Sensors and Materials, Vol. 33, No. 2 (2021) 601–613
MYU Tokyo

S & M 2480

Novel System Using Blockchain for Origin Traceability of Agricultural Products

Nguyen Minh Son,[1] Thanh-Lam Nguyen,[2*] Phan Thi Huong,[1] and Lam Thanh Hien[1]

[1]Faculty of Information Technology, Lac Hong University, Bien Hoa, Dong Nai, 810000, Vietnam
[2]Office of International Affairs, Lac Hong University, Bien Hoa, Dong Nai, 810000, Vietnam

(Received June 4, 2019; accepted January 25, 2021)

Keywords: blockchain, origin traceability, agricultural products, blockchain system

In recent years, many countries have faced inextricable problems in how to deal with the rapid increase in the number of different diseases, which mostly result from the environment and food taken daily; thus, eating healthy and clean foods is always a concern of almost every consumer. Consumers usually make their decisions on the basis of the information provided on the packaging. However, for agricultural products, ensuring that they get exactly what is mentioned on the packaging is a really thorny problem. In practice, several standards have been set up to help agricultural businesses and farmers improve their operational efficiency and ensure their food hygiene and safety. Standards such as Global Good Agricultural Practices (GlobalGAP), Vietnamese Good Agricultural Practices (VietGAP), and Hazard Analysis and Critical Control Points (HACCP) usually cover all production processes from farming inputs such as feeding materials, seeds, and related farming activities to the finally packaged outputs. If businesses and farmers are certified to meet certain standards and they strictly follow the guidelines during the production, consumers can trust in their own decisions. However, it is normally unknown if the production closely follows what has been certified or whether there has been any bribery, cheating, or other negative issues hidden for profit purposes because related information recorded or stored in farm log-books may also be erroneous for intentional or unintentional reasons. To overcome the problem, in this paper, we propose a novel method applying blockchain and IoT technology to support the origin traceability of agricultural products at farms. By using sensors and computational codes to read parameters that affect farming processes such as temperature, humidity, solute concentration, and pH, all related information and data used in origin traceability will be recorded and saved in the blockchain system in the form of logs in a ledger through smart contracts. Specifically, the system operates automatically on the basis of installed smart contracts, i.e., recorded data are stored on a blockchain through smart contracts and are free from human intervention. The proposed system has been constructed and tested with highly satisfactory results. Even if some nodes in the system are knocked down for some reason, when the knocked-down nodes are reconstructed, their original data are automatically and fully recovered from their friend nodes. Consequently, our proposed system provides not only an objective mechanism for collecting and storing data but also a secure environment to effectively trace the origin of agricultural products.

*Corresponding author: e-mail: green4rest.vn@gmail.com
https://doi.org/10.18494/SAM.2021.2490

ISSN 0914-4935 © MYU K.K.

1. Introduction

Several countries have been making a special effort to deal with food safety problems because contaminated foods lead to negative impacts on human health and social welfare. For instance, recent statistics by the World Health Organization show that "Unsafe food containing harmful bacteria, viruses, parasites or chemical substances, causes more than 200 diseases – ranging from diarrhoea to cancers. An estimated 600 million—almost 1 in 10 people in the world—fall ill after eating contaminated food and 420000 die every year, resulting in the loss of 33 million healthy life years (DALYs). Children under 5 years of age carry 40% of the foodborne disease burden, with 125000 deaths every year. Diarrheal diseases are the most common illnesses resulting from the consumption of contaminated food, causing 550 million people to fall ill and 230000 deaths every year".[(1)] Similarly, Nielsen also pointed that "67% of Americans said they will be prioritizing healthy or socially conscious food purchases in 2018".[(2)] These findings clearly illustrate the importance of food safety and public concerns as well as the changing behavior among consumers. Specifically, people are inclined to search for clean foods with guaranteed safety and origin traceability from their sowing, processing, and storing before they are sold to the end consumers. However, the existing data sources of foods have certain problems in terms of data security, validity, and public accessibility. In addition, the lack of trustworthy relationships among people in creating reliable data results in several issues in constructing an effective data management system.

