ARTICLE IN PRESS

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.

is to find the trade-off between information transparency and confidentiality. With more participants in a blockchain, more business data would be publicly shared; however, business confidentiality and secrets would be protected to a lesser extent. In this paper, we propose a solution to enabling the adoption of blockchain for accounting practice and ensuring that only permitted parties (e.g., auditors and regulators) can view sensitive, proprietary transaction data.

2.2. Bitcoin, smart contracts, and sidechains

Bitcoin is a peer-to-peer electronic currency system first introduced by Satoshi Nakamoto in 2008. Based on cryptographic algorithms (e.g., digital signature and hash function), Bitcoin uses transaction history to prove ownership and public confirmation to prevent double spending. The transaction history is recorded into an ongoing chain of blocks and shared with all users along the peer-to-peer network (Nakamoto, 2008). Each of the recent transactions is publicly announced and confirmed; then the confirmed transactions are written into a new block to be added to the end of the blockchain. As it is practically impossible to rebuild the entire blockchain by one or several dishonest users, the immutable blockchain will serve as the proof of all transactions included in the blockchain. Ethereum[6] is not only a kind of cryptocurrency but also a platform for running smart contracts encoded in blockchain (Buterin, 2014). A smart contract is a computerized self-executing protocol that enforces the execution of a predefined contract in a real-time manner (Szabo, 1994). Before the emergence of the blockchain, a smart contract relied on a trusted third party to program the terms into a contract. The Ethereum project enables all users to deploy and use smart contracts in a decentralized business network.

Every digital coin in blockchain is a token. The concept of "colored coins" refers to a class of digital coins for "representing and managing real-world assets" in the blockchain. A coin color dictionary could be distributed on the blockchain so that all the participants will use the same color consistently. For example, a yellow coin could represent a Bitcoin or a U.S. dollar, a green coin could represent raw materials, and an orange coin could represent a finished product. Therefore, mapping real-world business activities onto a blockchain network would need a massive amount of digital coins. Besides, an increasing number of blockchains are created to support the circulation of colored coins. How could these blockchains communicate with each other? Back et al. (2014) propose "pegged sidechains" to enable Bitcoins and other blockchain coins to be transferred between multiple blockchains, making it easy for multiple blockchains to interoperate with each other. The "pegged sidechains" technique creates a channel in which different coins can be exchanged, which gives existing users access to new blockchain protocols using the coins they already own. For example, a Bitcoin user can give up two Bitcoins in exchange for 60 Zcashs, and vice versa. As shown in Fig. 1, there are four blockchains among which α, β, and γ Sidechains need to communicate with the Main Blockchain. For example, when a β Sidechain user wants to transfer several β coins from β Sidechain to a Main Blockchain user, s/he can send the β coins to a special address where his/her β coins are locked up. In return, s/he would receive some Main Blockchain coins. The amount of coins will be based on the conversion rate between the β coin and the Main Blockchain coin. After receiving the Main Blockchain coin, s/he can transfer the coins to another user on the Main Blockchain.

3. Blockchain for accounting: a confidentiality-preserving design

3.1. Blockchain-based transaction processing systems

The deployment of an enterprise information system, such as SAP, increases the speed of business integration by connecting a firm with outside trading partners. Blockchain technology brings another wave of upgrading the management information systems and the business ecosystems. Based on blockchain technology, this paper proposes a design of Blockchain-based Transaction Processing System (Bb-TPS) and demonstrates the functionality in real-time accounting (Rezaee et al., 2000; Yermack, 2017). For example, in a blockchain-based business ecosystem, assets and resources (e.g., raw materials, inventory of finished goods, employee labor) have been defined and tokenized[7] in the blockchain. A supplier sends "raw materials" coins along with the raw materials to a manufacturer and will receive "cash" coins as payment. After the raw materials are turned into finished goods, the firm sells the products to a customer by sending a "product" coin along with the product and receiving "cash" coins as payment. Alternatively, the contractual terms, such as cash on delivery (COD), can be encoded in a smart contract to enforce the rule that the customer makes a payment at the time of product delivery.

Fig. 2-1 shows in a procurement-to-payment cycle a supplier sends "raw-materials" coins (e.g., wood) to a manufacturing firm M, which triggers four journal entries for two economic entities. For simplicity, we focus on firm M's accounting processes. When firm M receives the "raw-materials" coins, Bb-TPS automatically generates two electronic entries with the same amount of which one debits

[6] https://www.ethereum.org. Accessed 5/23/17 10:20 PM.

[7] With a tracking device (e.g., GPS, RFID), a real-world asset can be mapped onto a blockchain network and be represented by a colored coin or a token. The process of binding a class of real-world assets to a token is called asset tokenization. A wide implementation of Bb-TPS could start from many small blockchain networks in local business ecosystems formed by regulators, business associations, and companies along the supply chains. Then, a set of small blockchains could be connected via the sidechain technique (Back et al., 2014). Asset tokenization could also start with issuing tokens linked to high-value real-world assets, such as automobiles. As technology improves and tokenization cost decreases, many less expensive assets will be gradually taken into consideration for digitizing property records. Intangible assets, such as technology patents, music copyrights and software licenses, can be easily programmed into blockchain represented by a colored coin. As for tangible assets such as land, if the titles are encoded in blockchain, the process of buying and selling a piece of land can be simplified as the seller sends a "land" coin to the buyer.

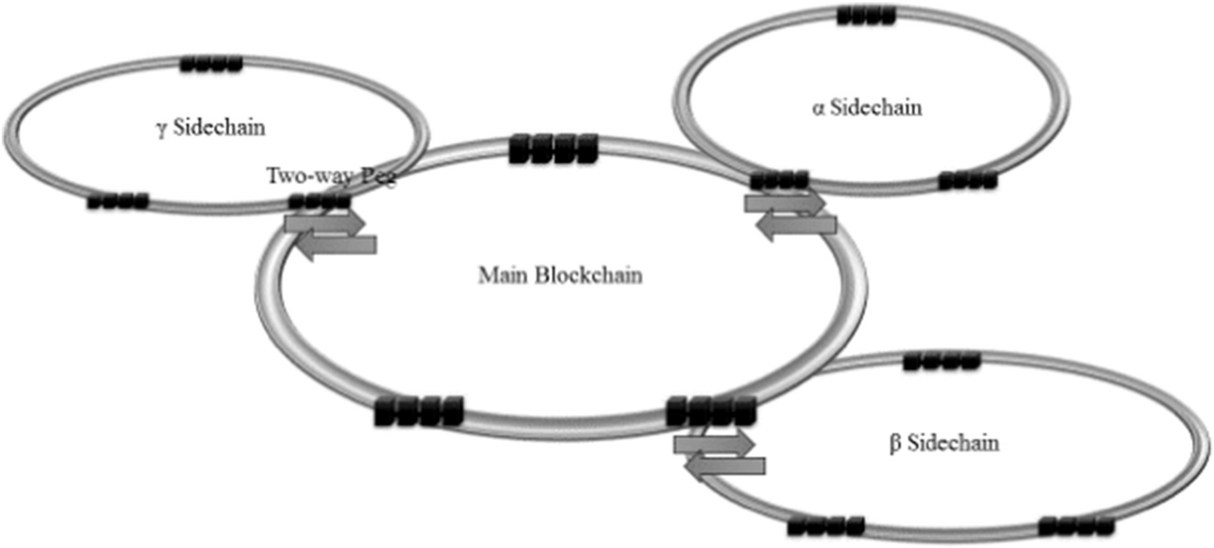


Fig. 1. Blockchain and sidechains.
Source: Back et al., 2014.

the raw materials account and the other one credits accounts payable. After firm M has received the raw materials and checked the quality and quantity of the goods, it could disburse "cash" coins to the supplier, which generates two more electronic entries of which one debits accounts payable, and the other one credits cash. Fig. 2-2 shows in an order-to-cash cycle firm M sells finished goods (e.g., a table) to a customer, which triggers four journal entries for two economic entities. When the customer is sent the "table" coins, Bb-TPS automatically generates two electronic entries with the same amount of which one debits cost of goods sold, and the other one credits inventory. Then, the customer pays for the table with a credit card, which generates another three electronic entries of which one debits cash, one debits credit card expenses, and the third one credits sales revenue.

In addition to inter-organizational transactions, Bb-TPS can also be a communication platform within a firm. In Fig. 2-3, firm M is a conglomerate firm whose subsidiaries form a complete industry value chain (e.g., from petroleum exploration and refinement to gas retail). Bb-TPS would link headquarter and subsidiaries and record intra-organizational transactions. From raw materials to finished goods, Bb-TPS needs to keep records of the manufacturing process of a plant. In this process, more than one type of coins is consumed and transformed into another type of coin. For example, "raw-materials" coins are transformed to "finished-product" coins. In Fig. 2-3, subsidiary A of firm M provides raw materials to another subsidiary B, and subsidiary B delivers finished goods to subsidiary C. For simplicity, we focus on the subsidiary B's accounting processes. When subsidiary B receives the "raw-materials" coins, Bb-TPS automatically generates two electronic entries coins with the same amount of which one debits raw materials, and the other one credits accounts payable. Then, subsidiary B consumes raw materials, labor, and manufacturing overhead and produces work-in-process, which generates four electronic entries of which three credit raw materials, wages payable and manufacturing overhead and one debits work-in-process. After the assembly process, Bb-TPS credits the work-in-process and debits finished goods inventory. In the end, the final products are delivered from subsidiary B to subsidiary C, which generates four electronic entries: two credit finished goods inventory and sales revenue and the other two debit COGS and accounts receivable.

In the manufacturing process, "raw-materials" coins are transformed into "work-in-process (WIP)" coins, and then "finished-goods" coins. To present the production process in which raw materials are transformed into finished products, subsidiary B first needs to identify the ownership of "raw-materials", "labor" and "manufacturing-overhead" coins and retire those coins to be turned. Retiring a coin refers to disposing of or destructing a real-world asset. Technically, a blockchain user will send the coin that s/he decided to dispose of to a specific wallet address. The special wallet will permanently lock up the coins and keep them out of circulation. After subsidiary B retires "raw-materials," "labor" and "manufacturing-overhead" coins, it could issue new "WIP" coins that would further be converted to "finished-goods" coins by binding them to the physical products with sensors.

