Building a Product Origins Tracking System based on Blockchain and PoA Consensus Protocol

An Cong Tran
College of ICT
Can Tho University
Can Tho, Viet Nam
tcan@cit.ctu.edu.vn

Pham Thi Xuan Diem
College ICT
Can Tho University
Can Tho, Viet Nam
ptxdiem@cit.ctu.edu.vn

Le Thi Thu Lan
College of Engineering and Technology
Tay Do University
Can Tho, Viet Nam
lttlan@tdu.edu.vn

Tran Van Toi
Tiengiang Telecommunications
VNPT
Tien Giang, Viet Nam
lemintran12@gmail.com

Lam Duong Quoc Binh
Tiengiang Telecommunications
VNPT
Tien Giang, Viet Nam
binhlam10796@gmail.com

***Abstract*— In recent years, the traceability of product origins is strongly concerned, particularly for food products as they directly influence human health. Therefore, there have been some efforts to develop product origins tracking systems. In this paper, we propose an approach to building a supply chain management system based on the blockchain technology for agriculture product origins tracking. The supply chain model is borrowed from Walmart's and it is implemented based on the Ethereum framework using the PoA (Proof of Authority) consensus algorithm. Our experiment shows that the proposed system not only fulfills the requirements of a product origins tracking but also takes the advantages of the blockchain technology such as the immutability and security of data, the low cost in making the transactions, and so on.**

Keywords*— *blockchain, supply chain management, product origins tracking, PoA

I. INTRODUCTION

In recent years, traceability of product origins is strongly concerned by consumers, particularly the agriculture products as they directly influence human health. The product origins tracking systems allow consumers to get full information about product, from the growing fields to the final products, including the information about exporters, importers, and packaging companies (or retailers). Such systems increase the transparency in the production process as well as the product origins, to help consumers believe on the safety of the food.

To meet this demand, many agriculture product origins tracking systems have been developed and they are being used by the manufacturers to provide their customers the capability to trace the product origins. Based on the data organization method, these systems can be classified into two types. The first type includes the systems that use the traditional database management systems (DBMS) such as Oracle, MySQL, etc. One of the basic features of these systems is that they base on the centralized management and data storage model. Therefore, they provide a low capability to connect the systems used by different manufacturers as the interconnection between the different systems is complicated and costly. As a result, it is hard to provide customers detailed information about the products from the growing stage (raw material) to the final product. Moreover, as all data and functions of the system are centrally managed by the manufacturer, the reliability and transparency of the system are also reduced. The manufacturers can modify the product data to benefit their business without the awareness of the customers. Data security is also one concern for this type of tracking system. For example, Oracle ERP [1] is one of the supply chain management systems in this category and it is used at Anova Farm Group[1] and thousands other companies to manage their production process and the product traceability. Another supply chain system in this category is the TraceChain developed by TraceVertified's. TraceChain is being applied to manage vegetable supply chain at VinCo (where vegetable supply for CoopMart supermarket), processed meat at BigC and Phu Quoc fish sauce. Agricultural products managed by these systems use QR Code so that users can access the source via mobile phones or computers.

Recently, blockchain technology is introduced and has gained considerable attention from both researchers and practitioners. It is recognized as the fifth evolution of computing and considered as important as the introduction of the internet [4, 8, 12]. This is a technology that enables peer-to-peer distributed ledgers combined with strong and rigorous encryption algorithms to counter the changing stored information as well as the attacks. Many studies on the application of blockchain technology have been conducted, particularly in financial-related applications such as digital assets management and payment systems [2, 7], warehouse management (logistics) [1], Internet of Thing (IoT) [5, 10], etc. The main reason that causes this technology attracts the attention of researchers is that it allows transactions and payments to be made without intermediaries. It totally changes the way that the traditional services have operated, which use an intermediary in transactions.

Blockchain technology provides safer and more transparent transaction processing process by the following key features [19]:

- *Ledger is distributed* on many different network nodes to increase the data safety because if one node is attacked, the data still remains on other nodes.
- There is a *distributed control* among the nodes in the network to create new transactions in the ledger.

[1] https://www.anovafarm.vn

978-1-7281-4723-9/19/$31.00 ©2019 IEEE
DOI 10.1109/ACOMP.2019.00012

- Each block added to the ledger must *link* to the previous block to against data tampering.
- Adding a new block to the ledger requires a *consensus* of all nodes in the blockchain network.

