IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received December 17, 2019, accepted December 22, 2019, date of publication December 25, 2019,
date of current version January 10, 2020.

Digital Object Identifier 10.1109/ACCESS.2019.2962274

Permissioned Blockchain-Based Double-Layer Framework for Product Traceability System

QINGYANG DING[1], SHENG GAO[1,2], JIANMING ZHU[1], AND CHONGXUAN YUAN[1]

[1]School of Information, Central University of Finance and Economics, Beijing 1008, China
[2]Grain Information Processing and Control, Key Laboratory of Ministry of Education, Henan University of Technology, Zhengzhou 450000, China

Corresponding author: Sheng Gao (sgao@cufe.edu.cn)

This work was supported in part by the National Key Research and Development Program of China under Grant 2017YFB1400700, in part by the National Natural Science Foundation of China under Grant 61602537 and Grant U1509214, in part by the Science and Technology Development Center of Ministry of Education under Grant 2019J02022, in part by the Central University of Finance and Economics Program of the Youth Talent Support Plan under Grant QYP1808, and in part by the Open Fund of Key Laboratory of Grain Information Processing and Control of Ministry of Education under Grant KFJJ-2018-202.

ABSTRACT Blockchain-based product traceability systems are receiving increasing attention from both industry and academia. Existing systems make full use of the traceability and non-modification characteristics of blockchain technology and realize the openness and transparency of product traceability information in the entire supply chain. However, existing systems do not consider government regulation, cannot protect enterprise sensitive private data effectively, and have performance bottlenecks. To address these problems, this paper proposes a product traceability scheme based on the permissioned blockchain within a double-layer framework. We introduce the double-layer framework and describe its advantages in detail. We also describe the smart contracts (chain code) in the double-layer framework. Finally, we test the performance of the proposed scheme through simulation experiments. The simulation results demonstrate the performance of nodes in the main layer, which is very important for consumers to obtain product traceability information, is optimized.

INDEX TERMS Product traceability, permissioned blockchain, double-layer framework, smart contracts, simulation experiment.

I. INTRODUCTION

Currently, blockchains are attracting increasing attention in various fields. Blockchain technology is used in various fields, such as renewable energy management [1], logistics management [2], IoT [3]–[6], and finance [7]. Product information traceability has also become an important application scenario for blockchain technology. More and more researchers and many companies are interested in realizing product traceability based on blockchain technology in the supply chain. Existing product traceability technology schemes based on blockchain technology make full use of the traceability and non-modification characteristics of blockchain technology and realize the openness and transparency of product traceability information in the entire supply chain [8], [9]. However, existing schemes that are based on a single-layer blockchain have weaknesses relative to scalability, privacy data protection, and performance [10]. In addition, existing blockchain-based product traceability systems are primarily developed for enterprises. It is difficult for government regulatory agencies to participate in these systems, even though involvement of government regulators in the product traceability process is of great significance [11], [12].

To address these problems, we propose a product traceability mechanism based on a permissioned blockchain within a double-layer framework. The proposed double-layer framework comprises a main layer and a sub-layer. In the main layer, the consortium blockchain is established. In the sub-layer, the private blockchain is deployed inside enterprise. The consortium blockchain is designed to share information among different organizations and provide an interface that allows consumers to access product traceability information. The private blockchain stores product information. The interfaces between the main layer and the sub-layer are hash pointers and application programming interfaces (APIs)

The main goal of this study is to improve blockchain-based product traceability systems rather than to develop

The associate editor coordinating the review of this manuscript and approving it for publication was Liang-Bi Chen.

a system that replaces government-based centralized record keeping systems. The primary contributions of this study are as follows.

First, we propose a double-layer framework for product traceability systems based on a permissioned blockchain. In the double-layer framework, data entry and data read functions are separated, which can improve the scalability and performance of a blockchain-based product traceability system.

Second, we describe the mechanism in the double-layer framework that allows regulatory agencies to participate in the system, how such participation is realized using smart contracts, and the data structure of consortium and private blockchains.

Third, we conduct a simulation experiment, test the performance of the proposed double-layer framework, and compare the proposed scheme to other product traceability schemes. The test results demonstrate that nodes in the main layer outperform nodes in the sub-layer, which is of crucial importance to improve the entire system's performance.

The remainder of this paper is organized as follows. Related work is reviewed in Section II. The double-layer framework for production traceability based on a permission blockchain is described in Section III. In this section, we also discuss the disadvantages of existing blockchain-based product traceability systems and the advantages of the double-layer framework. In Section IV, we describe smart contracts and explain how they are used in the double-layer framework. We also describe the block data structures of the main and sub-layers. A simulation experiment is described in Section V. In this section, we analyze node performance in the main layer and sub-layer. We also compare the proposed scheme to other blockchain-based product traceability schemes. Conclusions and suggestions for future work are presented in Section VI.

II. RELATED WORK

In recent years, realizing product traceability based on existing mainstream blockchain technology has attracted considerable attention. Previous studies can be categorized as studies investigating blockchain-based product traceability frameworks, case studies, and studies that examine the use of blockchain technology to realize the traceability various products, such as food products.

Messiry et al. proposed a complete blockchain-based framework for textile quality. They claimed that their proposed framework enabled near real-time performance, crosses chain information sharing with guaranteed authenticity and accuracy allowing quality defective batches to be identified in all systems as soon as they were detected in any system [13]. Si Chen et al. presented a framework in which a blockchain can be used to manage supply chain quality, and discussed how to improve supply chain management by adopting blockchain technology [14]. Petersen et al. developed a framework to evaluate the applicability of blockchain technology in supply chain management to improve traceability [15].

Reshma Kamath researched the case of Walmart, which was tackling food safety in the supply chain using blockchain technology. The case study highlighted the challenges of implementing blockchain solutions throughout the global food ecosystem to increase safety and reduce waste [16]. Frank Yiannas, Walmart's vice president of food safety, introduced the company's efforts to introduce traceability-based blockchain in the food supply chain. He referenced Walmart's proof of concepts for traceability of mangoes and pork, the company's foundation program, scaling trust in the food system, and the potential impact of the innovation [17]. Claudio Di Ciccio et al. investigated how to run a business process in the context of a supply chain on a blockchain infrastructure to provide full traceability of its runtime enactment. They showed the results of their investigation by means of an implemented software prototype, with a case study on the reportedly challenging context of a pharmaceutical supply chain [18].Xiwei Xu et al. shared a case of an origin chain and provided both qualitative and quantitative analyses of the software architecture of an origin chain [19].

Food is essential for human survival. Ensuring the safety, health, and sustainability of food production is one of the important government responsibilities. Realizing food traceability is conducive to food health and safety, sustainable food production, and reducing damage to the natural environment damage and natural resources waste. Therefore, development of food traceability based on blockchain technology has become a research hotspot. Qijun L et al proposed a food safety traceability system based on a blockchain and EPC information services. They also developed a prototype based on their proposed system [20]. Tharun Mohan investigated how blockchain technology can be used to provide greater asset traceability in today's food supply chain. Mohan created a blockchain model that could be implemented across food supply chains and described the benefits and limitations of his implementation [21]. Bettín-Díaz R et al. presented a method to integrate blockchain technology in the food industry supply chain to allow traceability along the process and provide the ultimate customer with sufficient information about the origin of the product to make an informed purchase decision. The authors pointed out that this methodology was suitable for any product, supply chain, and required system configurations due to its versatility and adaptability [22]. Feng Tian presented an agri-food supply chain traceability system based on RFID and blockchain technologies to prevent manipulation of the traceability system and prevent label replication. The concept of BigchainDB was introduced to solve the problem of insufficient scalability when a real-world blockchain needs to store large amounts of data [23], [24]. To solve the supply chain trust crisis, Jing H et al. proposed an agricultural provenance system based on blockchain techniques that considered numerous stakeholders. They thought that applying a blockchain to track the provenance of agricultural products not only widened the application domain but also supported

building a reliable community among different stakeholders associated with agriculture production [25]. Miguel Pincheira Caro et al. presented AgriBlockIoT, a fully decentralized, blockchain-based traceability solution for agri-food supply chain management. Their solution can seamlessly integrate IoT devices that produce and consume digital data along the chain [26].

In addition to these studies, researchers were investigated methods to trace specific products, e.g., soybeans [27], cacao and chocolate [28], integrated circuits [29], textiles and clothing [30], and dangerous goods [31], using blockchain technology.

Among these previous studies, methods to apply blockchain technology to realize the traceability of information of different products have received the most attention. However, few researchers considered the importance of government regulatory agencies in the product traceability mechanism, how to provide maximum protection for private enterprise data, or how to improve the performance of a production traceability system based on permissioned blockchain.

III. DOUBLE-LAYER FRAMEWORK

In existing consortium blockchain-based product traceability systems, the nodes are all enterprises, such as production, logistics, and sales enterprises. The consortium blockchain is dominated by enterprises that have an information technology advantage or play an important role in production supply chain traceability, such as Walmart and Jingdong's product traceability projects. These existing blockchain-based product traceability systems are established on the basis of close cooperation and mutual trust between enterprises, which participating enterprises to share information with other enterprises in the supply chain, break the ''information isolated island,'' and realize product information traceability. However, such approaches also have many disadvantages.

A. DISADVANTAGES OF EXISTING BLOCKCHAIN-BASED PRODUCT TRACEABILITY SYSTEMS

The disadvantages of existing blockchain-based product traceability systems are as follows.

1) LACK GOVERNMENT REGULATORTY AGENT PARTICIPATION IN BLOCKCHAIN-BASED PRODUCT TRACEABILITY SYSTEMS

Government involvement in product traceability is of great significance and necessary. First, government regulatory authorities' participation in blockchain-based product traceability processes can effectively compensate for deficiencies in government oversight activities, reduce regulatory loopholes, and realize information sharing among the different regulatory agencies. Second, government regulatory agencies that participate in blockchain-based production traceability systems can enrich traceable production information. Third, such participation can improve the reliability and credibility of product traceability information. Introducing government regulatory agencies into product traceability projects can effectively reduce corporate collusion and improve the reliability of product traceability information.

2) EXISTING BLOCKCHAIN-BASED PRODUCT TRACEABILITY SCHEMES DO NOT PROTECT PRIVATE ENTERPRISE DATA EFFECTIVELY

In existing blockchain-based product information traceability schemes, enterprises upload all production, transportation, sales, and other product information to the consortium blockchain. Such information is required to realize product traceability. However, this will result in information leakage and transparency in the consortium blockchain. Sensitive company data can also be leaked. If sensitive private data is leaked to competitors, it will have a huge negative impact on the operation of the enterprise. In existing product information traceability schemes based on blockchain technology, participants sign confidentiality agreement to protect enterprise privacy; however, such agreements are not particularly effective. Fundamentally, preventing leakage of private enterprise data is difficult.

