Developing Blockchain-Based System for Tracking The Origin of Chicken Products

Thanh Son Huynh, Luong Anh Tuan Nguyen

Abstract*: Recently, Blockchain-based solutions is being considered by many researchers. Blockchain-based solutions are applied in areas such as finance, banking, education, e-commerce, logistic, agriculture, etc. In Vietnam, many researchers and companies are also interested in applying Blockchain technology. This paper proposed a Blockchain-based system for tracking the origin of chicken products. This system includes components of Blockchain such as nodes, blocks, ledger, consensus, cryptography, transparency, etc. This system was implemented and experimented at the chicken farms, Cho Gao district, in Tien Giang province, Vietnam with many participants such as chicken farms, veterinary business agencies, wholesalers, retailers, veterinary station of Cho Gao district Tien Giang province, food hygiene and safety certification organizations, etc. Initial experimental results are very efficient and positive, a lot of farmers and stakeholders is excited to participate in the experiment.

***Index Terms*: Blockchain, tracking products, consensus, cryptography.**

I. INTRODUCTION

Satoshi Nakamoto invented Blockchain in 2008. At the time, Blockchain play role as the public transaction ledger of the cryptocurrency bitcoin [1]. Blockchain serves as a hierarchical database that stores information in linked blocks using encryption [2]. Each block contains the initialization time, transaction data, hash code and is associated with the previous block. Blockchain is designed to prevent data changes: When a block is accepted and add to the Blockchain, there is no way to change it. After the generation of Bitcoin in 2008, more and more researchers pay attention to BlockChain. Bitcoin is the most famous application of Blockchain. In addition, Blockchain can be applied into diverse applications such as financial, manufacturing, energy, agriculture supply chains, land registrations and etc. Blockchain technology is becoming one of the most promising technologies for new interaction systems in the Internet [3-4]. The paper proposed a Blockchain-based solution for tracking the origin of chicken products. The system was designed with nodes, structure of block, consensus policy, cryptography, transparency. This system was programmed with PHP programming language and experimented at the chicken farms, Cho Gao district, in Tien Giang province, Vietnam with many participants such as chicken farms, veterinary business agencies, wholesalers, retailers, veterinary station of Cho Gao district Tien Giang province, food hygiene and safety certification organizations, etc. The remainder of the paper is organized as follows. The Blockchain overview is discussed in Section 2. Section 3 describes in detail of the proposed system. In Section 4, the results of experiment are illustrated. Finally, Section 5 concludes this paper and figures out the future works.

II. BLOCKCHAIN OVERVIEW

The Blockchain technology is not only a mechanism to build trust, reduce costs and accelerate transactions, but also provide a secure chain of custody for assets through trust, consensus and security. The key characteristics of the Blockchain technology generally include components such as decentralization, persistency, anonymity and auditability [5-6].

Decentralization. In centralized systems, each transaction is validated through the trusted third party, that increases the cost and easy to block central servers. However, the Blockchain doesn't need the third party to validate, that helps to decrease the cost and not to cause network congestion.

Persistency. In the Blockchain, transactions cannot be deleted or edited. if blocks contain invalid transactions, it could be discovered immediately.

Anonymity. Users do not require disclosure of identity when interacting on the Blockchain.

Auditability. In the Blockchain, transactions could be easily checked and tracked.

The Blockchain can also be categorized into three types: *public Blockchain*, *private Blockchain* and *consortium Blockchain*. In public Blockchain, everyone could take part in the consensus process. In private Blockchain, only specific nodes could take part in the consensus process. A private Blockchain is fully controlled by one organization. In consortium Blockchain, only a small portion of selected nodes would be determined the consensus..

Features of Blockchain technology expressed through the following key features:

A. *The Consensus Algorithm*

All nodes of the Blockchain must comply with the rules of consensus. The consensus algorithm forms one of the key mechanisms in the creation of new blocks and adding them to the Blockchain.

Revised Manuscript Received on August 03, 2019.

Thanh Son Huynh, Ho Chi Minh City University of Transport, Vietnam.
Luong Anh Tuan Nguyen, Ho Chi Minh City University of Transport, Vietnam.

The most discussed algorithms are proof-of-work (PoW), proof-of-stake (PoS) and proof-of-authority (PoA) [7-9].