With the above characteristics, blockchain technology is considered as a promising technology for supply chain management systems to support the traceability of agricultural products due to the following reasons: i) information related to products within their life cycle can be easily recorded in a sustainable and immutable manner; ii) everything that involved in all steps of the production (e.g. growing, harvesting, exporting, and importing) can be easily recorded to the ledger; iii) invoices, expends, and documents can also be recorded; iv) digital assets like copyright, licenses, product bar codes, etc. can be managed identically as other physical assets. All processes of recording information in the system can be performed transparently by smart contracts based on consensus protocols.

IBM is recently developing a food supply chain management service based on their own distributed ledger technology to manage the food manufacturing process from farms to stores. Some big food companies are collaborating with IBM to develop and deploy this system such as Dole, Driscoll's, Golden State Food, Kroger, McCormick, McLane, Nestlé, Walmart,... [3]. This is a complex supply chain management system, which is designed primarily for big companies, and it is still in the development phase.

In this study, we propose a food supply chain management model based on Walmart's model using blockchain technology. This model is aimed at the small to moderate companies with a simple management procedure. This model will be implemented based on the Ethereum platform and the PoA consensus protocol for faster transaction processing time.

The paper is structured as follows: Section 2 presents the system architecture including the supply chain management model, the introduction of blockchain technology, and the model of food product origins management system based on blockchain technology. The system implementation and testing results are reported in Section 3. Finally, Section 4 presents our conclusion and future work of this study.

II. BACKGROUND

A. Blockchain technology

In general term, blockchain is a shared, distributed ledger of information to record transactions and manage both tangible and intangible assets. Most of things can be managed and shared through the blockchain network to reduce stakeholders' risk and cost [12].

In technical terms, blockchain is a peer-to-peer network including several nodes connected together. Each node stores all transaction data and they are always synchronized. Each transaction needs to be approved by all nodes in the network using a consensus protocol before it is stored in the chain. This means that all nodes in the network must agree on the execution of the transaction based on a predefined consensus protocol to have the transaction executed and the data is stored. This technology breaks conventional transactions model in which all transactions need an intermediary agent and under a centralized control.

In blockchain technology, transaction data is stored in blocks. These blocks are connected together to create a blockchain. Each block contains a serial number, timestamp, nonce value (calculated based on block data to create a block's hash that meets a given condition), data of one or more transactions, , hash code of the prior block, and its SHA-256 hash code. Figure 1 demonstrates one chain with three blocks.

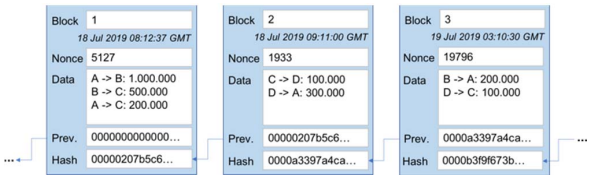

Figure 1 Data stored in chain of blocks in blockchain technology

With the above rule of blockchain, any change of data in a block will result in the hash of block being changed and the links of chain will be broken. Moreover, because blockchain is a peer-to-peer network, each node stores the entire data of blockchain. If one node change data, it will be detected by the remaining nodes in the network. This warranty the immutability and security for blockchain. Figure 2 shows that when data in one block is changed, the blockchain will be broken.

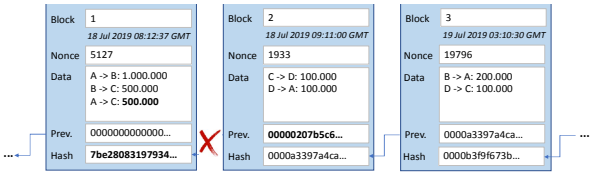

Figure 2 Changing data in 1 block breaks the chain

Procedure to process a transaction in a blockchain network is described in Figure 3.

