Designing Trustworthy Microfinance Blockchain System Based on PoA Consensus Mechanism

Xuyan Li[1], Supharoek Siriphen[2], Somsak Chanaim[3] and Suttida Suwannayod[4]

[1,2,3,4]International College of Digital Innovation, Chiangmai University, Chiang Mai, Thailand
[1]E-mail: xuyan_li@cmu.ac.th, [2]E-mail: supharoek_siriphen@cmu.ac.th,
[3]E-mail: somsak.c@cmuic.net, [4]E-mail: suttida.d@cmuic.net

Abstract

Affected Covid-19 hen farmers in Chiang Mai, Thailand, who obtained a loan from the "happy eggs Covid-19" microfinance project return their eggs to Sri Suphan temple every week until the loan is paid off. To record return the number of eggs information clearly, the temple uses a notebook or Microsoft Excel and a "line" group as a bookkeeping tool to record farmers' return eggs information. However, both bookkeeping tools are affected by objective and human factors, causing the recorded information is non-traceability and easy tampering problems, respectively. With the rapid rise of blockchain technology applications, focus on verification and storage of information in microfinance research, a private trustworthy microfinance blockchain based on PoA (Proof of Authority) consensus mechanism is designed in this paper to help the Sri Suphan temple record farmers' return eggs information. The system implementation process is that the farmer submits return eggs information, verifies its validity through a PoA consensus algorithm, and final the validity information is stored in the blockchain. By demonstrating the system's essential functions, the result shows that the recorded farmer's return eggs information can be queried and non-changed. It also shows that the system is trustworthy, easy to operate, and practical.

Keywords: Private Blockchain, PoA Consensus Algorithm, Verification and Storage of Information in Microfinance

1. Introduction

International College of Digital Innovation Chiang Mai University and Ministry of Higher Education, Science, Research and Innovation proposed a "happy eggs Covid-19" microfinance project to assist hen farmers in Chiang Mai, Thailand, who face additional challenges resulting from the Covid-19 pandemic. The specific implementation of this project is as follows. ICDI donated money to Sri Suphan temple as a microfinance platform to lend loans to farmers and supported them with innovation and technology in building "smart farms." Also, farmers are divided into 12 groups, each farmer in the group will get 200 hens (37,500 baht) and 12,500-baht (for purchasing feed) loans from the temple, which will be repaid by returning eggs (one egg is equal to 4 baht) every week.

Figure 1: ICDI and MHESI proposed this project

During the repayment process, the Sri Suphan temple and farmers wanted to know how many eggs farmers had returned each week until the loan was paid off exactly. Therefore, the temple uses a bookkeeping tool to record farmers' return eggs information. Initially, the Sri Suphan temple used a notebook to record farmers' return eggs information, and farmers sign their names after rechecking the recorded information, which means that the recorded information has been confirmed (see figure 2). Nevertheless, the disadvantage is that when a theft or fire accident occurs, the notebook is easily lost, so that it is difficult to track all the lost farmers' return eggs information.

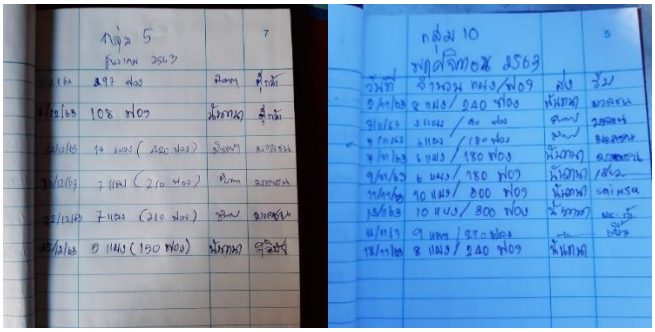

Figure 2: The temple used a notebook as record information

Subsequently, the Sri Suphan temple used Microsoft Excel instead of a notebook to record the farmers' egg return information (see Figure 3) and shared the recorded information with the "line" group for recheck and confirmation (see Figure 4). However, the recorded information in Microsoft Excel can easily be tampered with due to hackers or administrators. Based on the above shortcoming of the two types of bookkeeping tools used by the Sri Suphan temple to record farmers' return eggs information, this paper's main objective is to the recorded information so that it is traceable and non-tamperable.