3) PERFORMANCE BOTTLENECKS

There are performance bottlenecks in existing blockchain-based product traceability schemes. The consortium blockchain outperform the public blockchain on several metrics, such as reduced delay time and improved throughput. However, in a product traceability system, data read and storage operations are carried out on the same blockchain, which reduces performance significantly. For example, the theoretical transaction throughput of FastFabric, a permissioned blockchain system, is 20000 transactions per second (TPS) [32]; however, its actual transaction throughput is much less than 20000 TPS due to hardware constraints, network speed, data block capacity, and the transaction process.

B. DOUBLE-LAYER FRAMEWORK

To address the disadvantages of existing blockchain-based product traceability systems, this paper proposes a double-layer framework system. The framework comprises a main layer and a sub-layer (Figure 1). The main layer consists of a consortium blockchain, and the sub-layer consists of several private blockchains. Enterprise private blockchain is used to enable more enterprise departments to participate in the system of product traceability and enable the information temper resistance. Enterprises and government regulatory agencies participate in the consortium blockchain, and the private blockchains are built by enterprises.

In the double-layer framework, the main and sub-layers are not independent. As shown in Figure 1, the key node of the enterprise maintains two blockchains, i.e., the consortium blockchain in the main layer and the private blockchain in the sub-layer, which means that the key nodes in the private blockchain are in the sub-layer as well as the main layer. Key nodes in the enterprise private blockchain are responsible for interaction between the main and sub-layers. Interactions

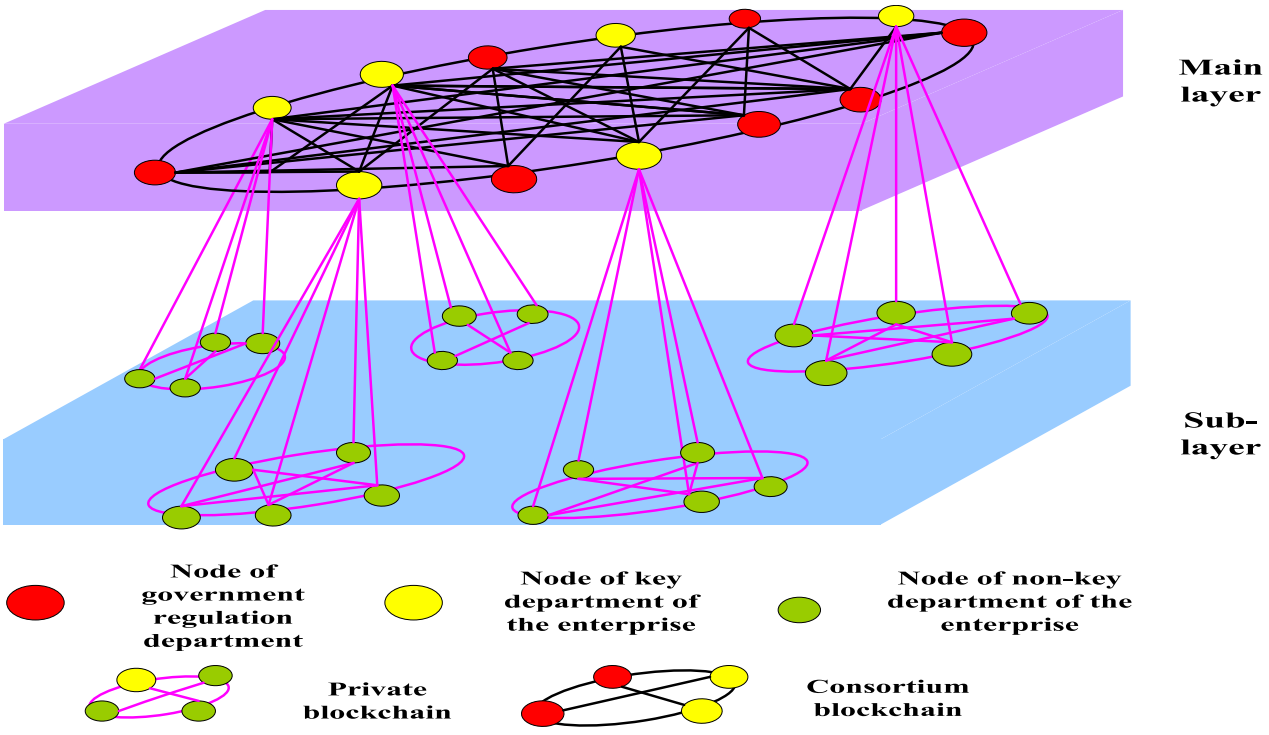

FIGURE 1. Schematic diagram of double-layer framework.

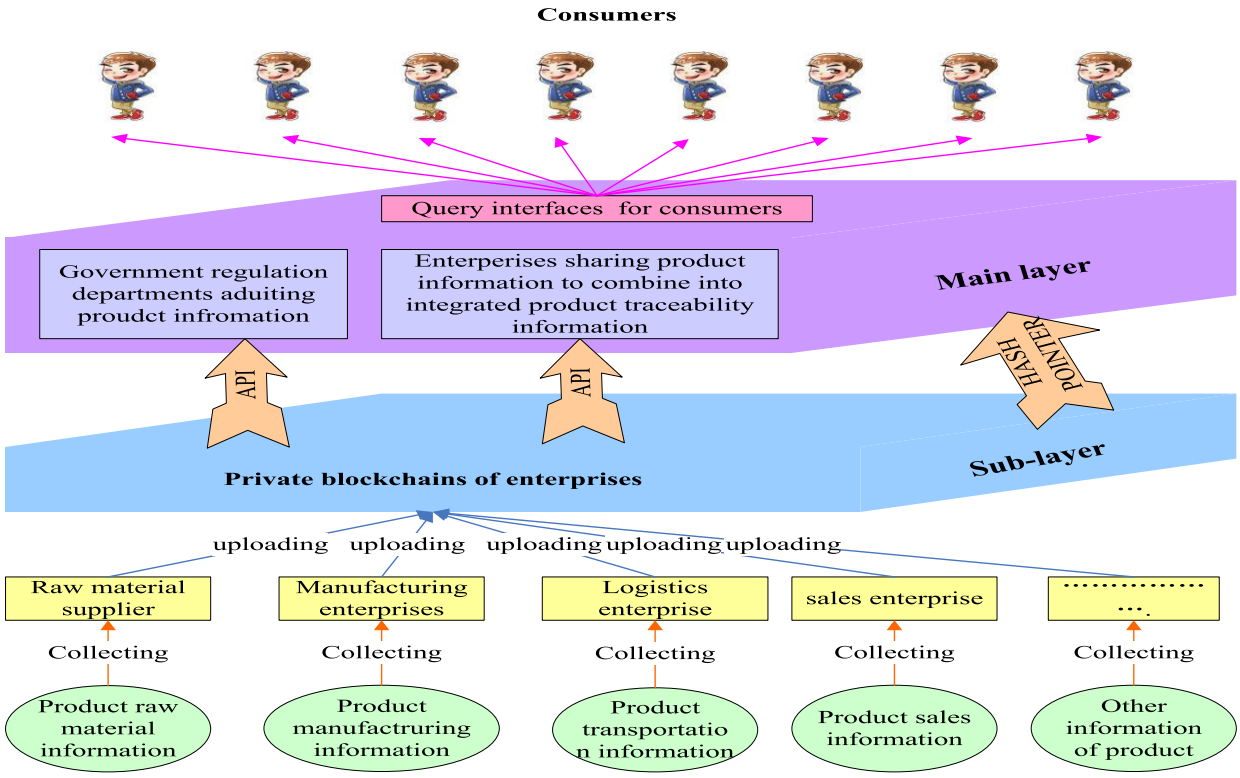

FIGURE 2. Product traceability system mechanism in double-layer framework.

between main and sub-layers occur via hash pointers and APIs. The hash pointer is provided to other nodes in the consortium blockchain to prove that the private enterprise blockchain has not been tampered with and indicate where data is stored. The API transmits detailed product traceability information to other nodes in the consortium blockchain.

When a consumer requests product traceability information, a key node in the main layer of the consortium blockchain can obtain product traceability information owned by a specific enterprise through an API and send it to the consumer.

A P2P networking mechanism is used in the consortium blockchain and a star network transmission mechanism is used in the private blockchain.

As shown in Fig. 2, the stakeholders involved in the product traceability system primarily include national regulatory agencies, consumers, and enterprises. According to their functions, national regulatory agencies can be divided into industrial and commercial administrative agencies, health and quarantine institutions, tax collection and inspection agencies, customs exit and entry management agencies, quality supervision, and management institutions, etc. Consumers are people who ultimately purchase goods and have traceability requirements for product information. Enterprises can be divided into production enterprises, logistics enterprises, and sales enterprises according to their position in the circulation of products. Enterprises in different links of a product supply chain have different functional departments involved in product traceability. Take product manufacturing enterprises as an example. The departments involved in product the traceability mechanism include the raw material purchasing, production, sales, transportation, information, and quality inspection departments. In the double-layer framework, different stakeholders are distributed in different layers. Government regulators and consumers are distributed in the main layer. Different departments of different enterprises are distributed in different layers, and enterprises are required to set up private blockchain according to their own actual conditions. The key departments of enterprises involved in the product traceability process function in the main layer and sub-layer simultaneously and are responsible for the data connection between private blockchains in the sub-layer and the consortium blockchain in the main layer.

In the double-layer framework, the functions of the main layer and sub-layers are different. The main layer is responsible for providing consumers with the query data port of product traceability information, and the government regulatory department can realize the supervision of products in the entire supply chain. Different supply chain enterprises can realize sharing of production information and strengthen overall coordination through the main layer. An enterprise private blockchain is responsible for storing raw materials, production, logistics, sales, and other product information, and can provide basic information for the entire product traceability information system.

In the product traceability system based on a double-layer framework permissioned blockchain, the key department node of the enterprise generates a hash pointer of the enterprise's private blockchain, and then sends it to the key department nodes of other enterprises and government regulatory departments to prove the enterprise's data has not been tampered with and identify the storage path of product traceability information. The APIs provided by key department nodes of enterprises are used to transmit the detailed product traceability information stored in private blockchains. When consumers request product traceability, the key node of the consortium blockchain determines whether the requests are valid. Criteria are used for key node of consortium blockchain to judge whether a consumer request is legitimate include whether the product traceability information requested by the consumer is included in the product traceability information system, and whether the frequency of consumer information query request is too high, etc. If the requests are considered valid, the key node of the consortium blockchain finds the corresponding data according to the hash pointer provided by the key department node of the enterprise's private blockchain, and then obtains the detailed product traceability information through the API. When the key node of the consortium blockchain obtains detailed product traceability information through the API, the data require of the key node of consortium blockchainis should be allowed by the key department node of the enterprise's private blockchain. The product traceability mechanism is illustrated in Fig. 3.