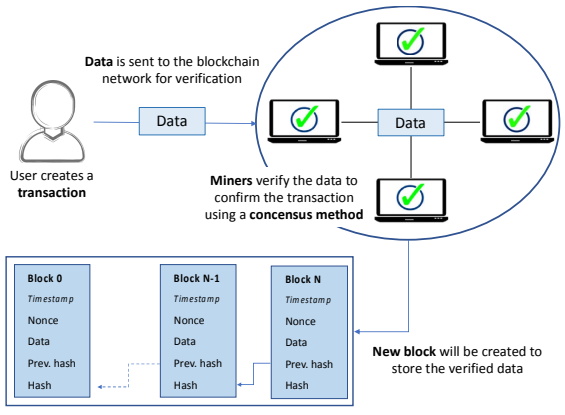

Figure 3 Transaction process procedure in blockchain

B. The consensus protocols

Blockchain is a peer-to-peer network and operates in self-determination and mutual trust mechanism between the nodes of the network without the need for a trusted middle-man. Consensus plays an important role in the blockchain network, which maintains the integrity and security of the system. The consensus is a mechanism in which all nodes in the blockchain network approve transactions. This mechanism ensures that the rule of blockchain is maintained and transactions are stored correctly and reliably.

Today, there have been some consensus protocols such as PoW (Proof of Work), PoA (Proof of Authority), PoS (Proof of Stake), PoET (Proof of Elapsed Time), PBFT (Proof of Byzantine Fault Tolerance), etc. Each protocol has its own advantages and disadvantages each of them is suited to a particular application. The mechanism of some common consensus algorithms is described as follows:

1) Proof of Work (PoW)

This is the first consensus algorithm that is associated with cryptocurrencies [1]. In this consensus, when the blockchain network needs to create a new block to store data of new transactions, all nodes complete with each other to calculate the value of the nonce field. The nonce value ensures the hash code of the new block satisfying a predefined pattern. For instance, in the example presented in Figure 1, the hash value of all blocks must start with five zero numbers. Therefore, whenever a new block needs to be created, the nodes in the network must calculate the nonce value for the new block so that the block's hash code starts with five zero numbers. When a node found the expected nonce value, it will send it to all other nodes to check for the correctness of the nonce value. If all nodes accept the new block, it will be added to the blockchain and the transactions complete. In this consensus protocol, nodes in the network are called miners and the first miner which found the correct nonce value will receive a reward (a certain number of cryptocurrencies). This consensus protocol can against the DDoS attacks. However, the main drawback is that it may take a huge computing resource to calculate the nonce value and the 51% attack method can be used [1].

2) Proof of Stake (PoS)

This consensus protocol avoids the resource wastage of PoW. In PoS, to participate in creating a new block in the chain, the nodes must deposit a certain amount of stake. There are many methods of selecting this node, such as random selection, stake-value-based selection, and so on. If any fraud is detected, the selected node will be punished. The algorithm is also capable of resisting the 51% attack because a node that wants to attack the network must have a deposit of more than 51% of the total of assets in the network. This is extremely difficult because the value of today's cryptocurrencies is huge. In addition, this consensus protocol has more benefits compared to PoW such as faster transaction execution time and flexibility in selecting verification node. However, the consensus also has some disadvantages like the difficulty of building sustainable communities because verification rights are in hands of those with a lot of assets (the rich get richer).

3) Proof of Authority (PoA)

The PoA consensus protocol chooses the nodes to verify the transaction bases on the "reputation" of the nodes in the network. Therefore, it is suited to private blockchains. This consensus protocol enhances the value of users' identity in the network. Nodes with high "reputation" will be selected to verify transactions. This means that the blockchain network will authorize trusted nodes on the network to perform authentication. This will encourage users in the network to maintain their reputation and restrict illegal actions. PoA can be considered a variant of the PoS in which reputation plays the role of deposit assets. However, because this model has the disadvantages of decentralized models and third-party exploitation, it can entice reputable users to perform illegal actions.

C. Smart contract

Smart contracts are computer codes that represent an agreement or a rule that governs transactions stored in the blockchain network and is executed as a part of the transactions [13]. A smart contract can have many contract terms and can be implemented in whole or in parts. When all parties are eligible for a smart contract, the contract will be automatically executed. Figure 4 depicts the components of the blockchain network and their location throughout the system.