Practically, with agricultural and aquacultural products, several international standards and sustainable certification programs have been successfully implemented. Some national/regional good agricultural practice (GAP) standards include EurepGAP, ASEAN G.A.P., and GlobalG. A.P., and more than 100 quality standards for agricultural products including HACCP have become important tools to support conscientious consumption by providing certified information to help consumers better understand product quality.[(3–6)] Such certification has greatly helped consumers in selecting better sources for their foods. However, although they know that the selected foods satisfy the standards set by the certification body mentioned on the package, consumers fail to fully understand the actual meaning of the printed marks or verify the underlying data because the verification of data integrity needs a time-consuming and expensive audit process. Moreover, the implementation of certification programs in some regions with high levels of corruption poses certain risks to the reliability of the certification standards. Advanced hardware and network architectures have been applied to trace the food origins in centralized supply chains. Nonetheless, whether the provided data in the systems are reliable is still questionable owing to maladministration and the possibility of bribery or even intentional changes made by system hackers or internal factors.

To overcome the existing problems, Feng proposed using a blockchain, a system where most information of food products can be stored and transparently shared among all members in a supply chain system.[(4)] Thanks to Peer2Peer apparatus and smart contracts, a blockchain can effectively distribute the data based on a decentralized consensus mechanism. In addition to the key fields of information to be stored, each block is also encrypted with other information, such as the transaction time or the time when the data are modified. Therefore, a blockchain can be

used in origin traceability in business supply chains. Feng proposed deploying a decentralized distribution system that uses IoT devices such as radio-frequency identification (RFID), wireless sensor network (WSN), and global positioning system (GPS) attached on physical products to collect and transfer data.[4] However, the system can only show that the provided information is either original or modified with inerasable tracks. As the data in the production stage are manually typed into the data system, Feng's approach still fails to deal with practical problems where the related data are dishonestly and incorrectly input for the sake of producers' profits. To overcome such a problem, for a more reliable system, related data input into the system should be directly and automatically recorded without human intervention. Consequently, in this paper, we propose a source-based traceability solution that uses a blockchain in combination with IoT devices to directly record relevant data into the tracking system. In particular, our proposed approach can effectively work even when the system is attacked.

To achieve the objectives, this paper is organized as follows. Section 2 briefly presents some literature about blockchains, Internet of Things (IoT), Message Queue Telemetry Transport (MQTT), and NoSQL. A database for a system constructed with our proposed approach and some experimental results are presented in Sect. 3. Some concluding remarks make up the last section.

2. Materials and Methods

2.1 Blockchain

The blockchain was first introduced by Haber and Stornetta, aiming to provide digital signatures for ease in registering digital documents.[7] In 2008, an encrypted currency named Bitcoin using blockchain technology was created by Nakamoto.[8] Since then, blockchain technology has gradually gained wider recognition through its successful applications in finance, education, health management, etc.[9] The recent advances in technology have created greater potential applicability of blockchains in practice, from digital currencies to legal contracts.[10]

Basically, a blockchain is understood as a peer-to-peer database including nodes with similar authority and mutual trust based on a consensus protocol. It contains a ledger that records all transaction information, which is fully copied to each node. Nodes are maintained by all participants in the blockchain. Each node can be considered as a miner whose task is to confirm transactions sent by the user based on the established smart contracts, then pack that transaction into a block on the system. Each block contains the information of a transaction as well as the hash code of the previous block, which helps the information to be stored into a blockchain. Each miner when completing a task will be rewarded with a "gas fee". Each transaction can result in the creation of a new block that will be notified to all miners in the system. Once a block is created, all miners need a consensus whether to accept the block or not. Some frequently used terms include:[11]

Distributed: Data are stored in parallel in all nodes of the system; thus, with the use of hash functions, blockchains are considered extremely secure.

Peer-to-peer: Information is shared to all participants, i.e., a running node is always connected to other nodes (also called friend nodes), and all private information or external transactions are shared among nodes in pairs. This action is then repeated with their connections.

Consensus protocol: This is the most revolutionary idea of this technology. It can identify correct blocks to add into the blockchain, whereas incorrect blocks will be rejected by other participants.