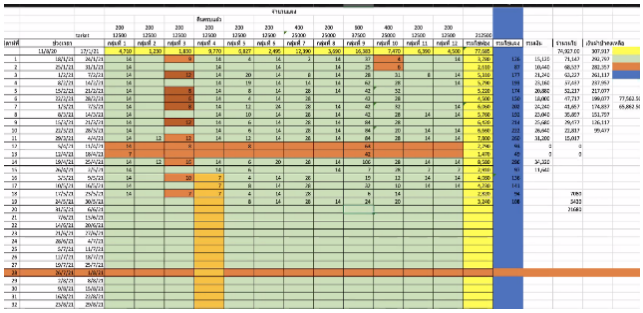

Figure 3: The temple used Microsoft Excel as record information

Figure 4: The temple shared the recorded information to the "line" group

However, the emergence of Bitcoin (Nakamoto, 2008) has brought a technical route to achieve this objective, and all walks of life have quickly recognized its underlying technology, blockchain. Blockchain, which means a chain composed of multiple blocks, is essentially a distributed data ledger that can be non-tamperable. Blockchain technology mainly relies on the verification node cluster in the peer-to-peer network. The verification nodes participate in the maintenance of the data ledger. The consensus mechanism of the verification node reaching a consensus is adopted to ensure that the transaction data is authentic, reliable, non-tamperable, and non-repudiation and realize the traceability of transaction records. Blockchain technology provides traceable and tamper-proof information processing processes by the following key features:

a. If the new block adds to the blockchain ledger, it will require the consensus of all network nodes in the blockchain indispensably.

b. Each new block added to the blockchain ledger has to connect to the previous block to prevent information from easily tampering.

c. The previous block and the back are connected to each other, and we can trace all the information in each block of the entire blockchain.

Blockchain can be divided into three primary ways: public blockchain, private blockchain, and consortium blockchain, under the operating mode of the participating nodes. The first introduction is the public blockchain. All information in the public blockchain is public and transparent. Everyone can be a participant who participates in the use and maintenance of the blockchain. For example, Bitcoin is the representative of the public blockchain. Next, the second introduction is a private blockchain managed and maintained by a single entity, usually for internal use, but the information is not public. In particular, banks and insurance institutions use a private blockchain to conduct business. Finally, the consortium blockchain is introduced. Its operating mode is between the public blockchain and the private blockchain. It is generally composed of multiple entities and jointly assumes management and maintenance responsibilities. Another characteristic is that the consortium blockchain has an access mechanism, and the nodes need to obtain authorization to access information. For instance, multinational corporations and industry alliances use consortium blockchain to conduct business with the exact business nature.

This paper will focus on the research on verification and storage of information in microfinance. According to research, we will design the trustworthy microfinance blockchain system based on the Proof-of-Authority consensus mechanism to help the Sri Suphan temple record farmers' return eggs information, ensuring traceability and tamper-proof. The entities involved in the blockchain are farmers and ICDI. ICDI is in charge of the verification and storage of information and system maintenance, and only for the Sri Suphan temple and farmers use this recorded farmers' return eggs information. Therefore, the system will adopt a private blockchain model.

The rest of the paper has been organized as follows. Section 2 claims the related work. Followed by section 3 is described the entire system design in detail. The system concrete implementation and testing results are exhibited and user evaluation in section 4. In the end, our conclusion and future work direction are presented.

2. Related work

Nowadays, blockchain technology is the fifth subversive innovation of the computing paradigm after mainframes, personal computers, the Internet, mobile Internet, and social networks, which has also attracted more and more attention from researchers and scholars at home and abroad.