3.2. Continuous monitoring and fraud prevention

When a business transaction occurs in the Bb-TPS, the business event represented by transferring a digital coin from one entity to another will be announced publicly and recorded in real-time. The Bb-TPS continuously adds transactions to the blockchain and shares the blockchain with all users; therefore, auditors can obtain a full copy of his/her client's transaction data. The real-time availability of transaction data makes it possible for auditors to monitor firm's global assets continuously. If an auditor wants to confirm a client's accounts receivable with its customers or accounts payable with suppliers, the auditor only needs to collect the relevant sales or procurement transaction data from the blockchain and perform analytical procedures (e.g., matching transaction amount to accounts receivable or payable). The automatic confirmation mechanism reduces the duplication of work for bank and

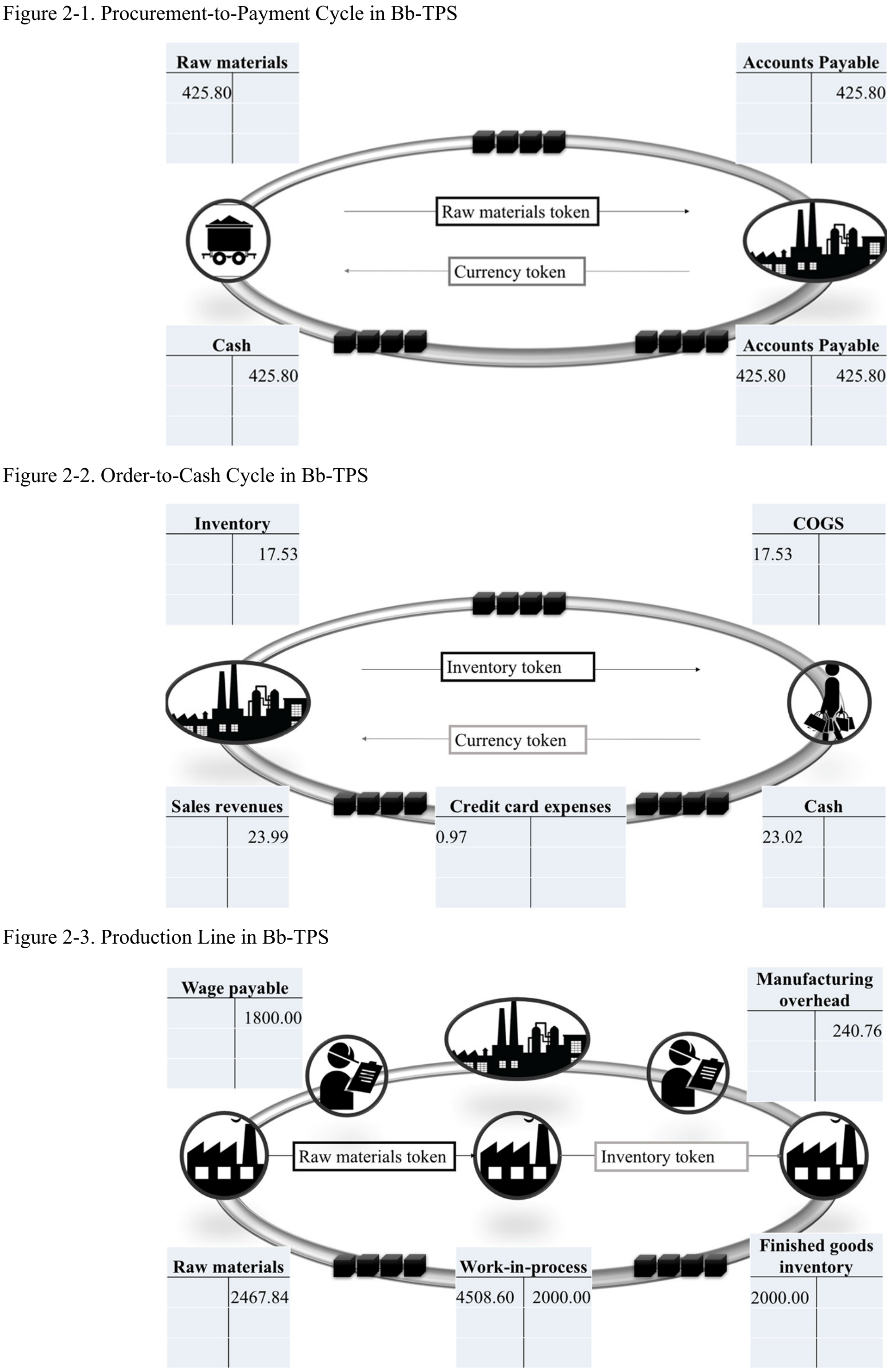


Figure 2-1. Procurement-to-Payment Cycle in Bb-TPS

Figure 2-2. Order-to-Cash Cycle in Bb-TPS

Figure 2-3. Production Line in Bb-TPS

Fig. 2. Real-time accounting in Bb-TPS.

cash reconciliations and improves audit efficiency. Besides, the transaction data from blockchain could serve as high-quality audit evidence as 100% transactions have been verified once occurred.

The Bb-TPS can trace the movement of firm's tokenized assets; therefore, it is able to proactively deter asset (e.g., cash or inventory) misappropriation.[8] The continuous monitoring based on blockchain makes it difficult for managers to engage in earnings management or commit fraud (Groomer and Murthy, 1989; Vasarhelyi and Halper, 1991). If a firm has engaged in a financial statement fraud scheme, Bb-TPS keeps the records of all relevant transactions, which could deliver valid evidence showing the possible accounting irregularities. For example, the criteria of revenue recognition can be encoded in a blockchain-based continuous monitoring system (Bb-CAS) using smart contracts to ensure that all conditions have been met before recognizing sales revenue. If the blockchain presents the fact that a high rate of return happens immediately after an abnormal high-volume year-end sale, the Bb-CAS could raise the alarm and send a message to the auditor about the potential "channel-stuffing" fraud and the revenue recognition concern. Bb-TPS can prevent managers from cooking the books or tampering with the data, such as creating fictitious transactions or backdating sales contracts or option compensation. In addition, related-party transactions could be self-disclosed; therefore, suspicious transfer of assets implying conflicts of interest can be spotted instantly. In order to defeat securities exchange fraud, Bb-TPS makes managerial ownership so transparent that insider buying or selling can be detected automatically in real time. Corporate voting using Bb-TPS could be more transparent, accurate and fast (Yermack, 2017). Furthermore, the transparency reduces opportunities for corruption or bribery behavior between regulators and firm's management.

3.3. Blockchain confidentiality and homomorphic encryption

The fact that every user has a full copy of transaction history is too much of a security risk for both organizational and individual users. The encryption of blockchain data is necessary to preserve a user's privacy and confidentiality. Encryption, such as public key cryptosystems (ElGamal, 1985), is a process to encode data that only authorized parties can access. Homomorphic encryption is a type of encryption algorithm that allows for computations to be done on encrypted data without first having to decrypt it (Gentry, 2009). For example, Alice sends Bob two messages: one is a number 8, and the other is a number 9. The data is encrypted so that 8 become 33 and 9 becomes 54. The encrypted numbers are added together resulting in 87 and sent through the channel. Bob only needs to decrypt 87 using his private key to provide the final answer of 17. A blockchain user could encrypt the transaction amount and calculate the balance, tax or interest based on the encrypted amount without releasing any transaction data.

Fig. 3 shows an example of how homomorphic encryption protects a Bb-TPS user's confidentiality. If a customer, named Alice, buys a luxury handbag and pays for it using an installment plan in Bb-TPS, she can send "cash" coins to the handbag store every month. As shown in Fig. 3-2, Alice's cryptowallet address[9] is anonymized by a hash function, her personally identifiable information (i.e., name) will never be disclosed in Bb-TPS. However, if a node is a frequent user having a long transaction history in Bb-TPS (e.g., a multinational company), sophisticated data mining and pattern recognition techniques could allow some other parties (e.g., a competitor) to infer the connections between the user's identity and his/her cryptowallet addresses. This type of "network analysis" for blockchain could even probably recognize the frequent user's transaction patterns, trace the user's trading partners and link the cryptowallet address to the IP address (Reid and Harrigan, 2013). Thus, the user's privacy could be at risk if a hacker is able to break into the host at an IP address and steal the user's assets. Even if a user could apply anti-tracking mechanisms (e.g., creating many anonymous wallets) to prevent a privacy attack, the big data of high-frequent trades will expose the user to malicious attackers and compromise its confidentiality.

To reduce exposure risk, Bb-TPS uses homomorphic encryption to encode sensitive transaction information into unreadable ciphertext. In the above handbag-shopping example, Alice can choose to encrypt her transaction details using her private key. Then, the encrypted transaction will be written into Bb-TPS in human-unreadable format. As shown in Fig. 3-3, not only the input and output addresses but also the input and output amount and transaction fees have been encrypted and recorded in the blockchain, which makes it difficult for an intruder to steal secrets based on the limited disclosures (i.e., block hash, transaction hash and timestamps). Moreover, with homomorphic encryption, we can set up mathematical operations (e.g., additions, multiplications, quadratic functions) between two ciphers. In Alice's case, although the transaction amount is encrypted, Bb-TPS can still calculate the account balance by aggregating the encrypted transaction amounts. In addition, by aggregating all transactions and offsetting the accounts receivable and accounts payable between two subsidiaries, Bb-TPS can deliver a consolidated statement automatically in real time. The utilization of homomorphic encryption enables a secure Bb-TPS with guaranteed confidentiality.

3.4. Blockchain confidentiality and zero-knowledge proofs

By encrypting the transaction data (i.e., sender, recipient, and amount), blockchain can provide a security protection and confidentiality-preserving business ecosystem. However, how can the public verify or confirm a transaction if the transaction details are unknown? For example, if only the trading partners have access to transaction details, the other Bb-TPS users would not be able to trace the asset transfers and identify the owner of that asset. To deliver a certain level of transparency while preserving transaction confidentiality, this paper uses zero-knowledge Succinct Non-interactive Argument of Knowledge (zk-SNARK) to create a confidentiality preserving and transaction verifiable Bb-TPS.

Zk-SNARK[10] uses a variant of zero-knowledge proofs (ZKP)[11] mechanism. The basic idea of the ZKP is that one party (prover)

[8] Physical controls are still needed to safeguard physical goods. Bb-TPS is used to identify possible misappropriation and concealment of assets or liabilities at the ownership level

[9] The cryptowallet address is the account identifier that a blockchain user owns for sending and receiving coins.

[10] For the technical details, please refer to Ben-Sasson et al., 2014. Succinct Non-Interactive Zero-Knowledge for a Von Neumann Architecture. Available at: https://eprint.iacr.org/2013/879.pdf. Accessed 5/23/17 10:33 PM.