Ledger: Each participant has a copy of the transaction history and it is always updated. This helps to check whether a person is trying to make a transaction with sufficient resources; thus, it can effectively solve the double spending problem, which is a form of fraud using two different transactions to spend the same balance of an account.

Anonymous: Participants can access the system using a private key and public key or wallet, which is a code including letters and alphanumeric numbers that can be seen by other participants.

Smart contract: A smart contract is a set of terms that are programmed to be automatically executed and enforced by the mentioned consensus protocol. A smart contract is identified by a fixed address. Once a smart contract is deployed onto the blockchain, the program codes of the smart contract cannot be tampered with, thus avoiding malicious interference actions in the execution of the contract terms.

Decentralized App (DApp): The decentralized app is a decentralized network application that uses blockchain technology to store data and logs, and a DApp must be an open source application and use a certain electronic currency unit.

There are three types of blockchain, private, consortium, and public, as shown in Table 1.[10] Among them, we select the consortium blockchain because we consider each farm as a node in the system and that many farms will together become an association. Specifically, a consortium blockchain is a blockchain where the consensus process is controlled by a set of preselected nodes; for example, with an agricultural cooperative of 15 farms, each farm only needs to operate one node, and a block becomes effective when it is endorsed by at least 10 nodes. Permissions to read the blockchain can be either public or limited to participants, and there are combinatory streams such as root hashes of publicized blocks with the API to allow community members to perform a limited number of queries and regain the cryptographic evidence of some parts of the blockchain status. These blockchains can be considered as partially decentralized.

Table 1
Types of blockchains.

Property	Private blockchain	Consortium blockchain	Public blockchain
Consensus determination	One organization	Selected set of nodes	All miners
Consensus process	Permissioned	Permissioned	Free
Read permission	Public or restricted	Public or restricted	Public
Centralization	Yes	Partial	No
Efficiency	High	High	Low
Immutability	Could be tampered with	Could be tampered with	Almost impossible to tamper with

2.2 IoT

IoT has emerged since the early days of the internet, when inventors wanted to connect everything through a homogeneous network to effectively control them to fit human purposes. IoT allows us to monitor and control remote physical items.[12] IoT is a scenario of the modern world, where every object is assigned with its own identifier, and all objects have the ability to exchange information and data across a homogeneous network without the need of direct interaction between people and people, or people with computers. IoT has evolved from the convergence of wireless technology, micro-electro-mechanical technology, and the internet. In short, with IoT, when everything is connected to each other over the internet, users/owners can effectively control them online with a smart device, such as a smartphone, tablet, PC, or even just a tiny smart watch.

2.3 MQTT

MQTT, a remote queuing communication protocol, is used in IoT for data transmission based on the publish/subscribe model, which is highly reliable and suitable with a low bandwidth or unstable transmission conditions.[13,14] At a high-level architecture, MQTT consists of two main components, a broker and clients, as shown in Fig. 1. Specifically, in a system that uses the MQTT protocol, many clients connect to a server called the MQTT broker. Each client needs to subscribe to receive messages from a topic and/or publish messages related to a topic. Any update to the topic is accordingly provided to related clients. Because of its high security and real-time performance, the MQTT protocol is deployed in this study.

To effectively perform the updates, the broker is in charge of receiving messages from the publishers, queueing the messages, and transferring them to specific addresses; thus, as shown in Fig. 1, the broker plays crucial roles in connecting the clients. The broker can also take on some additional tasks related to the communication process such as securing messages, storing messages, creating logs, etc. Meanwhile, clients are divided into two groups, publishers and subscribers. Clients are software components that operate at edge devices; hence, they are designed to have flexible operation. A client can either publish messages on a specific topic or subscribe to receive messages from a topic, or both.

Message: In the MQTT protocol, a message is also referred to as "message payload". It can be formatted in either plain text or other formats if needed.

Topic: A topic is considered as a logical "link" between publishers and subscribers. When the message of a topic is published, it will be automatically delivered to all related subscribers.

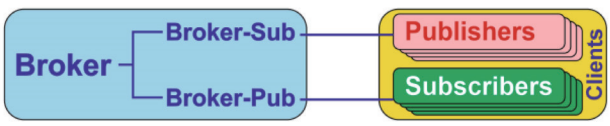


Fig. 1. (Color online) Two main components of MQTT protocol.

