Blockchain-based Payment Collection Supervision System using Pervasive Bitcoin Digital Wallet

Po-Wei Chen,
School of Software and Microelectronics,
Peking University
24th Jinyuan Road, Daxing Industrial District, Beijing 102600, China
powei.chen@pku.edu.cn

Bo-Sian Jiang, Chia-Hui Wang
Department of Computer Science and Information Engineering, Ming Chuan University,
No. 5 De Ming Rd., Gui Shan District, Taoyuan City 333, Taiwan
{05366070@me, wangch@mail}.mcu.edu.tw

***Abstract*—After years of tremendous development and research in digital currency, the most famous Bitcoin industry chain has been gradually completed including mining, exchange, currency exchange, ATM, pervasive digital wallet design and so on. Especially, its blockchain technology has become FinTech organizations' emerging business and research directions, also been applied in the interdisciplinary medical science, supply chain and Internet of things. Digitizing currency can solve many problems in physical currency, such as the rampant counterfeit banknotes. Thus, not only the transparency can be cost-effectively preserved in store's ledger, but also customer's rights and interests can be protected while using the digital wallet. For the government, the regulation and auditing of financial transaction can be made simpler and more convenient for tax collection issue. Digitized transaction details can be much easier to audit by any computing device than manually audit the conventional ledger books. Furthermore, to make merchandise store to use digitized currency much easier, in this paper, we propose and deploy a Bitcoin collection supervision system called BPCSS based on blockchain technology with cloud databases for customers and merchandise stores. The preliminary experimental results via the well-known pervasive digital wallet of Testnet Bitcoin demonstrate the proposed BPCSS can cost-effectively collect payment and supervise the transactions between customer and merchandise store running the implemented NFC-enabled Android Apps.**

***Index Terms*—Bitcoin, pervasive digital wallet, blockchain, cloud database, NFC, Android App.**

I. INTRODUCTION

IN the traditional centralized financial system, we will encounter many problems such as follows. First, we can do banking business only when bank's office hour, though all banks have opened a few transaction services over pervasive Internet with some limitations. Second, the transnational remittance will also encounter the review in international wire transfer. For example, if sending a sum of money from the local bank of United States to a bank in China, not only needs to wait for the office hours in these two different national banks, but also payee needs to wait three working days even after the wire transfer to China and the submission of declaration document to prove the source of this money. Third, the customer finally needs to pay a fee of up to NT$ 750. Among these many problems mentioned above in conventional money transactions, the emerging blockchain technology has become the best solution to solve the time difference problem of transnational remittance. Based on the peer-to-peer (i.e. P2P) architecture and anonymity in blockchain technology, so customers do not need to go to the bank to declare the source of funds, do not need to pay a high amount of cross-border wire transfer fee.

Bitcoin is a P2P electronic cash system, compared to traditional centralized financial institutions. Decentralized design can bring more advantages, such as reducing the risk of cyber-attacks, because the storage of blockchain is distributed across the Internet computers running full node[14] via P2P network technology[5]. Nowadays Bitcoin blockchain size has reached more than 100GB. All the data in Bitcoin transaction is permanently stored in blockchain since 2009. The computers running the Bitcoin system in the world are up to more than six thousand network nodes according to the statistics. It means that the blockchain information has been copied over six thousand times. Such a large number of network nodes for blockchain backup can ensure the stability of Bitcoin network. The failure of a host does not affect the normal operation of Bitcoin network. Besides, the decentralized system applied in Bitcoin network, people do not need to operate, manage and maintain manually at any time. So, Bitcoin system can run continuously without disruption in fair stability, very different from the traditional centralized financial organizations.

The traditional financial transaction system is composed of many traditional financial organizations. Users have to trust the closed payment flow to use these organizations' financial services. However, the centralized financial transaction system has some problems that need to be overcome. For example, since all transaction information is managed centrally, customers are not authorized to freely access their transaction information. These transactions are not publicly reviewed and customers are forced to trust their financial companies in the safety of funds, including the flow of funds.

If these traditional central financial institutions apply blockchain technology in their financial flow system. The blockchain technology will be inherited to indicate that the transaction records will be transparent to all the customers to review. So, there will be no unknown cash flow problems. It not only preserves money flow transparent, but also ensures that

978-1-5386-3839-2/17/$31.00 ©2017 IEEE

consumers' transaction records won't be changed and deleted. That's to say, the seller can believe that the algorithm's correctness by using blockchain technology to trust the transaction and further grasp all the transaction details clearly, or even the company's business status can be provided easily. Then, the human resources can be reduced to efficiently generate financial statement and statistics reports. Finally, the government can easily review and believe the correctness of all the business transaction information. For the tax collection, it also can have a standardized, trusted and fully automated operating procedure. It can reduce not only the labor cost, but also the errors in government taxation procedure.

Therefore, in this paper, we propose a Blockchain-based Payment Collection Supervision System, which is abbreviated as BPCSS, for transactions between customers and merchandise stores who use the pervasive Bitcoin digital wallet. All transaction details can be cost-effectively saved on the cloud database right after customers use their NFC-enabled[31] Android smartphone App to purchase RFID-tagged goods in merchandise store. The customers and merchants can review these transaction details without troubles mentioned before in traditional financial system.