Figure 3-1. Overview - Homomorphic Encryption in Bb-TPS

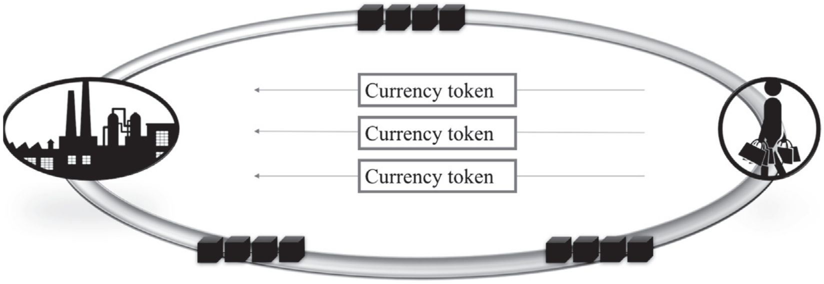
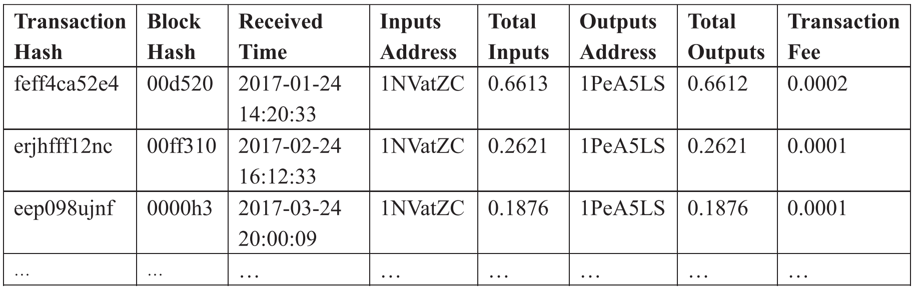
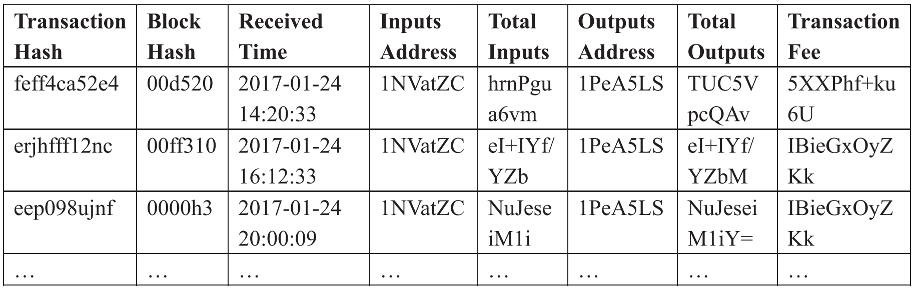


Figure 3-2. Example - Transaction Details



Transaction Hash	Block Hash	Received Time	Inputs Address	Total Inputs	Outputs Address	Total Outputs	Transaction Fee
feff4ca52e4	00d520	2017-01-24 14:20:33	1NVatZC	0.6613	1PeA5LS	0.6612	0.0002
erjhfff12nc	00ff310	2017-02-24 16:12:33	1NVatZC	0.2621	1PeA5LS	0.2621	0.0001
eep098ujnf	0000h3	2017-03-24 20:00:09	1NVatZC	0.1876	1PeA5LS	0.1876	0.0001
…	…	…	…	…	…	…	…

Figure 3-3. Example - Encrypted Transaction Details



Transaction Hash	Block Hash	Received Time	Inputs Address	Total Inputs	Outputs Address	Total Outputs	Transaction Fee
feff4ca52e4	00d520	2017-01-24 14:20:33	1NVatZC	hrnPgu a6vm	1PeA5LS	TUC5V pcQAv	5XXPhf+ku 6U
erjhfff12nc	00ff310	2017-01-24 16:12:33	1NVatZC	eI+IYf/ YZb	1PeA5LS	eI+IYf/ YZbM	IBieGxOyZ Kk
eep098ujnf	0000h3	2017-01-24 20:00:09	1NVatZC	NuJese iM1i	1PeA5LS	NuJesei M1iY=	IBieGxOyZ Kk
…	…	…	…	…	…	…	…

Fig. 3. Homomorphic encryption in Bb-TPS.

convinces another party (verifier) that its statements are true without revealing the content of that statement (Rackoff and Simon, 1991). For example, a person named Peggy claims that she knows the secret to open a door in a cave shaped like a circle (as shown in Fig. 4). Peggy wants to prove to a person named Victor that she knows the secret; however, she is not allowed to tell the secret to Victor. First, they decide to label the upper and lower paths A and B. Then, Peggy randomly takes A or B path and walks in while Victor waits outside without seeing which path Peggy takes. Next, Victor specifies the path where Peggy has to show up. If Peggy walks in the same path as Victor specifies, she can quickly return to the entrance; if Peggy doesn't walk in the path Victor specifies, she needs to go through the door and walk out to the entrance using another path. Suppose that Peggy indeed knows the secret, she could either use the secret to open the door or returns merely using the same path as she entered. However, if Peggy lies, she can only show up on the path which she uses to enter and fails on the other path if Victor picks it. For every trial, the dishonest Peggy will have 50% chance to guess it right. If they repeat the trials 50 times, her chance to guess all correct paths would be impossibly small.

The above example shows the standard interactive zero-knowledge proof, and a non-interactive zero-knowledge proof is a method by which no interaction between the prover and verifier is necessary. Based on prior work on non-interactive zero-knowledge proofs and recent breakthroughs of zk-SNARKs, Ben-Sasson et al. (2014) create a publicly shared ledger with strong privacy. Zk-SNARK is an efficient variant of ZKP protocol by which the other users in a blockchain can verify the ownership of Bitcoin while revealing no information to the public (Ben-Sasson et al., 2014). Using zk-SNARK, a sender could first encrypt the transaction details (e.g., sender, recipient, and amount), then generate a short proof[12] and announce the transaction and the short proof in the blockchain. Any

[11] The concept of ZKP was first conceived in a paper introducing an interactive proof system (Goldwasser et al., 1989), which is an abstract machine that models the computation as an exchange of messages between two parties. Blum et al. (1988) proved that if a common random string is shared between a prover and a verifier, the prover can convince the verifier that a certain statement is true without interacting with the verifier.

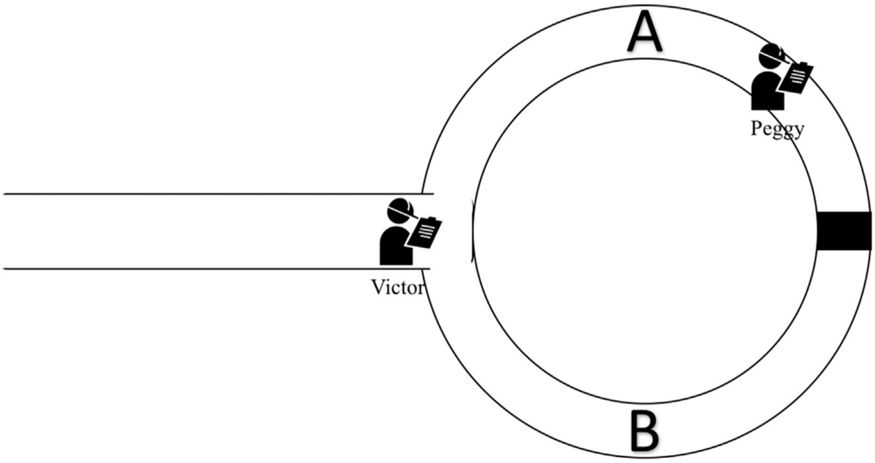


Fig. 4. Example of zero-knowledge proof.

blockchain user can apply a verification key to verify the short proof without having to interact with the sender. For the smart contract, Kosba et al. (2016) use ZKP to define a security-protection and privacy-preserving smart contract protocol called Hawk, and both Zcash and Hawk possess high efficiency in cryptographic computation.

By adopting zk-SNARK, the encrypted transactions in Bb-TPS can be verified without first decrypting the details. In this scheme, the other Bb-TPS users need to verify the following three statements: (1) “the sender has a valid source of that coin s/he is about to transfer”, (2) “the coin has not been double spent”, and (3) “the input amount equals the output amount”. To prove the three statements, a sender uses zk-SNARK to generate a short proof (which could be efficiently processed by the other users) and releases the verification key while encrypting transaction details. Then, s/he announces the transaction in the form of ciphertext. The other users, such as block miners, work together to verify the three statements by validating the short proof and verification key, but they will not be informed about any content of the three statements. Once the verification result is true, the encrypted transaction is ready to be written in a new block and added to the blockchain. Therefore, all business transaction data could be encrypted and confirmed based on the zk-SNARK scheme, and none of the transaction details would be publicly disclosed. On the other hand, if a user wants to disclose the transaction information voluntarily, s/he still has an option to announce the transaction details. If the user chooses to shield the information such as sender's address, recipient's address and transaction amounts, s/he must generate a zk-SNARK short proof and share it with the public for verification.

3.5. Blockchain neutrality

The blockchain is a single-entry system which keeps a record of the event of asset transfer. A “single-entry bookkeeping system in a blockchain” is introduced to replace the traditional double-entry system (Simon, 2016), while another group of cryptographers provides discussions about a “triple-entry”[13] system (Grigg, 2005). The blockchain based “triple-entry” system is an enhancement to the traditional double-entry system where all accounting entries are recorded by a third entry into the blockchain. In contrast to traditional accounting where the trading partners independently book debit and credit to their own accounts, blockchain's shared transaction records link the journal entries of trading parties, which provides additional assurance in auditing.

It should be noted that Bb-TPS should be conceived as a neutral and independent infrastructure that underpins business event recording. Similar to net neutrality (Jordan, 2009), blockchain neutrality represents the argument that the blockchain ledger is applicable to different accounting treatments or even different accounting standards (i.e., GAAP and IFRS). The generic neutrality of Bb-TPS design requires the separation of event recording and accounting treatment (e.g., period-end adjustments/closing), even if it is technically possible to encode accounting rules in a blockchain (e.g., an aging method can be programmed in a smart contract for doubtful accounts). In general, a blockchain serves as a neutral shared database that keeps transaction records per se, while journalizing and adjustments are processed on top of the Bb-TPS infrastructure using enterprise information systems. In this case, the Bb-TPS provides the transaction level assurance for the full population and presents the facts of business events, while the individual enterprise information systems could merely perform aggregation, materialization, and adjustments as necessary to prepare financial statements in accordance with the applicable accounting standards (e.g., US GAAP or IFRS).

This arrangement also allows auditors to aggregate individual transactions and verify financial reports based on accounting standards. Fig. 5 shows the Bb-TPS-neutrality principle: Bb-TPS is used for recording transactions per se, and each economic entity has freedom to build its accounting, auditing or taxation systems on top of Bb-TPS. Blockchain only contains the transaction data,

[12] A short proof consists of a single message sent from a prover to a verifier. In order to assure the zero-knowledge proof is non-interactive, short and therefore uploadable to blockchain, it is necessary to have an initial setup to generate a common random string shared between the prover and the verifier.

[13] The definition of a “triple-entry” accounting system used by blockchain-accounting practitioners is different from Ijiri's (1986) definition.

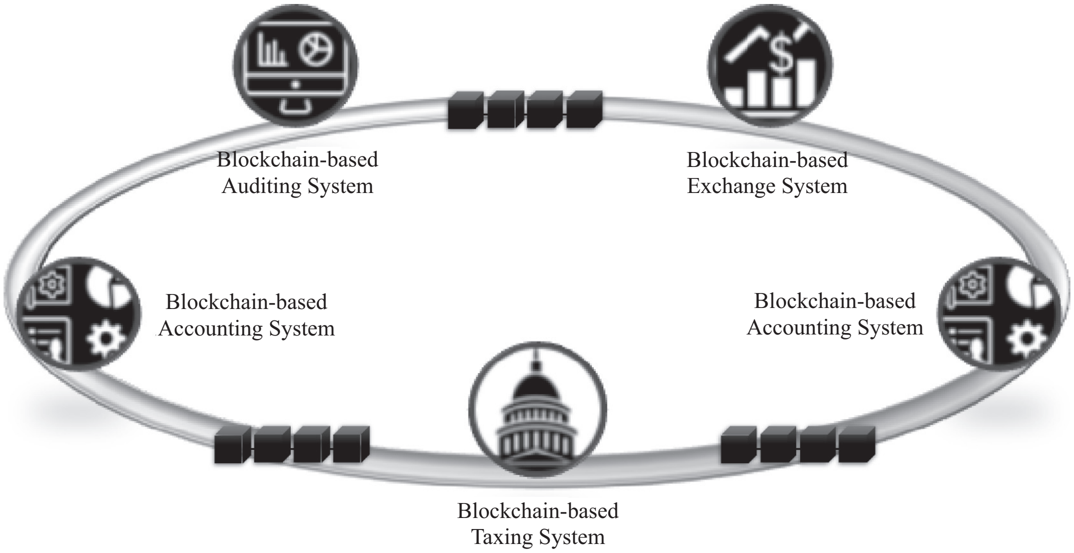

Blockchain-based Auditing System
Blockchain-based Exchange System
Blockchain-based Accounting System
Blockchain-based Accounting System
Blockchain-based Taxing System

Fig. 5. The neutrality of Bb-TPS.

while each firm's ERP system can automatically extract the data from blockchain, aggregate the transactions and provide information for use in producing financial statements.