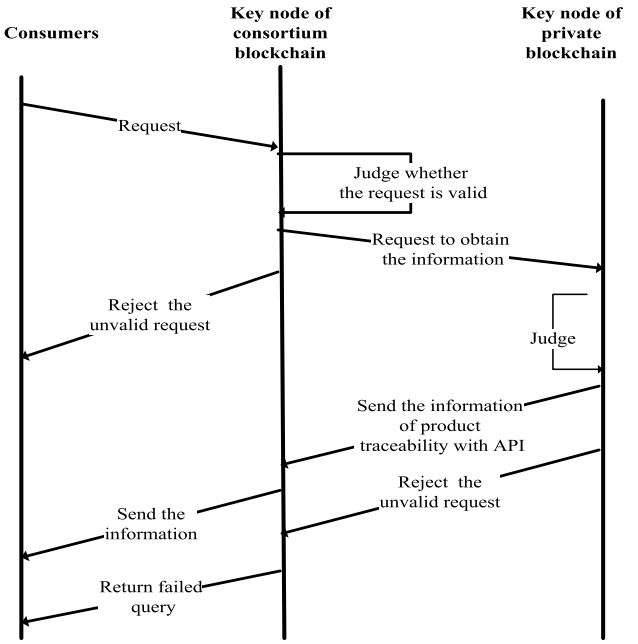

FIGURE 3. Product traceability information query mechanism in double-layer framework.

C. BENEFITS OF THE DOUBLE LAYER

The benefits of the double layer are as follows.

First, government regulatory departments can be involved in the product traceability process, which is conducive to both government regulation and the product traceability information credibility. In practice, it is difficult for government departments to obtain all product traceability information of enterprises, and even if government departments can obtain all product traceability information of enterprises, they also need to pay huge maintenance cost of information system, which undoubtedly greatly increases the public expenditure

of government departments. The double-layer framework allows government regulation departments to enter a product traceability system and make government regulation departments have a regulation function for the entire product supply chain, and reduces regulatory costs for government agencies.

Second, enterprises can effectively protect their sensitive privacy data. In the double-layer framework, the enterprise's product data are stored in the enterprise's private blockchain, and the key department of the company involved in the product traceability process is permitted to determine whether a request for product traceability information is harmful to enterprise privacy data protection, which can help formulate effective data sharing strategies to best protect the enterprise's privacy data based on the premise of product information traceability.

Third, the double-layer framework can effectively improve the performance of a blockchain-based product traceability system. In fact, data entry and storage operations will occupy a large amount of blockchain system resources and reduce the operating efficiency of the entire system. In the double-layer, the data entry and storage operations are completed in the sub-layer, and the query service of product traceability information is provided by the main layer. This means that operations with long delay time and high computing costs are completed by the enterprise in the sub-layer, and operations with short delay and low computing costs are completed in the main layer. This improves the performance of the consortium blockchain in the main layer. Once the enterprise completes data logging and storage in the sub-layer, consumers and government regulators can quickly query and audit product information in the main layer. Practically, the most important goal of a product traceability system is allowing consumers to quickly obtain accurate and comprehensive product traceability information. Applying the double-layer framework can realize this goal effectively, increases consumer utility, and improves the performance of blockchain-based product traceability systems.

Fourth, the double layer has better scalability. In the double-layer framework, besides government regulation departments, other third-party product quality inspection agencies can easily enter the product traceability system. Here they only need to enter the main layer and can share product information with other organizations. In addition, when other enterprises want to take part in a product traceability alliance, they do not need to upload all product information to the consortium blockchain; they only to build their private blockchains. This makes it easy to add more participating nodes. In fact, the product traceability system based on a permissioned blockchain can include many products because an enterprise can produce many different products, and enterprises that produce different types of products can also participate.

Five, compared to government-controlled centralized product traceability system, our scheme can be information tamper resistance and better for privacy data protection. Although, the government regulatory departments usually are trusted, the information of product traceability may be tampered and the privacy data of enterprise may be leaked, when the government regulatory department colludes with bad competitors. In product traceability system based on permissioned blockchain, the product traceability information is stored inside enterprises and the traceability information is consensual and shared in consortium blockchain, which is better for improve the information tamper resistance and privacy data protection.

D. COMPARISON BETWEEN PROPOSED DOUBLE-LAYER AND OTHER FRAMEWORKS

Although double-layer or multi-layer frameworks are used in the IoT system based on blockchain [33]–[35], the proposed double-layer framework differs from other multi-layer frameworks.

First, the proposed double-layer framework contains multiple blockchains, i.e., several private blockchains and one consortium blockchain. Private blockchains are used for data storage, and consortium blockchains are used for data sharing.

Second, the key node of the private blockchain maintains two blockchains, i.e., the enterprise's private blockchain and the product traceability alliance's consortium blockchain.

Third, the network of the enterprise's private blockchain is decentralized, and the status of each node in the enterprise is considered equal.

Fourth, the consortium blockchain in the main layer has good scalability. When the outside enterprises want to take part in the system, they only need get into the main layer of system, and it is not necessary to get the detailed information of enterprises which are in system and to store all the detailed product traceability information in the consortium blockchain. It makes outside enterprises easy to enter the system.

Simultaneously, the double-layer framework is similar to other multi-layer architectures, i.e., all such systems can effectively improve the entire system's performance.

IV. SMART CONTRACTS IN DOUBLE-LAYER FRAMEWORK

Here, we describe how to involve government regulatory departments in the product traceability system using smart contracts and how to update product traceability information to the enterprise private blockchain using smart contracts. In addition, we describe the information connection between private and consortium blockchains. The enterprise private blockchains supply the data basis for the entire product traceability system; thus, we first introduce the smart contract in the enterprise private blockchain. Relevant preliminary information is described in the following.

A. ROLE OF PARTICIPANTS AND SYMBOL DESCRIPTION

In the private blockchain, the enterprise selects a department as the key node of the private chain according to its actual situation, and the department selected as the key node can be an existing department of the enterprise (e.g., the production

TABLE 1. The role setting in the double-layer.

Role	The way of Selection	Responsibility
Key node of private blockchain	Selected by enterprises	Planning, building, and maintaining private blockchain, collecting transaction data, building data blocks, reviewing product information in private blockchain, and connecting private blockchain of company and consortium blockchain
Non-key node of private blockchain	Participation departments of enterprise, which aren't selected as key node	Inputting product information into the traceability system and verifying product information collected by key nodes.
Key node of consortium blockchain	Elected from all key nodes of private blockchains by companies taking part in product traceability alliance	Building data blocks, converging all APIs supplied by the key nodes of private blockchain, supplying interface for consumers and other participating members
Non key node of consortium blockchain	Key nodes of private blockchains ,which aren't elected as key node of consortium blockchain	Uploading product information of the enterprise, hash pointer of the private blockchain and other data needed by the regulatory authorities in the audit process
Nodes of government regulator	Government regulation departments	Reviewing and verifying the product information uploaded by enterprises.

TABLE 2. Notations and definition in smart contracts.

Notation	Definition
E_i	Different enterprises involved in the traceability blockchain.
R_i	Government regulatory department
S_n	The different departments of the enterprises involved in the traceability blockchain.
N	The number of enterprise departments
E_{S_n}	The different department of certain enterprise
$E^i_{S_n}$	Different department of enterprises
P_{E_i}	Private blockchain of different enterprise
$key\ node$	Key department node of the private blockchain.
$keynode_A$	Key department node of consortium blockchain
$non\text{-}key\ node$	Non-key node of the private blockchain
$non-key\ node_A$	Non-key department node of consortium blockchain
$node_A$	The node in consortium blockchain
D_m	The different product
E^i_{Dm}	The different product of different company
$D_m \rightarrow F_{E_i}$	The different product information of different company
$D_m \rightarrow F_{E_i} \rightarrow Appr_{R_i}$	The product compliance file or data required by government regulation departments of different enterprises' different products
$Appr_{R_i} \rightarrow F_{E_i}$	Different approval information of different law enforcement for different production information
$T_{P_{E_i}}$	The building time of last block of the private blockchain
T_A	The time of government node auditing
$Sig^p_{E_i}$	The digital signature of private blockchian key node, which is used in private blockchain
Sig_{E_i}	The digital signature of private blockchian key node, which is used in consortium blockchain.
$Sig^A_{E_i}$	The digital signature of consortium blockchian key node, which is used in private blockchain
Sig_{R_i}	The digital signature of different government regulation department
$Sig_{E^i_{S_n}}$	The digital signature of different departments of different enterprise
h	The hash value calculated by the hash algorithm
$Hash\ pointer$	Supplied by the key department node of enterprise private blockchain

or sales department) or a new department. The key node responsibilities include planning, building, and maintaining private blockchain, collecting transaction data, building data blocks, reviewing the product information in the private blockchain, and connecting the company's private blockchainto the consortium's blockchain. Other departments involved in the product traceability system are non-key nodes, which are also verification nodes. These nodes are responsible for inputting product information to the traceability system and verifying the product information collected by key nodes.

In the consortium blockchain, the government regulatory department is the verification node, which is responsible for reviewing and verifying product information uploaded by enterprises. The product information upload operation is performed by the enterprise's key node, which includes the hash pointer of the private blockchain and other data required regulatory authorities in the audit process, such as the production qualification, the enterprise's product approval number, etc. In the consortium blockchain, enterprises participating in the product traceability alliance elect one of the enterprise's key nodes as the key node of the consortium blockchain. After the government regulation department audits the product information, the data block is constructed by the consortium blockchain's key node. Other key nodes of the private blockchains, which are not elected as the consortium blockchain's key node, verify the block, and when verification reaches consensus, the key node of the consortium blockchain updates the consortium blockchain. Simultaneously, the consortium blockchain's key node collects all APIs supplied by the key nodes of the private blockchain to create an integrated interface for consumers and other participating members, including companies in the product traceability alliance and government regulation departments. Table 1 shows the role settings in the proposed double-layer framework.

Although we set a key node role in the double-layer framework, these key nodes are not Byzantine nodes, and they

play an important role in the product information traceability system based on permissioned blockchain, which is critical to realizing product traceability with trusted product information that can be obtained easily by consumers.

The notations used in the following are defined in Table 2.