This paper is organized as follows. In Section II, the blockchain technologies related to pervasive digital wallet are introduced. In Section III, the subsystems and their functions in proposed BPCSS system are described in details to provide blockchain-based payment collection supervision using Bitcoin digital wallet. In Section IV, preliminary digital currency transaction experiments on the implemented subsystems of BPCSS prototype are conducted via Bitcoin Testnet[29] and performance analysis is concluded. The last section summarizes the proposed solution and provides future work.

II. RELATED WORKS

In this section, we first introduce the popular financial transaction technology related to Visa without using physical currency. Then, the blockchain technology of Bitcoin digital currency is introduced to motivate our design and implementation of proposed BPCSS system for transactions using digital currency on mobile devices through pervasive Internet.

A. Visa Technology

Visa Debit[6] is a debit card, it can withdraw money from the ATM and also spend money directly in the store. A debit card can be charged directly from the user's deposit account. If the user's account balance is insufficient, the transaction process will not be completed. It does not produce over-the-limit, overdraft or the occurrence of revolving interest rate, so that cardholders can easily control the budget and expenses. Visa Debit uses the chip card reader to read the data in credit card. The data includes the Visa logo and the 16-digit card number. It is different from the credit card, Visa Debit is a product of deposit account, so the card holder will have a bank saving account.

Visa Token[7] is a random virtual code converted from the credit card's card number. It can replace the account information on traditional credit card to reduce the risk of account information being stolen. Visa was the first to develop this token code service technology to solve the security issue that the store has to keep a large amount of credit card account numbers from customers. With the Visa Token, when the store needs to charge on customer's credit card, the credit card reader will send the authorization request to the card issuer according to the token code. The card issuer will validate if the token code matches with the credit card number and then to complete the charge or not. Thus, the store will not directly get the card number of consumers. Actually, the card numbers are managed by a more secure Token Vault[16]. A group of card numbers can correspond to multiple sets of token codes and the codes can be also limited in their usage. So, if there is a token code accidentally stolen, the loss can be reduced much less than before. The higher level mobile payment services such as Apple Pay[17] and Android Pay[18] are all based on the Visa Token technologies.

B. Blockchain Technology

Since 2009, the birth of Bitcoin, an encrypted digital currency[2], setting off a new wave of monetary revolution. Based on cryptography, P2P networks, consensus algorithms and blockchain technology, they are combined into digital currency such as Bitcoin. It's still working vigorously after lots of attacks and fraud events in eight years so far. Bitcoin[1] has been the most representative digital currency over the Internet.

Bitcoin applies many technologies, they can be roughly divided into four blocks of the wallet address generation. These four blocks are Bitcoin transaction signature/broadcast, blockchain technology and decentralized ledgers respectively. Bitcoin is one of the most typical applications applying blockchain technology. We will describe some details of blockchain technology.

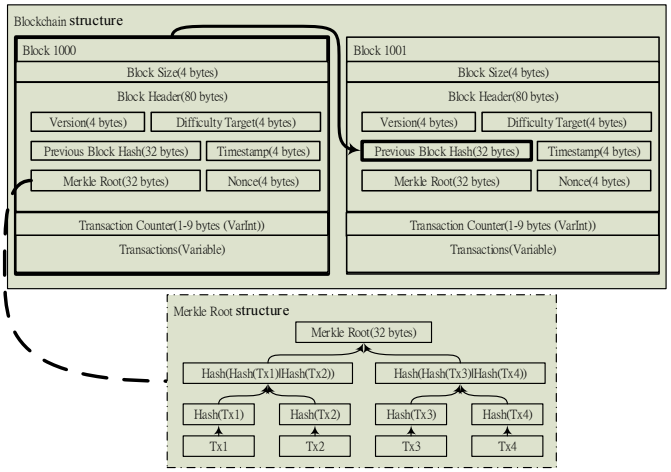

Fig. 1. Blockchain structure diagram

1) Blockchain structure

Blockchain structure as shown in Fig. 1 is divided into two parts. One is the block headers of the blockchain and the other is all transactions stored in the existing blocks. Block header includes block version, parent block hash value, Merkle root[10], timestamp, difficulty and nonce:

- *Block Version* (4 bytes): Store the relevant version number of the blockchain system and protocol.
- *Parent Block Hash Value* (32 bytes): Record the hash value of the previous block. According the parent block hash value, all blocks can be joined together to form a blockchain. Not only the virtual links can be established in blockchain, but also it makes the block more difficult to be tampered. It's because the new blocks are constantly being superimposed on the old blocks, the hash values of old pieces will continue to be passed to the latest piece. The more stacking of the hash value on the stack is indirectly cited more often, so the earlier created blocks are harder to be modified.
- *Merkle Root* (32 bytes): the hash value of Merkle tree root in blockchain can be used to quickly check the correctness of all stored transaction on current block.
- *Timestamp* (4 bytes): record the block generation time in year, month, day, hour and second.
- *Difficulty* (4-byte): difficulty target value for the solution of the proof-of-work algorithm[9].
- *Nonce* (4 bytes): record the current block of proof-of-work algorithm solution.