4. Prototyping and evaluation

4.1. Basic infrastructure

In order to test the proposed design framework, we develop a prototype of the Blockchain-based Transaction Processing System (Bb-TPS) using the core code from the Multichain[14] platform. Multichain.com is an open source platform for blockchain applications. It helps quickly build applications on blockchains and shared ledgers, and it also provides the functions of permissions management, asset issuance and data sharing. Based on the Multichain platform and four Windows servers at Rutgers CAR-Lab,[15] we create a four-node blockchain network and test the performance of the proposed Bb-TPS framework.

First, we created a new blockchain named "Achain" and initiated it on Server 92. Second, the other three servers (i.e., Server 109, Server 116 and Server 117) are used to connect to the "Achain." There are three subprocesses to complete the connection: 1) the other three servers send requests for connection permissions; 2) Server 92 grants connect (or together with send, receive and mine) permissions to the other three servers; 3) the other three servers use their public and private keys to connect to the "Achain". Finally, these four servers form a private blockchain network that serves as the infrastructure of Bb-TPS. Fig. 6 shows the steps of creating and initiating the "Achain" and connecting the nodes to it.[16]

4.2. The prototype of Blockchain-based transaction processing system

After creating "Achain" and connecting the nodes to it, we simulated the processes of issuing and transferring assets in the blockchain. As shown in Fig. 7, first we checked the issue permissions and established that only Server 92 has the permission to issue new assets. Then, 1000,000 new assets "Cash" were issued with the unit of 0.01, and 100 "Laptop" assets were tokenized with the unit of 1. Thus, the simulation of assets issuance and tokenization was completed. As there are many types of assets, for simplicity they are divided into 1) cash coin, 2) divisible assets and 3) indivisible assets. For each issuance of new assets, Bb-TPS will automatically create a reference ID that can be linked to a real-world asset. For example, a building as an indivisible asset can be encoded in blockchain by binding its physical address to the corresponding token's reference ID. The issuer's address is also linked to the reference ID, which provides a proof of the initial ownership. In this case, the indivisible assets could be encoded in blockchain one by one, while the tokenization of divisible assets needs to be done in a batch. For example, a factory creates a batch of inexpensive handbags that could be encoded in blockchain sharing the same reference ID. Cash coin is another type of divisible assets, which however could only be issued by central bank authorities. Table 1 shows the process of tokenization and the tokenized assets in

[14] http://www.multichain.com. Accessed 5/23/17 10:34 PM.

[15] http://raw.rutgers.edu/carlab.html. Accessed 5/23/17 10:35 PM.

[16] This prototype focused on the demonstration of Blockchain based Transaction Processing System without discussing the reward mechanisms for block mining. The authors understand the mining incentives are an important parameter in blockchain design, however our main objective is to apply this technology to bookkeeping and fraud prevention instead of encouraging participation. We hope this will stimulate further discussion of this issue.

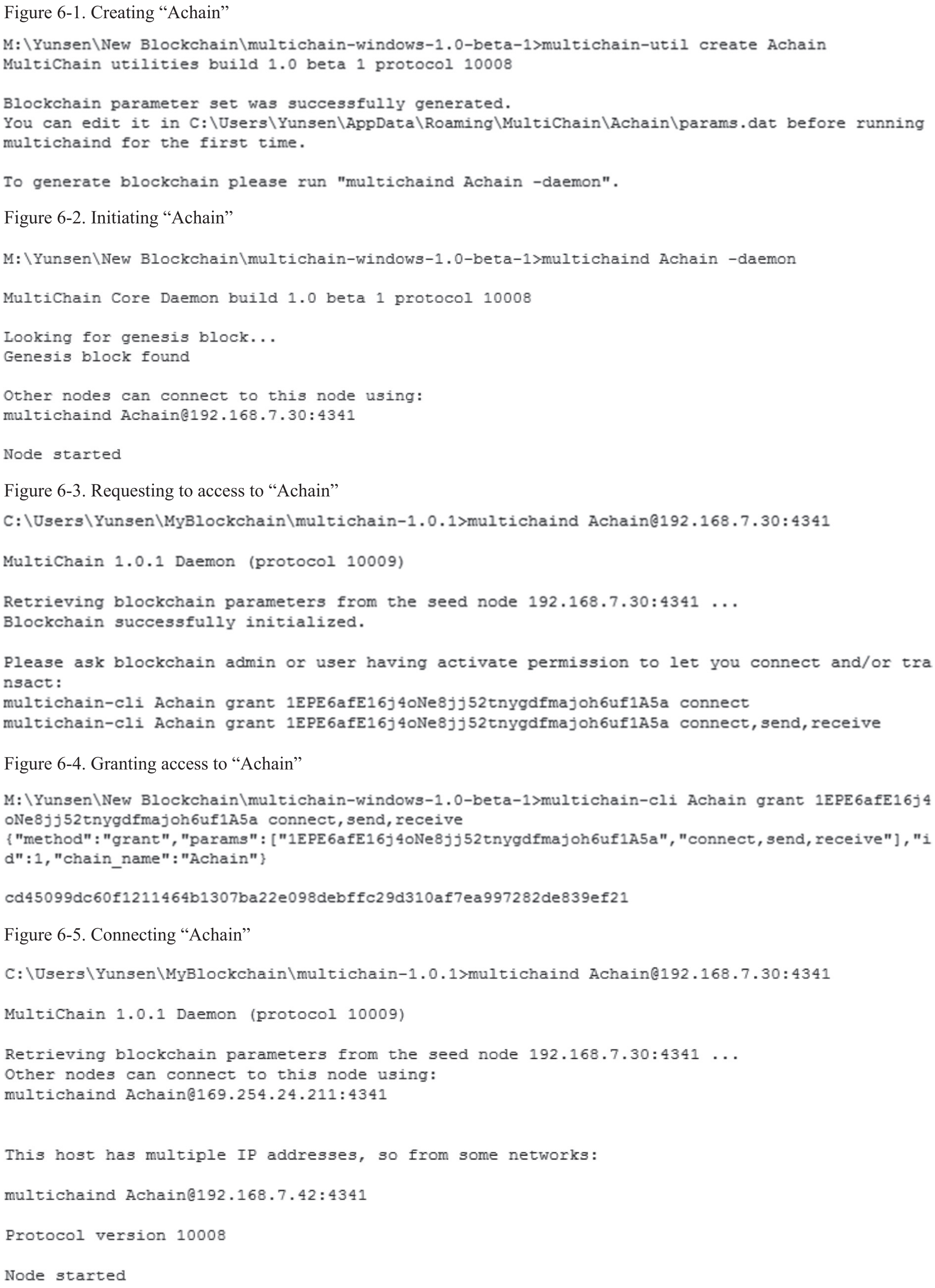


Figure 6-1. Creating “Achain”

```
M:\Yunsen\New Blockchain\multichain-windows-1.0-beta-1>multichain-util create Achain
MultiChain utilities build 1.0 beta 1 protocol 10008

Blockchain parameter set was successfully generated.
You can edit it in C:\Users\Yunsen\AppData\Roaming\MultiChain\Achain\params.dat before running
multichaind for the first time.

To generate blockchain please run "multichaind Achain -daemon".
```

Figure 6-2. Initiating “Achain”

```
M:\Yunsen\New Blockchain\multichain-windows-1.0-beta-1>multichaind Achain -daemon

MultiChain Core Daemon build 1.0 beta 1 protocol 10008

Looking for genesis block...
Genesis block found

Other nodes can connect to this node using:
multichaind Achain@192.168.7.30:4341

Node started
```

Figure 6-3. Requesting to access to “Achain”

```
C:\Users\Yunsen\MyBlockchain\multichain-1.0.1>multichaind Achain@192.168.7.30:4341

MultiChain 1.0.1 Daemon (protocol 10009)

Retrieving blockchain parameters from the seed node 192.168.7.30:4341 ...
Blockchain successfully initialized.

Please ask blockchain admin or user having activate permission to let you connect and/or tra
nsact:
multichain-cli Achain grant 1EPE6afE16j4oNe8jj52tnygdfmajoh6uf1A5a connect
multichain-cli Achain grant 1EPE6afE16j4oNe8jj52tnygdfmajoh6uf1A5a connect,send,receive
```

Figure 6-4. Granting access to “Achain”

```
M:\Yunsen\New Blockchain\multichain-windows-1.0-beta-1>multichain-cli Achain grant 1EPE6afE16j4
oNe8jj52tnygdfmajoh6uf1A5a connect,send,receive
{"method":"grant","params":["1EPE6afE16j4oNe8jj52tnygdfmajoh6uf1A5a","connect,send,receive"],"i
d":1,"chain_name":"Achain"}

cd45099dc60f1211464b1307ba22e098debffc29d310af7ea997282de839ef21
```

Figure 6-5. Connecting “Achain”

```
C:\Users\Yunsen\MyBlockchain\multichain-1.0.1>multichaind Achain@192.168.7.30:4341

MultiChain 1.0.1 Daemon (protocol 10009)

Retrieving blockchain parameters from the seed node 192.168.7.30:4341 ...
Other nodes can connect to this node using:
multichaind Achain@169.254.24.211:4341


This host has multiple IP addresses, so from some networks:

multichaind Achain@192.168.7.42:4341

Protocol version 10008

Node started
```

Fig. 6. Creation and initiation of “Achain”.

