IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received December 31, 2018, accepted January 25, 2019, date of publication February 12, 2019, date of current version February 27, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2897792

Food Safety Traceability System Based on Blockchain and EPCIS

QIJUN LIN, HUAIZHEN WANG, XIAOFU PEI, AND JUNYU WANG
State Key Laboratory of ASIC and System, Fudan University, Shanghai 201203, China

Corresponding author: Junyu Wang (junyuwang@fudan.edu.cn)

This work was supported by the National Key R&D Program of China under Grant 2017YFC1601800.

ABSTRACT In recent years, food safety issues have drawn growing concerns from society. In order to efficiently detect and prevent food safety problems and trace the accountability, building a reliable traceability system is indispensable. It is especially essential to accurately record, share, and trace the specific data within the whole food supply chain, including the process of production, processing, warehousing, transportation, and retail. The traditional traceability systems have issues, such as data invisibility, tampering, and sensitive information disclosure. The blockchain is a promising technology for the food safety traceability system because of the characteristics, such as the irreversible time vector, smart contract, and consensus algorithm. This paper proposes a food safety traceability system based on the blockchain and the EPC Information Services and develops a prototype system. The management architecture of on-chain & off-chain data is proposed as well, through which the traceability system can alleviate the data explosion issue of the blockchain for the Internet of Things. Furthermore, the enterprise-level smart contract is designed to prevent data tampering and sensitive information disclosure during information interaction among participants. The prototype system was implemented based on the Ethereum. According to the test results, the average time of information query response is around 2 ms, while the amount of on-chain data and query counts are 1 GB and 1000 times/s, respectively.

INDEX TERMS Food safety, traceability, blockchain, EPCIS, on-chain & off-chain, smart contract.

I. INTRODUCTION

In recent years, food safety issues have become more serious and keep threatening the public health. It is very important to track and trace the detailed event information within the whole food supply chain including food production, processing, warehousing, transportation, and retail. Establishing an accurate and effective food safety traceability system has become a key solution to the food safety issues.

The existing traceability systems adopt either of the two architectures: centralized architecture or distributed architecture. Centralized traceability system is managed and maintained by an authoritative third party. It may suffer the single node attack and has higher risk of data tampering and information disclosure. Distributed traceability system, such as the EPCIS-based distributed traceability system, can facilitate the creation and sharing of visibility event data concerning physical or digital objects both within and across enterprises [1]. The EPCIS specification defines four different events—ObjectEvent, AggregationEvent, QuantityEvent, TransactionEvent [2], which is good for the scalability of traceability system, but data tampering and information disclosure issues remain to be solved in the EPCIS-based system.

With the emergence and popularity of cryptocurrency, such as bitcoin, the brand-new decentralization architecture and distributed ledger technologies of blockchain have drawn attentions from various fields, including none-financial and IoT areas [3]–[6]. Traceability system based on the blockchain has gained much popularity because its decentralization and data tampering prevention might provide solutions to the shortcomings of conventional systems. However, the blockchain-based traceability system may also encounter some new technical difficulties like trust transfer, data explosion, etc.

The food safety traceability system implemented by the combination of blockchain and EPCIS can better solve the existing food safety problem, since it can guarantee the

The associate editor coordinating the review of this manuscript and approving it for publication was Jun Wu.

tamper-proof characteristic of sensitive information while ensuring the scalability of whole system. However, there is no report about practical implementation of traceability system based on blockchain technology and EPCIS in the literature, as far as we know. In this work, we identified the difficulties in establishing traceability systems with blockchain technology. Then, we proposed a collaborative food safety traceability system based on blockchain and EPCIS. This system adopted a novel enterprise-level smart contract to solve the issues of sensitive information disclosure, data tampering, and trust transfer. Within the blockchain, smart contract is the script residing on blockchain that minimizes the need for a trusted intermediary and the occurrence of malicious attacks [7]–[9]. Furthermore, the system adopts an innovative method to alleviate the data explosion problem on the blockchain using the dynamic management of on-chain & off-chain data.

The structure of this paper is as follows. Section II introduces the related works and identifies the main unsolved problems. Section III analyzes the user demand for the traceability system and introduces the system architecture. Section IV shows the system design process and the detail implementation. Section V gives test results of the prototype system. The last section concludes the paper and provides possible optimization direction for further system development.

II. RELATED WORKS

In the past few years, to combine blockchain technology with supply chain management has become a new trend. Blockchain technology has advantages such as decentralization and anti-tampering, and shows bright future to optimize the supply chain management. The current researches mainly work in two directions. One is to redesign the whole blockchain system from underlying architecture to meet the requirements of the application in supply chain management. The other is to make use of the existing mainstream blockchain architectures to optimize system security and solve some pain points of the supply chain management. In 2015, Shigeru Fujimura, Hiroki Watanabe, et al. developed a blockchain-based distributed permission management system in order to record the identities in the nodes of supply chains through blockchain and provide permission verification feature for the information interaction between different nodes [10]. In 2016, Feng Tian, et al. built an agricultural product supply chain traceability system based on blockchain and RFID technology. This system achieved automatic collection and storage of information through RFID systems and blockchain technology [11]. Kentaroh Toyoda P. Takis Mathiopoulos et al. created a blockchain smart contract model for supply chain management, using the Ethereum architecture. They also designed an item-level smart contract to manage the event information of product in the supply chain [12]. In the same year, IBM collaborated with Tsinghua University and Wal-Mart to develop a food supply chain management system based on IBM's Hyper-Ledger blockchain system to manage Wal-Mart pork supply chain information. A framework of blockchain with the set-up of high-authority verification node was designed to overcome some bottlenecks of the public blockchain: long time for uploading data on chain; the non-cancellability of information, etc. [13]. In 2017, Daniel Tse proposed the concept of applying blockchain technology to guarantee the information security of food supply chain, but it has not been implemented yet [14]. The AgriBlockIoT solution was proposed by Miguel in 2018, which integrated IoT and Blockchain technologies, implemented by both Ethereum and Hyperledger Sawtooth to realize a food traceability system. AgriBlockIoT could provide data transparency, fault tolerance, immutability and auditability for Agri-food traceability system [15].