B. SMART CONTRACT AND BLOCK DATA STRUCTURE IN PRIVATE BLOCKCHAIN

Operations performed with smart contracts in private blockchains include the key node of the private blockchain auditing the product traceability information supplied by the non-key nodes of the private blockchain, non-key nodes verifying the auditing result of the key node, the key node of private blockchain building the private blockchain's block and sending the hash pointer of the private blockchain to other consortium blockchain nodes, and supplying the product compliance file or data required by government regulation departments to the nodes of government regulation departments. Figure 4 shows a logical diagram of the smart contract in the private blockchain.

The function of part I(Fig. 4) of the smart contract, i.e., Algorithm1, in the private blockchain is that the key node of the private blockchain obtains and audits the integrity and veracity of the information submitted by non-key nodes of the private blockchain, and then returns the result of auditing to the non-key nodes of the private blockchain. The function of part II (Fig. 4) of the smart contract, i.e., Algorithm2, in the private blockchain is that non-key nodes of the private blockchain verify the auditing result sent by the key node of the private blockchain. The function of part III (Fig. 4) of the smart contract, i.e., Algorithm3, in the private blockchain is that the key node of the private blockchain obtains the verifying result sent by the non-key nodes of the private blockchain, builds the block of the private blockchain, uploads the block to the private blockchain, sends the hash pointer and compliance file or data to the nodes of government regulatory departments, and sends the hash pointer and hash value to the key node of the consortium blockchain and other nodes of the consortium blockchain.

In the enterprise private blockchain, the key node of the enterprise builds the data blocks of the blockchain. The data block of the private blockchain can be calculated according to the smart contract. The data block of the private blockchain comprises a block header and body.

The block header primarily encapsulates the current block hash value, the pre-block head hash value, and the department hash value of the enterprise department and version number, the Merkle root, and a timestamp. The hash value of the current block is a function value calculated by current block, which is verified by the key node and other nodes using the Hash256 encrypt algorithm. The pre-block head hash value is the hash value of the parent block. The department hash value of department of enterprise is the hash value of the relevant department involved in the specific production or circulation. The version number is for the entire blockchain system, and the Merkel root is obtained by Merkel calculation of the data

Algorithm 1 Key Node Audits Data

Import: $D_i \rightarrow F_{E_i}$ []
Output: Result of auditing []
function data auditing(i)
  for i in S_n[]:
    for i in D_m[]:
      check ($D_m \rightarrow F_{E_i}$)
      check ($Sig_{E^i_{S_n}}$)
    end for
    if $check(D_m \rightarrow F_{E_i})$ = True
      $check(Sig_{E^i_{S_n}})$ = True
    then append(*Result of auditing []*)
  end if
 end for
 send *Result of auditing []* to E_{S_i}
end function

Algorithm 2 Non-Key Node Verifies Auditing Result

Import: Result of auditing []
Output: Result of verifying []
function result verifying (i)
  check (*Result of auditing []*)
  check ($Sig^p_{E_i}$)
  if *check* (*Result of auditing []*) = True
    check ($Sig^p_{E_i}$) = True
    then append(*Result of verifying []*)
  end if
    send *Result of verifying[]* to the *key node*
end function

in the block. The timestamp is set by the key node after verification by the verified node.

The block body packages production traceability information, which is similar to transactions in a bitcoin data block, and digital signatures. In the product supply chain, the specific product information in the body of a data block in the private blockchain of different enterprises differs. For example, the data block of the production enterprise primarily includes product name, product category, product serial number, production date, production process, production machine number, production line number, product buyer, etc. Here, the digital signature is the signature of all participating departments in the product traceability process. By setting the digital signature, denial behavior between the internal departments of the enterprise can be prevented. Figure 5 shows an example block data structure of a private blockchain of a producing enterprise.

C. SMART CONTRACT AND BLOCK DATA STRUCTURE IN CONSORTIUM BLOCKCHAIN

The operations performed with smart contracts in consortium blockchains include government regulatory department auditing compliance information supplied by an enterprise, non-key nodes of the consortium blockchain collecting and

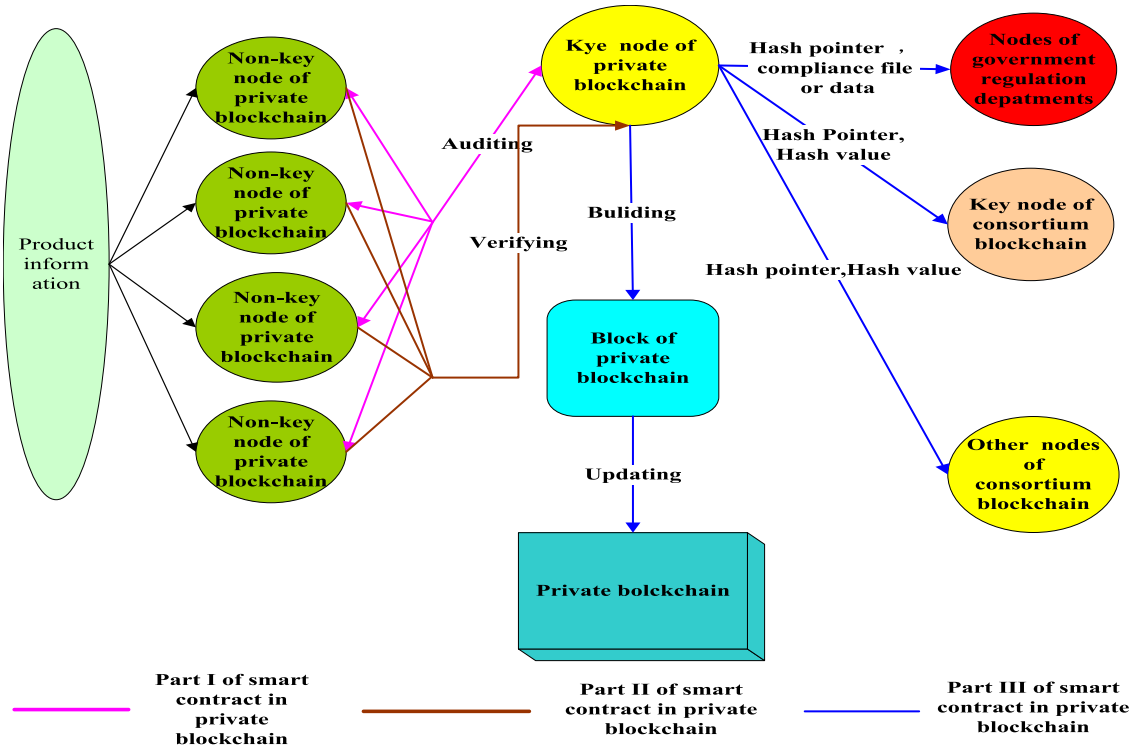

FIGURE 4. Logical diagram of smart contract in private blockchain.

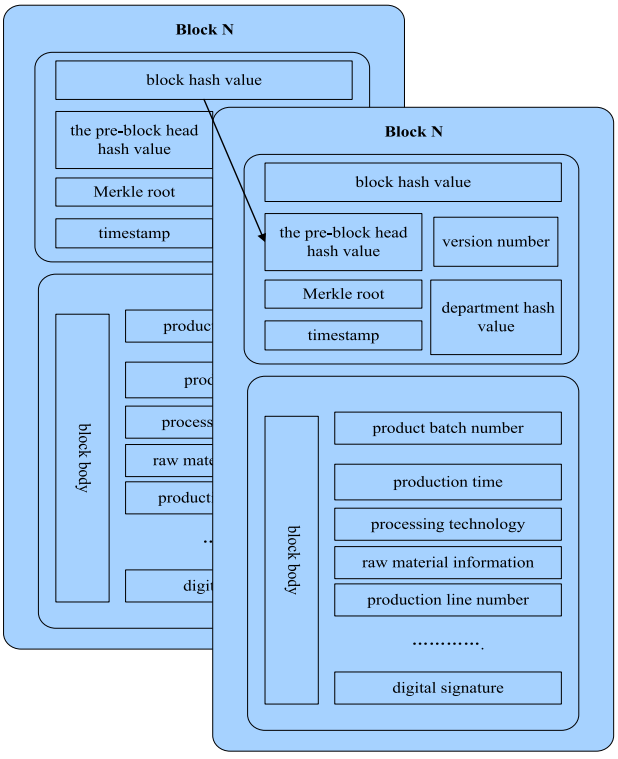

FIGURE 5. Example of data block construction of production private blockchain.

verifying the auditing result of government regulatory departments, and the key node of the consortium blockchain building and broadcasting the block of consortium blockchain to other participation nodes. Figure 6 is a logical diagram of a smart contract in the consortium blockchain.

The function of part I (Fig. 6) of the smart contract in a consortium blockchain, i.e., Algorithm4, is that nodes of government regulation departments audit product information submitted by a non-key node of the consortium blockchain and generate a dataset of the results of the auditing information. The function of part II (Fig. 6) of the smart contract in the consortium blockchain, i.e., Algorithm5, is that non-key nodes of the consortium blockchain verify the hash pointer of the enterprise private blockchain and the dataset of auditing information results generated by the nodes of government regulation departments. The function of part III (Fig. 6) of the smart contract, i.e., Algorithm6, in the consortium blockchain is that the key node of the consortium blockchain collects the result of verification of non-key nodes of the consortium blockchain, generates the block of the consortium blockchain, and broadcasts the status of the consortium blockchain to non-key nodes of the consortium blockchain.

In the consortium blockchain, the key node is responsible for building the data blocks of the consortium blockchain. The data block of the consortium blockchain can be calculated according to the smart contract. As shown in Fig. 7, the data block of the consortium blockchain consists of a block header and block body.