The block body of blockchain can be changed since it was designed for different applications. For examples, Bitcoin blockchain has been recording all transactions since 2009. Its transaction field has been designed to allow many transaction models of many-to-one, one-to-many, many-to-many and even the none-to-many (i.e. the reward for creating a block, and no certain source of Bitcoin). In addition to the digital currency like Bitcoin applying blockchain technology, there are many other diversified functions of the blockchain designs, such as the ticket blockchain[19] and food security blockchain[20] are under development and testing.

2) The advantages of blockchain for digital currency

a. Open and transparent trading information:

- Trustworthiness: On the basic architecture of public blockchain, all transaction records are open and transparent, so that all nodes involved in the storage for transaction block data can review the transaction data, then all people can check the correctness of each transaction record. Disclosure of transaction information makes the transaction data credible.
- Metadata: In addition to the trustworthiness which is the cornerstone of blockchain, open and transparent properties are allowing more developers or new companies to obtain raw materials in trading much easier. After all, in the cash financial system, all the transaction records are stored by the central financial institutions. It is not easy to extract the original transaction information from the central financial institution. The open and transparent nature of the blockchain has prompted financial companies to reduce the threshold of effort for obtaining raw data. Companies or scholars can make a visual development plan, or even use large data to analyze the valuable points of views never seen before.

b. Blockchain transaction data cannot be modified and deleted:

In the blockchain structure, all the information after the strict verification are recorded in the blockchain and they cannot be deleted. Based on the characteristics of blockchain, the hash value of the old block is stored in the new block during the connection of new block to the original blockchain. As long as a value in the block is modified, even a bit, will make the hash value is completely different, that is to say, avalanche effect will be happened. Because of this structure that all the information will never be changed, if the result of the verification is changed, the block will not be accepted by the system. Therefore, all the transaction records, which have been stored into the blockchain, cannot be modified and deleted.

c. Peer-to-peer network architecture:

Blockchain trading system is based on P2P network architecture and inherited the decentralized characteristics. Because of the P2P'de-centralized protocol, all nodes are not only playing the role of clients, but also playing the role of servers. In such decentralized network in the world, compared with the traditional centralized server usually presented in the web service with a single-digit scale of the server hosts, Bitcoin system can be expanded to more than six thousand nodes. So, Bitcoin network can do better job to prevent from the denial-of-service attacks. In recent years, because of the Bitcoin prevalence and anonymity, it become the main way to pay off to the ransomware. However, blockchain is based on the P2P network. Even a single node data is locked by the attacker's encryption from ransomware. Such an extortion to decentralized Bitcoin network does not pose a big threat, after all, there are a lot of data nodes in the Bitcoin network and will not have much impact from the damage of a single node.

d. Anonymity:

In current society, personal information protection has become the most important issue for companies. All accounts created in the blockchain system do not establish a direct relationship to the entities in the real world, then anonymity is established. All the accounts in blockchain system seem to be created in separate anonymous individuals can effectively protect the privacy for consumers. However, the Visa transaction is different and users will reveal a lot of personal information to the centralized host machine in Visa company. This may introduce the risk of personal information leakage. In the blockchain technology, this problem can be avoided cost-effectively.

e. Autonomous system:

In the blockchain system, the operation relies on some algorithms including the consensus algorithm[21]. Therefore, in such an autonomous system, no one (e.g. node or miner) can directly determine the rules of the system operation. If you find a serious error in the Bitcoin system that needs to be corrected, you can propose to upgrade the Bitcoin system with Bitcoin Improvement Proposals[22]. The proposed Bitcoin Improvement Proposals are required to be supported by more than a certain number of miners in the Bitcoin system before the upgraded modules can be officially run on Bitcoin system. Because of this kind of democratic mechanism, the blockchain

system usually cannot make a major variation, but it is relatively stable.

3) Bitcoin blockchain problem

a. Insufficient Block capacity:

The Bitcoin was originally designed to apply the proof-of-work algorithm so that the creation of a Bitcoin block could be completed on average about every ten minutes. The block size is default to set as 1MB. Assuming that block is fully filled with transactions, according to the average size of 300 bytes in one Bitcoin transaction currently, then each block can accommodate up to three thousand transactions. That is to say, up to 5 to 6 transactions per second can be completed in Bitcoin system. The centralized electronic payment company such as VISA usually has reached average 2000 and maximum 4000 transactions per second. Up to 4,000 deals per second. However, Bitcoin system can only handle 5 to 6 transactions per second and it has a lot of room for improvement.

b. Long-time block generation:

According to the proof-of-work algorithm applied in Bitcoin. The above-mentioned difficulty parameter is the key factor of the generation time of the Bitcoin block. But solution time of the unexpected proof-of-work problem is not stable. For example, in Bitcoin blockchain, the fastest time to solve a problem is three seconds and the longest time is more than 50 minutes to solve a problem. We can shorten the block generation time via reducing the complexity of the proof-of-the-work problem, so that the block generation time can be down to average generation time such as five minutes. But, we also need to consider that if the block generation time is too short, all the data nodes cannot complete the blockchain synchronization. This will incur so-called blockchain fork[23], and then the Bitcoin system crashes.

c. Non-scalable technical extension:

In the Bitcoin system, its blockchain structure was designed to record only transaction records and cannot be extended with more features and applications. There are many developers who want to extend Bitcoin system to other applications like smart contracts[24]. But, they later found it's a challenging work based on the original Bitcoin system framework. Thus, Vitalik, the author of the world's second largest digital currency called Ethereum[25], has also created Ethereum virtual machine. So, the created smart contract can be run on the unified Ethereum platform. Ethereum breaks the technical bottleneck of Bitcoin.