For example, a smart contract determines the contract terms in which the deposits will be returned to customers or a smart contract defines the terms of travel insurance in which insurance company pays insurance payments to customers if customer's flights are delayed more than 6 hours,…

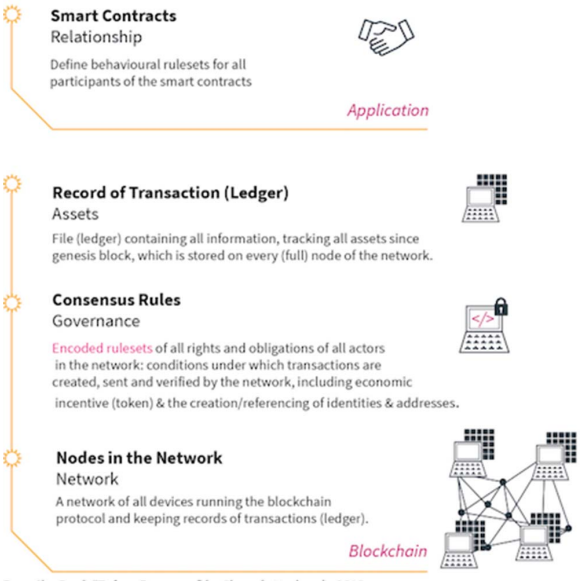

Figure 4 The components of blockchain and their roles

Once a contract is deployed, it cannot be modified. Therefore, smart contracts provide superior security and reduce cost and time compared to the conventional contracts, which require a middle-man. A smart contract is written in a certain programming language, depending on the blockchain platform. For example, the Ethereum platform [20] uses Solidity language while Hypeleger Fabric uses JavaScript, GOLANG, and Java [1].

III. SYSTEM ARCHITECTURE

A. The supply chain management and product origins tracking model

A supply chain is a network including importing materials, transforming materials to products and distributing products to consumers [11]. Supply chains contain organizations that engage to manufacture, transport and sell products to customers. Supply chains do not only consist of manufacturers and suppliers, but also the logistics, storages, retailers and customers. Figure 5 describes a common supply chain model.

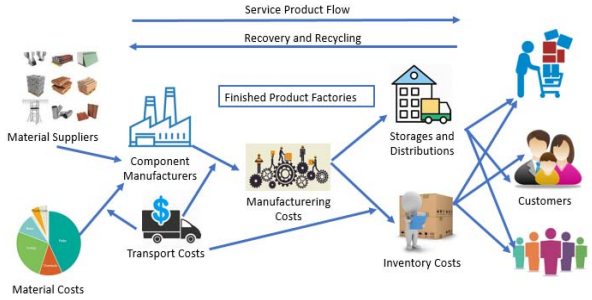

Figure 5 Common supply chain model (Nguồn: Vakaxa[2])

Supply chain models are dynamic because they are affected by the manufacturing and distribution processes of products. A supply chains does not only include the final product manufacturer, but also involve other information related to the production progress such as the production materials. It also depends on particular requirements of the stakeholders.

In this study, we build a product origins tracking system, in particular for agricultural products. The system allow customers to access product information from cultivation to the final product. For example, a customer who buys a mango at a supermarket can look up where the mango is grown, how it is harvested, what are importers, exporters and the packing company (or retailer). In each stage of the supply chain, customers can search related information such as when the fruit was grown or which fertilizers were used at the farming stage, etc. This model is based on Walmark's retail supply chain management model, which is illustrated in Figure 6.

Figure 6 Walmart supply chain model (Source: Walmart[3])

Aimed at small to moderate companies, we simplify the Walmart's model. The agricultural supply chain model proposed includes five steps: farming, harvesting, exporting, importing and packaging. Figure 7 depicts the proposed model and the corresponding actor of each step.

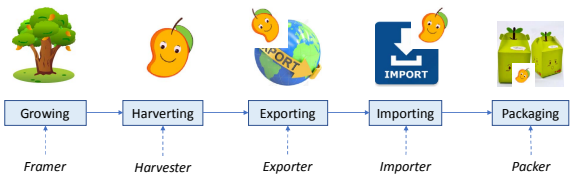

Figure 7 Proposed supply chain model for agriculture products

B. System architecture

Our proposed model includes five stages: farming, harvesting, exporting, importing and processing as described in Figure 3. The information of each stage is updated to the blockchain, which is used to track the product origins. When buying a product, customers can access the system to check where the product was produced. Based on the proposed model, we design the architecture for the agriculture product tracking application including three components as described in Figure 8.