In order to make a feasible solution for the traceability system based on blockchain, the main issues, including data explosion on the blockchain, trust transfer, and sensitive information disclosure, have to be solved.

A. TRUST TRANSFER

Trust transfer takes place when information interaction occurs between two none-adjacent transaction nodes in the supply chain. Trust transfer is a common problem confronted by current traceability systems, which can be explained by the illustrative four-node supply chain model shown in Fig.1.

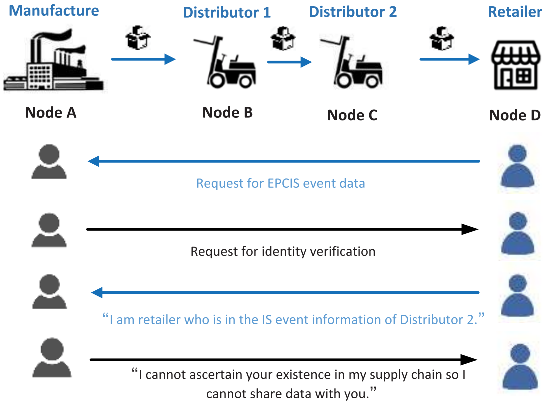

Manufacture
Distributor 1
Distributor 2
Retailer
Node A
Node B
Node C
Node D
Request for EPCIS event data
Request for identity verification
"I am retailer who is in the IS event information of Distributor 2."
"I cannot ascertain your existence in my supply chain so I cannot share data with you."

FIGURE 1. The trust transfer problem in a supply chain.

The four nodes (A, B, C, D) correspondingly represent: manufacturer A, distributor B, distributor C, retailer D. (A, B), (B, C) and (C, D) are direct-trust pairs (direct transaction happens within each direct-trust pair). However, data request will not always happen beyond the direct-trust pair levels. When node D initiates a request for EPCIS event data to node A, node A needs to confirm the authenticity of this requester for safety consideration. In fact, it is always a tough task to ensure this authenticity without direct ties between them. The trust relation is recorded in the EPCIS event data captured by node B and C. Due to the lack of direct trade tie between node A and C, node A cannot acquire requisite proof from node C. Likewise, node D is unable to obtain proof from node B. One solution to this problem is using interaction and iterative cooperation to determine the veracity of this indirect trade relation, which is a burdensome task for the whole system.

B. DATA EXPLOSION

Another issue of the blockchain-based traceability system is data explosion. Since each block of nodes of the blockchain stores the full data set, data explosion problem tends to happen on the blockchain when the traceability data grows eventually. Data explosion will increase the cost of the whole system, and reduce the performance of data query and data management, and thus hamper the application of blockchain in the traceability system to a great extent.

C. DISCLOSURE OF SENSITIVE BUSINESS INFORMATION

In the traceability system, some business information is sensitive and can only be accessed by trusted business partners, including identities and transaction details. The disclosure of sensitive business information might happen due to the transparent and traceable operation within a blockchain-based traceability system. Therefore, it is imperative to design a classification for the information to be uploaded on the blockchain so that the safety of sensitive information can be guaranteed.

However, most of the previous blockchain-based traceability systems have not been fully implemented or exploited. In this work, we combine the blockchain technology with EPCIS to design a smart contract module to solve those three problems, and a prototype system is developed.

III. REQUIREMENT ANALYSIS AND SYSTEM ARCHITECTURE

A. USER REQUIREMENTS

The participators in the food traceability system can be divided into three types: enterprise, consumer and government regulator. The demand for the system of each type of participators is defined as follows:

- **Enterprise:** The main needs of enterprises in the food supply chain are: 1) the specific accessibility of their data shared on the blockchain must be assured to prevent the leakage of sensitive information and to provide confidentiality. 2) the maintenance cost of blockchain system should be appropriately controlled. Only by satisfying the above needs will this system truly benefits enterprises.
- **Consumer:** For consumers, the most basic and essential requirement of the system is to provide traceability for the product they purchased. The characteristic of data according to the demand of consumer ought to be tamper-proof as well as confidential. Additionally, the system needs to be available for the public by the concise and low-cost design.
- **Government Regulator:** As for the demand of government regulators, we should provide highest accessibility to them to monitor all data on the traceability system in order that they can pinpoint the culpable sector as soon as possible once the food safety event occurs. Also, they should have capability to ensure that all data uploaded by the enterprise is legal and verified.

B. REQUIREMENTS FOR SYSTEM DESIGN

Based on the analysis of previous part, we made design spec for our food safety traceability system:

- Data on the blockchain should be as concise as possible.
- Data on the blockchain shouldn't include sensitive l information of the enterprises.
- System should provide mechanism to guarantee the quality and legitimacy of the data uploaded to the blockchain.
- System should be able to resist Spam Attack.
- System should guarantee the accessibility of sharing data among enterprises in specific supply chain and the inaccessibility of other enterprises.
- Data in the system must be tamper-proof.
- Cost of the whole system should be controlled at an appropriate level.