The block header encapsulates the current block hash value, the pre-block head hash value, and the enterprise's hash value and version number, Merkle root, and timestamp. The hash value of the current block is a function value calculated by the current block and is

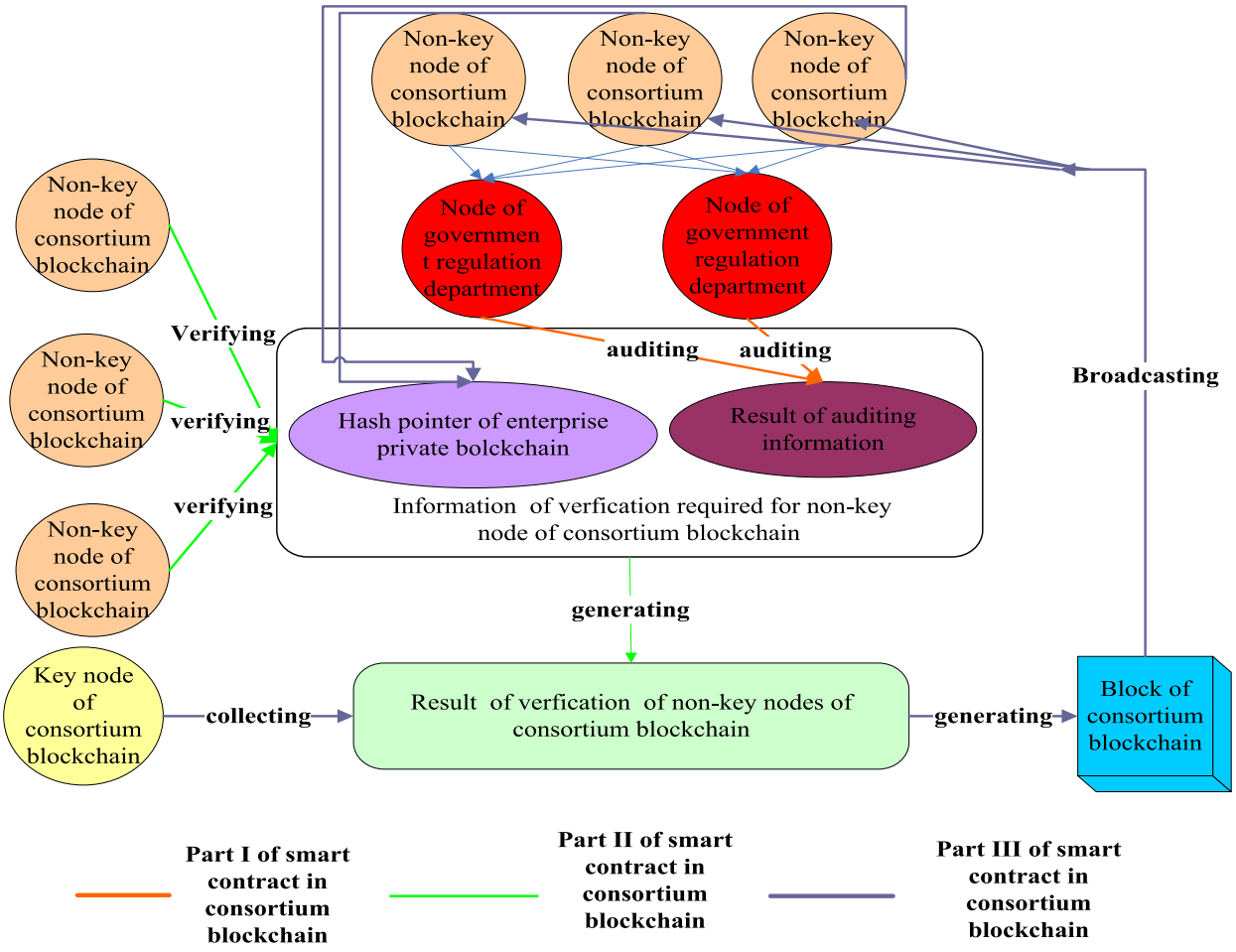

FIGURE 6. Logical diagram of smart contract in consortium blockchain.

verified by government supervision departments using the Hash256 encrypt algorithm. The pre-block head hash value is the hash value of the parent block. The enterprises hash value is the hash value of the names of enterprises in a production traceability league. The version number is the version number of the entire blockchain system. The Merkel root is obtained by Merkel calculation of the data in the block. The timestamp is set by the key node of the important enterprise in the entire production supply chain.

The block body encapsulates the auditing result, the auditing and verification results of various regulatory departments, and the hash pointer of the private blockchain and digital signatures. In a real economic environment, enterprises in the supply chain are subject to the supervision of several government regulatory departments; thus, there will be auditing results from multiple regulatory departments in the block body of the data block of the consortium blockchain. The auditing results of each department are the auditing results of relevant documents submitted by different regulatory departments. The compliance files or data submitted by the enterprise are the corresponding proofing data provided by the enterprise to government departments, such as production qualification certificates, product legitimacy certificates, etc. The hash pointer of the private blockchain is used to link the private blockchain of the enterprise and prove that the data of the private chain of the enterprise have not been tampered with. The digital signatures are the digital signatures of all participants, which can be used to prevent repudiation.

D. SMART CONTRACT OF DATA ACCESS CONTROL OF KEY NODE IN PRIVATE BLOCKCHAIN

In traditional single-layer and single-blockchain-based product traceability systems, the enterprise is requested to disclosure their all information of product in system, which may leak the enterprise's privacy data to competitors and other enterprises in the product traceability alliance. In the double-layer framework, detailed product data of the enterprise are stored in a private blockchain of the enterprise, and the hash values of blocks and hash pointers of the private blockchains are shared in the consortium blockchain. Thus, other enterprises cannot obtain the detailed product information. When other nodes of the consortium blockchain need to obtain product traceability information, they should send a data call request to the key node of the private blockchain. After allowed by the key node of private blockchain, other nodes of the consortium blockchain can obtain the product

Algorithm 3 Key Node Builds Private Block

Import: Result of verifying []
Output: Block of Result of verifying [], $h_{P_{E_i}}$ and *Hash pointer*

function private block building(i)
  for i in *non-key node*[]:
    get *Result of verifying []*
    K = i + 1
    if $K = N$
      then generate *block*($D_m \rightarrow F_{E_i}$[])
        generate $h_{P_{E_i}}$,*Hash pointer*
        generate $Sig_{E_i}(h_{P_{E_i}})$
        broadcast *block*($D_m \rightarrow F_{E_i}$[])
        send $h_{P_{E_i}}$ to $keynode_A$
        send *Hash pointer* to $keynode_A$
        send $h_{P_{E_i}}$ to *non- keynode*$_A$
        send *Hash pointer to non-Keynode*$_A$
        send $h_{P_{E_i}}$ to R_i
        send *Hash pointer* to R_i
        send $D_m \rightarrow F_{E_i} \rightarrow Appr_{R_i}$ to R_i
    end if
  end for
end function

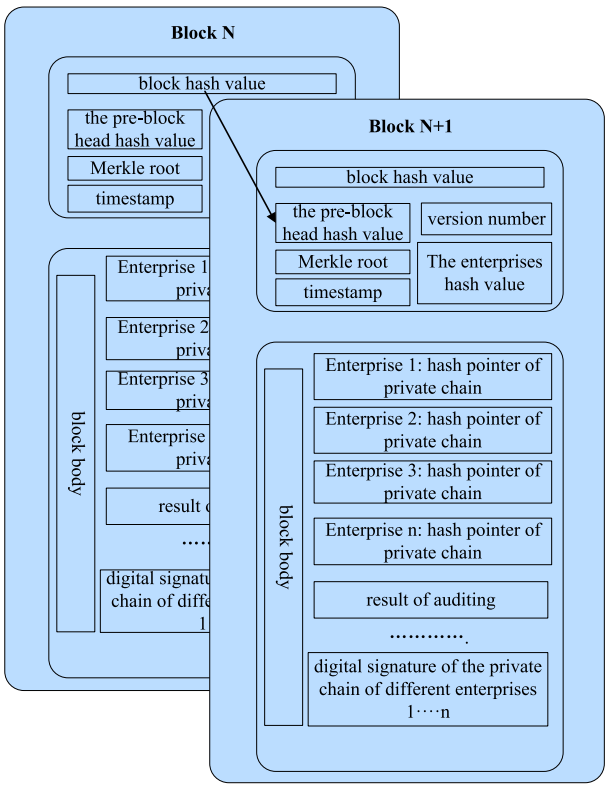

FIGURE 7. Data structure diagram of consortium blockchain in main layer.

traceability information stored in the enterprise private blockchain through the API supplied by the key node of the enterprise private blockchain. The mechanism of the data access control can prevent the enterprises' data from being called without knowing it, which protects the private data of the enterprises. We designed the smart contract for data access control, i.e., Algorithm 7, for the key node of the private blockchain in the main layer.

Algorithm 4 Government Regulation Departments Auditing

Import: Product compliance file or data required by government regulation departments
Output: Result of auditing $Appr_{R_i} \rightarrow F_{E_i}$ []

function regulation auditing(i)
  for i **in** *key node*[]:
    get $D_m \rightarrow F_{E_i} \rightarrow Appr_{R_i}$[]
    for i **in** $D_m \rightarrow F_{E_i} \rightarrow Appr_{R_i}$[]:
      check ($D_i \rightarrow F_{E_i} \rightarrow Appr_{R_i}$[])
      check (Sig_{E_i})
      if $T_{P_{E_i}} >= T_{\mathbf{A}}$
        then send back false to *key node*
        else
          check ($h_{P_{E_i}}$)
          check (*Hash pointer*)
          if *check* ($h_{P_{E_i}}$) = $\emptyset$
            check (Hash pointer)= $\emptyset$
            then send back false to *key node*
          end if
      end if
      if *check*($D_m \rightarrow F_{E_i} \rightarrow Appr_{R_i}$) = True
        check(Sig_{E_i}) = True
          then append($Appr_{R_i} \rightarrow F_{E_i}$)
      else send back false to *key node*
      end if
    send $Appr_{R_i} \rightarrow F_{E_i}$[] to *key node*
  end for
end function

V. SIMULATION EXPERIMENT AND EVALUATION

We developed a simulation platform based on Hyperledger Fabric and tested the performance of the proposed framework. In the simulation experiment, the Hyperledger local mode was used for the performance test. The test machine was a Linux Ubuntu server (64 cores, 32 GB RAM), and four business nodes and one order node were configured.

A. SIMULATION EXPERIMENTAL SCHEME

The overall design concept of the simulation experiment is described as follows. First, the double-layer framework was simulated based on the Hyperledger platform. Second, the smart contracts of the private and consortium blockchains were deployed to realize verification and auditing. Finally, existing performance testing tools were used to test the proposed double-layer framework.

1) SIMULATION OF DOUBLE-LAYER FRAMEWORK

In the proposed double-layer framework, nodes in the sub-layer and main layer implemented data entry and data reading separately, i.e., nodes in the sub-layer implemented the data

Algorithm 5 Non-Key Node of Consortium Blockchain Verifying $h_{P_{E_i}}$, *Hash Pointer*, and Auditing Result of Government Regulatory Department

Import: $h_{P_{E_i}}$,*hash pointer*, result of $Appr_{R_i} \rightarrow D_i \rightarrow F_{E_i}[]$
Output: Result of verifying[]
function non-key node verifying(i)
  get $h_{P_{E_i}}[]$
  get *Hash pointer[]*
  get $Appr_{R_i} \rightarrow F_{E_i}[]$
  for i in $h_{P_{E_i}}[]$:
    check ($h_{P_{E_i}}$)
    if *check*($h_{P_{E_i}}$) = Ture
      then append *Result of verifying[]*
    end if
  end for
  for i in *Hash pointer[]*:
    check (*Hash pointer*)
    if *check (Hash pointer)* = Ture
      then append *Result of verifying[]*
    end if
  end for
  for i in $Appr_{R_i} \rightarrow F_{E_i}[]$:
    check ($Appr_{R_i} \rightarrow F_{E_i}$])
    if *check* ($Appr_{R_i} \rightarrow F_{E_i}$) = Ture
      then append *Result of verifying[]*
    end if
  end for
  sent *Result of verifying[]* to *key* $node_A$
end function

TABLE 3. Software environment.