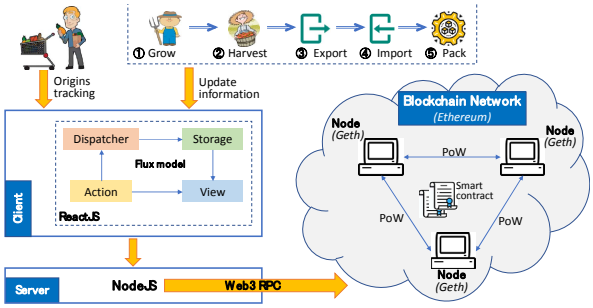

Figure 8 Proposed model for product origins tracking

The Client interacts with the users and gets their requirements such as create a new product, update the supply chain information, inquiry the product origins, etc. Then it will send user requirements to Server, get the server response and display the results to users.

When Server receives the requests from Client, it will interact with the blockchain network using Web3RPC to process user's requests. For example, when users want to login to the Server, the requests are transferred to the Server and the Server calls function `login()` in the smart contract SuppyChainUser of the blockchain network to verify user account. The login result is replied to the Client and it will be displayed to users. As another example, when a farmer wants to update fertilizer information used for a product, the request is sent to the Server. Then, the Server calls function `setFarmInspectorData()` in smart contract SupplyChain to store the information.

The last component is the blockchain network. It stores supply chain data to against the modification and prevent data from attacks. Besides, the blockchain network also stores smart contracts related to user interactions such as update and inquiry information of products.

IV. IMPLEMENTATION AND RESULT

A. System implementation

The implementation of the system is described in Figure 8. We utilize the Relux model and ReactJS framework [14] for the Client implementation. These are popular front-end techniques for the web interface. NodeJS is used to build the Server and Web3.js RPC is used to interact with the blockchain network.

For the blockchain network, we use the Ethereum framework [22], which is the platform of the Ethereum

[2] https://vakaxa.com/vi/supply-chain-la-gi-vai-tro-va-loi-ich-cua-chuoi-cung-ung/

[3] https://corporate.walmart.com/global-responsibility/global-compliance-program-report-on-fiscal-year-2018

cryptocurrencies. This framework has a big user community and supports most of the basic features of blockchain such as smart contracts and PoW and PoA consensus protocols. In addition, the installation of Ethereum is straight forward and the number of supporting libraries are very large. Each node in the network is deployed with Geth client [4] and PoA consensus protocol. The cost (time and computing power) to create a new block with PoA is much higher than PoW.

The smart contracts in the system are written by the Solidity language. The system has five smart contracts and some data structures to store user information and supply chain data as described in Figure 9.

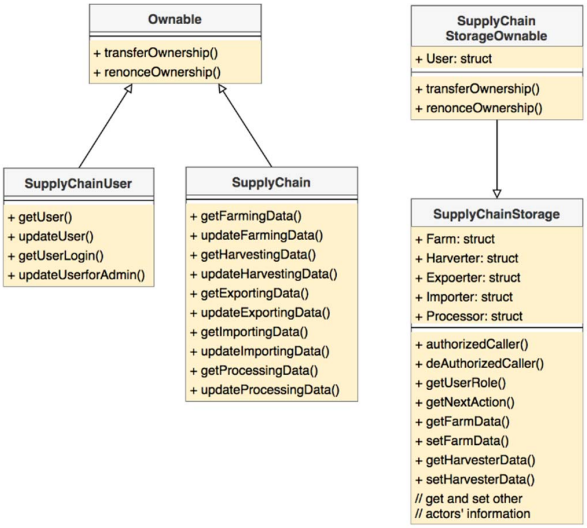

Figure 9 Smart contracts in the system

- Ownable and SupplyChainOwnable: contain the functions for user and role management.
- SupplyChainUser: inherits the Ownable smart contract and it is used to create user's data.
- SupplyChainStorage: inherits the SupplyChainStorageOwnable smart contract. It contains functions for creating the data of farmers, harvesters, importer, exporter and processors.
- SupplyChainProcess: inherits the Ownable smart contract and it is used to update data of the products.

B. Results and discussion

We successfully built a supply chain management system for the agriculture product origins tracking purpose. The system is implemented based on the Ethereum framework using the PoA consensus protocol. The basic functions of the system will be demonstrated as follows.

The system administrator can create, update and inquiry information related to users and products. Figure 10 demonstrates the user management function of the administrator and Figure 11 depicts the user interface for the administrator to create a new product.