Moreover, we hope these items can become consensual goals for the future research in academia.

C. SYSTEM ARCHITECTURE

The proposed Food Safety Traceability System based on blockchain and EPCIS consists of enterprise-user server and consumer traceability client. The design of enterprise-user server is based on the architecture of EPCIS, which is mainly used for the acquisition and management of key traceability information of products. While consumers trace the information of the products they purchased mainly through the consumer traceability client. The overall system architecture is shown in Fig.2.

The enterprise-user server is composed of five modules. Detailed description of their features is as follows:

- **Traceability Information Capture Module:** This module is designed to collect key traceability information brought forth by the process of production, storage, circulation of food. It can work automatically and manually to identify and create detailed event information from the circulation of food in the supply chain.
- **Event Information Database:** This database is mainly used for the preservation and management of all food information from the capture module.
- **Information Extraction Module:** This module is primarily devised for extracting information that needs to be uploaded on blockchain from the traceability information database as well as preparing the data for the uploading.
- **Blockchain Module:** Blockchain module has two functions. One is the data interaction including the upload of key traceability information on blockchain, the request of on-chain information and the verification of event information. The other is to provide options for users to be the full blockchain node or the light-weight blockchain node i.e. to decide whether or not to participate in the maintenance of the blockchain.

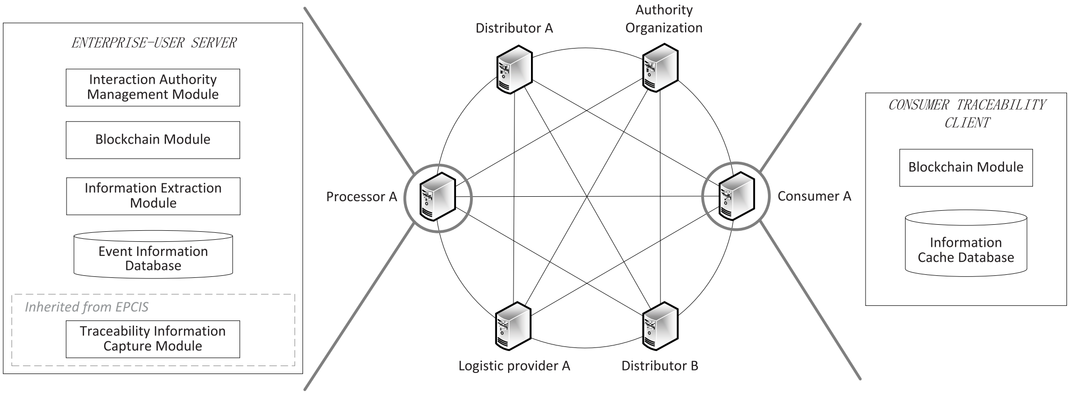

ENTERPRISE-USER SERVER
Interaction Authority Management Module
Blockchain Module
Information Extraction Module
Event Information Database
Inherited from EPCIS
Traceability Information Capture Module
Distributor A
Authority Organization
Processor A
Consumer A
Logistic provider A
Distributor B
CONSUMER TRACEABILITY CLIENT
Blockchain Module
Information Cache Database

FIGURE 2. The architecture of food traceability system based on Blockchain and EPCIS.

- **Interaction Authority Management Module:** This module is in charge of the verification of enterprise identity when there is any event information interaction i.e. to determine whether the requester who initiates the request for event information is in this supply chain.

The Consumer Traceability Client is composed of two modules:

- **Blockchain Module:** This module is designed for the link between the client and system, through which it can request information on the blockchain and verify the legitimacy of the information. A light node is chosen for this module to lower user's maintenance cost.
- **Information Cache Database:** This cache database is built to cache the corresponding food traceability data requested by users.

IV. SYSTEM DESIGN AND IMPLEMENTATION

A. COLLABORATIVE MANAGEMENT MODEL OF ON-CHAIN & OFF-CHAIN DATA

We use a novel data management model (as shown in Fig.3) which called the collaborative management model of on-chain & off-chain data to improve our system performance. The main feature of this model is to keep most of the information on food supply chain off the blockchain such as the local server or the cloud server. Besides, we use blockchain to store the proof information and some key traceability information so as to reduce the amount of on-chain data.

Most of the data interaction process takes place off the blockchain. The on-chain information is mainly used to provide support for the process e.g. enhancing the credibility of the information, providing information discovery services, etc. Through the application of this model, we can provide solutions to the concerns for privacy disclosure and data explosion:

- **Protection of Sensitive Businesses Information:** One key attribute of blockchain is the visibility for all members. Moreover, every full node maintains the same dataset, which is apparently unacceptable to enterprises. Therefore, our system designed an acquisition module for key traceability information. Specifically, we devised a mechanism to expose some event information of a product to the public while keeping the sensitive business information in tamper-proof need preserved and managed by the blockchain.
- **Alleviation of Blockchain Data Explosion:** Due to the irreversibility and immutability of the time vector of blockchain, data preserved by the blockchain keeps accumulating and expanding. Through our collaborative management model, we alleviate this problem by filtering out data which is of little demand for the consumer and keeping these data with local server or cloud server off the blockchain.

The detailed mechanism of this management model is described below:

1) OFF-CHAIN MODULE

We inherited the data preservation and management from EPC network. Six types of events are used by us to describe all supply chain actions including: 1) Object Event; 2) Transaction Event; 3) Aggregation Event; 4) Dissolution Event; 5) Transformation Event; 6) Transport Event. The function of each type of event is described in Table.1 below:

Each type of data is stored as a key-value pair where we use the EPC code of the food as the key of the event due to its uniqueness. In other words, users can get the corresponding event data through specific EPC code of the food.