B. *Blockchain*

A Blockchain includes blocks, each block contains the data, its own hash value and a pointer to the hash of the previous block. Figure 1 describes the structure of a block. Figure 2 describes the structure of a Blockchain.

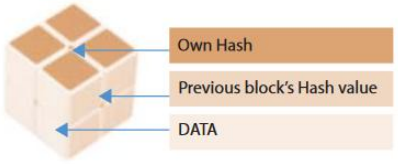

Figure 1. Structure of block

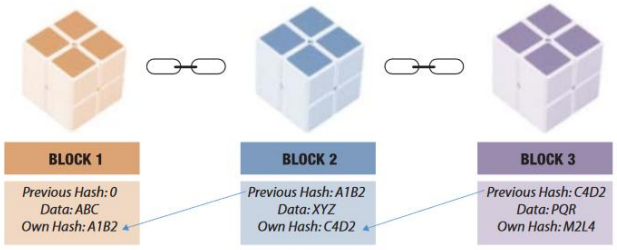

Figure 2. Structure of Blockchain

C. *Data Encrypt*

Encryption provides data conversion techniques that make it useless for unwanted recipients. Encryption helps us prevent and detect interventions, falsify information or disallow access and use of data. Encryption is developed based on two main technical platforms: hash function and digital signature to ensure data integrity across the system.

The hash function is used to convert information into a piece of code. Any fraudulent attempt to change any of the Blockchain data will be detected immediately because the new hash value will not match the old information on the Blockchain. In this way, information security science has become an effective tool for open trading.

A digital signature is an encrypted message attached to another data to authenticate the person who sent the message. The electronic signature used in Blockchain is built on public key cryptography [10], also known as asymmetric cryptography. The signing and signature verification process is done as follows: The sender wants to send a message to the other party to use a hash function and hash of the original message into a "Message Digest", this algorithm is called a hashing algorithm (hash function). The sender encrypts the message summary with his secret key to form a digital signature. After that, the sender continues to attach this digital signature to the original data and sends the data attached to the signature securely to the recipient. After receiving it, the recipient will use the sender's public key to decrypt the digital signature into the message summary. The recipient also uses the same hash function as the sender did for the received message to transform the received message into a message summary. The recipient compares these two message summaries, if they are identical, that digital signature is authenticated and the message has not been changed on the route. Figure 3 describes the implementation process of digital signature.

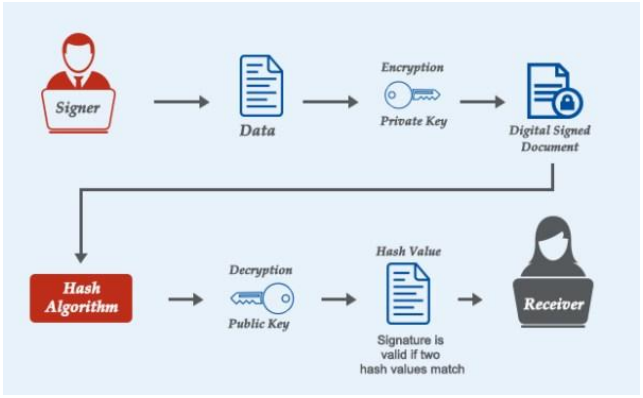

Figure 3. Digital signature

D. *Peer-to-Peer Network*

Peer-to-Peer network consists of many network nodes directly linked to each other, each of which has the same role and position. A distributed database is a database in which data may be stored in multiple servers. These servers may be located in the same physical location or may be dispersed over a network of interconnected servers [11]. Distributed database contains all records of transactions and shared between participants in peer-to-peer networks that are kept absolutely safe. Figure 4 describes the structure of peer-to-peer network in the Blockchain system.