4) Blockchain's Applications

However, based on the blockchain technology, applications other than digital currency can be created. These applications are such as the free network domain name resolution service called Namecoin[26], the electronic contract called Ethereum, the use of ring signatures technology to furnish the full anonymous transactions in electronic money system called Monero[27] and the decentralized blog called STEEM[28].

In [8], Melanie Swan said that the blockchain applications can be divided into three categories of blockchain 1.0, blockchain 2.0 and blockchain 3.0 as described as follows:

a. Blockchain 1.0 - Digital Currency:

Blockchain 1.0 is mainly embodied in money, such as money transfer, exchange and payment systems. The most common is to Internet cryptocurrency, while Bitcoin is the most famous one. Bitcoin blockchain is the most effective transnational flow system in many countries around the world. The Internet cryptocurrency use the blockchain technology to complete the fund transfer of funds between users.

b. Blockchain 2.0 - Smart Contract:

The practice of Blockchain 2.0 is smart contract. Today's blockchain technology focuses on the application of market economy and finance. In addition to simplicity of the transfer of funds, the financial products created in life can be also the objects to apply blockchain. They include such as stocks, bonds, futures, loans, property rights, smart assets and smart contracts. The initial stage of blockchain 1.0 is widely used in the storage of transactions. In addition to the application of transaction records, blockchain can be viewed as a database and inventory list for recording, tracking and transferring of all assets. Moreover, it can be as a record of any formation of asset registration, inventory and transaction information.

c. Blockchain 3.0 - Decentralized Applications:

Blockchain 3.0 not just disengage from the applications the market economy and finance. It emphasizes more on government, health, science, literature, culture, art and other fields. For example, in the Estonian government since last year, the national identity card is built in the blockchain, to sign a commercial contract or an application for marriage certificate.

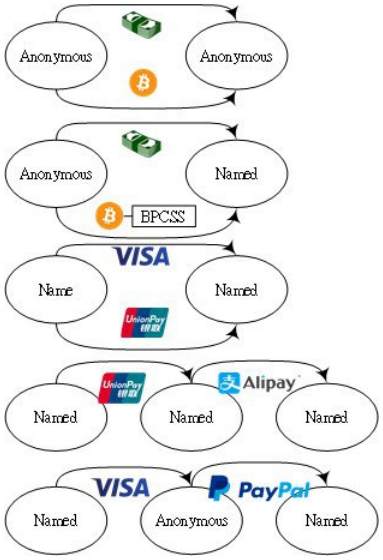

Fig. 2. Five digital currency transaction models (customer-to-store)

III. Proposed Blockchain-based Payment Collection Supervision System

According to the above-mentioned characteristics and current status of blockchain-enabled digital currency, in this paper, not only the solutions to transaction dispute and government supervision are proposed for digital currency transaction between customer and store in prevalent models (as

shown in Fig. 2) of anonymous-to-anonymous and anonymous-to-named, but also the demonstration platform is designed and implemented for the real-world digital currency transaction between customers and stores who are using Bitcoin.

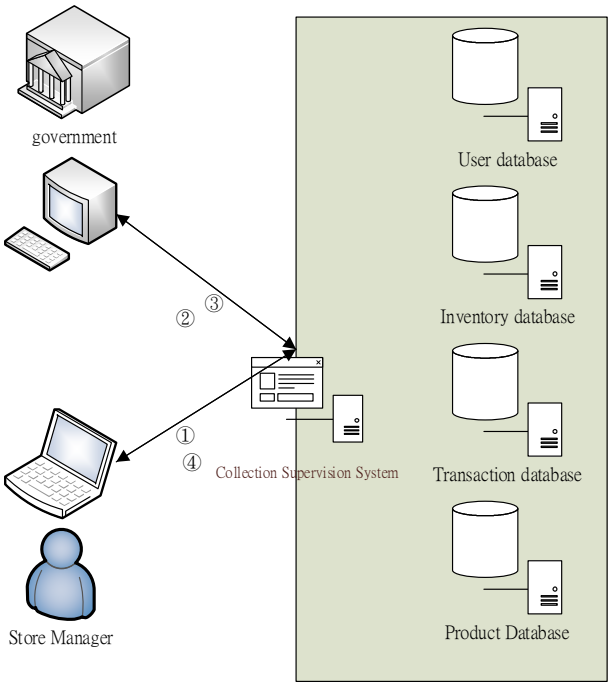

Fig. 3. The core architecture of BPCSS and merchant registration flow

In the proposed BPCSS system, the blockchain-based payment collection supervision is practiced on Bitcoin digital currency, the BPCSS includes three subsystems which are SMIMSS(Store and Merchandise Information Management Sub-System), SMCTSS(Store Mobile payment Collection and Transaction Sub-System), CMPTSS(Client Mobile Payment and Transaction Sub-System) and we will describe these subsystems later. Moreover, BPCSS applies four cloud databases which are business information, business product, inventory and transaction databases. As shown in Fig. 3, the functions of these cloud databases are described as follows:

1) Merchant database: stores information of the businesses which are under review or have already been audited by government. The stored information includes the merchant ID, business name, business location, merchant's digital currency address, and GPS coordinates.
2) Product database: Only the authorized users can log in to add or modify the information about the products for trading. The product database content includes product identification number, product name, product description, dates, prices and other related information.
3) Inventory database: including product number, merchant number, product inventory amount and other related information.
4) Transaction database: it records values including the transaction serial number, the product identification number, product trading amount, merchant's digital currency payee address, the consumer's digital currency payment address, the merchant ID, and last to-be-confirmed field.