In application terms, the value of blockchain technology is not only applied to Bitcoin and other cryptocurrency payment systems, but all walks of life are actively excavating and exploring the application of blockchain technology in their respective fields to solve problems. Therefore, the traces of blockchain can be seen in all fields, especially in the financial field. Jaag and Bach (2017) proposed how to apply blockchain technology in finance; Zhou LiQun and Li Zhihua (2016) introduced the use of blockchain technology in supply chain finance in detail; Song Wenpeng and Wang Zhenyan (2017) stated the application of blockchain technology to on the crowdfunding platform; Xia Xinyue (2016) described to apply blockchain technology to the purchase and transfer of equity assets. In other fields, there is also much research based on blockchain. Xu et al. (2017) described how to use blockchain technology in the field of architectural design; Huang Yonggang (2016) considers trying to create electronic health records using blockchain technology; Xu Yue and Ma Xiaofeng (2016) applied blockchain technology to the comprehensive evaluation system of student behavior; An Rui et al. (2017) proposed the design of an anti-counterfeiting system based on blockchain technology; Xia Youqing (2016) introduced how blockchain technology can fully play a role in firewall technology; Li Yi and Hu Danqing (2017) proposed how blockchain technology can be implemented in the field of social welfare; Tian Haibo et al. (2017) proposed how to design a privacy protection fair contract agreement based on blockchain technology; Taixue (2016) introduced the realization of blockchain technology in the energy Internet in detail; Lv Furong and Chen Sha (2016) mentioned how to use blockchain technology in the quality and safety of agricultural products.

Technically speaking, the blockchain is a peer-to-peer network involving multiple nodes linked together. It also shows that all transaction data is not stored on one node, but each node always maintains automatic synchronization and stores all transaction data. In addition, every transaction needs to be approved by all nodes in the network using a consensus mechanism before storing it in the blockchain. In other words, all nodes in the network must agree to the execution of the transaction through a predefined consensus mechanism to execute the transaction and store data. Therefore, consensus plays a vital and indispensable role in the blockchain network and keeps the security and integrity of the entire system. Each mechanism that has its advantages and disadvantages applies to specific situations. Based on the analysis of the trustworthy microfinance blockchain system, ICDI has become the core part of the system operation-the verification node, responsible for verifying transactions, packaging and generating blocks, and other blockchain operations. Therefore, consensus algorithms of completely decentralized or stock voting rights are not suitable for the design requirements of this system. Secondly, farmers have no appeal for the rewards of “mining” related to the blockchain. For this reason, the consensus algorithm based on computing power is not suitable for this system. Accordingly, the PoA consensus algorithm can meet the design requirements of the system.

The term PoA was proposed by Gavin Wood (2015), the co-founder of Ethereum and Parity Technology. PoA is a consensus algorithm based on authoritative reputation, introducing a practical and effective solution for alliance and private blockchain. Among them, Polkadot is the first blockchain to support PoA. In a blockchain system that supports PoA, transactions and blocks are verified by an authorized account. The account in the blockchain system is mainly for information verification and the existence of consensus nodes. The PoA consensus algorithm uses the value of the node's identity, which means that the block verification node no longer pledges its digital currency but its reputation. The PoA model relies on a limited number of miners, making it high performance and high scalability. In the PoA blockchain system, individuals who hold few digital currencies and do not have immense computing power can become consensus nodes, but they must maintain a specific reputation value and not be affected by a negative reputation. However, the PoA blockchain system may cause severe imbalances in consensus nodes with high "reputation" and may even form a monopoly or oligopoly, lack of dispersion to a certain extent, and may have a particular risk of evil.

An et al. (2019) suggested using the blockchain and PoA consensus mechanism to design the product origin tracking system. The advantage of this system is that the data is encrypted and distributed among the nodes in the network, which achieves immutability, transparency, and high security.

Xia Chenyi et al. (2020) put forward a non-quoted electricity trading mechanism based on the Proof of Authority (PoA) consensus in the alliance blockchain. Traditional microgrid electricity trading is through a centralized trading organization, and this model has certain hidden dangers. For example, trading institutions' user information and transaction data are easily tampered with, which cannot effectively guarantee information security, and there is a single point of failure risk in centralized transactions. Thus, using the PoA consensus algorithm to build a microgrid power trading in the alliance blockchain can reduce network congestion and not compete through computing power to generate blocks, save power consumption, reduce forks, and achieve higher consensus efficiency.