2) ON-CHAIN MODULE

Our system uses smart contracts to manage the on-chain data of food in the supply chain. Traditional preservation and management of key traceability information require the appendix of traceability information to the transaction information of blockchain system. Under this circumstance, when a consumer issues the request for traceability information, the full node has to index level by level to return the message (i.e. tracing from the last trade to the previous upper-level transactions, during which complete traceability information will be acquired). However, when the supply chain is complex, this approach increases the cost of system response inadvertently.

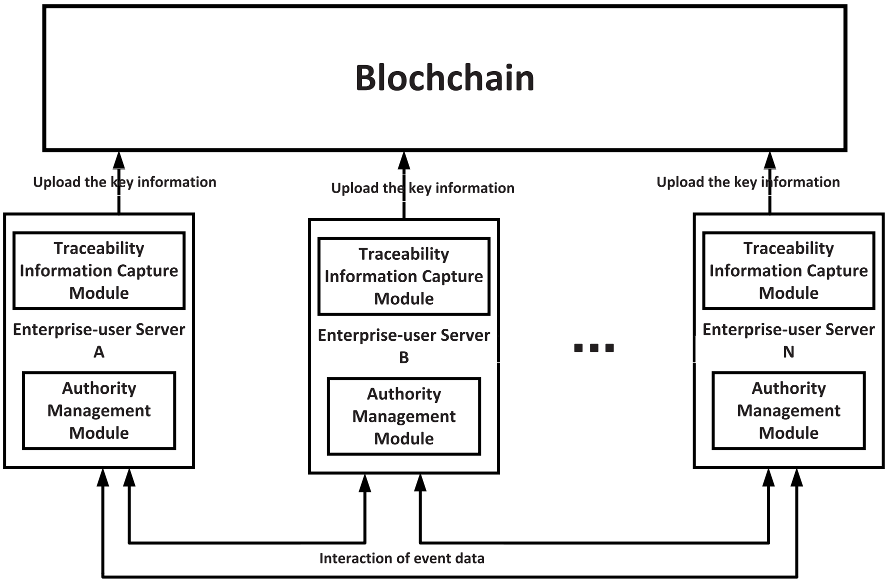

Blochchain
Upload the key information
Upload the key information
Upload the key information
Traceability Information Capture Module
Enterprise-user Server A
Authority Management Module
Traceability Information Capture Module
Enterprise-user Server B
Authority Management Module
...
Traceability Information Capture Module
Enterprise-user Server N
Authority Management Module
Interaction of event data

FIGURE 3. The diagram of collaborative management model of on-chain and off-chain data.

TABLE 1. Type of the event in the traceability system.

Name of the Event	Type of the Event	Function of the Event
ProduceEvent	Bson	Preserve and manage the event information in food producing
Object Event	Bson	Preserve and manage the information of the food
AggregationEvent	Bson	Preserve and manage the aggregate information generated by the package in transportation
Dissolution Event	Bson	Preserve and manage the dissolution information of the food
TransactionEvent	Bson	Preserve and manage the transaction event information
TransformEvent	Bson	Record relevant event information in food processing

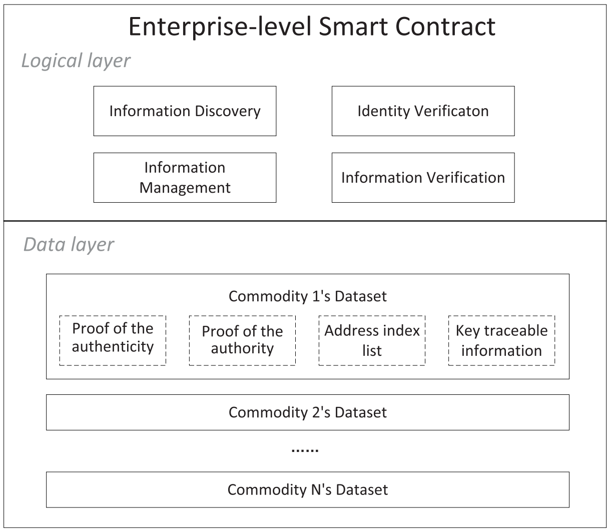


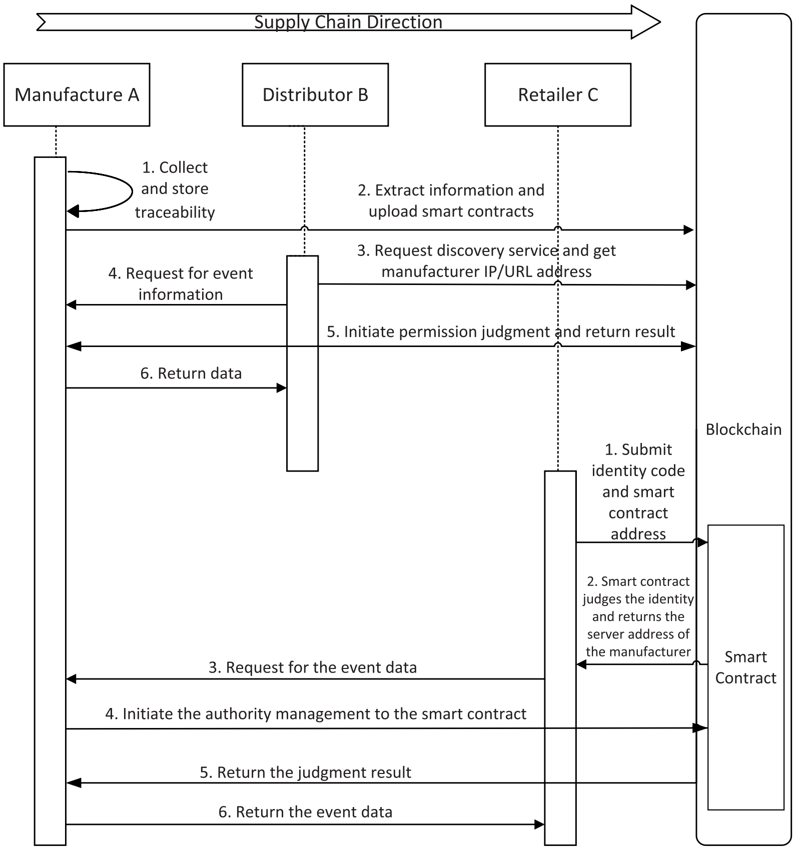
FIGURE 4. The structure of smart contract in the food traceability system.