2.4 NoSQL database

There are still some challenges in deploying blockchains in practice. For example, owing to the size limit of a block, no more than seven transactions can be handled in a second;[15] moreover, the rapid increase in the number of blocks leads to several problems in the storage space and synchronization.[16] Therefore, to provide enough data for users/consumers to effectively trace the origin of an agricultural product, in addition to the information stored in blocks, related data are also stored on a non-relational SQL (NoSQL) database owing to its large storage capacity and advantage of continuous update. All data uploaded onto NoSQL are always encrypted to ensure security.

Among the several NoSQL databases, we deploy MongoDB owing to its flexible structure and ability to deal with data of different formats. In fact, MongoDB is a document-oriented database where the data are stored in JSON format instead of tabular format as required in a relational database, i.e., data are stored in documents (similar to rows in a table) and collections (similar to tables); hence, the queries on MongoDB are normally executed quickly.

3. Proposed System of Blockchain and IoT Devices

Hounsell *et al.* pointed out that aquaponics systems provide several advantages such as easier harvesting and monitoring of the nutrient supply for the plants as well as the use of less water and smaller amounts of plant protection chemicals and pesticide/insecticides.[17] Consequently, in our experimental study, an aquaponics system is used to analyze the performance of our proposed system. Specifically, our proposed system, which uses a blockchain to automatically collect and store the information for origin traceability, is shown in Fig. 2. Typically, devices

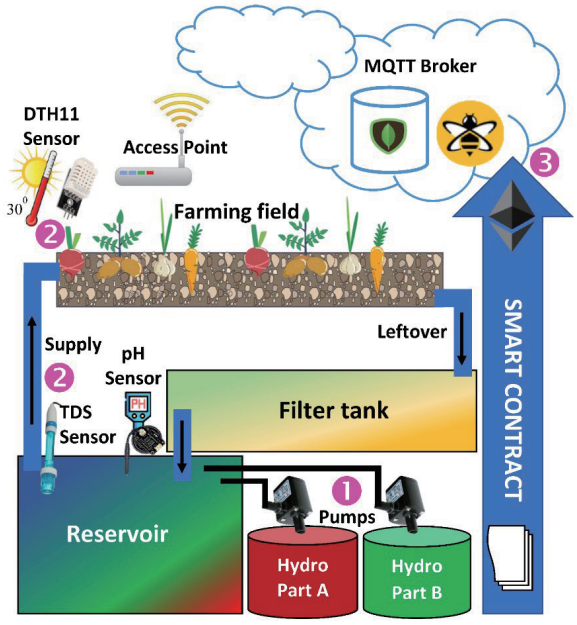


Fig. 2. (Color online) Components in the proposed system at a farm.

integrated with sensors are used to monitor the water supply and growth process while a terminal sensor is used to determine key parameters of the system. As shown in Fig. 2, the system includes the following components:

3.1 Hydro Part A and Hydro Part B

These contain key active nutrient ingredients for plants. In particular, the leftover nutrients supplied from the reservoir are collected in a tank, which filters out residue before useable components are moved to the reservoir. On the basis of the changes in the reservoir contents, the solutions in Hydro Part A and Hydro Part B are accordingly pumped into the reservoir to achieve a specified concentration. The mixture of solutions in the reservoir is then pumped to the farming field to supply nutrients to plants.

3.2 Sensors

Several sensors measuring pH level, solute concentration, temperature, humidity, etc., are used to monitor and control the whole process of growing plants in a close cycle. Specifically, the DTH11 sensor is a temperature and humidity sensor with VCC, GND, and OUT pins. It can effectively measure humidity ranging from 20 to 90% RH with a tolerance of ±5% RH and an environment temperature ranging from 0 to 50 °C with ±2 °C tolerance. Moreover, our system has two key sensors: one is used to measure the pH level and one is used to measure total amounts of dissolved solids (TDS) as the pH level and TDS are critical to the crop water.[18–21] Meanwhile, the TDS sensor is used to measure the TDS, minerals, and nutrients in the water in parts per million (ppm) with a tolerance of ±10% F.S. at the environment temperature of 25 °C.[14] The TDS sensor uses a 3.3–5 V DC power supply. Its signal outputs are in analogue form from 0 to 2.3 V, corresponding to a measurement range from 0 to 1000 ppm, i.e., a higher TDS signal indicates a more soluble substance existing in the water and lower purity as shown in Fig. 3.