Meanwhile, in proposed BPCSS architecture, merchants need to have registration to the Collection Supervision System (i.e SMIMSS) in the following 4 steps as also shown in Fig. 3:

1) The merchant must register an account with BPCSS with a proof of business certificate from government regulations.
2) BPCSS will automatically submit the business application to the corresponding government financial supervisory unit for reviewing the store's digital currency transaction business.
3) If the government approved the application from the store's digital currency business, the server will activate the store's account created by the merchant in this collection supervisory system.
4) Then, the merchant is free to sign in to the account and add the products that the merchant wants to sell and check their digital currency transaction data such as product inventory and product transaction records.

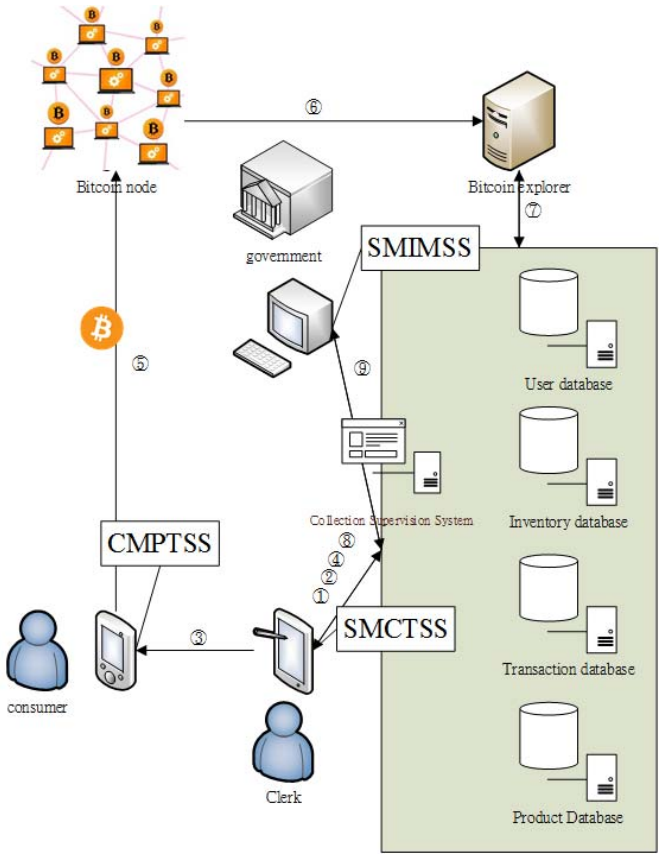

Fig. 4. The overall operational flow of BPCSS

Moreover, the realistic BPCSS operation flow for digital currency transaction is as shown in Fig. 4 above. First, we need to connect to blockchain explorer[30]. The proposed BPCSS monitoring system can apply the blockchain explorer to match the transaction activity with the recorded transaction in BPCSS. Such a design can help BPCSS to achieve the immediacy and correctness in digital currency trading. If immediacy and correctness were worried about the results only from a blockchain explorer, we can use multiple blockchain explorers

for cross references to avoid the business impact from a blockchain explorer company's mistakes. The purpose of using blockchain explorer is to quickly and accurately conclude the deal. It's one of the major steps to make the whole transaction from issuing to completion.

As shown in Fig. 4, the steps to create a transaction in BPCSS are described as follows:

1) Merchant's clerk will log in to an account as created from previous steps shown in Fig. 3 to access the service in SMCTSS with a handheld tablet or even a smartphone. As mentioned before, the merchant account must be audited by government agencies before being able to log in to the system.
2) While successfully log in to SMCTSS for merchant digital currency flow monitoring system, the mobile device will load the store product information registered via SMIMSS and then create the product catalog. The store's clerk can pick the required product and the quantity according to the customer's needs.
3) After clerk using his/her devices to complete the product information of selected goods from customer. The NFC technology on the mobile devices can be used to pass product information to consumer's mobile device from near clerk's mobile device without physical interactions. Then, consumer can easily record his/her own consuming information as a reference like invoice. At the mean time of receiving a message of buying product from merchant clerk device to customer device, the customer device will also send a message of its own Bitcoin payment address to the merchant's mobile device.
4) After the merchant's handheld device receives the corresponding information from customer's confirmation of buying selected product, it will send a copy of transaction information to the SMIMSS monitoring system. The consumer information includes the transaction serial number, the merchant ID number, the merchandise number, the quantity of the merchandise purchased, and the payee address of the digital currency, as well as the payment address of the consumer.
5) After receiving the consumer transaction information, this confirmation will enable to pay by the digital currency such as Bitcoin. At mean time the digital currency for this transaction will be issued to be signed in Bitcoin network for verification and recording.
6) Then, the blockchain explorer will begin to analyze all transactions cached in the Bitcoin network, as well as the transactions that have been recorded in the blockchain.
7) The proposed transaction monitoring system BPCSS will make a request to the blockchain explorer. This request data includes not only the digital currency payee address from the transaction copy stored in BPCSS as described in the fourth step of Fig. 3, but also the digital currency payment address of customer's expected payment. The blockchain explorer use the request data to check whether the transaction has been stored in the blockchain or the transaction is still waiting to be confirmed. If the transaction has been confirmed and stored in the blockchain, the value of the transaction "to-be-confirmed" field in the transaction database is changed to "1", otherwise its default value is zero.
8) While the value in the transaction "to-be-confirmed" field is "1", the "Transaction is completed" message can be sent to the SMCTSS running on store's tablet.
9) Government financial supervisory unit can review all the transaction information in the proposed BPCSS for the auditing reference in tax collection.

