International Journal of Accounting Information Systems xxx (xxxx) xxx–xxx

Contents lists available at ScienceDirect

International Journal of Accounting Information Systems

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

Designing confidentiality-preserving Blockchain-based transaction processing systems☆

Yunsen Wang[a,b], Alexander Kogan[a,*]

[a] Rutgers, The State University of New Jersey, Department of Accounting and Information Systems, One Washington Park, Newark, NJ 07102-3122, United States of America

[b] Southwestern University of Finance and Economics, Chengdu 611130, China

ARTICLE INFO

Keywords:
Blockchain
Transaction processing systems
Continuous monitoring
Information confidentiality

ABSTRACT

Blockchain is one of the most disruptive and promising emerging technologies, and it appears to have the potential for significantly affecting the accounting and auditing fields. Using blockchain technology, zero-knowledge proof, and homomorphic encryption, this paper presents a design for a blockchain-based transaction processing system (TPS) and develops a prototype to demonstrate the functionality of the blockchain-based TPS in real-time accounting, continuous monitoring and fraud prevention. The computational performance of a blockchain-based TPS versus relational databases is evaluated and discussed. In anticipation of the wider applicability of blockchain technology to support enterprise information systems and continuous monitoring systems, this paper presents an innovative design that utilizes the advantages of blockchain technology while overcoming some of the key barriers to its adoption.

1. Introduction

The topics of continuous financial disclosure and publicly shared databases have been discussed ever since the 1970s (Pastena, 1979). Today's business ecosystems demand information sharing and data communication to improve trading efficiency and effectiveness. However, there is a trade-off between transparency and confidentiality: the more information is shared, the more transparent the business will be, and the more potential for business secrets[1] and confidentiality to be compromised. The trade-off between information transparency and data confidentiality is one of the tension points of today's business: cooperation versus competition (Bengtsson and Kock, 2000).

Blockchain is one of the most disruptive and promising emerging technologies, and it appears to have the potential for significantly affecting the accounting and auditing fields. Essentially, blockchain is a freely open and publicly shared database that keeps track of transactions and protects data from tampering (Iansiti and Lakhani, 2017; Yermack, 2017; Dai and Vasarhelyi, 2017). Once a transaction is committed, it is practically irreversible and immutable unless the majority of the blockchain users collude[2] (Nakamoto,

☆ Acknowledgement: The authors are thankful to Miklos A. Vasarhelyi, Michael Alles, Graham Gal, Hussein Issa, Uday Murthy, Robert Reimer, and the participants of the 26th Annual Research Workshop on Strategic and Emerging Technologies, 2017 Annual Meetings of the American Accounting Association, the UWCISA's 10th Biennial Symposium and the Ph.D. seminar at Rutgers University for useful comments. The authors are also thankful for the financial support from Rutgers Business School.

* Corresponding author.
E-mail addresses: yunsen.wang@rutgers.edu (Y. Wang), kogan@business.rutgers.edu (A. Kogan).

[1] Such as, pricing strategy, trading partner information, business process details.

[2] The most infamous potential risk is known as “51% attack”. In hypothetical, a group of blockchain users who control more than 50% of the network's computing power would be able to reverse the completed transactions and alter transaction history. http://www.coindesk.com/ahead-bitcoin-halving-51-attack-risks-reappear/. Accessed 4/5/2018 4:14 PM.

https://doi.org/10.1016/j.accinf.2018.06.001

2008). Blockchain technology provides a method to share a database among the participants even if they do not trust each other, and it creates a marketplace to transfer assets based on a peer-to-peer network without a central authority.

Blockchain technology has attracted significant investment from venture capitalists, multi-national bankers, and attention from regulators. Nasdaq announced in December 2015 that issuers could make securities transactions on its private blockchain (Nasdaq, 2015). Sydney Stock Exchange (SSX)'s first blockchain prototype was launched in May 2016, which is "*their first step toward an instantaneous settlement-and-transfer-upon-trade*" exchange platform (Rizzo, 2016). Meanwhile, the exploration of blockchain applications by audit firms could improve audit efficiency and effectiveness (PwC, 2016; Deloitte, 2016; EY, 2016; KPMG International, 2017). The convergence of accounting and blockchain technology shows great promise for reducing redundant manual effort, increasing the speed of transaction settlement, and preventing financial reporting fraud. It could drastically change the way of corporate finance and governance just as the 1933 and 1934 Securities and Exchange Acts did (Yermack, 2017).