In addition, a pH sensor is used to measure the pH level of the water with a pH probe and send the read data to a BNC port. It uses a 5 V DC power supply and can read pH values in the range of 0–14. In an environment temperature ranging from 0 to 60 °C, it has a tolerance of ±0.1 pH.

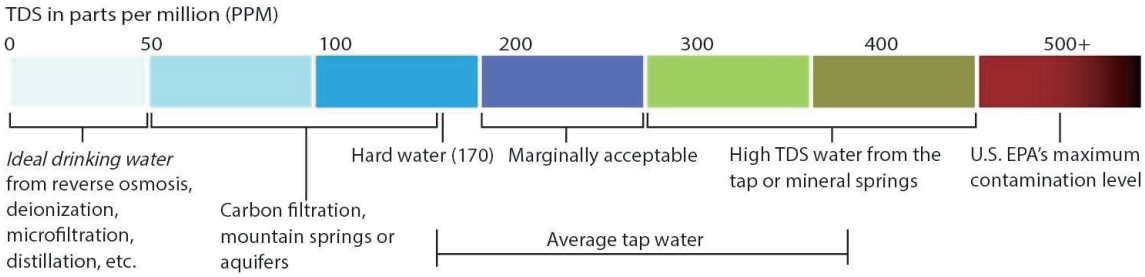


Fig. 3. (Color online) Scale of water purity.

3.3 IoT devices

The IoT devices used in this study consist of a low-cost ESP32 chip for Wi-Fi and Bluetooth connection, a Tensilica LX6 dual-core 240 MHz processor (one core for high-speed connection and one core for independent programming), a built-in UART CP2102 load circuit, a 5 V DC power source, and 34 GPIOs. The ESP32 chip is used to read sensor signals and communicate with the MQTT broker. The ESP32 chip is selected in this system because it can effectively work in environments of various temperatures ranging from −40 to +125 °C.[22] The IoT devices use the MQTT protocol to collect signals from the sensors in the farm and store related data on cloud-based services of MongoDB and blocks concurrently.

3.4 Ethereum Virtual Machine

An Ethereum Virtual Machine (EVM) is a physical computer that is installed and configured to become a node in the blockchain. The EVM is configured with Intel(R) Core i7-8750 CPU@2.2 GHz (12 CPUs), 8192 MB RAM with GeForce GTX 1050 Ti 4018 MB, HDD 250 GB, 1 Gbps internet connection (NIC), OS Ubuntu 14.04 with Linux 3.13, and Ethereum V.2.02. Each EVM handles the terms in the smart contract without relying on a central server. The information is exchanged among the EVMs through Whisper protocol, which is an encrypted protocol, allowing nodes to send information directly to each other safely. The general idea of implementing the blockchain technology for the origin traceability of agricultural products planted in several farms is shown in Fig. 4.

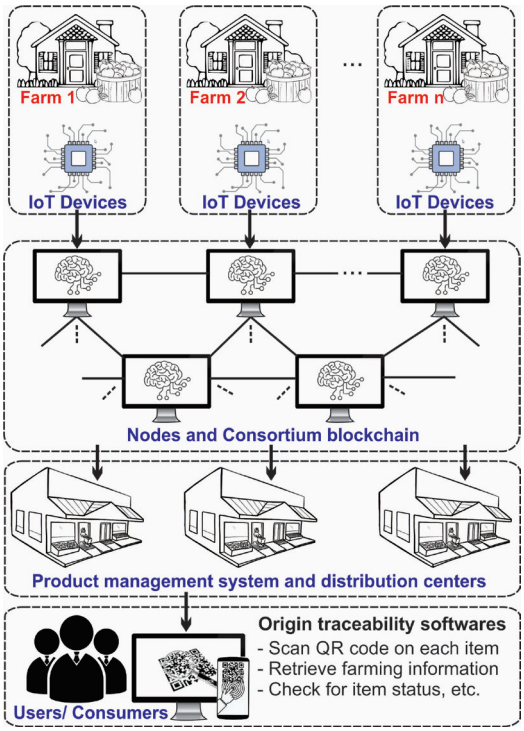


Fig. 4. (Color online) Overall system using blockchain for origin traceability.