While our system is built with smart contracts to store key traceability information of the food. First, our system will find corresponding smart contract for the food. Our system then traces the key traceability information of food in the data layer of the contract.

Additionally, Smart contract can implement any function because of its Turing completeness thus increase the degree of freedom of the system.

Through overall analysis, the structure of the smart contract is shown in Fig.4. The smart contract is comprised of two layers: logic layer and data layer. Following requirements need to be met through the logic layer of the smart contract:

- **Information Discovery:** In order to provide interaction ways for nodes in the same supply chain, smart contract needs to enable enterprise node to discover node address for the product in the supply chain.
- **Identity Verification:** To determine whether a node belongs to one supply chain, our design should be able to verify the identity of one node when it issues a data request to the smart contract.
- **Information Management:** Smart contracts need to save all information of food supply chain of an enterprise and return the non-confidential information to the consumer node.
- **Information Verification:** Smart contracts have to be capable of verifying whether the requested event information has been tampered.



Supply Chain Direction
Manufacture A
Distributor B
Retailer C
Blockchain
1. Collect and store traceability
2. Extract information and upload smart contracts
3. Request discovery service and get manufacturer IP/URL address
4. Request for event information
5. Initiate permission judgment and return result
6. Return data
1. Submit identity code and smart contract address
2. Smart contract judges the identity and returns the server address of the manufacturer
Smart Contract
3. Request for the event data
4. Initiate the authority management to the smart contract
5. Return the judgment result
6. Return the event data

FIGURE 5. **Process of uploading data to the blockchain.**

The data layer of smart contract includes four types of information: 1) proof of the authenticity of food in the supply chain (Hash value of certain event data of the food); 2) proof of the identity of the company in a certain supply chain of food (the enterprise's public key, corresponding address for public key e.g. Bitcoin System); 3) address index list (the IP/URL address of the data's location); 4) key traceability information.

B. DATAFLOW OF THE SYSTEM

The dataflow of the system includes the process of uploading data to the blockchain, the interaction of off-chain data and consumer query. These three processes are designed as follows:

1) UPLOADING DATA TO THE BLOCKCHAIN

Fig.5 shows how uploading data flows in a simple three-node supply chain. There is a complete process of uploading data to the blockchain explained as follows:

Step 1: food manufacturer A produces food and assigns unique identification e.g. EPC code to individual food or batches through RFID tags. The collection of event data of the food is accomplished by the data collection modules of the enterprise-user server of the manufacturer A. Then the manufacturer A uses Traceability Information Database or cloud to store the collected information;

Step 2: Manufacture A extracts key traceability information through Information Extraction Module and automatically generates transaction to A's smart contract through the Blockchain Module. When the transaction is accepted by the Peer-to-Peer (P2P) network and successfully uploaded to the blockchain, the manufacturer will transfer the goods;

Step 3: When the distributor B receives these products, it needs to verify the legitimacy of the goods by initiating a discovery service request to the corresponding manufacturer A's smart contract. Then the smart contract will determine the identity of the requester, i.e., whether it is the recipient of the product. The information will then be uploaded by the manufacturer A to the smart contract. If the distributor B passes the verification, the Blockchain Module will execute the resolution service and return the IP/URL of the manufacturer server;

Step 4: Distributor B requests for the sharing of the event information about the product from the manufacture;

Step 5: Manufacture A needs to determine whether Distributor B is in the supply chain of A by initiating a permission judgement service of corresponding smart contract's authentication function. If the judgement passes, smart contract will return the notification of pass;

Step 6: The manufacturer A's server returns requested event information to distributor B. The server of distributor B can initiate an information verification to the smart contract to check whether the returned information was tampered by means of comparing the hash value on chain and the generated hash value;

These six steps represent the dataflow of the uploading process in the supply chain.

2) INTERACTION OF OFF-CHAIN DATA

Fig.6 presents a three-node supply chain model, in which a detailed process of the event data interaction is demonstrated. The whole process can be divided into six steps:

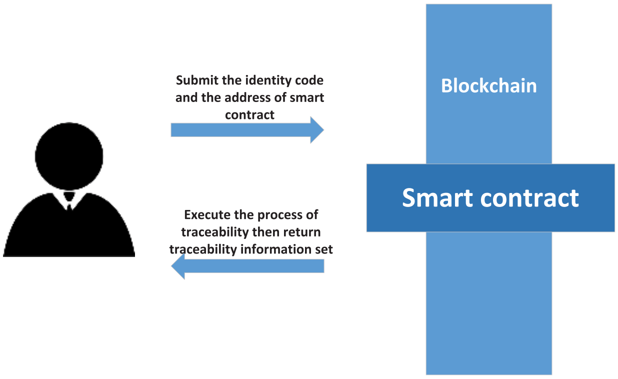

Submit the identity code and the address of smart contract
Execute the process of traceability then return traceability information set
Blockchain
Smart contract

FIGURE 6. Query process of consumer.