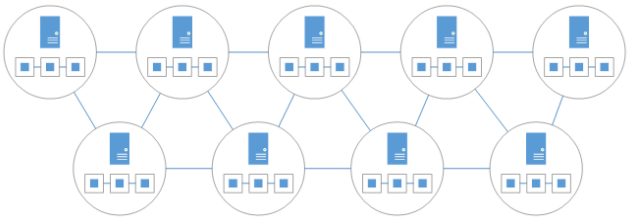

Figure 4. Blockchain distribution across a peer-to-peer network

III. PROPOSED SYSTEM

The proposed system model is described in Figure 5. The proposed system includes the following components:

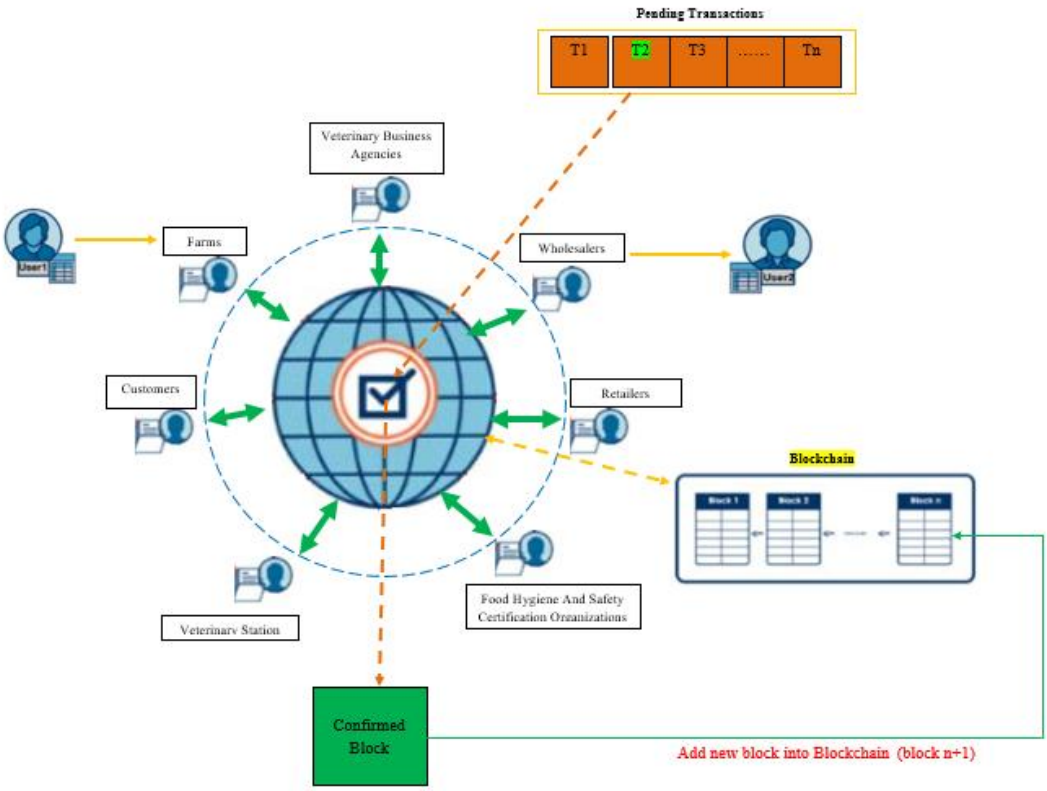

Figure 5. Proposed system model

A. *Nodes*

Each entity participating in the system is a node, as a group, each group has many users.

1) Chicken Farm

Including many farms, each farm raises chickens and sells chickens to wholesalers. Each farm is a user in the system. Figure 6 describes the chicken farm.

Figure 6. Chicken farm

2) Veterinary Business Agency

Including many agencies, each of them doing business selling baby chickens, food, and veterinary drugs. Each agency is a user in the system. Figure 7 describes the veterinary business agency.

Figure 7. Nhat Truong veterinary business agency

3) Wholesaler

Including many wholesaler, each wholesale buys chickens from the farm, then processes and sells chickens to the retailers. Each wholesaler is a user in the system.

4) Retailer

Including many retailers, each retailer buys finished chicken products from wholesalers and sells chicken products to consumers. Each retailer is a user in the system.

5) Veterinary Station of Cho Gao District

The staffs of veterinary station are authorized to certify transactions between farms and veterinary business agency, farms and wholesalers.

The staffs can statistics and find information in the Blockchain system. Each staff is a user in the system.

6) Food Hygiene And Safety Certification Organization

The staffs of food hygiene and safety certification organization are authorized to certify transactions between wholesalers and retailers. The staffs can statistics and find information in the Blockchain system. Each staff is a user in the system.