Zhang Jiehui (2020) proposed to solve the current problem of false seat occupation in civil aviation through an improved PoA consensus mechanism. In the past, significant airlines formed alliances, and each airline corresponded to a node on the alliance blockchain. Now introduce credit points and grading mechanisms, improve the original PoA mechanism, use the new PoA consensus mechanism as the consensus algorithm of the alliance blockchain, and select nodes that meet the conditions as the authoritative nodes responsible for packaging and generating blocks.

In summary, blockchain technology is constantly evolving and developing in cryptocurrency and is widely and broadly used in finance, construction industries, supply chain, etc. Concurrently, the blockchain system is based on a consensus mechanism that relies on each verification node to complete the verification and storage of data information. Given the microfinance repayment process in this paper, the bookkeeping tools used by the Sri Suphan temple have the problems of being difficult to trace and easy to be tampered with in the recorded farmers' return eggs

information. Hence, this paper focuses on the trustworthy microfinance blockchain system is based on a PoA consensus mechanism to realize the verification and storage of information and ensure that the information can be traceable and non-tamperable.

3. System design

This section mainly introduces how to design a trustworthy microfinance blockchain system based on the Proof-of-Authority consensus mechanism. There are three critical components in our designed system: system architecture, storage management of chain storage, and system workflow. The details are as follows: The system architecture is included a framework of the whole design and information flow. The storage management introduces block structure and blockchain formation. The system workflow is described as validating nodes and non-validating nodes respectively how to work.

3.1. System architecture

According to the PoA consensus mechanism is classified into validating nodes and non-validating nodes according to the function. In addition, the specific roles are ICDI and farmers in this system. The system architecture diagram is shown in figure 5.

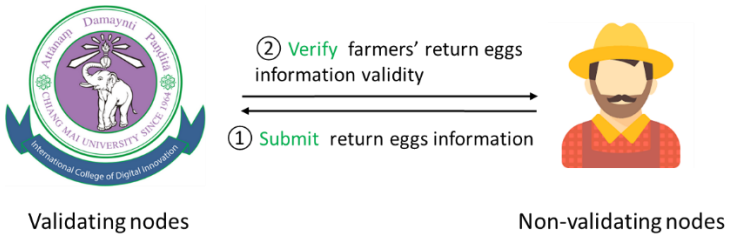

Figure 5: System architecture diagram

ICDI is the core module of the trustworthy microfinance blockchain system. Because it is a validating node in the PoA consensus mechanism, as a validating node and a mining node, it verifies whether the farmers' return eggs information is valid. Still, the blockchain cannot generate new reward tokens during package verification's "mining" process, only completed the distributed bookkeeping of the microfinance blockchain ledger.

Farmers are as non-validating nodes in the system, the following function as follows:

a. After verified validity return eggs information by validating nodes (ICDI), non-validating nodes can synchronize the latest ledger information but not modify the information in the ledger.

b. Only non-validating nodes have a submit return eggs information function. After the farmers have delivered eggs to the Sri Suphan temple, they need to record the eggs returned.

3.2. Storage management of chain structure

The microfinance blockchain is composed of blocks one by one. Each block contains a block header and a series of farmers' return eggs information that forms blockchain. The previous block's hash value contained in the block header of each block allows this block to be linked to the previous block, eventually becoming a chain structure. We can see that all blocks in the blockchain can be traced back to the Genesis block through this field. There have other vital fields in the block header of each block. For example, the Root field for root hash of the Merkle Tree formed by all return eggs information farmers; the Time field for a record of the timestamp of when the block was packed, and so forth. Each farmer's return eggs information includes the receiver's (ICDI) address, the number of eggs sent, and the sender's address (farmer). Figure 6 is displayed the block structure of the blockchain.