Step 1: After receiving the product, the retailer submits the identification code of the product and the address of smart contract to the blockchain to request for the Information Discover Service.

Step 2: Smart contract judges the identity of the requester to decide whether it is in the same supply chain with the manufacturer. Once affirmed, smart contract will return the server address of the manufacturer to the retailer.

Step 3: Retailer initiates the request for event data to the server of the manufacturer and submits its identification (including the public key and the digital signature created from its private key).

Step 4: The Interaction Authority Management Module of the manufacturer's server initiates authority verification request to the smart contract.

Step 5: Smart contract judges the authority of the retailer then returns the result.

Step 6: Based on the judgment of smart contract, the Interaction Authority Management Module verdicts whether to return the event data.

3) INTERACTION OF OFF-CHAIN DATA

As shown in Fig.6, when the consumer initiates the request for the query of purchased goods, the main process is as follows:

Step 1: The consumer initiates a request for query to the full node on the blockchain and provides the identity code of the product as well as the address of the manufacturer's smart contract;

Step 2: The full node on the blockchain responds to the query request and sends the identity code to the corresponding smart contract;

Step 3: Smart contract executes the process of traceability and returns the traceability information;

Step 4: The full node on the blockchain returns the corresponding information to complete the query process;

Furthermore, we have set super authority for government regulators so that they will have the right to access all information in the supply chain.

C. SYSTEM IMPLEMENTATION

The implementation of the five modules of enterprise-user server is the key to the whole system implementation. The details are as follows:

- **Traceability Information Capture Module:** the food information is captured in two ways: automatic collection through RFID and manual input. The Bson is applied as data interchange format of food event data, which can offer faster response and more convenient operation. The food identity code adopts the EPC coding standard. EPC coding standard defines representations of an EPC identifier and the structure of the URI syntax and binary format, as well as the encoding and decoding rules to allow conversion between these representations.
- **Event Information Database:** MongoDB is used to store and manage food event data due to its high writing speed and various query expressions. The JSON markup format of query instruction makes it easy to query the objects and arrays embedded in the documents. This database has three interfaces to realize three functions of retrieval, insert and deletion.
- **Information Extraction Module:** two methods are provided by this module:1) to traverse all event data generated within that period once an hour through an independent thread. The on-chain data in the event data is preserved by a list. 2) users can choose specific event data that to be extracted. The extracted information contains key traceability information and the hash value of event data. The key traceability information should not disclose any business sensitive information. In our system, the key traceability information includes basic data (food name, certificate number, expiry date, etc.), extending information and storage information.
- **Blockchain Module:** this module is the core part of the system. We chose the platform of Ethereum Geth 1.8.2 to set up the Blockchain. The smart contract is designed by the Solidity program language. The blockchain module consists of six submodules: 1) key traceability information upload, 2) key traceability information tracing, 3) food identity code resolution, 4) event information verification, 5) smart contract registration, 6) blockchain maintenance. The SHA-256 hash algorithm is used to encrypt event information in the event information verification submodule. The asymmetric cryptographic algorithm is used for identity verification in the smart contract registration submodule. Through these cryptography technologies, the system reliability and information authenticity can be further guaranteed.

- **Interaction Authority Management Module:** first, this module uses the public key of requester to verify the digital address signature. If passed, the public key would be generated as an address through hash algorithm. The module initiates authority request to corresponding smart contract and submits the encrypted address as well as the food identity code. The smart contract determines whether the address is in the address index list and returns True/False.

V. TEST RESULTS AND ANALYSIS

A. SYSTEM TEST

Six test machines form our blockchain network, of which four machines operate as the full node and two machines are light-weight nodes. The whole system is developed by Java on the Eclipse Luna platform of Windows 7. The detailed test environment is shown as the table 2 and table 3 below:

TABLE 2. Software environment.

Development Platform	Eclipse Luna
Operation System	Windows 7
Database	MongoDB 3.6
Blockchain Module	Ethereum Geth 1.8.2
Running Environment	JAVA 8.0.1610.12

TABLE 3. Hardware environment.

CPU	Intel(R) Core (TM)i3-4710
Hard Disk	SATA2 7200 120G
Memory	4G DDR3 REG ECC
CPU Cache	8MB
FSB	800MHz

The time of information upload and the time of information response are the main indices of system performance. The system test results of the above two items are shown in Fig.7-9.

Fig.7 shows that the time of information upload is affected by the frequency of upload request. As the frequency of the request of upload varies from 100 times per second to 900 times per second, the time of information upload sees an upsurge from about 7s to 47s. There is an obvious increase from the point at 600 to 700, where the upload time climbs from around 25s to 42s. The main cause of this circumstance may be the restriction of consensus algorithm of the blockchain, whose single block has limited processing amount of transactions.

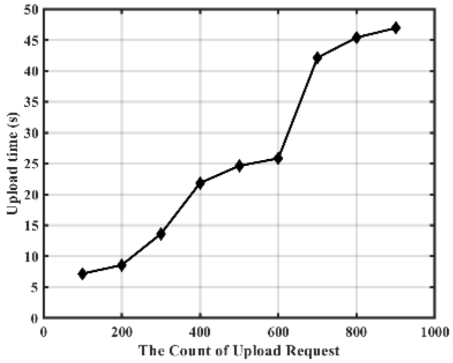


FIGURE 7. The relation between upload time and upload request.