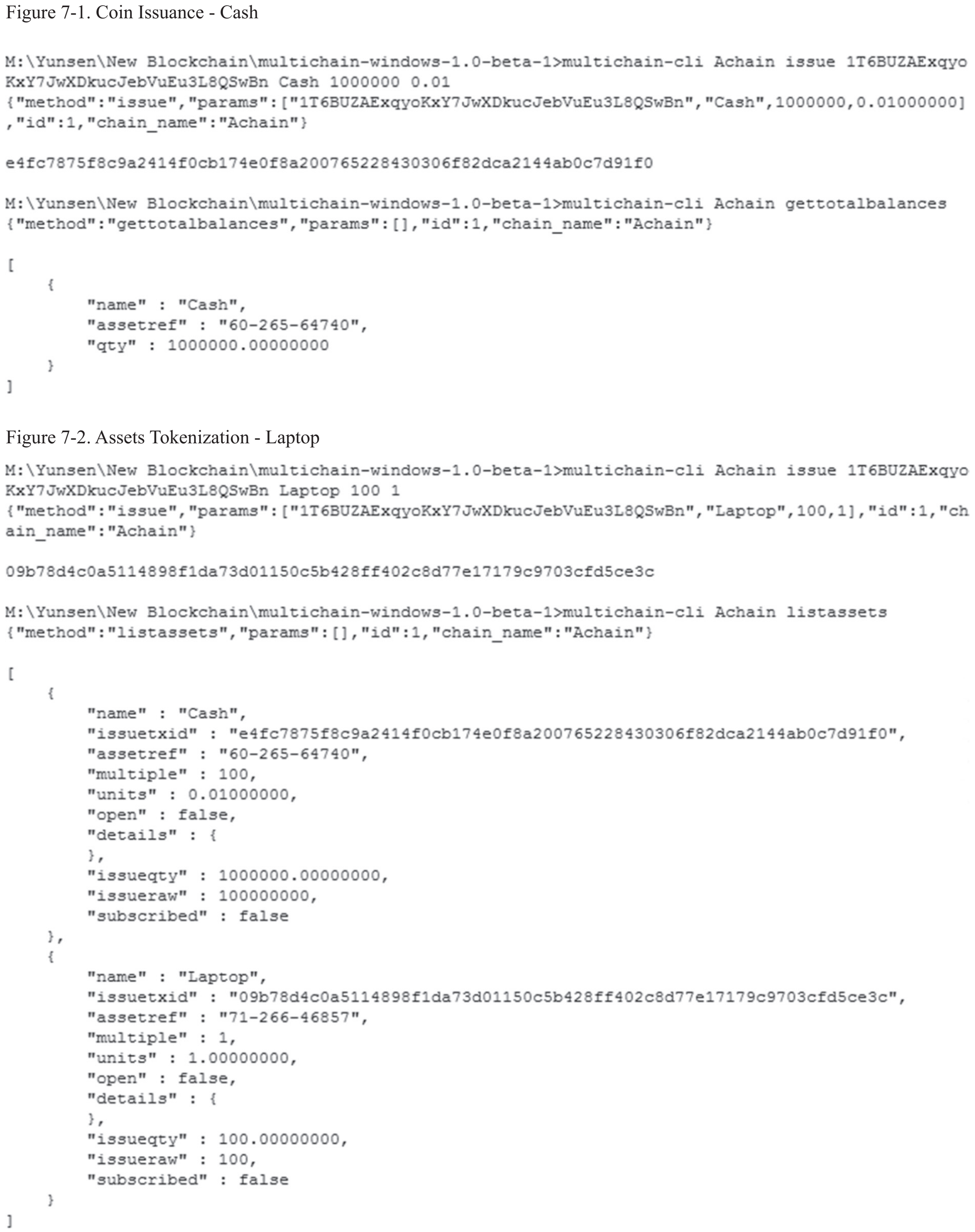


Figure 7-1. Coin Issuance - Cash

```
M:\Yunsen\New Blockchain\multichain-windows-1.0-beta-1>multichain-cli Achain issue 1T6BUZAExqyo
KxY7JwXDkucJebVuEu3L8QSwBn Cash 1000000 0.01
{"method":"issue","params":["1T6BUZAExqyoKxY7JwXDkucJebVuEu3L8QSwBn","Cash",1000000,0.01000000]
,"id":1,"chain_name":"Achain"}

e4fc7875f8c9a2414f0cb174e0f8a200765228430306f82dca2144ab0c7d91f0

M:\Yunsen\New Blockchain\multichain-windows-1.0-beta-1>multichain-cli Achain gettotalbalances
{"method":"gettotalbalances","params":[],"id":1,"chain_name":"Achain"}

[
    {
        "name" : "Cash",
        "assetref" : "60-265-64740",
        "qty" : 1000000.00000000
    }
]
```

Figure 7-2. Assets Tokenization - Laptop

```
M:\Yunsen\New Blockchain\multichain-windows-1.0-beta-1>multichain-cli Achain issue 1T6BUZAExqyo
KxY7JwXDkucJebVuEu3L8QSwBn Laptop 100 1
{"method":"issue","params":["1T6BUZAExqyoKxY7JwXDkucJebVuEu3L8QSwBn","Laptop",100,1],"id":1,"ch
ain_name":"Achain"}

09b78d4c0a5114898f1da73d01150c5b428ff402c8d77e17179c9703cfd5ce3c

M:\Yunsen\New Blockchain\multichain-windows-1.0-beta-1>multichain-cli Achain listassets
{"method":"listassets","params":[],"id":1,"chain_name":"Achain"}

[
    {
        "name" : "Cash",
        "issuetxid" : "e4fc7875f8c9a2414f0cb174e0f8a200765228430306f82dca2144ab0c7d91f0",
        "assetref" : "60-265-64740",
        "multiple" : 100,
        "units" : 0.01000000,
        "open" : false,
        "details" : {
        },
        "issueqty" : 1000000.00000000,
        "issueraw" : 100000000,
        "subscribed" : false
    },
    {
        "name" : "Laptop",
        "issuetxid" : "09b78d4c0a5114898f1da73d01150c5b428ff402c8d77e17179c9703cfd5ce3c",
        "assetref" : "71-266-46857",
        "multiple" : 1,
        "units" : 1.00000000,
        "open" : false,
        "details" : {
        },
        "issueqty" : 100.00000000,
        "issueraw" : 100,
        "subscribed" : false
    }
]
```

Fig. 7. Assets issuance and tokenization.

Table 1
Assets tokenization simulation.

Asset name	Reference ID	Issuer address
Cash coin	213-267-35883	18FWJdyLDLdQU59EEg8UQHE3RZWAh6JCoxpnco
Handbags	192-266-38671	1RzU4qqiyaH6y6jDDQSJtAKNDqviJNgvn5Tiqe
Building 1 WP	784-643-67849	1HpDPEK8pnegtXVKdkzN67nEtwsMmmCs2JFsuv
…	…	…

This table shows the process of tokenization and the tokenized assets in "Achain." In this table, there are at least three asset tokens. Asset name describes the real-world names of the tokenized assets, Reference ID indicates the unique identifiers of the tokenized assets, and Issuer Address shows who initially encoded an asset into blockchain.

"Achain." For the asset retirement, the Bb-TPS provides a specific wallet address where the users can send the tokens. Then, those tokens are out of circulation.

It should be noted that the audit of the tokenization process becomes crucial because the initial ownership represents the starting point of the provenance of an asset. The first owner of a token should be responsible for the existence and integrity of the corresponding real-world asset that the token links to, and a detailed audit must be performed on the asset's tokenization process. A detailed audit of asset tokenization involves the procedures that auditors must perform to verify that the reference ID of a new coin is linked to the issuer's cryptowallet address as well as the physical asset's serial number. Once an audited asset is hashed to the blockchain, the blockchain will then automatically keep track of the asset for its useful life. Moreover, a complete audit is also necessary when a Bb-TPS environment is set up and initiated. In the near future, as a large number of real-world objects have had coins associated with them, the tamper resistance and irreversibility of blockchain will become the core functionalities for auditing and fraud prevention.

After simulating the cash coin and inventory, a transaction of the order-to-pay cycle was demonstrated as follows (Fig. 8). First, we checked the firm M's cash coin and inventory balance. As shown in Fig. 8-1 and -2, firm M has 19,574.2 cash coins and 6 handbags, while its supplier has 425.8 cash coins and 14 handbags. Then, firm M ordered 6 handbags from the supplier, and the supplier shipped the goods immediately (Fig. 8-3), which completed the transfer of the 6 handbags' ownership from the supplier to firm M. As soon as firm M received the goods in the warehouse, it immediately disbursed the payment of 425.8 cash coins to the supplier (Fig. 8-4). Finally, we checked the ending balance of both accounts after the procurement transaction (Fig. 8-5 and -6) and finished the procurement transaction.

4.3. Simulation of permissions management

Bb-TPS with access controls only allows authorized users to read or create transactions. For example, only the shipper has permissions to transfer "goods" coins to a customer under a certain credit limit, and only the procurement staff can purchase raw materials from suppliers. Bb-TPS can properly separate job duties when sufficient competent staff are available at the entity. A properly designed Bb-TPS can precisely and dynamically control who can connect to the blockchain, initiate transactions and mine blocks. For example, a firm can build a blockchain network with its trading partners, stakeholders, and regulators in which only regulators are allowed to confirm transactions, generate blocks, and grant permissions to new users. Furthermore, in order to remove central authorities, Bb-TPS can allow more than one sophisticated user to grant access and/or mine blocks. For example, a long-tenured user who has created a large number of transactions in Bb-TPS could participate in mining blocks and maintaining the blockchain, or that user could in turn grant access to a limited number of new users.

If a user has been actively participating in Bb-TPS for a long period, some of the "senior" users can consider promoting this user to be a maintainer or blockchain miner.[17] As shown in Fig. 9-1, a user was granted the permission of mining, and the user is able to participate in confirming and writing transactions to the blockchain. In Fig. 9-2, this user is listed in the mining permission list, and it can start to mine the new blocks. Fig. 9-3 shows a new block mined by a node. In this block, it lists the block parameters: hash, miner, height, nonce,[18] difficulties[19] and mined time. The transaction records are recorded in the blocks and impossible to be changed in the future.

4.4. Simulation of automatic confirmation

Fig. 10-1 shows that in the order-to-pay cycle, a customer made a payment to firm M for goods received and Fig. 10-2 shows the payment details. All users of Bb-TPS automatically confirmed this payment transaction, and the payment details can be used as evidence by the auditors. Furthermore, all the transaction details including goods shipment and payment between the customer and firm M can be collected and calculated in real time, and the accounts receivable, and payable between firm M and the customer can be easily calculated automatically.

[17] Auditors could serve as the blockchain miners or maintainers who verify the transactions and provide assurance regarding transaction immutability. The ZKP and homomorphic encryption mechanisms will be embedded in the blockchain protocol, so accountants and auditors do not have to setup them manually."

[18] A nonce is a value that sets the hash of the block containing many leading zeroes.

[19] Difficulties is a measure of how difficult it is to find a nonce for a given target hash containing leading zeroes.