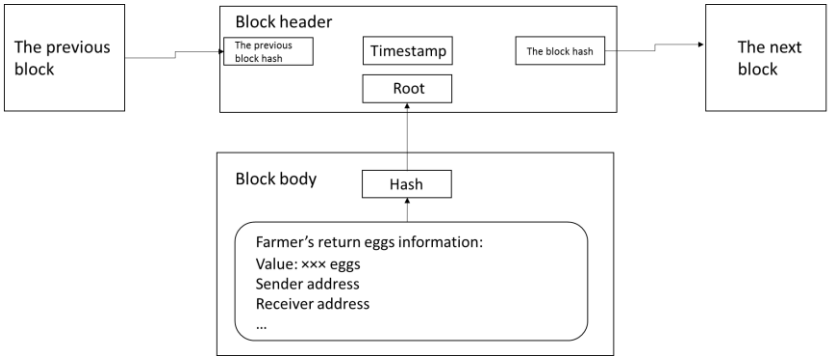

Figure 6: Block structure of the blockchain

3.3. System workflow

Based on the working principle of the PoA consensus mechanism, the steps indicating the forming process of a new block in the microfinance blockchain system are as follows (see figure 7):

a. Only non-validating nodes have a submit return eggs information functions and submit the information requests to the blockchain P2P network.

b. The validating nodes in the network continuously receive information requests and put them into its information pool or information queue.

c. The system is based on an algorithm principle that assigns one validating node as a primary.

d. The primary validating node executes information in order, and illegal or inexecutable information is rejected. After packing all legal information into a new block, use the private key of the primary validating node to sign and send it to other validating nodes in the network for verification.

e. Other validating nodes receive the new block and verify it according to the rules. If it passes, the new block is added to the chain of blocks. If it fails, the new block is not added to the blockchain and forms a "wrong" mark.

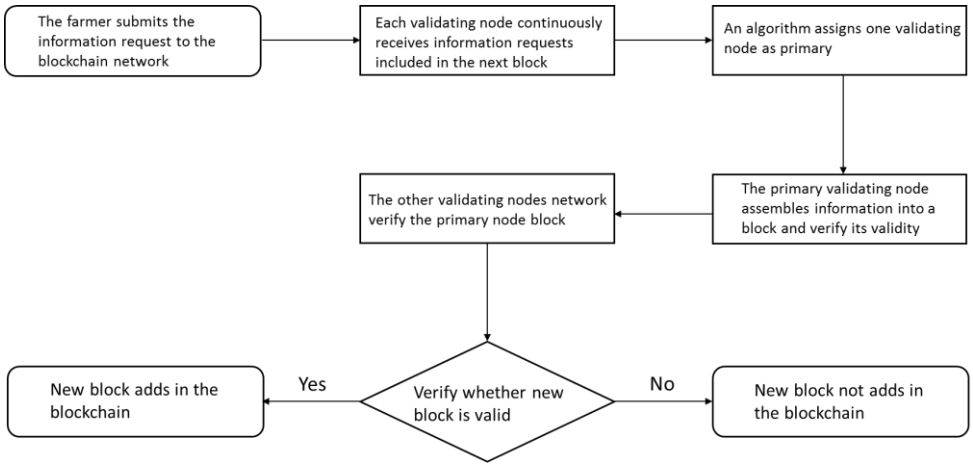

Figure 7: Forming process of a new block in the microfinance blockchain

4. Implementation and result

4.1. System implementation

The system designed in this paper is implemented (see figure 8). The steps indicating the flow of our system are as follow:

a. Farmer creates a submit return eggs information order.

b. Successfully verified farmer's return eggs information is valid by the Proof-of-Authority (PoA) consensus mechanism, and unsuccessfully information is eliminated.

c. The validity information is added into a block.

d. The block is then created and added to the already existing chain of blocks (blockchain), and, at this time, it is immutable as it cannot be altered, while declined information is eliminated.

e. The farmer submit return eggs information is now completed.

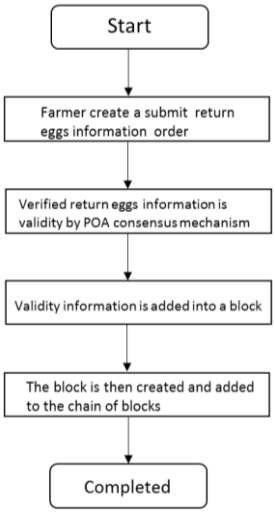

Figure 8: Farmer submit return eggs information of flow process

4.2. Results and discussion

What is successful is that we designed the trustworthy microfinance blockchain system for the recorded farmer's return eggs information traceability and tamper-proof primary purpose, based on the PoA consensus mechanism. The essential functions of this system will be exhibited as follows.

a. Farmer submit a return eggs information application

Farmer enters the system interface and clicks on the "return" button in the list on the left to fill in return eggs information (see figure 9). Farmer first checks whether the receiver address (ICDI) is correct, then fills return number of eggs, uploads "return the number of eggs" photos, and clicks the "ask for password" button to receive the verification code from his/her registered E-mail. After filling in all the information, the farmer finally clicks the "confirm" button to submit the return eggs information application.