However, one of the challenges impeding the adoption of blockchain is that firm's managers are concerned about their financial confidentiality and business secrets because all participants in a public blockchain have a full copy of every transaction. The more nodes[3] are added to a network, the more reliable the data are, and the less confidential the blockchain is. This concern led to the development of private blockchains in which only permitted parties[4] can read records and create transactions. Although a private blockchain provides a relatively closed, secure business environment, it sacrifices data transparency and public participation, which could limit its tamper resistance because the managers have full control over the private blockchain. Therefore, the tamper resistance of private blockchain cannot be guaranteed if management is able to manipulate the transaction data for personal gain. The dilemma of adopting blockchain in accounting and auditing is to find the trade-off between information confidentiality and transparency. A choice has to be made between a private blockchain with diminished tamper resistance and a public blockchain exposed to the risk of a confidentiality breach.

To apply blockchain for accounting and auditing and preserve its confidentiality, we propose a framework design - a Blockchain-based transaction processing system (Bb-TPS) - using zero-knowledge proof (ZKP). The ZKP is a cryptographic method by which one party can prove to the other parties that the initiated transaction is valid without releasing any sensitive information. For example, a transaction initiator can prove to the transaction verifiers that his/her transaction is valid without releasing the identity of the trading partners and transaction amounts. We also describe the application of homomorphic encryption in Bb-TPS, which is an encryption algorithm that allows complex mathematical operations to be done on encrypted data (Gentry, 2009). The Bb-TPS we propose can provide real-time accounting and continuous monitoring services, prevent transaction fraud, and deliver guaranteed confidentiality protection.

The remainder of the study is organized as follows: Section 2 motivates this study and introduces the background of blockchain technology, Section 3 proposes a framework of applying blockchain technology to designing real-time accounting and continuous monitoring systems, Section 4 provides a prototype of the framework and evaluates the performance, and Section 5 concludes the paper and discusses future studies.

2. Motivation and background

2.1. The dilemma: transparency and confidentiality

The objective of Nakamoto's (2008) Bitcoin protocol is to create an online payment system without needing a trusted central authority to prevent fraudulent transactions. Based on a peer-to-peer network, this protocol allows all users to get involved in updating (i.e., initiating a new transaction) and maintaining (i.e., mining a new block) the shared database (i.e., blockchain). Therefore, all users have access to every transaction's detail, such as the sender, recipient and amount. Although the Bitcoin protocol uses cryptographic algorithms (e.g., hash function) to anonymize a user's information, it is still vulnerable to privacy attacks. While the direct disclosure of crypto-wallets' personally identifiable information (PII) is not harmful since the information is sanitized, the transactional level details could allow inferences to be made (Gal, 2008). "*The unprecedented transparency of transactions sits uneasily with the privacy needs…*" (Shubber, 2016). For example, if a firm voluntarily discloses all of its transaction details on the blockchain, its rivals will have access to the firm's proprietary information, such as pricing strategy and customer base. The objective of adopting blockchain is to reduce the cost of information integrity protection and guarantee nearly certain verifiability of transactions.

However, the public disclosure of all transactions presents a significant security and privacy risk for most organizations. Therefore, some firms have sought to deploy the blockchain protocol within a secure and closed network, which is the so-called private blockchain. A private blockchain is based on the blockchain protocol that allows only permitted parties to have access to all the transactions (Yermack, 2017).[5] There will inevitably be a central authority that maintains the private blockchain and manages the permissions of participants, which concentrates the operational risk in a single or several points of failure and loses the primary advantage of blockchain – decentralization. More severely, if a dishonest manager is in charge of the central authority, s/he is capable of retroactively manipulating the private blockchain for personal gain. The irreversibility and tamper resistance could not be guaranteed in a private blockchain if the central authority is corrupt. The dilemma of adopting blockchain in accounting and auditing

[3] In the peer-to-peer network system, every participant using a computer to access the network is called a node.

[4] For example, if an organization or a select number of organizations own a private blockchain, only the employees within these organizations are allowed to participate in the blockchain transactions.

[5] Alternatively, instead of using private blockchains, firms may share certain information on the public blockchain relying on the standard encryption procedures and public key infrastructure to protect confidentiality.