Specifically, each farm has its own EVM system and connects with other farms using blockchain technology. Each farm can grow one or more special type of vegetable/fruit. The related information of the growing process will be stored on the blockchain if and only if it is endorsed by all of the nodes on the system. A gas fee will be charged to the farm of the endorsed information. All information in digital format available for the public is stored on MongoDB via MQTT and HTTP protocols by a wireless network as shown in Fig. 5. All IoT devices are programmed to send data to the blockchain via the MQTT protocol and to MongoDB through the HTTP protocols at a specified time interval.

Each node is configured with a limited number of times to send data to the blockchain; we make it four times/day, corresponding to four time intervals: 0–6, 6–12, 12–18, and 18–24 h. In each interval, the system has the predefined function *iRandomTheTimeInDay*(*int hMin, int hMax*) to randomize the time to transmit the data for storage in the blockchain system. This means that the system is free from human interference and cannot be cheated; thus, the data stored on the blockchain objectively reflect the growth process of the agricultural products.

In our proposed system, the smart contract comprises the programs written in the blockchain Ethereum, in which a certain number of ETHs are allocated to the smart contract so that it can be activated on the system. A typical example of the storage of the smart contract is shown in Fig. 6, and users can access the sensor values from the blockchain system via an ID as shown in Fig. 7.

Each agricultural product is labelled with a QR code that stores key information about the growth process so that consumers/users can trace its origin with a simple app such as a QR

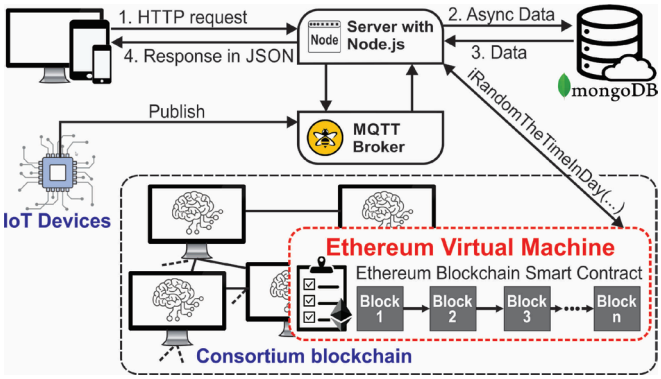


Fig. 5. (Color online) Data flow in blockchain and MongoDB.

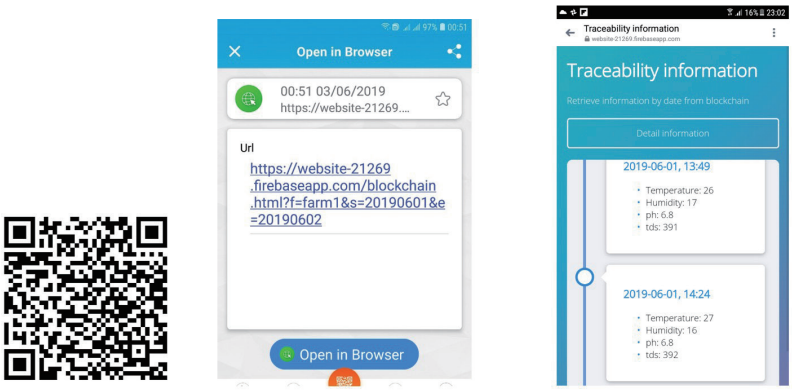
```
pragma solidity ^0.5.0;
contract ESP8266 {
    int256 public Index = 0;
    struct Sensor {
        string temperature;
        string humidity;
        string tds;
        string pH;
    }
    mapping (int256 => string) public tblId;
    mapping (string => Sensor) tblSensor;

    // insert data:
    function Insert (string memory id, string memory temperature, string memory humidity, string memory tds, string memory pH) public {
        tblId [Index++] = id;
        tblSensor [id] = Sensor (temperature, humidity,tds,pH);
    }

    // geting data:
    function Find (string memory id) public view returns (string memory temperature, string memory humidity,string memory tds, string memory pH) {
        Sensor storage result = tblSensor [id];
        return (result.temperature, result.humidity,result.tds,result.pH);
    }
}
```

Fig. 6. (Color online) Typical example of a smart contract with four sensor signals from the system.