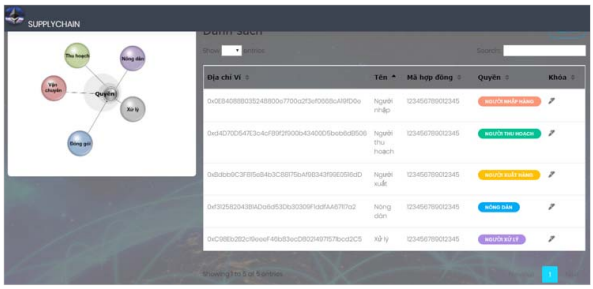

Figure 10 Administrator creates and updates users' information

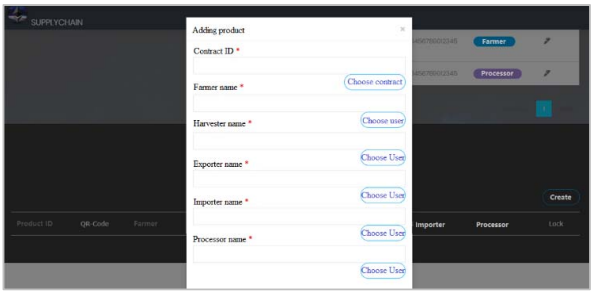

Figure 11 Interface to add a new product of the administrator

For other stages in the production steps, the user in each stage can update the related information of that stage. A user can only update the information if the previous stage had been finished. For example, the user at the packaging step can only update the product information at that step after the importer update the import information. Figure 12 and Figure 13 show the user interfaces of two main functions for the user at the packaging step including listing the list of their products and updating the product information.

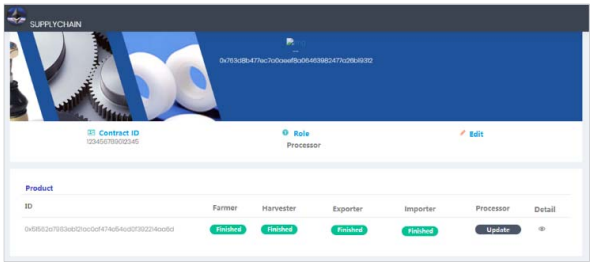

Figure 12 The packager can see the list of their products

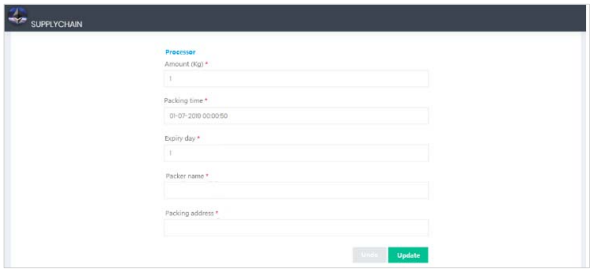

Figure 13 The packager updates the packaging information

[4] https://geth.ethereum.org/

Finally, the customer can track the origins of a product including the information of five steps in the production process as well as the initial step. Figure 14 demonstrates the result of the tracking product origins function for the customer. Due to the space limit, we present information about some steps in the production process.

We also investigate the process of the block creation in the blockchain network to verify its functionality. Figure 15 shows information of two blocks in the chain after we performed some transactions in the system. Each block contains the expected data as described in Section **Error! Reference source not found.** such as the block number, timestamp, transaction data, hash code, parent hash code, and nonce value. In addition, each block has also some extra information specialized for the Ethereum framework such as block size, block miner, gas used (cost for block verification), etc. For example, block 4802096 contains data of 10 transactions and also has the hash value of the previous block 4802095 to against any change in block 4802095. Similarly, any changes in block 4802096 cause the block hash code updated and the next block, 4802097 broken.

A remarkable point of the system is that the average time to create a block of the system is about 15 seconds. This is much faster than the PoW consensus protocol, which has the block creation time is about 10 minutes per block. That means in the PoW consensus protocol, a transaction has to wait about 10 minutes to be confirmed. This is one of the main advantages of PoA in comparison to PoW.