IV. Digital Currency Transaction Experiments and Results on Bitcoin Testnet

To validate and demonstrate the feasibility and effectiveness of proposed PBCSS for Bitcoin payment collection supervision, we implemented its subsystems of SMIMSS running on Java application for merchant's merchandise management and maintenance, SMCTSS running on Android App for merchant's clerks, and CMPTSS running on App for customers.

As shown in Fig. 5, SMIMSS java application can help merchant to login to system or create a new account. After the authorized merchant logins to the system successfully, the merchant can insert or update the product list as shown in Fig. 6. The implemented SMIMSS java application performs functions described in previous section.

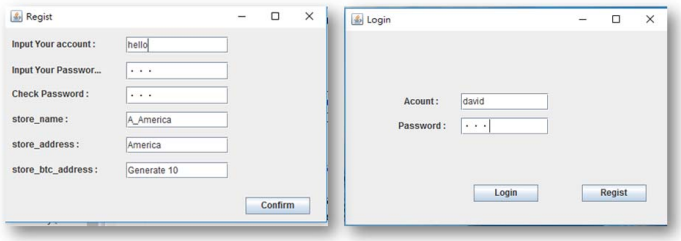

Fig. 5. Registration and login interfaces of Java application for SMIMSS

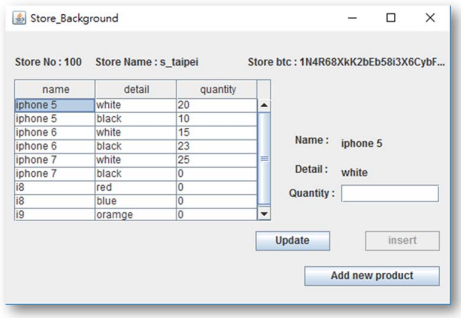

Fig. 6. Insert or Update product catalog for authorized merchant in SMIMSS

After the merchant's product information including RFID tags are stored in the cloud database via SMIMSS, the clerk in merchant store can use our implemented Android App of SMCTSS with enabled NFC listener to read RFID tag information from customer's purchasing products in shopping cart. In the first activity as shown in Fig. 7, merchant clerk has to login to get the authorized access to SMCTSS functions. Then, in the 2nd activity, the SMCTSS App can list the scanned products in the shopping cart via checking the product RFID tag information with the cloud databases applied in SMIMSS and show them to the customer. In the 3rd activity of Fig. 7,

customer can request clerk to remove a purchasing item to confirm the final purchase. Finally, SMCTSS App will automatically use the Bitcoin Testnet to help clerk to confirm the issuing the payee address for this digital currency transaction, as shown in the 4th activity of Fig. 7.

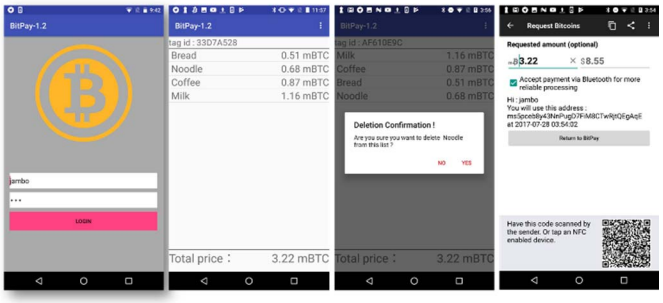

Fig. 7. 4 activities of login, items listed in shopping cart, confirmation to remove item, and Bitcoin payment confirmation in SMCTSS App.

At the meantime, customer will use the CMPTSS Android App corresponding with SMCTSS App to complete the purchasing product transaction via Bitcoin digital currency. As shown in Fig. 8, the first activity indicates the customer's confirmation for the purchasing products to create the transaction list to transaction database, the 2nd activity indicates the confirmation of payment including the amount and payer Bitcoin address, the 3rd activity shows the transaction history of transaction as a buyer or even a seller, Finally the invoice of detailed purchasing products for a single transaction is shown in 4th activity.