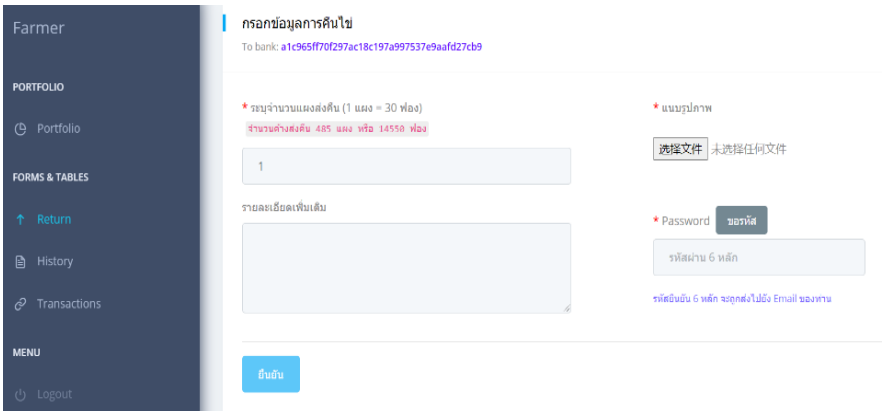

Figure 9: Farmer's return eggs information page

b. Administrator (ICDI) verifies whether the farmer return eggs information is valid

Figure 10 shows the page where the administrator verifies that the farmer's returned egg information is valid. After the farmer successfully submits the return eggs information application, this record will be added to the administrator's pending return eggs information. The administrator checks the farmer's return eggs information in detail, such as the number of eggs, farmer personal information, group, etc. If it is correct, click the "confirm" button on the page, and this status of information is changed into confirmed. It means that the farmer's return eggs information is valid. The valid return eggs information will be packaged, created a new block, and added to the blockchain. Once it is added, it is non-tamperable.

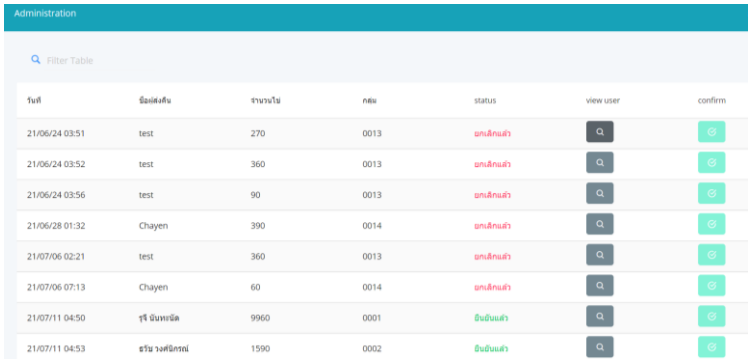

Figure 10: The administrator verifies that whether the farmer return eggs information is valid on page

c. Farmer return eggs information query

As shown in Figure 11, the farmer eggs return information query supports accurately query based on the farmer's address, the number of eggs, Contract ID, and Relative time. For example, the farmer enters the "transaction" page after logging in and enters his/her own address 4e9740c09d3c0f71da3c1ecdbb68ff095389ea20, then two return eggs information will be displayed, and the status will be displayed as "confirm". A piece of information is on Sat Aug 07, 2021, 22:16:30, the number of eggs returned is 7380, and the information is stored in block 8. Another piece of information is on Sat Aug 07, 2021, 22:19:03; the number of eggs returned is 210, and the information is stored in block 16.