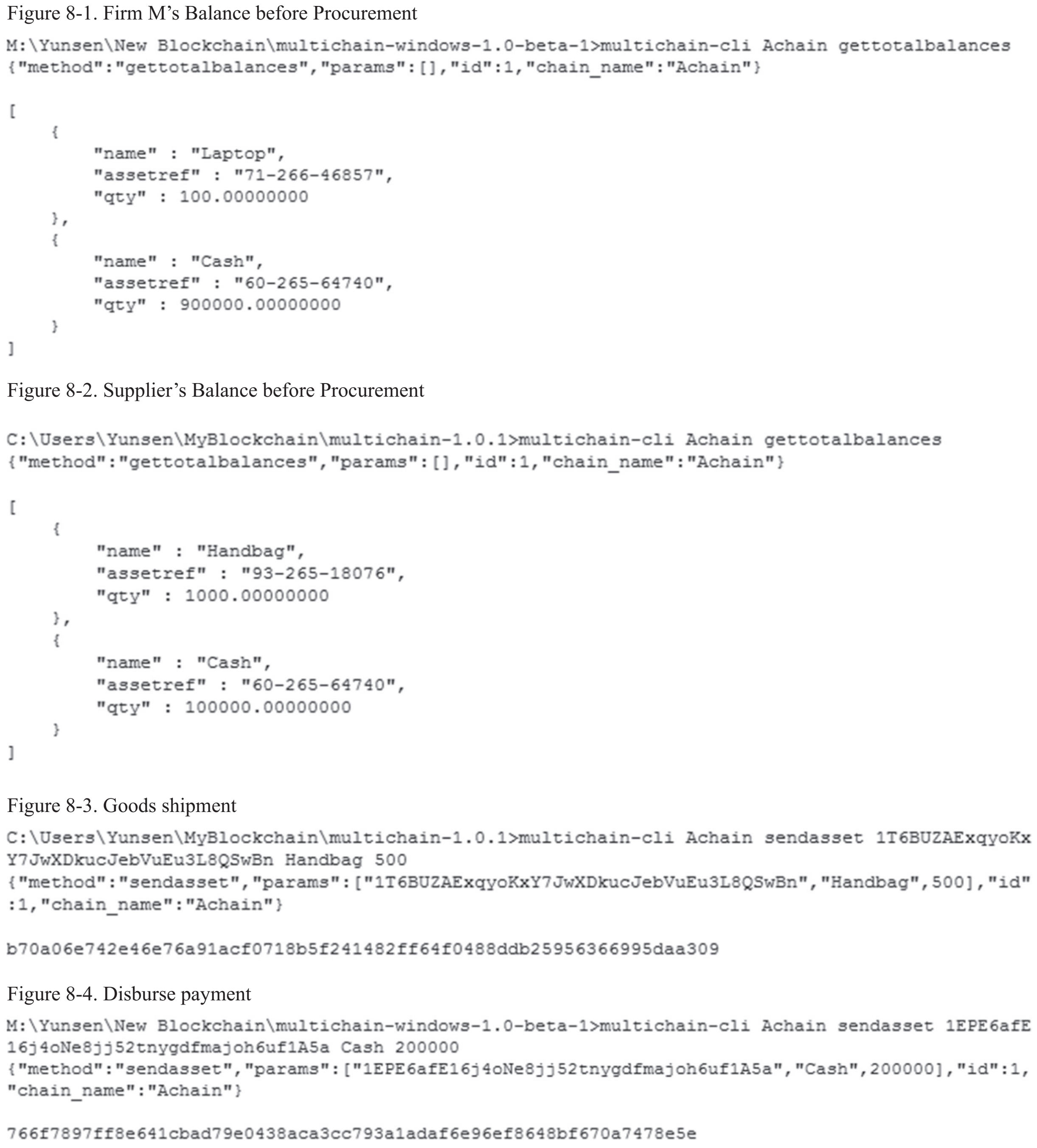


Figure 8-1. Firm M's Balance before Procurement

```
M:\Yunsen\New Blockchain\multichain-windows-1.0-beta-1>multichain-cli Achain gettotalbalances
{"method":"gettotalbalances","params":[],"id":1,"chain_name":"Achain"}

[
    {
        "name" : "Laptop",
        "assetref" : "71-266-46857",
        "qty" : 100.00000000
    },
    {
        "name" : "Cash",
        "assetref" : "60-265-64740",
        "qty" : 900000.00000000
    }
]
```

Figure 8-2. Supplier's Balance before Procurement

```
C:\Users\Yunsen\MyBlockchain\multichain-1.0.1>multichain-cli Achain gettotalbalances
{"method":"gettotalbalances","params":[],"id":1,"chain_name":"Achain"}

[
    {
        "name" : "Handbag",
        "assetref" : "93-265-18076",
        "qty" : 1000.00000000
    },
    {
        "name" : "Cash",
        "assetref" : "60-265-64740",
        "qty" : 100000.00000000
    }
]
```

Figure 8-3. Goods shipment

```
C:\Users\Yunsen\MyBlockchain\multichain-1.0.1>multichain-cli Achain sendasset 1T6BUZAExqyoKx
Y7JwXDkucJebVuEu3L8QSwBn Handbag 500
{"method":"sendasset","params":["1T6BUZAExqyoKxY7JwXDkucJebVuEu3L8QSwBn","Handbag",500],"id"
:1,"chain_name":"Achain"}

b70a06e742e46e76a91acf0718b5f241482ff64f0488ddb25956366995daa309
```

Figure 8-4. Disburse payment

```
M:\Yunsen\New Blockchain\multichain-windows-1.0-beta-1>multichain-cli Achain sendasset 1EPE6afE
16j4oNe8jj52tnygdfmajoh6uf1A5a Cash 200000
{"method":"sendasset","params":["1EPE6afE16j4oNe8jj52tnygdfmajoh6uf1A5a","Cash",200000],"id":1,
"chain_name":"Achain"}

766f7897ff8e641cbad79e0438aca3cc793a1adaf6e96ef8648bf670a7478e5e
```

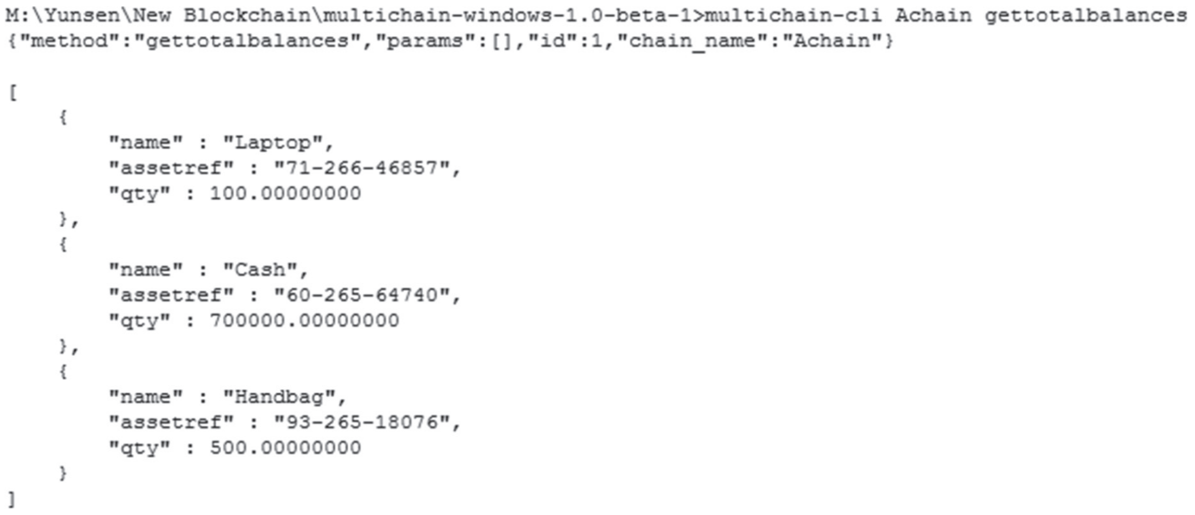
Fig. 8. Order-to-pay transaction.

4.5. Computational overhead: Blockchain vs. database

Contemporary transaction processing systems (e.g., ERP systems) are designed on the basis of relational databases and database management systems (DBMS). Blockchain can be an alternative to keep business transactions records with high information integrity and low transmission cost. In order to compare the computational performance of relational databases and blockchain, we conduct an experiment to simulate a significant number of transactions and measure the computational overhead (i.e., computational time and data size) of the blockchain and database. We use the SQLite[20] database to simulate transaction recording (SQLite is a C library that

[20] https://docs.python.org/3.6/library/sqlite3.html. Accessed 5/23/17 10:36 PM.

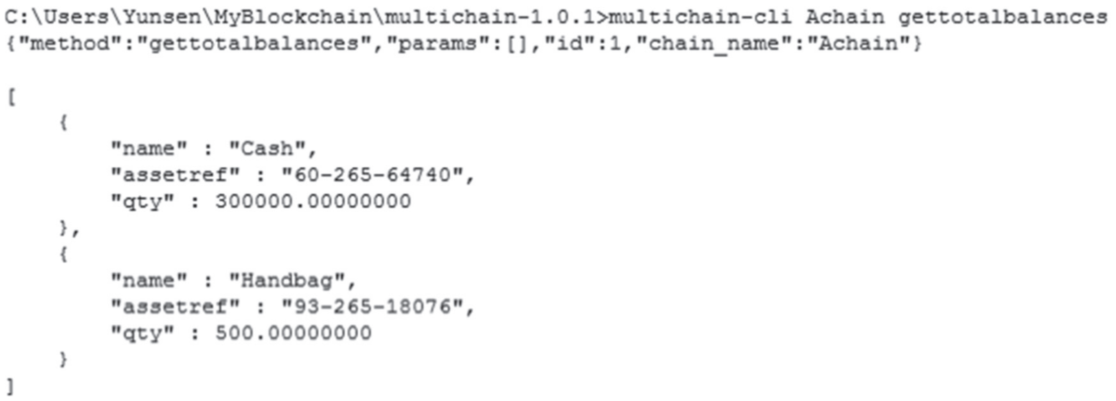
Figure 8-5. Firm M’s balances after procurement



```
M:\Yunsen\New Blockchain\multichain-windows-1.0-beta-1>multichain-cli Achain gettotalbalances
{"method":"gettotalbalances","params":[],"id":1,"chain_name":"Achain"}

[
    {
        "name" : "Laptop",
        "assetref" : "71-266-46857",
        "qty" : 100.00000000
    },
    {
        "name" : "Cash",
        "assetref" : "60-265-64740",
        "qty" : 700000.00000000
    },
    {
        "name" : "Handbag",
        "assetref" : "93-265-18076",
        "qty" : 500.00000000
    }
]
```

Figure 8-6. Supplier’s balances after procurement



```
C:\Users\Yunsen\MyBlockchain\multichain-1.0.1>multichain-cli Achain gettotalbalances
{"method":"gettotalbalances","params":[],"id":1,"chain_name":"Achain"}

[
    {
        "name" : "Cash",
        "assetref" : "60-265-64740",
        "qty" : 300000.00000000
    },
    {
        "name" : "Handbag",
        "assetref" : "93-265-18076",
        "qty" : 500.00000000
    }
]
```

Fig. 8. (*continued*)

provides a lightweight disk-based database). Sqlite3 is the Python module that serves as the interface for the SQLite database. The transactions were automatically generated on Server 92, while Server 109 played the role of the trading partner. At the start of generating transactions, we monitored the account balance of the “trading partner” server and measured the time taken to complete these transactions in the blockchain, and also measured the time of recording these transactions in the SQLite database on Server 92.

Table 2 shows the comparison of computational overhead between the blockchain and database. We find that to record the same number of transactions the blockchain system consumes significantly more computational overhead than the database system. Although more computational time is consumed to complete recording transactions in the blockchain than in the database, it increases linearly in the number of transactions. It is anticipated that with the rapidly improving information technology[21] and decreasing computation cost, the blockchain scalability and computational resources should not be a big concern for accounting and auditing applications. Blockchain provides an infrastructure for transaction processing systems to keep records of business transactions with high information integrity and low transmission cost. However, to guarantee irreversibility and tamper resistance we need to sacrifice computational resources and runtime efficiency. Nevertheless, with advances in computing technology, blockchain could be the most promising technology in accounting and fraud prevention in the near future.