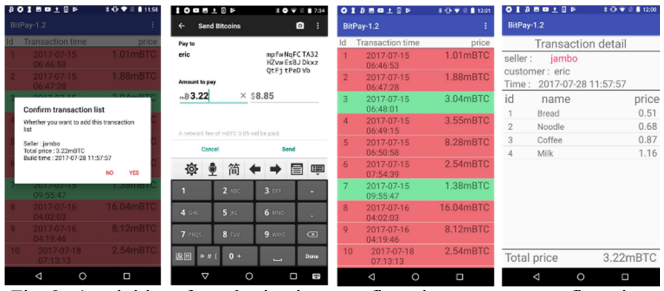

Fig. 8. 4 activities of purchasing item confirmation, payment confirmation, transaction history, and purchasing invoice in CMPTSS App.

According to Bitcoin's peer-to-peer architecture, though the transaction details between customer and store has been quickly stored to cloud databases, officially confirming the transaction to current Bitcoin blockchain usually takes much longer time, since the number in "to-be-confirmed" field is needed to be secured against double spending [32] after the transaction broadcasting to Bitcoin P2P network and stored to the cache pool.

Thus, to validate that our proposed BPCSS won't affect the transaction completion time via using digital currency like Bitcoin, we sequentially recorded information of 30 transactions in our Testnet experiment. Meanwhile, we firstly used a blockchain tool as shown in the first snapshot of Fig. 9, secondly used Testnet to sequentially conduct 30 Bitcoin transactions as shown in the middle snapshot of Fig. 9, Finally the 30 transaction completion times are all recorded in blockchain explorer. The experimental results show that all transactions in experiments are sent to cache pool of Bitcoin network about 3 seconds (2.97 in average, standard deviation is less than 1), the average transaction completion time confirmed in Bitcoin blockchain is 522.33 seconds in average (less than 9 minutes) and the standard deviation is about 339. The preliminary experimental results on the Bitcoin Testnet demonstrate that our proposed BPCSS can cost-effectively perform the blockchain-based payment collection supervision.

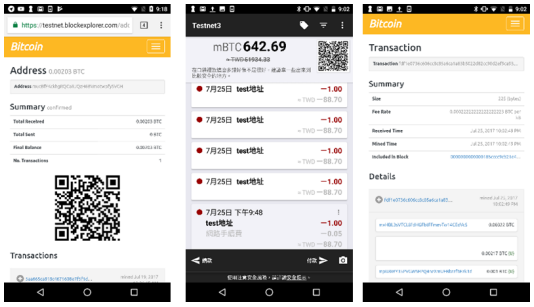

Fig. 9. Using blockchain explorer to validate the during of transaction stored in Bitcoin blockchain

V. Conclusion and Future Works

In this paper, we propose and implement a blockchain-based payment collection supervision system called BPCSS not only for customer and merchant who respectively spend and earn digital currency, but also for government financial supervisory unit to audit digital currency transactions and then to help to raise the tax collection. Moreover, the preliminary results of digital currency transaction experiments, using the famous pervasive digital wallet of Testnet Bitcoin and cloud databases with our implemented Java application and Android Apps, demonstrate the preserved cost-effectiveness in digital currency transactions and supervision between payer and payee in proposed BPCSS. The proposed BPCSS architecture also includes the following characteristics:

1) Business registration to proposed BPCSS can be subject to government approval.
2) All the goods for sale will be subject to government review.
3) Consumers are still anonymous to ensure the privacy of personal information.
4) Consumers' transaction records cannot be deleted.
5) If consumers have questions about the transaction to appeal, they need to present the transaction invoice or prove that access right of the address of payer or payee.
6) All transaction records are open and transparent.
7) The original transaction data is recorded by the blockchain technology, with high reliability, the de-centralized and the untampered data.
8) The government can check the transaction records from the proposed BPCSS system to review the tax information in a cost-effective way.

The advantages of proposed BPCSS are summarized as follows:

1) *For consumers*: The transaction information is open and transparent, so the rights and interests of consumers are protected. Since the transaction is credible and has clear timestamp. When consumers need to appeal their transactions to their consumer rights, they can have more

effective and credible proofs from proposed system.

2) *For business*: Businesses can do statistics and calculations for their own business purposes based on all the digitized transaction information. This can reduce the errors in computing results from manual operation. The statistical data can be even combined with store's inventory management to make goods and funds in required balance, to further improve the business in accounting accuracy and labor cost.
3) *For government*: In the process of resolving the transaction dispute, more credible evidence can be provided for reference. The digital transaction receipts also can solve the problem of the paper receipt faked or lost. Considering taxation, government can review the details of the business transactions with high credibility as a tax calculation procedure to find out the standards of taxing rates to reduce many disputes in tax collection.

In the near future, we will furnish the implementation of the supervision functions for government financial supervisory unit. Especially, we need consider a cost-effective way to enhance the security and privacy protection in accessing cloud databases for customers, stores and financial supervisory units.

ACKNOWLEDGEMENT

This work is partially supported by the Ministry of Science and Technology, Taiwan, Project Number is MOST 105-2221-E-130-006.