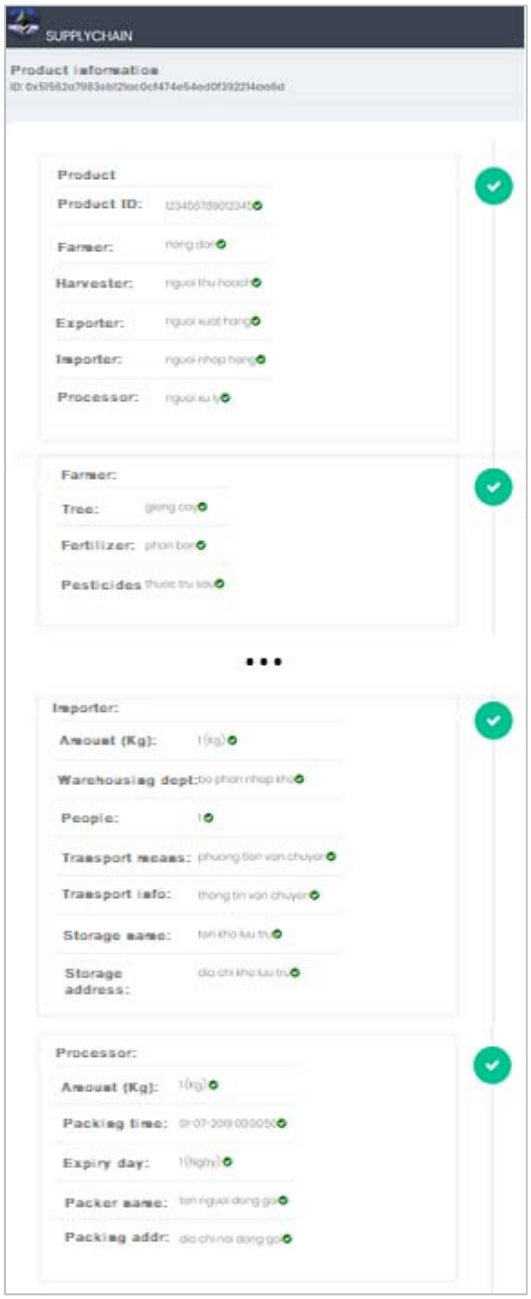

Figure 14 Product origins information

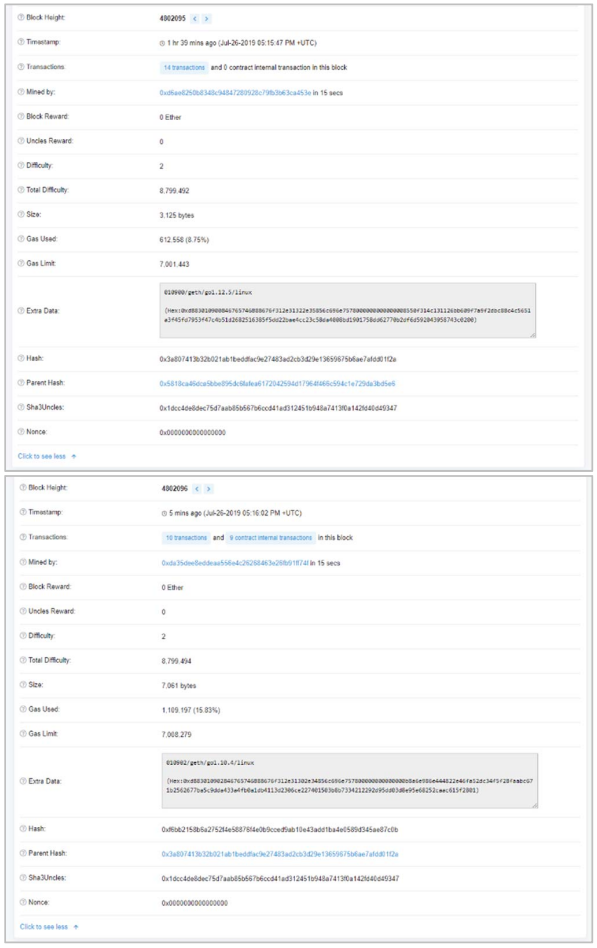

Figure 15 Blocks created after the transactions executed

V. CONCLUSION AND FUTURE WORK

In this research, we offered a model of supply chain management based on blockchain technology. A product origin tracking application was implemented successfully based on the proposed model using the Ethereum framework and PoA consensus protocol. We tested the system using a case study to demonstrate all functions of the system. The testing result shows that users can update and access product origins information, which catches up with the initial requests. The product information of each stage is shown in detail. The investigation on the network shows that data in the system is created under the PoA consensus protocol. It is encrypted and distributed in all the network nodes. This ensures the security, transparency and against data modification. These features make the blockchain technology is more suitable than the conventional database management systems, particularly in this application domain.