7) Customers

Consumers can look up chicken product information in the system based on the QR code of each product.

B. *Transactions*

There are four types of transaction as follows:

- Transaction between farms and veterinary business agencies: buy chicken breeds, food and veterinary medicine.
- Transaction between farms and wholesalers: buy and sell chickens.
- Transaction between wholesalers and retailers: buy and sell processed chicken products.
- Transaction between retailers and customers: buy and sell finished chicken products.

C. *Consensus Policy with Types of Transaction*

Each type of transaction will have its own consensus confirmation policy.

1) Transaction between farms and veterinary business agencies

Confirming consensus for this type of transaction by the staff of veterinary station.

2) Transaction between farms and Wholesalers

Confirming consensus for this type of transaction by the staff of veterinary station.

3) Transaction between Wholesalers and Retailers

Confirming consensus for this type of transaction by the staff food hygiene and safety certification organizations.

D. *Data Structure*

1) QR Code

Each chicken will have a QR code that is generated on the system when the purchase of breeding chickens between the farm and the veterinary business agency.

2) Block Structure

A block structure is described in Figure 8.

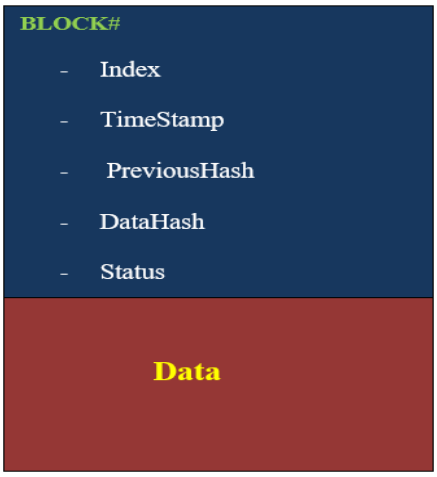

Figure 8. Block structure

A block structure includes the following components:

- Index: Ordinal number of blocks
- Timestamp: Time to create block
- Data: Data of a successful transaction.
- DataHash: Transaction data in the block has been encrypted by SHA256. When the data is changed, the data string in Data Hash changes accordingly..
- PreviousHash: contains the encrypted transaction data of the previous block.
- Status: Transaction confirmation status. When the status is yes, the transaction is successful. When the status is no, the transaction is pending.

Each block contains only one transaction.

3) Blockchain Structure

A Blockchain structure is described in Figure 9.

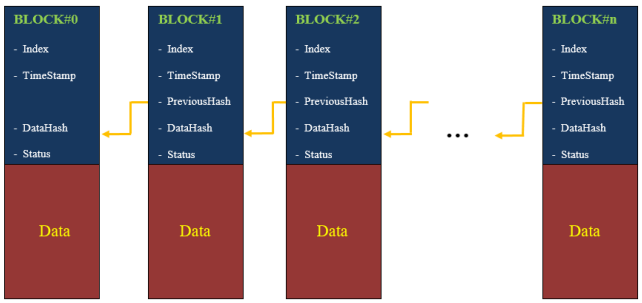

Figure 9. Blockchain structure

A Blockchain structure includes the following components:

- Block # 0: is the initial block in the Blockchain system, called Block Genesis.
- A hash pointer is used to point to previous DataHash.
- The system compares the hashed data in PreviousHash and DataHash to ensure data integrity consistency.
- When a new block is created. The system will recalculate to find the last block for the new block to point.

IV. EXPERIMENT RESULT

This section describes the experimental setup and the results of experiments.

A. Experimental Setup

We built up a local peer-to-peer network to experiment with nodes as follows:
- at chicken farms
- at Veterinary Business Agencies
- at Veterinary Station of Cho Gao District
- at Food Hygiene And Safety Certification Organizations
- at wholesalers
- at retailers

A Blockchain-based system was designed and implemented via PHP programming language. A GUI system includes two components as follows:
- A GUI system for staff at nodes to create transaction, confirm consensus, etc.
- A GUI system for customer to track the origin of chicken products.

