International Journal of Computational Science and Engineering

ISSN online: 1742-7193 - ISSN print: 1742-7185
https://www.inderscience.com/ijcse

A food safety traceability system based on trusted double chain

Haoran Chen, Jiafan Wang, Hongwei Tao, Yinghui Hu, Yanan Du

DOI: 10.1504/IJCSE.2024.10063226

Article History:

Received:	05 July 2023
Last revised:	02 February 2024
Accepted:	04 February 2024
Published online:	21 December 2024

A food safety traceability system based on trusted double chain

Haoran Chen*, Jiafan Wang, Hongwei Tao and Yinghui Hu

School of Computer Science and Technology,
Zhengzhou University of Light Industry,
Zhengzhou 450002, China
Email: chenhaoran@zzuli.edu.cn
Email: wangjiafan006@163.com
Email: hongweitao@zzuli.edu.cn
Email: hyingh6@163.com
*Corresponding author

Yanan Du

School of Health Management,
Anhui Medical University,
Hefei 230032, China
Email: duyanan@ahmu.edu.cn

Abstract: In recent years, global food safety issues have been increasingly prevalent, posing threats to people's health and lives. Traditional food traceability systems face significant challenges due to centralised storage, data silos, and the potential for information tampering. This article proposes an improved RAFT consensus algorithm for the first time, applied to trace the production process of food based on private chains. Subsequently, an enhanced PBFT consensus algorithm is introduced for tracing the distribution process of food based on consortium chains. Finally, a reliable dual-chain food quality and safety traceability system based on the Ethereum blockchain platform is presented. This system effectively addresses data reliability issues on the chain by introducing a reliability measurement evaluation module. Moreover, the application of aggregated signature technology enhances the performance of the traceability system, ensuring the authenticity, reliability, and tamper resistance of traceability information. This innovation not only strengthens the privacy protection and data security of food quality and safety tracking but also helps maintain the commercial interests of all parties involved.

Keywords: food traceability; blockchain; cross-agency traceability system.

Reference to this paper should be made as follows: Chen, H., Wang, J., Tao, H., Hu, Y. and Du, Y. (2025) 'A food safety traceability system based on trusted double chain', *Int. J. Computational Science and Engineering*, Vol. 28, No. 1, pp.114–125.

Biographical notes: Haoran Chen is a Lecturer at Zhengzhou University of Light Industry. He graduated from Beijing University of Technology with a PhD in 2019. His primary research areas include blockchain technology, big data analysis, and pattern recognition.

Jiafan Wang received her BS in Engineering in 2017 and is currently pursuing her MS degree at Zhengzhou University of Light Industry. Her current research interests include blockchain technology, machine learning and pattern recognition.

Hongwei Tao is an Associate Professor with Zhengzhou University of Light Industry, China. He received the PhD degree in Computer Applications Technology from East China Normal University in 2011. His current research interests include software trustworthiness measurement, big data analysis and formal methods.

Yinghui Hu received his BS degree from Zhengzhou University of Light Industry in 2018 and MS degree from Zhengzhou Institute of Light Industry in 2022. His current research interests include blockchain technology and artificial intelligence.

Yanan Du is a Lecturer at Anhui Medical University. She received her PhD in Management from Hefei University of Technology in 2017. She worked as a Postdoctoral Fellow in the direction of Business Administration at the School of Management, Hefei University of Technology from 2017 to 2019. Her research interests include text mining and big data analytics.

1 Introduction

Recently, frequent food safety incidents have caused significant losses to people's lives and properties and have seriously impacted the Chinese government's image (Deng, 2008). The traceability of information throughout food production to sale is crucial in ensuring food quality and safety.

Traditional food traceability system adopts centralised network management, primarily maintained by local government agencies and industry-leading companies. This centralised system faces significant issues, with most consumers needing help accessing complete transaction information or tracing the origin of products. Furthermore, data is susceptible to tampering, making effective verification challenging, which results in a lack of assurance regarding the completeness, authenticity, and accuracy of traceability information. The reliability of information transfer among participants in the food supply chain remains unresolved, and issues such as data silos and counterfeiting persist (Chen et al., 2016).

Blockchain utilises technologies such as timestamps, consensus mechanisms, and smart contracts (Xu et al., 2023) for data characteristics that cannot be tampered with and are fully traceable. It offers a solution to the challenge of centralised data storage and simultaneously provides the technical underpinning for establishing cross-organisational traceability systems (Xu et al., 2018; Zeng et al., 2021). Blockchain technology has introduced fresh approaches and concepts to food quality and safety traceability. When integrated with blockchain technology, a food quality and safety traceability system can be constructed, encompassing the collection and uploading of data and information associated with producing, processing, and selling agricultural products. It underscores end-to-end supervision, spanning from the farmland to the dining table. Such a system detects, tracks, and tracks food items. In a food safety incident, an agricultural product traceability system can precisely and promptly pinpoint the problematic links, ascertain the root causes, assign accountability, and contain the further spread of the incident. This is a very effective way to address the current food safety issues (Zeng et al., 2021).