Fig. 7. (Color online) Typical example of information accessed with an ID.



(a) (b) (c)

Fig. 8. (Color online) Consumers/users scan QR code to retrieve information from blockchain. (a) QR code. (b) Details to show on web. (c) Typical tracking results.

scanner and a device connected to the internet. For example, by using a QR scanner on a smart phone to scan a QR code of a product, as shown in Fig. 8(a), a consumer is directed to view full details in a browser as shown in Figs. 8(b) and 8(c). Consumers/users can also access full data from MongoDB for the origin traceability as shown in Fig. 9.

We tested the reliability of the system by purposely knocking down some nodes and we found that the knocked-down nodes were reconstructed and their original data were automatically and fully recovered from their friend nodes. Consequently, our proposed system provides not only an objective mechanism for collecting and storing data but also a secure environment to effectively trace the originality of agricultural products. In particular, compared with the traditional QR code, the performance of our proposed approach was found to be better in terms of performance (latency and transaction speed, maintenance costs, redundancy, scalability), trust (lack of trusted third parties, accountability, immutability, multiple non-trusting writers, peer-to-peer transactions, input data from sensors), context (traceability of transactions, verifiability of transactions, data/transaction notarization, data transparency, security, privacy), and consensus (rules of engagement, need for verifiers, autonomous/dynamic interactions between transactions of different writers). Our findings further agree with those by Aramyan *et al.*[23] and Casino *et al.*[24]

Fig. 9. (Color online) Chart showing value of sensor signals stored on MongoDB.

4. Conclusion

Nowadays, people are increasingly concerned about the quality of foods for the sake of their health; thus, getting to know more about how foods are made has become critical. The origin traceability of foods, especially agricultural products, has been an interesting research topic for several years. However, the existing approaches may encounter some issues related to the reliability of the data and information from consumer/user perspectives owing to the possibility of human intervention on documents stored on the system. To overcome this shortcoming, in this paper, we propose using a blockchain, a modern technology, in combination with IoT devices to automatically record the data on a blockchain system. Specifically, our proposed system not only provides real-time information to all related members about food safety and security but also reduces the risk of centralized information systems because it offers a fully distributed, transparent, and more collaborative working environment. All components in the system are quite cheap and commercially available; thus, we strongly believe that our proposed approach is applicable in practice.

References

1 Food safety: https://www.who.int/news-room/fact-sheets/detail/food-safety (accessed December 2018).
2 Fad or fundamental? What's next for health & wellness in 2018: https://www.nielsen.com/us/en/insights/news/2018/fad-or-fundamental-whats-next-for-health-wellness-in-2018.html (accessed December 2018).
3 Agricultural Quality Standards—Standards and Recommendations: http://www.unece.org/tradewelcome/steering-committee-on-trade-capacity-and-standards/tradeagr/standards-and-recommendations.html (accessed December 2018).
4 F. Tian: Int. Conf. Service Systems and Service Management (Dalian, 2017) 1–6. https://doi.org/10.1109/ICSSSM.2017.7996119
5 Sustainable Development Goals: https://www.globalgap.org/uk_en/what-we-do/un-sustainable-development-goals (accessed December 2018).
6 The GLOBALG.A.P. Fruit & Vegetables Standard: https://www.globalgap.org/uk_en/for-producers/globalg.a.p./integrated-farm-assurance-ifa/crops/FV (accessed December 2018).
7 S. Haber and W. S. Stornetta: J. Cryptol. **3** (1999) 99. https://doi.org/10.1007/bf00196791
8 A peer-to-peer electronic cash system: www.en.bitcoinr.cz/includes/img/bitcoin.pdf (accessed December 2018).
9 The Blockchain Report: Welcome to the Internet of Value: https://www.weusecoins.com/assets/pdf/library/The%20Blockchain%20Report%20-%20Needham%20(Huge%20report).pdf (accessed December 2018).
10 A next-generation smart contract and decentralized application platform: https://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf (accessed December 2018).
11 On Public and Private Blockchains: https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains (accessed December 2018).
12 R. Hummen, M. Henze, D. Catrein, and K. Wehrle: Proc. 2012, IEEE, 4th Int. Conf. Cloud Computing Technology and Science (IEEE, 2012) 232–240.
13 MQTT protocol specification: http://mqtt.org/documentation (accessed December 2018).
14 R. A. Atmoko, R. Riantini, and M. K. Hasin: J. Phys. Conf. Ser. **853** (2017) 12003. https://doi.org/10.1088/1742-6596/853/1/012003
15 Purely P2P crypto-currency with finite mini-blockchain: http://www.bitfreak.info/files/pp2p-ccmbc-revl.pdf (accessed December 2018).
16 G. Foroglou and A. L. Tsilidou: Proc. 2014. Student Conf. Managerial Science and Technology, https://www.researchgate.net/publication/276304843_Further_applications_of_the_blockchain (accessed December 2018).
17 N. B. Hounsell, B. P. Shrestha, J. Piao, and M. McDonald: IET Intell. Transp. Syst. **3** (2009) 419. https://doi.org/10.1049/iet-its.2009.0046.