B. Experimental Process and Result

In this experiment, we conducted experiments on 100 breeding chickens as follows:
- The farm ordered 100 breeding chickens from veterinary business agency through transaction in Figure 10.
- The veterinary business agency agree to sell to the farm by accepting this transaction as Figure 11.
- The above transaction is confirmed consensus as Figure 12.
- The farm ordered food and drugs from veterinary business agencies through transaction in Figure 13.
- The veterinary business agency agree to sell to the farm by accepting this transaction as Figure 14.
- The above transaction is confirmed consensus as Figure 15.
- The wholesaler ordered 50 chickens from the farm and that transaction is accepted by the farm as Figure 16.
- The above transaction is confirmed consensus as Figure 17.
- The wholesaler slaughter and process the chickens, the transaction is confirmed by Food hygiene and safety certification organization as Figure 18.
- The retailer ordered 30 finished chickens from the wholesaler and that transaction is accepted by the wholesaler as Figure 19.
- The above transaction is confirmed consensus as Figure 20.
- The customer tracks the origin of chickens as Figure 21.

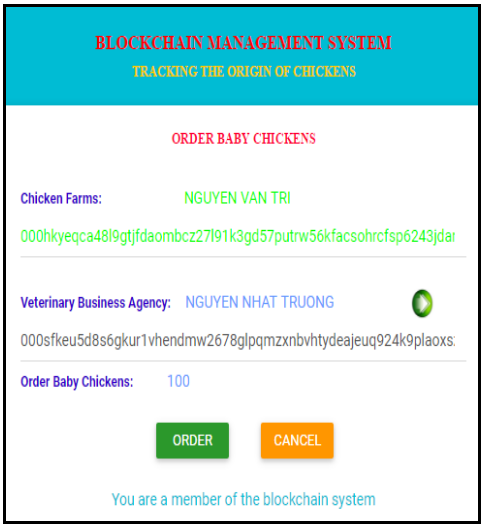

Figure 10. "Ordered 100 breeding chickens" transaction

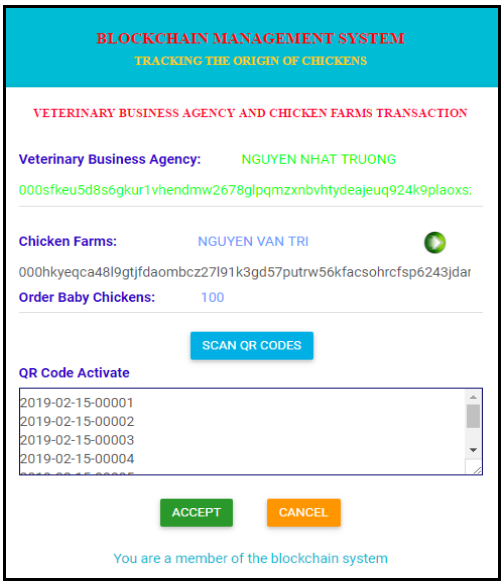

Figure 11. Accepting transaction

Figure 12. Confirming consensus

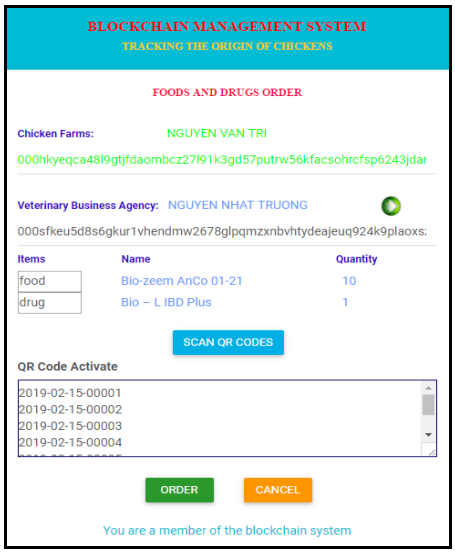

Figure 13. "Ordered food and drugs" transaction

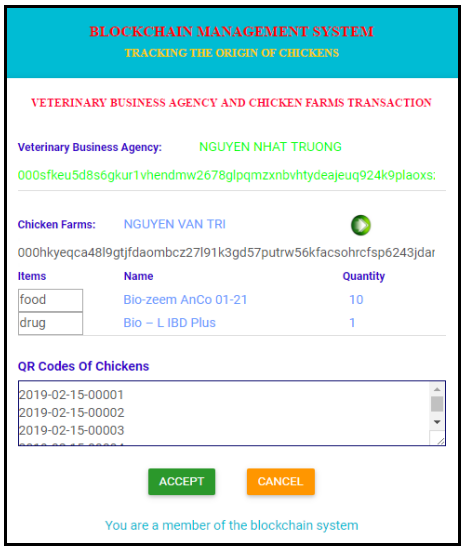

Figure 14. Accepting transaction

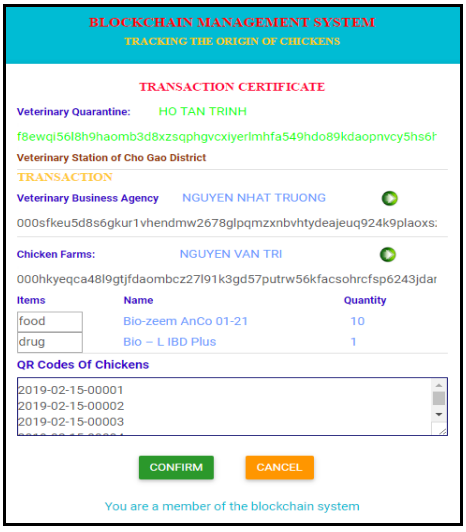

Figure 15. Confirming consensus

Figure 16. Accepting transaction