As a product of the convergence of various technologies, blockchain faces numerous challenges in its development and application. One of the most critical challenges is the continuous increase in performance requirements for blockchain systems. Blockchain traceability products have stringent real-time demands, thus necessitating higher performance levels. The choice of consensus algorithm is a pivotal consideration in blockchain-based systems, as it directly affects the overall system's performance. Common consensus mechanisms in Blockchain include proof-of-work (POW) (Cortier et al., 2017), the PAXOS mechanism (Bin and Jiang, 2020), the RAFT mechanism (Benaddi et al., 2021), practical byzantine fault tolerance (PBFT) (Onireti et al., 2019), and more. However, it is challenging to balance factors such as throughput, latency, fault tolerance, and others (Dixit et al., 2020).

The transparency of blockchain allows users to access all transaction and supply chain information, including amounts and contract details. However, data in the supply chain should remain confidential, as rival companies or individuals could benefit from analysing transaction data, which could directly harm a company's interests. Therefore, blockchain traceability systems must address the issue of privacy leaks in blockchain and ensure the security of user information (Li et al., 2021). In traditional data privacy protection solutions, data is stored on central servers, and data management centres can enhance the server's resilience to attacks to achieve data privacy protection. In a blockchain system, all transaction data is stored in distributed full nodes, each with varying defence capabilities, and malicious nodes may join the blockchain system to obtain transaction data (Gang et al., 2022). Thus, more than traditional data privacy protection solutions are needed for blockchain.

In order to improve the anonymity of blockchain technology and protect the privacy of user identity and transaction data, a variety of blockchain privacy protection techniques have been proposed, which can be categorised into three types: techniques based on mixed-coin protocols, techniques based on cryptographic protocols, and techniques based on secure channel protocols (Ramos et al., 2019). However, there are still many problems with the security and reliability of existing technologies. Users using off-chain transactions need to publish the final transaction status to the whole network; third-party platforms have the possibility of leaking users' information; attackers obtain users' transaction patterns and transaction information by analysing users' off-chain payment routes (Dai et al., 2017).

In summary, existing blockchain traceability systems primarily focus on tracking and tracing data, but they do not inherently address the credibility of on-chain data, which is resistant to tampering once recorded on the blockchain. If data users analyse and rely on inaccurate or inferior data, it can result in significant and unforeseeable losses. Additionally, the performance of the entire process, from data publication to consensus establishment, validation, and subsequent uploading to the blockchain, needs to be optimised. Moreover, concerns about potential privacy leaks must also be considered.

This paper proposes a novel food quality and safety traceability system based on dual-chain technology, offering an innovative solution for comprehensive tracing of food production and distribution processes, thereby enhancing the efficiency and reliability of food safety management.

In the process of designing the traceability solution, we introduce improved versions of the RAFT and PBFT consensus algorithms. By optimising the consensus algorithms, we enhance the system's stability, scalability, and real-time performance, ensuring the accuracy and integrity of traceability data.

Furthermore, we introduce a reliability indicator evaluation module and aggregate signature technology to

further enhance the performance and security of the traceability system. The reliability indicator evaluation module helps users assess the credibility of data on the chain, reducing the risks associated with information uncertainty. Aggregate signature technology reduces the computational cost of signature verification, improves system processing efficiency, protects user privacy, and enhances system acceptability and practicality.

The remaining sections of the paper are structured as follows: Section 2 provides an overview of related work, following that, Section 3 provides a detailed overview of the traceability scheme for food production processes based on private chains, including the proposed improved RAFT consensus algorithm and specific implementations. Section 4 then delves into the traceability scheme for food distribution processes based on consortium chain, outlining the proposed improved PBFT consensus algorithm and specific implementations. Section 5 explores the system structure, modules, and specific implementation schemes in detail. In Section 6, we present a comparative analysis of the advantages of the traceability system proposed in the paper. Finally, Section 7 summarises the main research content of this paper and outlines potential directions and topics for future research.