18 R.S. Ayers, and D.W. Westcot: Water Quality for Agriculture (FAO Irrigation and Drainage, Rome, 1985) Paper 29 Rev 6-12.
19 Guidelines for municipal wastewater irrigation (Alberta Environment, Alberta, 2000) pp. 3–12.
20 Canadian Water Quality (Canadian Council of Ministers of the Environment, Ottawa, 2008) pp. 206–209.
21 Gravity: Analog TDS Sensor/Meter for Arduino: https://www.dfrobot.com/product-1662.html (accessed December 2018).
22 ESP32 Series Datasheet: https://www.espressif.com/sites/default/files/documentation/esp32_datasheet_en.pdf (accessed December 2018).
23 L. H. Aramyan, A. G. J. M. Oude Lansink, V. D. Vorst, G. A. J. Jack, and O. V. Kooten: SCM **12** (2007) 304. https://doi.org/10.1108/13598540710759826
24 F. Casino, T. K. Dasaklis, and C. Patsakis: Telemat. Inform. **36** (2019) 55. https://doi.org/10.1016/j.tele.2018.11.006

About the Authors

Nguyen Minh Son was born in 1988. In 2008, he received his diploma in Industry 3/7 specializing in industrial electricity from Dong Nai Technician School. In 2011, he obtained his engineer degree in information technology from Lac Hong University. Since 2011, he has been a lecturer at the Faculty of Information Technology, Lac Hong University, majoring in computer engineering. He received his Master's degree in information technology from Lac Hong University in 2016. His main research directions are the design of control systems, embedded systems, and mobile devices.
(sonm88@gmail.com, nmson@lhu.edu.vn)

Thanh-Lam Nguyen received his Ph.D. degree from National Kaohsiung University of Applied Sciences (KUAS, now NKUST), Taiwan, in 2014. He is currently the head of the Office of International Affairs, Lac Hong University. His research interests include quality management, fuzzy statistics, and business administration. He has several publications, as shown in ORCID at https://orcid.org/0000-0002-8268-9854 (green4rest.vn@gmail.com).

Phan Thi Huong received her diploma in Industry 3/7 specializing in information technology from Dong Nai Technician School in 2005. She received her B.S. degree from Lac Hong University, Vietnam, in 2011 and her M.S. degree from the same university in 2015. Since 2011, she has been a lecturer at the Faculty of Information Technology, Lac Hong University, majoring in computer engineering. Her research interests are mobile device programming, AI, blockchains, and embedded systems.
(phanhuong16@gmail.com, pthuong@lhu.edu.vn)

Lam Thanh Hien received his Ph.D. degree in 2015 from Vietnam Academy of Science and Technology, Vietnam. He is currently the vice rector of Lac Hong University. His research interests include robotics, data mining, machine learning, and image processing. (lthien@lhu.edu.vn)