goldreich, O., 2013. General cryptographic protocols: the very basics. In: Prabhakaran, M.M., Sahai, A. (Eds.), Secure Multi-party Computation. 1–24. IOS Press, Amsterdam, the Netherlands.

Grigg, I., 2005. Triple Entry Accounting. Available on. http://iang.org/papers/triple_entry.html.

Healy, P., Palepu, K., 2001. Information asymmetry, corporate disclosure, and the capital markets: a review of the empirical disclosure literature. J. Account. Econ. 31, 405–440. https://doi.org/10.1016/S0165-4101(01)00018-0.

International Accounting Standards Board (IASB), 2018. Conceptual Framework for Financial Reporting, Chapter 1, "The Objective of General Purpose Financial Reporting," and Chapter 2, "Qualitative Characteristics of Useful Financial Information." (London, United Kingdom).

Jensen, M., Meckling, W., 1976. Theory of the firm: managerial behavior, agency costs and ownership structure. J. Financ. Econ. 13, 305–360.

Kajüter, P., Klassmann, F., Nienhaus, M., 2016. Do reviews by external auditors improve the information content of interim financial statements? Int. J. Account. 51, 23–50.

Kokina, J., Mancha, R., Pachamova, D., 2017. Blockchain: emergent industry adoption and implications for accounting. J. Emerging Technol. Account. https://doi.org/10.2308/jeta-51911 In-Press.

Kolaczyk, E., 2009. Statistical Analysis of Network Data Methods and Models. Springer, New York, NY.

Krahel, J.P., Titera, B., 2015. Consequences of big data and formalization on Accounting and Auditing Standards. Account. Horiz. 29 (2). https://doi.org/10.2308/acch-51065.

Nakamoto, S., 2008. Bitcoin: A Peer-to-Peer Electronic Cash System. Available at. https://bitcoin.org/bitcoin.pdf.
Peffers, K., Tuunanen, T., Rothenberger, M., Chatterjee, S., 2007. A design science research methodology for information systems research. J. Manag. Inf. Syst. 24 (3), 45–77.
Power, M., 1997. The Audit Society: Rituals of Verification. Oxford University Press, Oxford.
Simon, H., 1996. The Sciences of the Artificial. 3rd ed. MIT Press, Cambridge, MA.
Strogatz, S., 2001. Exploring complex networks. Nature 410. https://doi.org/10.1038/35065725.
Tyra, J., 2014. Triple entry bookkeeping with bitcoin. Bitcoin Magazine 2014 February 10. Available at. http://bitcoinmagazine.com/9969/triple-entry-bookkeeping-bitcoin.
Vasarhelyi, M., Kogan, A., Tuttle, B., 2015. Big data in accounting: an overview. Account. Horiz. 29 (2). https://doi.org/10.2308/acch-51071.
Watts, R., Zimmerman, J., 1981. The Markets for Independence and Independence Auditors. Working Paper. University of Rochester, Rochester, NY.
Yoon, K., Hoogduin, L., Zhang, L., 2015. Integrating different forms of data for audit evidence: markets research becoming relevant to assurance. Account. Horiz. 29 (2). https://doi.org/10.2308/acch-51076.