[21] To provide real-time verification of transactions, blockchain miners compete to solve a mathematical puzzle, which is known as Proof-of-Work (PoW). The PoW process requires a significant amount of computational overhead. Many computer scientists and cryptographers seek to address this issue by designing new consensus mechanisms, such as Proof-of-Stake (PoS). Instead of consuming computation overhead to solve puzzles, PoS allows a node to mine a percentage of transactions according to its ownership stake. Therefore, a PoS based blockchain could save a great deal of overhead relative to a PoW based blockchain. The blockchain architecture provided by IBM enables PoS as the function of consensus mechanism. (https://eprint.iacr.org/2014/452. Accessed 4/5/2018 1:35 AM).

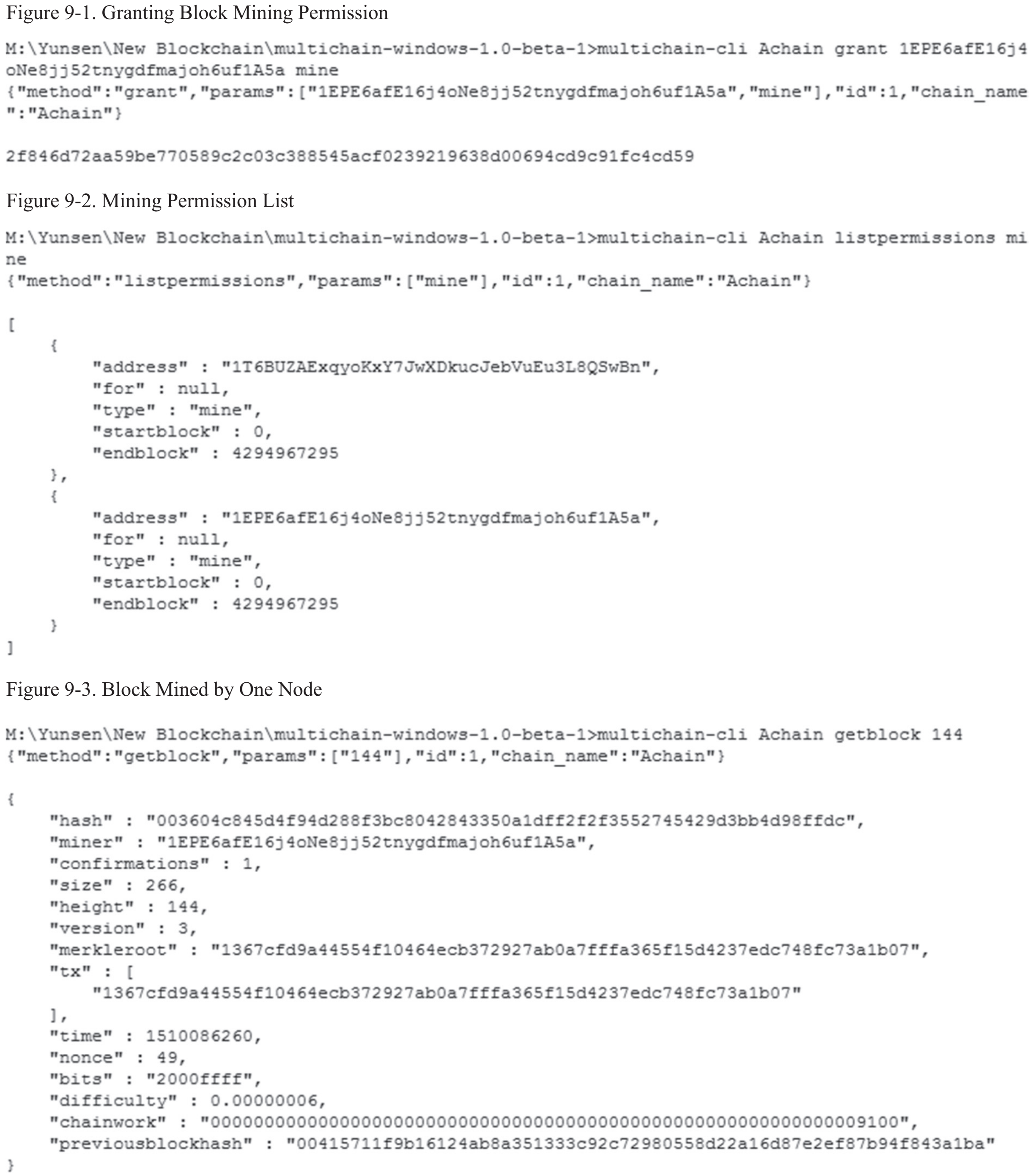


Figure 9-1. Granting Block Mining Permission

```
M:\Yunsen\New Blockchain\multichain-windows-1.0-beta-1>multichain-cli Achain grant 1EPE6afE16j4
oNe8jj52tnygdfmajoh6uf1A5a mine
{"method":"grant","params":["1EPE6afE16j4oNe8jj52tnygdfmajoh6uf1A5a","mine"],"id":1,"chain_name
":"Achain"}

2f846d72aa59be770589c2c03c388545acf0239219638d00694cd9c91fc4cd59
```

Figure 9-2. Mining Permission List

```
M:\Yunsen\New Blockchain\multichain-windows-1.0-beta-1>multichain-cli Achain listpermissions mi
ne
{"method":"listpermissions","params":["mine"],"id":1,"chain_name":"Achain"}

[
    {
        "address" : "1T6BUZAExqyoKxY7JwXDkucJebVuEu3L8QSwBn",
        "for" : null,
        "type" : "mine",
        "startblock" : 0,
        "endblock" : 4294967295
    },
    {
        "address" : "1EPE6afE16j4oNe8jj52tnygdfmajoh6uf1A5a",
        "for" : null,
        "type" : "mine",
        "startblock" : 0,
        "endblock" : 4294967295
    }
]
```

Figure 9-3. Block Mined by One Node

```
M:\Yunsen\New Blockchain\multichain-windows-1.0-beta-1>multichain-cli Achain getblock 144
{"method":"getblock","params":["144"],"id":1,"chain_name":"Achain"}

{
    "hash" : "003604c845d4f94d288f3bc8042843350a1dff2f2f3552745429d3bb4d98ffdc",
    "miner" : "1EPE6afE16j4oNe8jj52tnygdfmajoh6uf1A5a",
    "confirmations" : 1,
    "size" : 266,
    "height" : 144,
    "version" : 3,
    "merkleroot" : "1367cfd9a44554f10464ecb372927ab0a7fffa365f15d4237edc748fc73a1b07",
    "tx" : [
        "1367cfd9a44554f10464ecb372927ab0a7fffa365f15d4237edc748fc73a1b07"
    ],
    "time" : 1510086260,
    "nonce" : 49,
    "bits" : "2000ffff",
    "difficulty" : 0.00000006,
    "chainwork" : "0000000000000000000000000000000000000000000000000000000000009100",
    "previousblockhash" : "00415711f9b16124ab8a351333c92c72980558d22a16d87e2ef87b94f843a1ba"
}
```

Fig. 9. Granting block mining permission.

5. Conclusion, discussion and future research

Blockchain is a promising technology for real-time accounting and continuous monitoring. Essentially, it is a publicly shared database that keeps records of all transactions ever executed within the ecosystem for a specified domain. Using cryptographic algorithms (e.g., digital signature and hash function), the blockchain protocol is able to guarantee data integrity, making it impossible to tamper with the transaction history. The property of irreversibility and tamper resistance could be applied in auditing for continuous monitoring and fraud prevention. However, to successfully deploy blockchain in enterprise information systems and achieve high-level data tamper resistance requires a large number of participants who would have access to the full copy of every transaction.

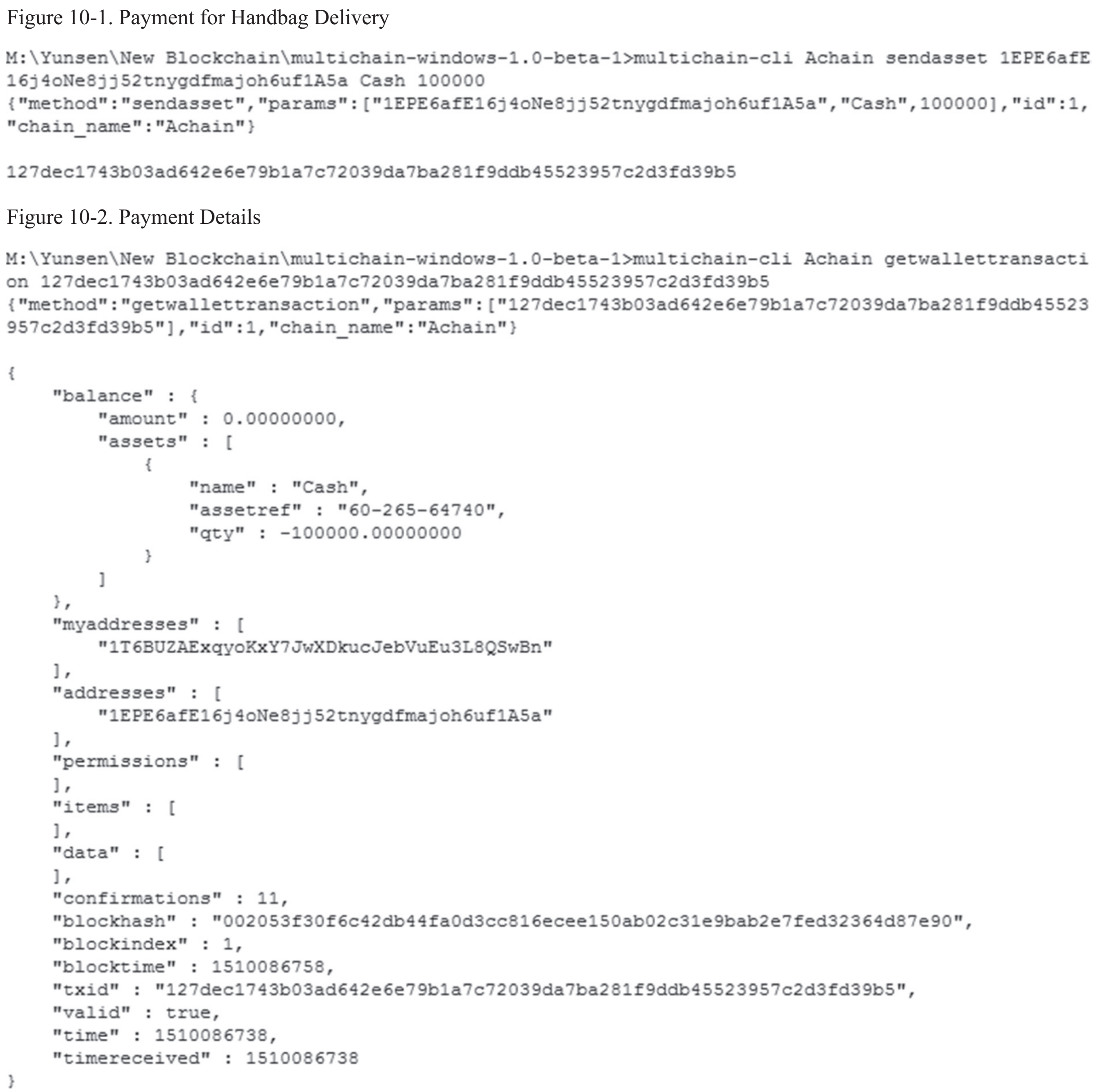


Figure 10-1. Payment for Handbag Delivery

```
M:\Yunsen\New Blockchain\multichain-windows-1.0-beta-1>multichain-cli Achain sendasset 1EPE6afE
16j4oNe8jj52tnygdfmajoh6uf1A5a Cash 100000
{"method":"sendasset","params":["1EPE6afE16j4oNe8jj52tnygdfmajoh6uf1A5a","Cash",100000],"id":1,
"chain_name":"Achain"}

127dec1743b03ad642e6e79b1a7c72039da7ba281f9ddb45523957c2d3fd39b5
```