Software	Name
Development Platform	Hyperledger Fabric
Operation System	Ubuntu 18.04LTS
Database	Level DB
Blockchain Module	Fabric 1.0
Running Environment	Docker 18.06.0-ce

TABLE 4. Hardware environment.

Hardware	Performance
CPU	Intel xeon E5-2450
Hard Disk	2TB
Memory	128G
CPU Cach	20M
FSB	800MHz

entry and storing operations, and nodes in the main layer implemented the data reading operation. Inspired by Spring Cloud (https://spring.io/projects/spring-cloud), we simulated the double-layer framework using Hyperledger Fabric by setting up different nodes to store different data. The details of the simulation experiment are shown in Tables 3 and 4.

In reference to the literature [36]–[39], we created four peer nodes as an application built based on the blockchain system (Table 5,) which all had the same copy database.

Algorithm 6 Key node of consortium blockchain building block and broadcast

Import: Result of verifying[]
Output: Block of consortium blockchain
function consortium block building(i)
  get *Result of verifying[]*
  for i in *non-key* $node_A[]$:
    compare *Result of verifying[]*
    K = i + 1
    if $K > 2N/3$
      then generate *block(Result of verifying[])*
        broadcast *block(Result of verifying[])*
    end if
  end for
end function

Algorithm 7 Key Node of Private Blockchain Judging Data Call Request

Import: data call request of consortium blockchain nodes
Output: data access of private blockchain
function data call request judgment(i)
  for i **in** $node_A(i)$
    judge *data call request*
    if judge(*data call request*) = True
      then sent the data access to $node_A(i)$
    else
      sent error to $node_A(i)$
    end if
  end for
end function

TABLE 5. The seting of nodes.

Layer	Key node of layer	Nodes
The main layer	Peer1	Peer1
		Peer2
The sub-layer	Peer3	Peer3
		Peer4

We interacted with the application using Json form lists. The peers obtained or posted Json data, and wrote these data in Level DB. By using rate controllers to send unit test cases to our smart contracts, we design some use cases of data reading and data writing, and the performances of use cases of data writing and reading can reflect the performances of nodes in main layer and sub-layer. Figure 8 shows the data storage scheme. As shown in Fig. 8, the hash value is calculated after signing, to reduce the storage pressure of system.

2) DEPLOYING SMART CONTRACTS AND BENCHMARKING PLATFORM

We deployed smart contracts using the Go language in the double-layer-framework (Sections IV-A, IV-Band IV-C). The blockchain standard used to code the smart contracts was

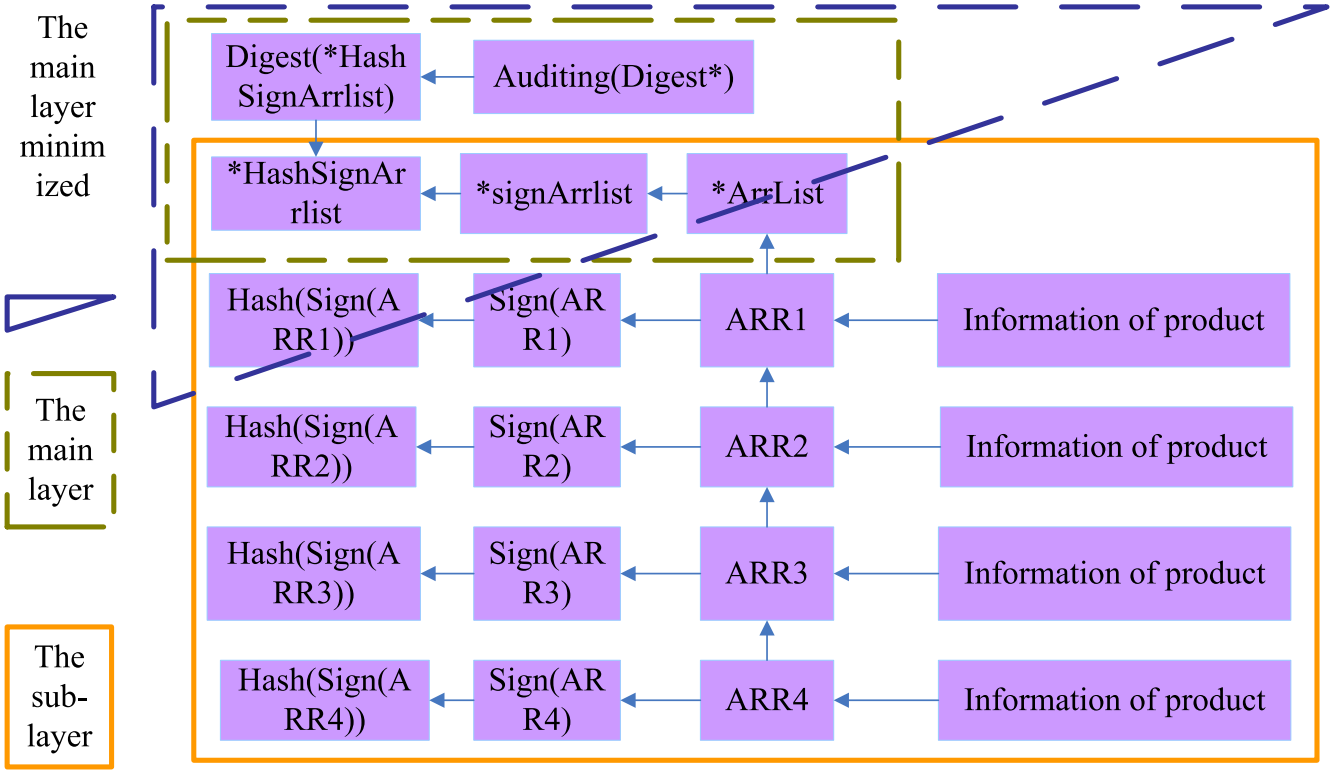

FIGURE 8. Data storage scheme.

primarily from Hyperledger Fabric, which made the smart contract concept named "Chain Code".

Hyperledger Caliper was used for the performance analysis. Hyperledger Caliper is a highly credible blockchain benchmarking tool that allows users to measure the performance of a particular blockchain implementation using a predefined set of use cases. Performance metrics for major measures include TPS, transaction latency, and resource utilization. The Hyperledger Caliper component primarily includes (1) an adaptation layer used to integrate multiple blockchain solutions into the Caliper framework (Figure 9), (2)an adapter, which is responsible for converting the Caliper NBI into the corresponding blockchain protocol, and (3) Caliper NBIs, which are a group of connectors that provide data intersections between test cases and the target blockchain network in the test framework.

Note that we used local mode for performance testing. We implemented experiments based on the proposed consensus mechanism and overall framework using Node.js.

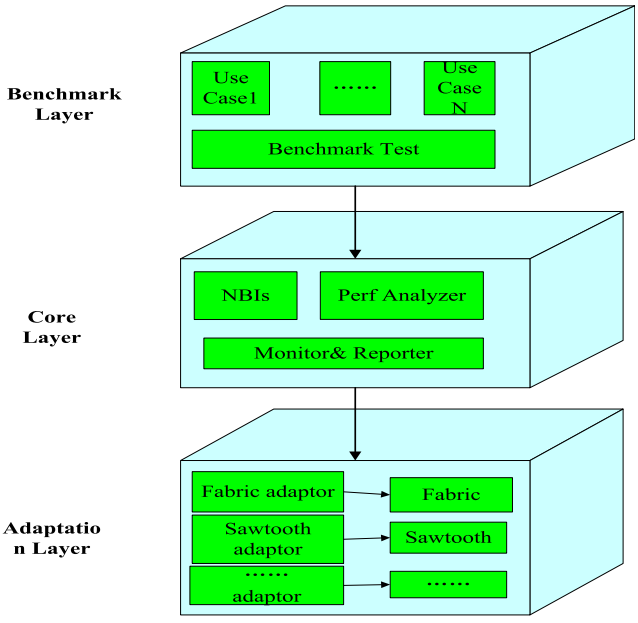

FIGURE 9. Implementation framework of Hyperledger Caliper.

B. TEST RESULTS

To obtain accurate test results, we performed 20,000 unit tests, which were divided into ten groups of 2000 unit tests. The indicators of the group tests were maximum latency, minimum latency, and throughput. Here, maximum latency represents the maximum delay time that a transaction (one unit test) executed in each group test, and the minimum latency the minimum delay time that a transaction (one unit test) executed in each group test. Throughput is the number of requests/TPS.

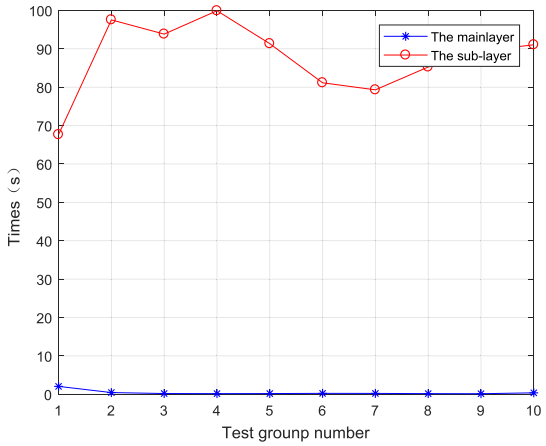

FIGURE 10. Comparison of maximum latency of nodes in the main layer and sub-layer.

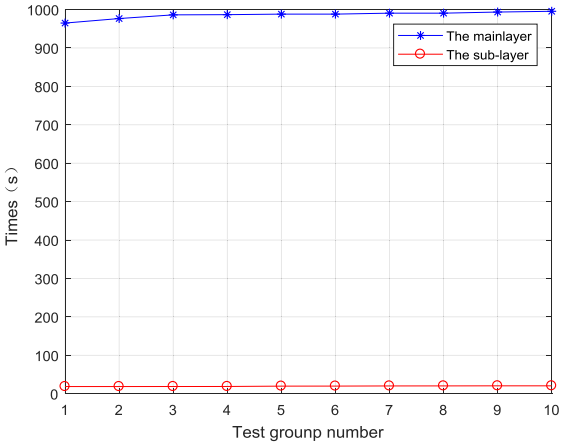

FIGURE 12. Comparison of throughput of nodes in the main layer and sub-layer.