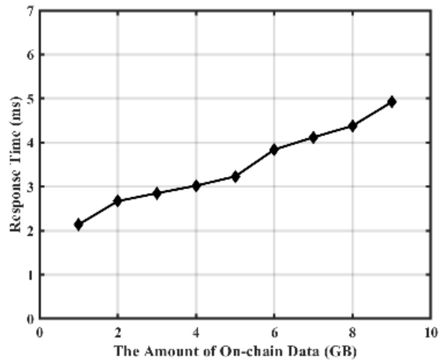


FIGURE 8. The relation between response time and on-chain data amount.

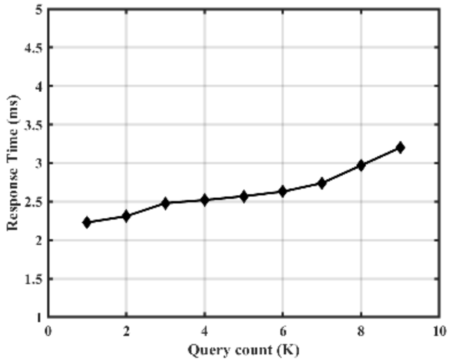


FIGURE 9. The relation between response time and query count.

Fig.8 and Fig.9 show that the time of information response is influenced by both the amount of on-chain data and the frequency of traceability request. Fig.8 demonstrates the time of information response growing from around 2ms to 5ms when the amount of on-chain data expands from 1G to 9G. Fig.9 indicates the time of information response rising slightly from around 2.2ms to 3.2ms with the traceability request increasing from 1,000 times per second to 9,000 times per second while the amount of on-chain data is set to 1G. The reason for the two correspondences is the mode of data query and P2P networking.

B. COMPARISON

After the analysis of test results, we conclude that our system has following advantages:

- **Higher Degree of Decentralization:** Our system is completely decentralized in that we removed the centralized server, which can avoid the monopoly and ameliorate the credibility of the system.

- **Stronger System Robustness:** Blockchain-based design and Collaborative Data Management Model of On-chain and Off-chain Data guarantee the tamper-proof and lost-prevention ability of the system.
- **Higher Security of Data Interaction:** Only companies belonging to the same supply chain can share event data with each other. In this way, sensitive business data will not be easily divulged.
- **High-reliability of Data Acquisition:** With our system, the decentralized data can still be tamper-proof with the blockchain technology.

TABLE 4. The comparison of performance of this work and current mainstream system.

Items	Centralized system	EPCIS-based system	Blockchain-based system	This work
Information Traceability	Yes	Yes	Yes	Yes
Tamper-proof Ability	Low	Low	High	High
Privacy Protection	No	No	Yes	Yes
Degree Of The Decentralization	No	Low	High	High
Amount of on-chain data	/	/	high	low

We compared the performance of our system with mainstream systems. The comparison results are displayed in Table 4 [16], from which we can safely drew the conclusion that our system demonstrates high-performance compared with the centralized traceability system, EPCIS-based system and blockchain-based system. All the systems can complete the basic function, information traceability. However, our system has better tamper-proof ability than centralized system and EPCIS-based system, since the EPCIS-based system uses electronic pedigree to prevent data tampering. Also, our system has advantages in privacy protection and high degree of decentralization. Compared with the ordinary based-blockchain system, this system alleviates the data explosion problem on the blockchain.

VI. CONCLUSIONS

This article first introduces the difficulties and challenges of current mainstream food traceability systems. Then through the thorough analysis of the major demands of system user, we designed a decentralized system based on the blockchain and EPCIS network. To alleviate the data explosion problem, we use collaborative management of on-chain and off-chain data to successfully reduce the amount of data of single node. To protect the sensitive business information, we use the enterprise-level smart contract instead of traditional transaction records to save and manage food data as well as verify the identity of enterprise. In this way, we can ensure the security of information and avoid spam attacks.

Through the comparison with current mainstream systems, we can safely draw the conclusion that our system can not only fulfill the basic requirements of the traceability system but also show superior performance in: 1) tamper-proof ability; 2) privacy protection; 3) decentralization degree; 4) the amount of on-chain data. Besides, due to the flexibility of our system, we can reduce the cost of the use of traceability system for small-scale and medium-scale food enterprises.

Here are also some future works to optimize the proposed food safety traceability system:

1) OPTIMIZATION OF P2P NETWORK MODE

After the analysis of our test results, we found that one of the crucial factors that limit our system performance is the amount of data. In this paper, we propose a fragmented blockchain network to solve this problem. Specifically, original overall P2P network is divided into several different regions. Different region stores food data of different categories. Some super nodes are able to communicate with different regions to manage the whole system. Thus, next step will be the implementation of the fragmentation mode.

2) OPTIMIZATION OF THE CONSENSUS ALGORITHM OF THE BLOCKCHAIN

The speed of data uploading to the blockchain is primarily restricted by the consensus algorithm. Therefore, we should optimize the consensus algorithm to improve the system throughput and accelerate the uploading process.

3) INFORMATION CLIPPING

For some special food that has a specific expiration date, information clipping function can be set up to reduce the amount of data. For instance, the information of an apple would have no sense after three or five years. The strategy and techniques of the data removal or transfer are still under research.

REFERENCES

[1] G. O. Young, "Synthetic structure of industrial plastics," in *Plastics*, vol. 3, 2nd ed., J. Peters, Ed. New York, NY, USA: McGraw-Hill, 1964, pp. 15–64.