For future works, we will detail the supply chain process to meet the requirements of the complicated systems. Moreover, the application security such as user role also needs more investigation and improvement.

ACKNOWLEDGMENT

This study is funded in part by the Can Tho University Improvement Project VN14-P6, supported by a Japanese ODA loan.

REFERENCES

[1] Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., Enyeart, D., Ferris, C., Laventman, G., Manevich, Y. and Muralidharan, S., 2018, April. Hyperledger fabric: a distributed operating system for permissioned blockchains. In Proceedings of the Thirteenth EuroSys Conference (p. 30). ACM.

[2] Baliga, A., 2017. Understanding blockchain consensus models. In Persistent.

[3] Burleson, D.K. and Estabrook, G., 1999. Oracle SAP Administration. O'Reilly & Associates, Inc.

[4] Casado-Vara, R., González-Briones, A., Prieto, J. and Corchado, J.M., 2018. Smart contract for monitoring and control of logistics activities: pharmaceutical utilities case study. In The 13th International Conference on Soft Computing Models in Industrial and Environmental Applications (pp. 509-517). Springer, Cham.

[5] Christidis, K. and Devetsikiotis, M., 2016. Blockchains and smart contracts for the internet of things. IEEE Access, 4, pp.2292-2303.

[6] Davis, S.C., Mastercard International Inc, 2016. Method and system for processing blockchain-based transactions on existing payment networks. U.S. Patent Application 14/718,930.

[7] Dorri, A., Kanhere, S.S. and Jurdak, R., 2017, April. Towards an optimized blockchain for IoT. In Proceedings of the Second International Conference on Internet-of-Things Design and Implementation (pp. 173-178). ACM.

[8] Huh, S., Cho, S. and Kim, S., 2017, February. Managing IoT devices using blockchain platform. In 2017 19th international conference on advanced communication technology (ICACT) (pp. 464-467). IEEE.

[9] Iansiti, M. and Lakhani, K.R., 2017. The truth about blockchain. Harvard Business Review, 95(1), pp.118-127.

[10] Kamath, R., 2018. Food traceability on blockchain: Walmart's pork and mango pilots with IBM. The Journal of the British Blockchain Association, 1(1), p.3712.

[11] Laurence, T., 2019. Blockchain for dummies. John Wiley & Sons.

[12] Litke, A., Anagnostopoulos, D. and Varvarigou, T., 2019. Blockchains for Supply Chain Management: Architectural Elements and Challenges Towards a Global Scale Deployment. Logistics, 3(1), p.5.

[13] Fredendall, L.D. and Hill, E., 2016. Basics of supply chain management. CRC Press.

[14] Gackenheimer, C., 2015. Introducing flux: An application architecture for react. In Introduction to React (pp. 87-106). Apress, Berkeley, CA.

[15] Gupta M., 2017, Blockchain for Dummies, IBM Limitted Edition. John Wiley & Sons.

[16] Novo, O., 2018. Blockchain meets IoT: An architecture for scalable access management in IoT. IEEE Internet of Things Journal, 5(2), pp.1184-1195.

[17] Rae, C. and Thorwirth, N.J., Verimatrix Inc, 2017. Systems and Methods for Decentralizing Commerce and Rights Management for Digital Assets Using a Blockchain Rights Ledger. U.S. Patent Application 15/336,778.

[18] Sharples, M. and Domingue, J., 2016, September. The blockchain and kudos: A distributed system for educational record, reputation and reward. In European Conference on Technology Enhanced Learning (pp. 490-496). Springer, Cham.

[19] Shermin V., 2019. Token Economy: How Blockchains and Smart Contracts Revolutionize the Economy. BlockchainHub Berlin.

[20] Suresh, N. and Choudaiah, S., 2019. Blockchains and Smart Contracts for the Internet of Things. 24(1), pp.16-16.

[21] Swan, M., 2015. Blockchain: Blueprint for a new economy. O'Reilly Media, Inc.

[22] Wood, G., 2014. Ethereum: A secure decentralised generalised transaction ledger. Ethereum project yellow paper, 151(2014), pp.1-32.

[23] Zheng, Z., Xie, S., Dai, H., Chen, X. and Wang, H., 2017, June. An overview of blockchain technology: Architecture, consensus, and future trends. In 2017 IEEE International Congress on Big Data (BigData Congress) (pp. 557-564). IEEE