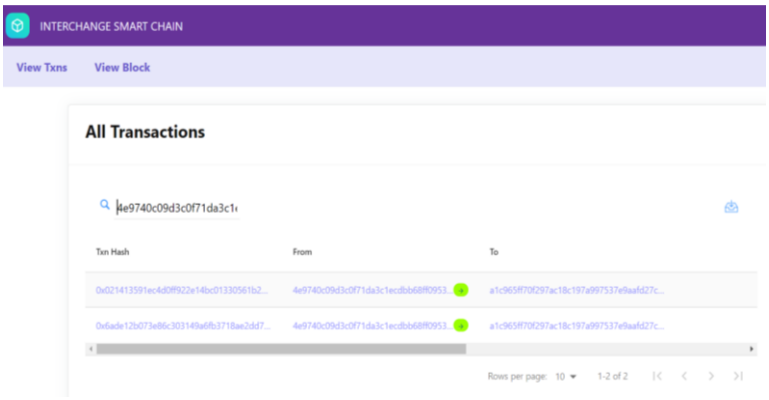

Figure 11: Farmer return eggs information query page

d. View block

we can see that valid farmer's return eggs information can be placed in the block, and the previous block is linked with the block by Hash value to form a blockchain (see figure 12). Let us look at Block 8 as an example. The "Block Hash" in the figure represents the Hash value of the block; "From" represents the sender address (Farmer) 4e9740c09d3c0f71da3c1ecdbb68ff095389ea20; "Document" represents the content of the information, and "Previous Hash" represents the hash value of the previous block.

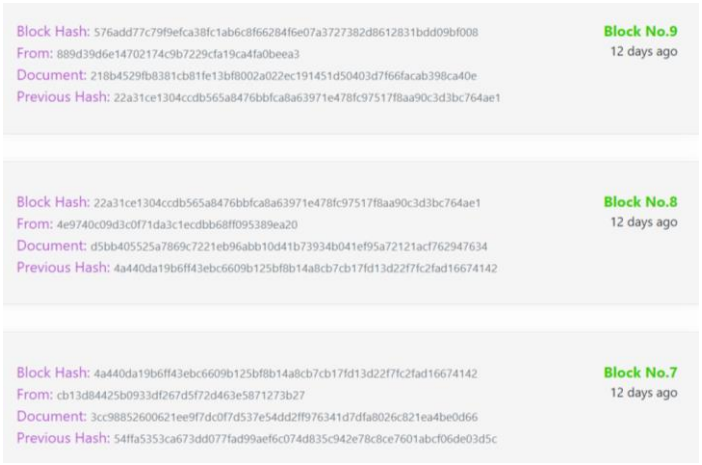

Figure 12: View block page

User evaluation:

Farmer 1: At present, when I use this "trustworthy microfinance blockchain system based on PoA consensus mechanism", it dramatically improves the "untrustworthy" of returning egg information in the past, which means that the information is easily tampered with and leads to an "untrustworthy" attitude. Moreover, the recorded information can be inquired about all the time. The overall design of the system is simple and beautiful and easy to operate.

Farmer 2: To use this system, you do not need to have superb skills to use it, which is convenient and convenient. After the farmers have delivered eggs to the Sri Suphan temple, we need to record the eggs returned to the system.

Sri Suphan temple: The previous use of notebooks and Microsoft Excel had challenging to trace and easy to tamper with. This system completely solved the troubling problems. What is more, farmers express a more "trusting" attitude, which is the most important.

5. Conclusion and future work

Blockchain has been developed for more than ten years, from the enlightenment era of Bitcoin to the awareness of blockchain. At present, blockchain technology is still in the exploring and developing stage, and we still face more challenges and opportunities how to apply blockchain technology into specific areas and establish improved blockchain applications still a challenging subject.

Blockchain technology can be seen as a new thing that we will use its advantages to solve social issues. Moreover, we should do repeated attempts and experiments in the blockchain field so that the characteristics of blockchain technology are fully utilized.

In addition, all blockchain application scenarios must solve the problem of reaching a consensus in a completely free and public network that lacks information. That is, the problem of the distribution of bookkeeping rights generated by the block and the verification problem after the block is generated. That is the “consensus mechanism.”