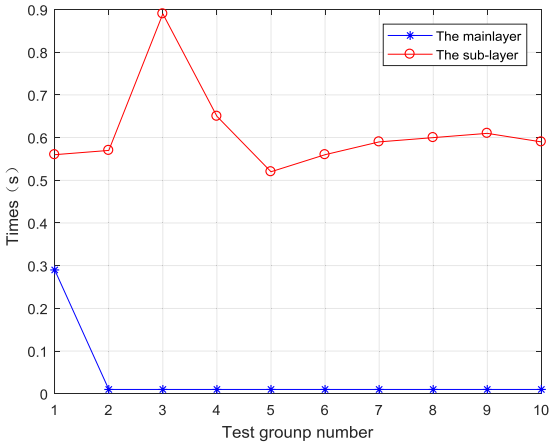

FIGURE 11. Comparison of minimum latency nodes in the main layer and sub-layer.

We calculated the average of the unit tests for each group. Figure 10 compares the maximum latency of a node in the main layer and a node in the sub-layer. As can be seen, the maximum latency of the node in main layer is much less than that of the node in the sub-layer (nearly 1000 times greater than the node in the main layer).

Figure 11 compares the minimum latency of a node in the main layer and a node in the sub-layer. As shown, the difference is small.

As can be seen in Figs. 10 and 11, the runtime of the main layer is much faster than that of the sub-layer.

Figure12 compares the throughput of nodes in the main layer and sub-layer. As can be seen, the throughput of the main layer node is much greater than that of the nodes in the sub-layer. The throughput of the main layer node is nearly 50 times greater than that of the nodes in the sub-layer, which means nodes in the main layer outperform nodes in the sub-layer.

As shown in Figs. 10, 11, and 12, the performance of nodes in the main layer is much higher than that of the nodes in the sub-layer. This means that a lot of time and computing resources are required to achieve product traceability within the enterprise. Efficient product traceability information sharing can be achieved among enterprises, between enterprises and government departments, and between enterprises and consumers. The node in the main layer can directly provide consumers with the product traceability information query; thus, for consumers, node optimization in the main layer optimizes the entire traceability system.

In fact, if a monolayer framework is adopted, the responsibilities of nodes in the enterprise include data entry and data storing of product traceability information, as well as sharing product traceability information and responding to consumer query requests, node performance will be inferior than that of the private blockchain in the sub-layer. By applying the double-layer framework, the operational performance of nodes in the main layer can be improved by optimizing the data storage scheme. The optimization of the node performance in the main layer is crucial for consumers because it means that they can enjoy faster and more convenient product traceability information services, which can effectively improve utility. It is helpful to improve the sustainability of product traceability technology solutions based on blockchain technology.

C. COMPARISONS

We compared the proposed scheme to existing production traceability schemes, and the results are given in Table 6. As can be seen, the proposed scheme has regulatory convenience, a high degree of privacy protection, and good performance.

The proposed scheme fully exploits the advantage of blockchain, i.e., it decentralized, and can trace product information effectively and prevent data tampering. We implemented the double-layer framework in the proposed scheme; thus, it has better scalability and can easily incorporate government departments into a blockchain-based product traceability system. In the proposed scheme, there

TABLE 6. The comparison of our scheme and existing production traceability schemes.

Item \ Solution	Traditional multi-layer centralized system[40][41]	blockchain-based Scheme [20][23][24] [26]	Our scheme
Information Traceability	√	√	√
Prevent tampering	×	√	√
Decentralization	×	√	√
Multiple layerframework	√	×	√
Multi-blockchain	/	×	√
Separation data entry from data reading	√	×	√
Participation of government regulatory department	×	×	√
Mechanism of privacy data protection	√	×	√

are two layers and several blockchains, which allows enterprise product traceability information to be stored inside an enterprise. Relative to satisfy consumer demand and government regulation, the enterprise can make itself information sharing plan according to the actual situation of the enterprise to maximize protection of its secret information. In addition, in the double-layer framework, data reading in the main layer is separated from data entry and storage in the sub-layer, which can improve the system's throughput and operational efficiency, and reduce customer waiting time. Therefore, the proposed scheme's sustainability is greater than that of the existing blockchain-based product traceability system.

D. SECURITY ANALYSIS

In our design, the double-layer permissioned blockchain-based product traceability system can solve problems related to data security and privacy protection in the product traceability process.

1) MALICIOUS WRITING PRODUCT TRACEABILITY INFORMATION

The key node of the private blockchain audits product traceability data written by non-key node in an online manner, and the enterprise department selected as the key node supervises other departments writing real information into the private blockchain in an offline manner. This ensures that information written in the private blockchain is true and real. The government regulatory department node can obtain product information using an API supplied by the enterprise and can check the authenticity of product information online. In addition, a government regulatory department can access the enterprise to inspect production and operation activities in an offline manner. This ensures that enterprises will not produce illegitimate product traceability information. Malicious writing product traceability information can be prevented from being written into the blockchain system by online auditing and offline inspection.

2) PRODUCT TRACEABILITY INFORMATION TAMPERING

In the double-layer framework, the data of product traceability information is stored in private blockchain, so if the data stored in private blockchain can't be tampered, the system will be information tampering resistant. In the double-layer framework, sub-layer and main layer are connected by hash pointer, so, it will be found easily and the owner of the private blockchain will be punished by the product traceability alliance or the government regulatory authority, ifthe data stored in private blockchain is tampered. This mechanism reduces companies' willingness to tamper the data, makes the cost of tampering information high and can protect the product traceability information from being tampered. In addition, the enterprise can improve the security of hardware and software to protect the data sorted in private blockchain from being tampered by hackers.

3) PRIVACY PROTECTION

In the double-layer framework, the privacy data of the enterprise is stored in a private blockchain, and data are shared via access control, which can help protect the enterprise's privacy from being known by other non-key node of consortium blockchain. This mechanism will realize the privacy protection. But, there will another risk, which is the key node of the consortium blockchain will obtain the detailed product traceability information through the API. The risk may lead privacy to leak. So, the department of enterprise selected as key node of consortium blockchaiin must be trusted by the other members of product traceability alliance. Once the key node of consortium blockchain is compromised and leak the enterprise' privacy, it should be replaced by other node of consortium blockchain to protect the privacy data of member of traceability alliance.

4) DDoS ATTACK RESISTANT

A product traceability system based on the permissioned blockchain requires nodes to authenticate real identities, which can mitigate against major DDoS attacks from other nodes in the system. In addition, the key nodes of the consortium and private blockchains can reject visitor data access require if they confirm that visitor access frequency is too high.

5) COMPROMISED KEY NODE

The key nodes of the consortium and private blockchains are important in the product information traceability system based on the permissioned blockchain. If key nodes are attacked and fail, the other non-key node can be selected as a key node in the double framework, which can minimize the impact of a compromised key node on the system.

VI. CONCLUSION

In this paper, we have proposed a product traceability scheme based on the permissioned blockchain, and we have designed a double-layer framework according to the proposed scheme.

We analyzed the advantages and operating mechanisms of the double-layer framework. We have also introduced details about the smart contracts deployed in a double-layer framework, as well as the block data structures of private and consortium blockchains. The result of a simulation experiment indicates that the performance of the main layer is much higher than that of the sub-layer. The function of the main layer is to provide traceability information directly to consumers; thus, optimization of the main layer's performance represents overall optimization of the entire traceability system. We also compared the proposed scheme to existing production traceability schemes, and the comparison results demonstrate the features and advantages of the proposed scheme.

Note that potential applications of the double layer are not limited to product traceability, e.g., this concept can be widely applied to other blockchain technology applications, such as energy management, transportation, and financial communication [42]. The double-layer framework can improve the scalability of blockchain-based systems and can effectively mitigate performance bottlenecks and prevent corporate data leakage caused by the existing single-blockchain and single-layer frameworks. We believe that it has important significance for broadening the application of blockchain technologies.

REFERENCES

[1] J.-H. Huh and S.-K. Kim, "The blockchain consensus algorithm for viable management of new and renewable energies," *Sustainability*, vol. 11, no. 11, pp. 3184–3201, Jun. 2019.

[2] E. Tijan, S. Aksentijević, K. Ivanić, and M. Jardas, "Blockchain technology implementation in logistics," *Sustainability*, vol. 11, no. 4, pp. 1185–1203, Feb. 2019.

[3] A. Bogner, M. Chanson, and A. Meeuw, "A decentralised sharing app running a smart contract on the ethereum blockchain," in *Proc. 6th Int. Conf. Internet Things (IoT)*, 2016, pp. 177–178. [Online]. Available: https://dl_acm.gg363.site/citation.Cfm?id=2998465

[4] M. Samaniego and R. Deters, "Blockchain as a service for IoT," in *Proc. IEEE Int. Conf. Internet Things (iThings), IEEE Green Comput. Commun. (GreenCom), IEEE Cyber, Phys. Social Comput. (CPSCom), IEEE Smart Data (SmartData)*, Dec. 2016, pp. 433–436. [Online]. Available: https://ieeexplore_ieee.gg363.site/abstract/document/7917130/

[5] B. Lee and J.-H. Lee, "Blockchain-based secure firmware update for embedded devices in an Internet of Things environment," *J. Supercomput.*, vol. 73, no. 3, pp. 1152–1167, Mar. 2017.

[6] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, Apr. 2016.

[7] W.-T. Tsai, R. Blower, Y. Zhu, and L. Yu, "A system view of financial blockchains," in *Proc. IEEE Symp. Service-Oriented Syst. Eng. (SOSE)*, Mar. 2016, pp. 450–457. [Online]. Available: https://ieeexplore_ieee.gg363.site/abstract/document/7473060

[8] H. M. Kim and M. Laskowski, "Towards an ontology–driven blockchain design for supply chain provenance," *Intell. Syst. Accounting, Finance Manage.*, vol. 25, no. 1, pp. 18–27, 2018.

[9] K. Korpela, J. Hallikas, and T. Dahlberg, "Digital supply chain transformation toward blockchain integration," in *Proc. 50th Hawaii Int. Conf. Syst. Sci.*, 2017. [Online]. Available: https://scholarspace.manoa.hawaii.edu/handle/10125/41666

[10] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, "Blockchain challenges andopportunities: A survey," *Int. J. Web Grid Services*, vol. 14, no. 4, pp. 352–375, 2018.