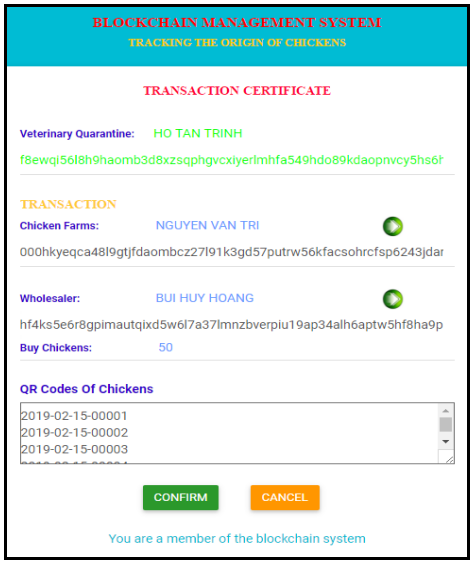

Figure 17. Confirming consensus

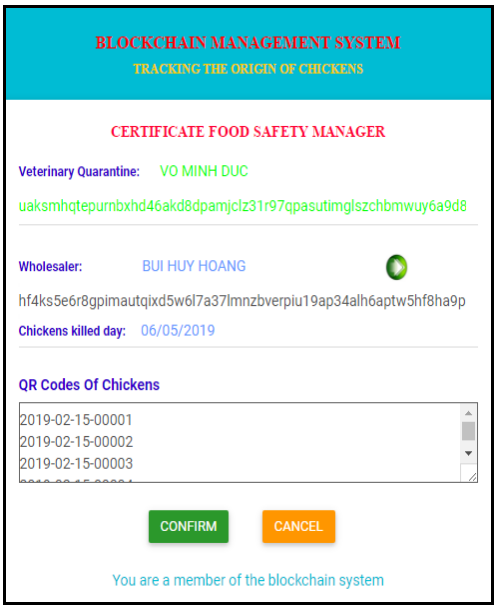

Figure 18. Confirming consensus

Figure 19. Accepting transaction

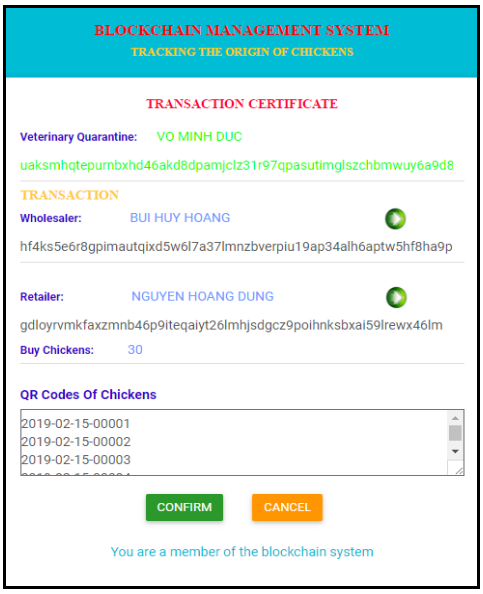

Figure 20. Confirming consensus

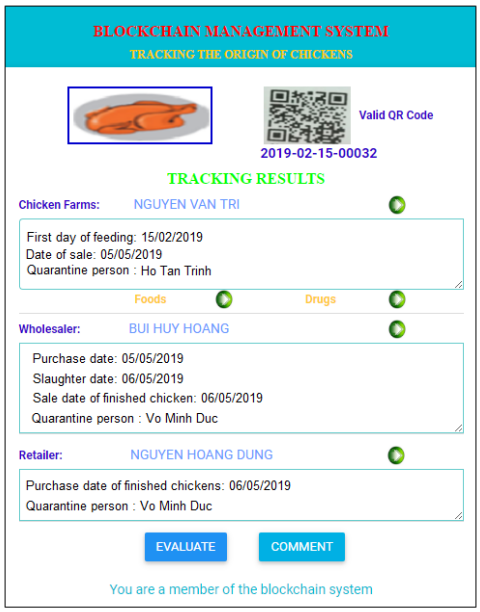

Figure 21. Tracking the origin of chickens

V. CONCLUSION

This paper describes the Blockchain technology overview and the key features of the Blockchain. The paper proposed Blockchain-based solution for tracking the origin of chicken products. The proposed system was programmed by PHP language and experimented at the chicken farms, Cho Gao district, in Tien Giang province, Vietnam with many participants such as chicken farms, veterinary business agencies, wholesalers, retailers, veterinary station of Cho Gao district Tien Giang province, food hygiene and safety certification organizations, etc. The experimental results are very effective and positive. In the furture, Our team will conduct experiments for many different chicken lots and gradually conduct applications in practice.

ACKNOWLEDGMENT

The authors thank reviewers for their reading of our manuscript and their insightful comments and suggestions.

REFERENCES

1. S. Nakamoto, Bitcoin: a peer-to-peer electronic cash system. 2018.
2. Blockchain. Available: https://vi.wikipedia.org/wiki/Blockchain
3. Kosba, A., Miller, A., Shi, E., Wen, Z. and Papamanthou, C. (2016) 'Hawk: the Blockchain model of cryptography and privacy-preserving smart contracts',Proceedings of IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, pp.839–858.
4. Noyes, C. (2016a) Bitav: Fast Anti-Malware by Distributed Blockchain Consensus and Feedforward Scanning, arXiv preprint arXiv:1601.01405