REFERENCES

[1] Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system,"(2008):28, http://s3.amazonaws.com/academia.edu.documents/32413652/BitCoin_P2P_electronic_cash_system.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1501401070&Signature=QmIcxT%2FIEHKCgRvMhxWwqbFEkc0%3D&response-content-disposition=inline%3B%20filename%3DBitcoin_A_Peer-to-Peer_Electronic_Cash_S.pdf

[2] Grinberg, Reuben. "Bitcoin: An innovative alternative digital currency."(2011), http://www.bitcointrading.com/pdf/bitcoinbyreubengrinberg.pdf

[3] Gilbert, Henri, and Helena Handschuh. "Security analysis of SHA-256 and sisters," Selected areas in cryptography. Springer Berlin/Heidelberg, 2004.

[4] Anoop, M. S. "Elliptic curve cryptography," An Implementation Guide (2007), https://pdfs.semanticscholar.org/c392/80642a84f3067f5ced358122f552a4769fbc.pdf?_ga=2.1902578.216214653.1501397973-747388919.1501397973

[5] Fox, Geoffrey. "Peer-to-peer networks." Computing in Science & Engineering 3.3 (2001): 75-77.

[6] Buba, Zirra Peter, and Gregory Maksha Wajiga. "Cryptographic algorithms for secure data communication." International Journal of Computer Science and Security (IJCSS) 5.2 (2011): 227-243.

[7] Stapleton, Jeff, and Ralph Spencer Poore. "Tokenization and other methods of security for cardholder data." Information Security Journal: A Global Perspective 20.2 (2011): 91-99.

[8] Swan, Melanie, "Blockchain: Blueprint for a new economy," O'Reilly Media, Inc.", 2015.

[9] Svensson, Jonatan, and Johan, Zeeck. "Proof-of-Work, "http://www.csc.kth.se/utbildning/kth/kurser/DD143X/dkand12/Group5Mikael/report/JonatanSvensson_JohanZeeck.pdf

[10] Szydlo, Michael. "Merkle tree traversal in log space and time," International Conference on the Theory and Applications of Cryptographic Techniques. Springer Berlin Heidelberg, 2004.

[11] González, Andrés Guadamuz. "PayPal: the legal status of C2C payment systems," Computer law & security review 20.4 (2004): 293-299.

[12] Lifan, Qiao. "something about privacy leak of Alipay platform." http://d.wanfangdata.com.cn/Periodical/ranj-jyxdh201606466

[13] Preibusch, Sören, et al. "Shopping for privacy: Purchase details leaked to PayPal," Electronic Commerce Research and Applications 15 (2016): 52-64.

[14] Antonopoulos, Andreas M, "Mastering Bitcoin: unlocking digital cryptocurrencies," O'Reilly Media, Inc.", 2014.

[15] Garzik, Jeff. "Making decentralized economic policy." (2015).

[16] Token Vault, https://www.rambus.com/blogs/what-is-a-token-vault/

[17] Apple Pay, https://www.apple.com/apple-pay/

[18] Android Pay, https://www.android.com/pay/

[19] Mathieu, Florian, and Ryno Mathee. "Blocktix: Decentralized Event Hosting and Ticket Distribution Network," (2017), https://blocktix.io/public/doc/blocktix-wp-draft.pdf

[20] Tian, Feng. "An agri-food supply chain traceability system for China based on RFID & blockchain technology." Service Systems and Service Management (ICSSSM), 2016 13th International Conference on. IEEE, 2016.

[21] Lamport, Leslie, Robert Shostak, and Marshall Pease. "The Byzantine general's problem," ACM Transactions on Programming Languages and Systems (TOPLAS) 4.3 (1982): 382-401.

[22] Gervais, Arthur, et al. "Is Bitcoin a decentralized currency?" IEEE security & privacy 12.3 (2014): 54-60.

[23] Buterin, Vitalik. "Bitcoin network shaken by blockchain fork." Bitcoin Magazine 12 (2013).

[24] Christidis, Konstantinos, and Michael Devetsikiotis. "Blockchains and smart contracts for the internet of things." IEEE Access 4 (2016): 2292-2303.

[25] Buterin, Vitalik. "Ethereum white paper." (2013), https://github.com/ethereum/wiki/wiki/White-Paper

[26] Ali, Muneeb, et al. "Blockstack: A Global Naming and Storage System Secured by Blockchains." USENIX Annual Technical Conference. 2016.

[27] Noether, Surae. "Review of CryptoNote white paper," http://monero.cc/downloads/whitepaper_review.pdf

[28] Larimer, D., N. Scott, V. Zavgorodnev, B. Johnson, J. Calfee, and M. Vandeberg (2016) "Steem: An incentivized blockchain-based social media platform," Available at https://steem.io/SteemWhitePaper.pdf

[29] Wiki, Bitcoin. "Testnet." (2011), https://en.bitcoin.it/wiki/Testnet

[30] H. Kuzuno and C. Karam, "Blockchain explorer: An analytical process and investigation environment for bitcoin," 2017 APWG Symposium on Electronic Crime Research (eCrime), Scottsdale, AZ, 2017, pp. 9-16.

[31] Ortiz, C. Enrique. "An introduction to near-field communication and the contactless communication API," Oracle Sun Developer Network. Retrieved on Jun 30 (2008): 2010.

[32] Karame, Ghassan O., Elli Androulaki, and Srdjan Capkun. "Double-spending fast payments in bitcoin." Proceedings of the 2012 ACM conference on Computer and communications security. ACM, 2012.