[2] R. Wang, S. Prives, R. Fischer, M. Salfer, and W. A. Gunthner, "Data analysis and simulation of auto-ID enabled food supply chains based on EPCIS standard" in *Proc. IEEE Int. Conf. Autom. Logistics (ICAL)*, Aug. 2011, pp. 58–63.

[3] J. Wu, S. Luo, S. Wang, and H. Wang, "NLES: A novel lifetime extension scheme for safety-critical cyber-physical systems using SDN and NFV," *IEEE Internet Things J.*, to be published. doi: 10.1109/JIOT.2018.2870294.

[4] J. Wu, M. Dong, K. Ota, J. Li, and Z. Guan, "Big data analysis-based secure cluster management for optimized control plane in software-defined networks," *IEEE Trans. Netw. Service Manag.*, vol. 15, no. 1, pp. 27–38, Mar. 2018.

[5] Z. Guan, Y. Zhang, L. Wu, J. Wu, Y. Ma, and J. Hu, "APPA: An anonymous and privacy preserving data aggregation scheme for fog-enhanced IoT," *J. Netw. Comput. Appl.*, vol. 125, pp. 82–92, Jan. 2019.

[6] J. Wu, M. Dong, K. Ota, J. Li, and Z. Guan, "FCSS: Fog computing based content-aware filtering for security services in information centric social networks," *IEEE Trans. Emerg. Topics Comput.*, to be published. doi: 10.1109/TETC.2017.2747158.

[7] M. Swan, *Blockchain: Blueprint for a New Economy*. Newton, MA, USA: O'Reilly Media, 2015.

[8] S. Nakamoto. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[9] M. Iansiti and K. R. Lakhani, "The truth about blockchain," *Harvard Bus. Rev.*, vol. 95, no. 1, pp. 118–127, 2017.

[10] H. Watanabe, S. Fujimura, A. Nakadaira, T. Yamada, A. Akutsu, and J. J. Kishigami, "BRIGHT: A concept for a decentralized rights management system based on blockchain," in *Proc. IEEE 5th Int. Conf. Consum. Electron. (ICCE)*, Berlin, Germany, Sep. 2015, pp. 345–346.

[11] F. Tian, "An agri-food supply chain traceability system for China based on RFID & Blockchain technology," in *Proc. 13th Int. Conf. Service Syst. Service*, 2016, pp. 1–6.

[12] K. Toyoda, P. T. Mathiopoulos, I. Sasase, and T. Ohtsuki, "A novel blockchain-based product ownership management system (POMS) for anti-counterfeits in the post supply chain," *IEEE Access*, vol. 5, pp. 17465–17477, 2017.

[13] R. Aitken. (2017). *IBM & Walmart Launching Blockchain Food Safety Alliance in China with Fortune 500's JD.Com*. [Online]. Available: https://www.forbes.com/sites/rogeraitken/2017/12/14/ibm-walmart-launching-blockchain-food-safety-alliance-in-china-with-fortune-500s-jd-com/#556eb5fe7d9c

[14] D. Tse, B. Zhang, Y. Yang, C. Cheng, and H. Mu, "Blockchain application in food supply information security," in *Proc. IEEE IEEM*, Dec. 2017, pp. 1357–1361.

[15] M. P. Caro, M. S. Ali, M. Vecchio, and R. Giaffreda, "Blockchain-based traceability in agri-food supply chain management: A practical implementation," in *Proc. IoT Vertical Topical Summit Agriculture Tuscany (IOT Tuscany)*, May 2018, pp. 1–4.

[16] B. Sohn, S. Woo, J. Han, H. Cho, J. Byun, and D. Kim, "GS1 Connected car using EPCIS-ONS system," in *Proc. IEEE Int. Congr. Big Data*, Jun./Jul. 2016, pp. 426–429.

QIJUN LIN was born in Liaoning, China. He received the B.S. degree in microelectronics from the Hefei University of Technology, China, in 2016, and the M.S. degree from the School of Microelectronics, Fudan University, China, in 2018. He is currently a Researcher in blockchain. His main research interests include the blockchain architecture and multi-chain technology.

HUAIZHEN WANG was born in Sichuan, China. She received the B.S. degree in electronic information science and technology from Sichuan University, China, in 2018. She is currently pursuing the M.S. degree in microelectronics with the Auto-ID Lab, Fudan University, China. Her research interests include the area of the Internet of Things, especially Electronic Product Code Information Services and traceability systems, and the blockchain architecture and applications.

XIAOFU PEI was born in Yunnan, China. She is currently pursuing the B.S. degree with the School of Microelectronics, Fudan University, Shanghai, China. In 2017, she joined the Auto-ID Lab, Fudan University, as a Research Assistant. Her research interests include biomedical circuit and systems, mixed-signal system modeling, and the Internet of Things.

JUNYU WANG was born in Xiangtan, Hunan, China, in 1973. He received the Ph.D. degree from the University of Science and Technology, Beijing, in 2002.

From 2003 to 2005, he held a Postdoctoral position at Fudan University, where he is involved in the research on anti-counterfeit solutions based on the RFID technology. From 2008 to 2009, he was a Visiting Associate Professor with MIT, where he was involved in the research on the security issues and solutions of the Internet of Things. He is currently the Associate Director of the Auto-ID Lab and a Professor with Fudan University. His research interests include RFID reader and tag design, RFID anti-collision algorithm, RFID security, RFID sensor tag, blockchain, and the Internet of Things for food/drug safety.