In this paper, to help the Sri Suphan temple record farmers’ return eggs information, we design a trustworthy microfinance blockchain system based on the private blockchain combined with the PoA consensus algorithm, ensuring the recorded information traceability and tamper-evidence. The system’s actual test results prove that the recorded farmer’s return eggs information is inquired and non-changed. Moreover, the system interface is simple in operation, straightforward and beautiful on the page, robust and steady, trustworthy, and has significant practical worth.

To optimize the trustworthy microfinance system designed in this paper is our future research work:

a. Based on this system design, we can further use the advantages of blockchain smart contracts to extend the breadth and depth of verification and storage of information.

b. Based on the PoA consensus algorithm currently used in this system, we combine new algorithms with improving operational efficiency.

Although there are specific technical difficulties and challenges in completing the above tasks quickly, because blockchain technology has received more and more attention and input from researchers and industry professionals, the future research process will also be smoother.

Acknowledgment

The author gratefully acknowledges the support from the Graduate School, Chiang Mai University, and thank our supervisor in this research for all suggestions for improving the paper.

References

An Rui, He Debiao, Zhang Yunru, & Li Li. (2017). Design and implementation of anti-counterfeiting system based on blockchain technology. *Chinese Journal of Cryptography*, 4(2), 199-208.

An, A. C., Diem, P. T. X., Van Toi, T., & Binh, L. D. Q. (2019, November). Building a product origins tracking system based on blockchain and PoA consensus protocol. In *2019 International Conference on Advanced Computing and Applications (ACOMP)* (pp. 27-33). IEEE.

Gavin, W. (2015). Poa private chains. *URL: https://github. com/ethereum/guide/blob/master/poa. md*.

Huang Yonggang. (2016). Security construction of electronic health records based on blockchain technology. *Chinese Journal of Medical Library and Information*, (10), 38-40.

Jaag, C., & Bach, C. (2017). Blockchain technology and cryptocurrencies: Opportunities for postal financial services. In *The changing postal and delivery sector* (pp. 205-221). Springer, Cham.

Li Yi, & Hu Danqing. (2017). Application practice of blockchain in the field of social welfare. *Information Technology and Standardization*, 3, 25-27.

Lv Furong, & Chen Sha. (2016). Research on the construction of my country's agricultural product quality and safety traceability system based on blockchain technology. *Rural Finance Research*, (12), 22-26.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *Decentralized Business Review*, 21260.

Song Wenpeng, & Wang Zhenyan. (2017). Application of Blockchain in Crowdfunding Platform. *Information Technology and Standardization*, 3, 28-30.

Tai Xue, Sun Hongbin, & Guo Qinglai. (2016). Blockchain-based power transaction and congestion management methods on the Internet of Energy. *Power System Technology*, 40(12), 3630-3638.

Tian Haibo, He Jiejie, & Fu Liqing. (2017). The signing of a fair contract for privacy protection based on public blockchain. *The Journal of Cryptography*, 4(2), 187-198.

Xia Chenyi, Cai Qingsong, & Wu Jie. (2020). Micro-grid non-quoted transaction mechanism based on PoA alliance blockchain. *Computer System Application*, 29(11), 57-65.

Xia Xinyue. (2016). *Design and implementation of block chain-based equity asset purchase and transfer* (Master's thesis, Inner Mongolia University).

Xia Youqing. (2016). Research on Anti-APT firewall technology based on blockchain technology. *Information and Computer*, (14), 30-32.

Xu Yue, & Ma Xiaofeng. (2016). Research and implementation of a comprehensive evaluation system for student behaviour based on blockchain. *Information Technology and Informatization*, (12), 131-133.

Xu, X., Weber, I., Staples, M., Zhu, L., Bosch, J., Bass, L., ... & Rimba, P. (2017, April). A taxonomy of blockchain-based systems for architecture design. In *2017 IEEE international conference on software architecture (ICSA)* (pp. 243-252). IEEE.

Zhang Jiehui. (2020). *Research on the solution of vacant seats in civil aviation based on blockchain technology* (Master's thesis, Civil Aviation University of China).

Zhou Liqun, & Li Zhihua. (2016). Application of Blockchain in Supply Chain Finance. *Information System Engineering*, (7), 49-51.