Figure 10-2. Payment Details

```
M:\Yunsen\New Blockchain\multichain-windows-1.0-beta-1>multichain-cli Achain getwallettransacti
on 127dec1743b03ad642e6e79b1a7c72039da7ba281f9ddb45523957c2d3fd39b5
{"method":"getwallettransaction","params":["127dec1743b03ad642e6e79b1a7c72039da7ba281f9ddb45523
957c2d3fd39b5"],"id":1,"chain_name":"Achain"}

{
    "balance" : {
        "amount" : 0.00000000,
        "assets" : [
            {
                "name" : "Cash",
                "assetref" : "60-265-64740",
                "qty" : -100000.00000000
            }
        ]
    },
    "myaddresses" : [
        "1T6BUZAExqyoKxY7JwXDkucJebVuEu3L8QSwBn"
    ],
    "addresses" : [
        "1EPE6afE16j4oNe8jj52tnygdfmajoh6uf1A5a"
    ],
    "permissions" : [
    ],
    "items" : [
    ],
    "data" : [
    ],
    "confirmations" : 11,
    "blockhash" : "002053f30f6c42db44fa0d3cc816ecee150ab02c31e9bab2e7fed32364d87e90",
    "blockindex" : 1,
    "blocktime" : 1510086758,
    "txid" : "127dec1743b03ad642e6e79b1a7c72039da7ba281f9ddb45523957c2d3fd39b5",
    "valid" : true,
    "time" : 1510086738,
    "timereceived" : 1510086738
}
```

Fig. 10. Simulation of automatic payment confirmation.

Table 2
Computational overhead: Blockchain vs. database.

	Blockchain		Database	
Number of transactions	Computational time (s)	Record size (byte)	Computational time (s)	Record size (byte)
1	3.71	570	0.00	201
10	19.70	5700	0.01	2010
100	193.07	57,000	0.01	20,100
1000	1927.13	570,000	0.02	201,000

This table shows the comparison of computational overhead between the blockchain and database. This study simulated 1000 transactions and recorded the corresponding computational time (in seconds) from initiation of the first transaction to completion of the last transaction in both blockchain and SQLite database. This table also shows the data size of the records in both blockchain and SQLite database.

It is necessary to find a trade-off between the benefit of information sharing and the cost of weakening confidentiality, which is the motivation for the solution presented in this paper to protect confidential information in a public blockchain.

Based on the recent technical innovation of zero-knowledge proofs, we propose a Blockchain-based transaction processing system (Bb-TPS) and demonstrate its functionalities of real-time accounting, continuous monitoring, and permission management using a prototype. Furthermore, Bb-TPS uses the zk-SNARK scheme and homomorphic encryption to provide high-level confidentiality-preserving mechanisms. Finally, the comparative computational performance of blockchain and relational database in transaction recording is evaluated and discussed. This study contributes to the accounting information systems literature by (1) applying blockchain technology to accounting and auditing by designing a framework of Blockchain-base Transaction Processing Systems, (2) demonstrating the functionality of Bb-TPS in real-time accounting, continuous monitoring, and fraud prevention, (3) configuring the homomorphic encryption and zero-knowledge proofs to improve the confidentiality and security of Bb-TPS, and (4) developing a prototype to validate the framework and evaluate the performance of a Bb-TPS.

The accounting-blockchain convergence shows great promise for improving information integrity, decreasing transmission cost, increasing the speed of transaction settlement, and preventing fraudulent transactions. Furthermore, using zero-knowledge proofs and homomorphic encryption ensures data tampering resistance while preserving data confidentiality. Therefore, the deployment of blockchain enables improvement in the efficiency and effectiveness of accounting and audit practice. The limitation of this research is that it does not specify the details of the block mining and rewarding mechanisms as well as the implementation of zk-SNARK for Bb-TPS. The future research can continue developing the details of BB-CASs that comprise a series of smart contracts, which can continuously monitor transaction activities and automatically send notifications when trigger conditions are met.[22] Although at the current stage the computational overhead of blockchain is still significant compared to that of a relational database, it is expected that technology improvements will result in cost reductions allowing blockchain to become a widely utilized infrastructure for enterprise information systems and continuous monitoring systems.

Acknowledgments

The authors are grateful for the valuable comments provided by the discussants and participants at University of Waterloo Centre on Information Integrity and Information Assurance 10th Biennial Symposium.

References

Back, A., Corallo, M., Dashjr, L., Friedenbach, M., Maxwell, G., Miller, A., Poelstra, A., Timón, J., Wuille, P., 2014. Enabling Blockchain Innovations With Pegged Sidechains. Available at. https://blockstream.com/sidechains.pdf (Accessed 5/8/18 1:54AM).

Bengtsson, M., Kock, S., 2000. "Coopetition" in business networks—to cooperate and compete simultaneously. Ind. Mark. Manag. 29 (5), 411–426.

Ben-Sasson, E., Chiesa, A., Tromer, E., Virza, M., 2014. Succinct Non-Interactive Zero Knowledge for a Von Neumann Architecture. (Paper read at USENIX Security Symposium).

Blum, M., Feldman, P., Micali, S., 1988. Non-interactive Zero-knowledge and Its Applications. (Paper read at Proceedings of the twentieth annual ACM symposium on Theory of computing).

Buterin, V., 2014. A Next-Generation Smart Contract and Decentralized Application Platform. (white paper).

Dai, J., Vasarhelyi, M.A., 2017. Toward Blockchain-based accounting and assurance. J. Inf. Syst. 31 (3), 5–21.

Deloitte, 2016. Blockchain: Democratized Trust - Distributed Ledgers and the Future of Value. Deloitte University Press Available at. https://www2.deloitte.com/insights/us/en/focus/tech-trends/2016/blockchain-applications-and-trust-in-a-global-economy.html?id=us%253A2sm%253A3li%253Adup3039%253Aawa%253Acons%253A022516%253Att16%253Aauthoralumni (Accessed 5/11/18 8:00PM).

ElGamal, T., 1985. A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Trans. Inf. Theory 31 (4), 469–472.

Ernst & Young LLP, 2016. Blockchain Reaction: Tech Plans for Critical Mass. Available at. http://www.ey.com/gl/en/industries/technology/ey-blockchain-reaction-tech-plans-for-critical-mass (Accessed 5/8/18 2:03AM).

Gal, G., 2008. Query issues in continuous reporting systems. J. Emerg. Technol. Account. 5 (1), 81–97.

Gentry, C., 2009. A Fully Homomorphic Encryption Scheme. Stanford University.

Goldwasser, S., Micali, S., Rackoff, C., 1989. The knowledge complexity of interactive proof systems. SIAM J. Comput. 18 (1), 186–208.

Grigg, I., 2005. Triple Entry Accounting. Available at. http://financialcryptography.com/mt/archives/000501.html (Accessed 5/8/18 2:04AM).

Groomer, S.M., Murthy, U.S., 1989. Continuous auditing of database applications: an embedded audit module approach. J. Inf. Syst. 3 (2), 53–69.

Iansiti, M., Lakhani, K.R., 2017. The truth about blockchain. Harv. Bus. Rev. 95 (1), 118–127.

Ijiri, Y., 1986. A framework for triple-entry bookkeeping. Account. Rev. 745–759.

Jordan, S., 2009. Implications of internet architecture on net neutrality. ACM Trans. Internet Technol. (TOIT) 9 (2), 5.

Kosba, A., Miller, A., Shi, E., Wen, Z., Papamanthou, C., 2016. Hawk: The Blockchain Model of Cryptography and Privacy-preserving Smart Contracts. (Paper read at Security and Privacy (SP), 2016 IEEE Symposium).

KPMG International, 2017. Blockchain Accelerates Insurance Transformation. Available at. https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2017/01/blockchain-accelerates-insurance-transformation-fs.pdf (Accessed 5/8/18 2:04AM).

Nakamoto, S., 2008. Bitcoin: A Peer-to-Peer Electronic Cash System. Available at. https://bitcoin.org/bitcoin.pdf (Accessed 5/8/18 2:04AM).

Nasdaq, 2015. Nasdaq Linq Enables First-Ever Private Securities Issuance Documented With Blockchain Technology. Available at. http://ir.nasdaq.com/releasedetail.cfm?releaseid=948326 (Accessed 5/8/18 2:04AM).

Pastena, V., 1979. Some evidence on the SEC's system of continuous disclosure. Account. Rev. 776–783.

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 (Accessed 5/8/18 2:04AM).

Rackoff, C., Simon, D.R., 1991. Non-interactive Zero-knowledge Proof of Knowledge and Chosen Ciphertext Attack. (Paper read at Annual International Cryptology Conference).

Reid, F., Harrigan, M., 2013. An analysis of anonymity in the bitcoin system. In: Security and Privacy in Social Networks. Springer, pp. 197–223.

[22] For example, if a BB-CAS detects that an employee ID of a purchase payment transaction is identical to the employee ID of the corresponding purchase order transaction, the BB-CAS would raise an alarm of the violation of separation of duties. Blockchain neutrality needs to be carefully taken into consideration when using smart contacts to design the BB-CAS.

Rezaee, Z., Ford, W., Elam, R., 2000. Real-time accounting systems. Intern. Audit. 57 (2), 62–67.

Rizzo, P., 2016. Sydney Stock Exchange Completes Blockchain Prototype. Available at. https://www.coindesk.com/sydney-stock-exchange-blockchain-prototype/ (Accessed 5/8/18 2:05AM).

Shubber, K., 2016. Banks find blockchain hard to put into practice. Financ. Times Available at. https://www.ft.com/content/0288caea-7382-11e6-bf48-b372cdb1043a (Accessed 5/8/18 2:06AM).

Simon, G., 2016. Blockchain and the Introduction of Single-Entry Bookkeeping. Available at. https://medium.com/@Loyyal/blockchain-and-the-introduction-of-single-entry-bookkeeping-5e5b201db09 (Accessed 5/8/18 2:06AM).

Szabo, N., 1994. Smart Contracts. Unpublished manuscript. Available at. http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html (Accessed 5/8/18 2:07AM).

Vasarhelyi, M.A., Halper, F.B., 1991. The continuous audit of online systems. Auditing. J. Pract. Theory 10 (1), 110–125.

Yermack, D., 2017. Corporate governance and blockchains. Rev. Financ. 21 (1), 7–31.