5. X. Zhou, Q. Wu, B. Qin, X. Huang, and J. Liu, "Distributed bitcoin account management," in Proc. IEEE Trustcom/BigDataSE/ISPA, Aug. 2016, pp. 105–112
6. Khan C, Lewis A, Rutland E, Wan C, Rutter K, Thompson C. A Distributed-Ledger Consortium Model for Collaborative Innovation. Computer 2017;50(9):29-37
7. L. Lamport, R. Shostak, and M, Pease, "The Byzantine generals problem," ACM Transactions on Programming Languages and Systems, vol. 4, no. 3, pp. 382-401, 1982
8. D. Schwartz, N. Youngs, and A. Britto, "The Ripple protocol consensus algorithm," 2014
9. D. Ongaro and J. K. Ousterhout, "In search of an understandable consensus algorithm," in Proceedings of 2014 USENIX Annual Technical Conference, Philadelphia, PA, 2014, pp. 305-319
10. Diffie, Whitfield; Hellman, Martin (8 June 1976). "Multiuser cryptographic techniques".
11. Distributed Database, Available: https://en.wikipedia.org/wiki/Distributed_database

AUTHORS PROFILE

Thanh Son Huynh received B.Sc. degree in Computer Science from Ho Chi Minh City University of Transport, Viet Nam. Currently, He is preparing to get a M.Sc degree in Computer Science. His current research interests include Network Security, Soft Computing and Artificial Intelligence.

Luong Anh Tuan Nguyen is the head of Information System Depatment, Ho Chi Minh City University of Transport, Viet Nam. He received B.Sc. and M.Sc. in Computer Science from University of Science Viet Nam National University Ho Chi Minh City. He also received Ph.D. degree in Control Engineering and Automation. His current research interests include Artificial Intelligence, Soft Computing, Control Engineering and Security.