[11] G. Blossey, J. Eisenhardt, and G. Hahn, "Blockchain technology in supply chain management: An application perspective," in *Proc. 52nd Hawaii Int. Conf. Syst. Sci.*, 2019, pp. 1–9. [Online]. Available: https://scholarspace.manoa.hawaii.edu/handle/10125/60124

[12] S. Ølnes, J. Ubacht, and M. Janssen, "Blockchain in government: Benefits and implications of distributed ledger technology for information sharing," *Government Inf. Quart.*, vol. 34, no. 3, pp. 355–364, Sep. 2017.

[13] M. ElMessiry and A. ElMessiry, "Blockchain framework for textile supply chain management," in *Proc. Int. Conf. Blockchain*. Cham, Switzerland: Springer, 2018. [Online]. Available: https://www.academia.edu/download/58091788/Blockchain_Framework_for_Textile_Supply_chain_management_treated.pdf

[14] S. Chen, R. Shi, Z. Ren, J. Yan, Y. Shi, and J. Zhang, "A Blockchain–Based Supply Chain Quality Management Framework," in *Proc. IEEE 14th Int. Conf. e-Bus. Eng. (ICEBE)*, Nov. 2017. [Online]. Available: https://ieeexplore_ieee.gg363.site/abstract/document/8119146

[15] O. Petersen and F. Jansson, "Blockchain technology in supply chain traceability systems" M.S. thesis, Dept. Ind. Eng. Manage., Lund Univ., Lund, Sweden, 2017. [Online]. Available: http://lup.lub.lu.se/luur/download?func=downloadFile&recordOId=8918347&fileOId=8919918

[16] R. Kamath, "Food traceability on blockchain: Walmart's pork and mango pilots with IBM," *JBBA*, vol. 1, no. 1, pp. 3712–3724, Jan. 2018.

[17] F. Yiannas, "A new era of food transparency powered by blockchain," *Innov., Technol., Governance, Globalization*, vol. 12, nos. 1–2, pp. 46–56, Jul. 2018.

[18] C. C. Di, A. Cecconi, and J. Mendling, "Blockchain-based traceability of interorganisational business processes," in *Proc. Int. Symp. Bus. Modeling Softw. Design*. Cham, Switzerland: Springer, 2018. [Online]. Available: https://link_springer.gg363.site/chapter/10.1007/978-3-319-94214-8

[19] X. Xu, Q. Lu, Y. Liu, L. Zhu, H. Yao, and A. V. Vasilakos, "Designing blockchain-based applications a case study for imported product traceability," *Future Gener. Comput. Syst.*, vol. 92, pp. 399–406, Mar. 2019.

[20] Q. Lin, H. Wang, X. Pei, and J. Wang, "Food safety traceability system based on blockchain and EPCIS," *IEEE Access*, vol. 7, pp. 20698–20707, 2019.

[21] T. Mohan, "Improve food supply chain traceability using blockchain," Ph.D. dissertation, Pennsylvania State Univ., Philadelphia, PA, USA, 2018. [Online]. Available: https://etda.xlibraries.psu.edu/files/final_submissions/16822

[22] R. Bettín-Díaz, A. E. Rojas, and C. Mejía-Moncayo, "Methodological approach to the definition of a blockchain system for the food industry supply chain traceability," in *Proc. Int. Conf. Comput. Sci. Appl.* Cham, Switzerland: Springer, 2018. [Online]. Available: https://link_springer.gg363.site/chapter/10.1007/978-3-319-95165-2_2

[23] F. Tian, "An agri-food supply chain traceability system for China based on RFID & blockchain technology," in *Proc. 13th Int. Conf. Service Syst. Service Manage. (ICSSSM)*, Jun. 2016, pp. 1–4. [Online]. Available: https://epub.wu.ac.at/6090/1/Dissertation_of_Feng_Tian.pdf#page=66

[24] F. Tian, "A supply chain traceability system for food safety based on HACCP, blockchain & Internet of Things," in *Proc. Int. Conf. Service Syst. Service Manage.*, Jun. 2017. [Online]. Available: http://epub.wu.ac.at/6090/1/Dissertation_of_Feng_Tian.pdf#page=85

[25] J. Hua, X. Wang, M. Kang, H. Wang, and F.-Y. Wang, "Blockchain based provenance for agricultural products: A distributed platform with duplicated and shared bookkeeping," in *Proc. IEEE Intell. Vehicles Symp. (IV)*, Jun. 2018. [Online]. Available: https://ieeexplore_ieee.gg363.site/abstract/document/8500647

[26] M. P. Caro, M. S. Ali, and M. Vecchio, "Blockchain-based traceability in agri-food supply chain management: A practical implementation," in *Proc. IoT Vertical Topical Summit Agricult.-Tuscany (IOT Tuscany)*, May 2018, pp. 1–4. [Online]. Available: https://ieeexplore_ieee.gg363.site/abstract/document/8373021/

[27] K. Salah, N. Nizamuddin, R. Jayaraman, and M. Omar, "Blockchain–based soybean traceability in agricultural supply chain," *IEEE Access*, vol. 7, pp. 73295–73305, 2019.

[28] A. A. Arsyad, S. Dadkhah, and M. Köppen, "Correction to: Two-factor blockchain for traceability cacao supply chain," in *Proc. Int. Conf. Intell. Netw. Collaborative Syst.* Cham, Switzerland: Springer, 2018, p. 1. [Online]. Available: https://link_springer.gg363.site/content/pdf/10.1007/978-3-319-98557-2_50.pdf

[29] M. N. Islam, V. C. Patii, and S. Kundu, "On IC traceability via blockchain," in *Proc. Int. Symp. VLSI Design Automat. Test (VLSI-DAT)*, Apr. 2018, pp. 1–4. [Online]. Available: https://ieeexplore_ieee.gg363.site/abstract/document/8373269
[30] T. K. Agrawal, A. Sharma, and V. Kumar, "Blockchain-based secured traceability system for textile and clothing supply chain," in *Artificial Intelligence for Fashion Industry in the Big Data Era*. Singapore: Springer, 2018, pp. 197–208. [Online]. Available: https://link_springer.gg363.site/chapter/10.1007/978-981-13-0080-6_10
[31] A. Imeri and D. Khadraoui, "The security and traceability of shared information in the process of transportation of dangerous goods," in *Proc. 9th IFIP Int. Conf. New Technol., Mobility Secur. (NTMS)*, Feb. 2018, pp. 1–5. [Online]. Available: https://ieeexplore_ieee.gg363.Site/abstract/document/8328751
[32] C. Gorenflo, S. Lee, and L. Golab, "FastFabric: Scaling hyperledger fabric to 20,000 transactions per second," in *Proc. IEEE Int. Conf. Blockchain Cryptocurrency (ICBC)*, Jan. 2019, pp. 1–9. [Online]. Available: https://arxiv.org/pdf/1901.00910
[33] C. Li and L. J. Zhang, "A blockchain based new secure multi-layer network model for Internet of Things," in *Proc. IEEE Int. Congr. Internet Things (ICIOT)*, Jun. 2017. [Online]. Available: https://ieeexplore_ieee.Gg363.site/abstract/document/8039052
[34] S. Badr, I. Gomaa, and E. Abd-Elrahman, "Multi-tier blockchain framework for IoT–EHRs systems," *Procedia Comput. Sci.*, vol. 141, pp. 159–166, Jan. 2018.
[35] F. Paolucci, "Network service chaining using segment routing in multi–layer networks," *J. Opt. Commun. Netw.*, vol. 10, no. 6, p. 582, Jun. 2018.
[36] H. Sukhwani, "Performance modeling of PBFT consensus process for permissioned blockchain network (hyperledger fabric)," in *Proc. IEEE 36th Symp. Reliable Distrib. Syst. (SRDS)*, Sep. 2017, pp. 253–255. [Online]. Avaiable: https://ieeexplore_ieee.gg363.site/abstract/document/8069090/
[37] Q. Zhang, "LedgerGuard: Improving blockchain ledger dependability," in *Proc. Int. Conf. Blockchain*. Cham, Switzerland: Springer, 2018, pp. 251–258. [Online]. Available: https://link_springer.gg363.site/chapter/10.1007/978-3-319-94478-4_18
[38] A. Sharma, "How to databasify a blockchain: The case of hyperledger fabric," 2018, *arXiv:1810.13177*. [Online]. Avaiable: https://arxiv.org/abs/1810.13177
[39] A. Baliga, "Performance evaluation of the quorum blockchain platform," 2018, *arXiv:1810.13177*. [Online]. Avaiable: https://arxiv.org/abs/1809.03421
[40] M. Jansen-Vullers, C. Van Dorp, and A. Beulens, "Managing traceability information in manufacture," *Int. J. Inf. Manage.*, vol. 23, no. 5, pp. 395–413, Oct. 2003.
[41] Y.-S. Kang and Y.-H. Lee, "Development of generic RFID traceability services," *Comput. Ind.*, vol. 64, no. 5, pp. 609–623, Jun. 2013.
[42] J. M. Zhu, Q. Y. Ding, and S. Gao, "Distributed framework of SWIFT system based on permissioned blockchain," (in Chinese), *J. Softw.*, vol. 30, no. 6, pp. 1594–1613, 2019. [Online]. Available: http://www.jos.org.cn/1000-9825/5738.htm

QINGYANG DING was born in Hebei, China. He received the B.S. degree in management from the Institute of Disaster Prevention, in 2014, and the M.S. degree from the School of Accounting, Inner Mongolia University of Finance and Economics, in 2017. He is currently pursuing the Ph.D. degree with the School of Information, Central University of Finance and Economics.

He is currently a Researcher of blockchain. His main research interests include the blockchain application and digital economy.

SHENG GAO received the B.S. degree in information and computation science from the Xi'an University of Posts and Telecommunications, in 2009, and the Ph.D. degree in computer science and technology from Xidian University, in 2014.

He is currently an Associate Professor with the School of Information, Central University of Finance and Economics. He has published more than 30 research articles in refereed international journals and conferences. His current research interests include data security, privacy computing, and blockchain technology.

JIANMING ZHU was born in Shanxi, China. He received the Ph.D. degree from the Xidian University of Electronic Technology, Xi'an.

From 2008 to 2009, he was a Research Fellow with The University of Texas at Dallas. He is currently a Professor and the Ph.D. Supervisor with the School of Information, Central University of Finance Economics. His current research interests include blockchain technology, information, and network security, and digital economy. He has published over 100 refereed articles in these areas.

CHONGXUAN YUAN was born in Shandong. He received the B.S. degree in engineering from Shandong University, in 2017. He is currently pursuing the M.S. degree with the School of Information, Central University of Finance and Economics.

He is currently a Researcher of blockchain. His main research interests include the blockchain and software systems.