2 Related works

Recently, more and more scholars have actively explored the application of blockchain technology in traceability. Abeyratne and Monfared (2016) elaborated on the common problems in supply chain management and analysed the prospect and trend of applying blockchain technology to supply chain management. Zhao (2019) argued that there are information barriers between government departments and enterprises, and between enterprises and enterprises, resulting in traceability information cannot be shared, and proposed that the use of blockchain technology can break the barriers between the information, to achieve the circulation of information elements, which is convenient for the departmental supervision and social supervision. Gao et al. (2020) established a food supply chain based on the Hyperledger Fabric blockchain development platform traceability system, aggregating all enterprises in the supply chain and conducting transactions on the blockchain to achieve reliable traceability based on transactions. Wang Wang et al. (2020) also constructed a traceability model based on the Hyperledger Fabric blockchain development platform, but the model mainly traces agricultural products. Aiming at the characteristics of the agricultural supply chain, they establish the system model of 'one link, one ledger' to reduce the complexity of the storage structure and take ginger products as the traceability object to verify the model's effectiveness. Chen et al. (2022) based on hyperledger fabric smart contract, using distributed RAFT consensus protocol, combined with IoT device services precise authority control, to achieve reliable and trustworthy IoT data storage traceability, as well as redundant data filtering and access control based on attributes, which greatly reduces the redundant data and improves the security. Liu et al. (2022) developed a trusted traceability system for agricultural product quality and safety based on the Hyperledger Fabric blockchain platform and put forward the 'on-chain + off-chain' collaborative management and storage strategy for agricultural product quality and safety traceability information, which solves the problem of high data storage pressure, querying efficiency and high reliability of node data storage, as well as the problems of data storage pressure and querying efficiency of node data storage and querying efficiency of node data storage. At the same time, the Kafka consensus mechanism is adopted to realise the consensus operation with the participation of multiple subjects to provide the processing capability of real-time data with high throughput and low latency, and the traceability of the quality and safety of black tea products is verified and analysed. George et al. (2019) implemented a food traceability prototype system based on blockchain and product identifiers, which applies the food quality index (FQI) algorithm to generate FQI values based on data obtained from various stakeholders in the food supply chain. The FQI values, in turn, help to determine whether a food is fit for consumption based on specified parameters. In addition to enhancing food (product) traceability, the prototype also helps in grading food quality. Li et al. (2019) improved the degree of decentralisation and consensus mechanism in the public chain, applied the improved scheme to food traceability, and demonstrated the scheme's effectiveness through application cases. Shi et al. (2019) established a blockchain-based fruit and vegetable agricultural products traceability system, where consumers can scan the code to obtain all the information of fruit and vegetable agricultural products from farmland to table, realising the positive and negative bidirectional tracking of agricultural products. Xu et al. (2019) applied the blockchain application programming method the software architecture community proposed to a traceability system named origin chain. They reconfigured the current blockchain application programming method by replacing the central database with a blockchain to improve the traceability system chain and reconstruct the current system by replacing it with a blockchain. The reconfigured originChain enables automated compliance checking and adaptation in product traceability scenarios. Kentaroh et al. (2017) developed a novel product ownership management system using the Ethereum blockchain platform as an add-on to anti-counterfeiting RFID, which can be used to solve the problem that the authenticity of RFID tags cannot be guaranteed in the post-supply chain. Feng (2016) combined RFID with blockchain technology to construct a traceability system and introduced the Big chain DB database to alleviate the blockchain storage pressure. Zeng et al. (2018) proposed a food safety traceability system architecture of IoT + blockchain and used the alliance chain and Hyperledger fabric blockchain development platform to implement the prototype system. The system can monitor the food supply chain in real-time and improve the efficiency and transparency of the supply chain.

3 Private chain-based traceability solution for food production processes

3.1 Private chain consensus algorithm

The private chain consensus algorithm is derived from enhancements made to the RAFT algorithm. Consensus nodes, excluding management, are categorised into candidate and follower sets based on their reliability and stability. The candidate set comprises consensus nodes affiliated with critical departments such as production planning, key production, and factory sales. Meanwhile, the follower set encompasses all other consensus nodes apart from management.

There are four roles involved in the algorithm: leader node, candidate node, follower node, and supervisor node. Only nodes from the candidate set can serve as leader nodes or candidate nodes. The leader node is responsible for recording uplinked data and generating new blocks. Candidate nodes can compete for the leader node position, which serves as a transitional state in scenarios such as re-election due to the expiration of the leader node's term, failure, or detection as a malicious node. At the end of the election process, the candidate node will either become a leader node or a follower node. Follower nodes participate in the leader node election by voting and verify the submitted uplinked data. The supervisor node, representing management, collects feedback on the computation results from both the leader node and follower nodes. It assesses problematic nodes and updates the candidate and follower sets accordingly.

Algorithm 1 Private chain consensus algorithm

Step 1 Election step: A node is selected as the leader node from the candidate set according to the RAFT algorithm, and the rest of the consensus nodes, except the supervisor node, become the follower nodes

Step 2 Verification step: The leader node is responsible for assembling the received request upload data into a block and disseminating it across the entire network for verification. The follower node will verify the leader's broadcast block according to the request upload data received by its node and broadcast the verification result to the whole network, verification encompasses confirming the identity of the leader node, validating the accuracy of the submitted block, and scrutinising the data contained within the block

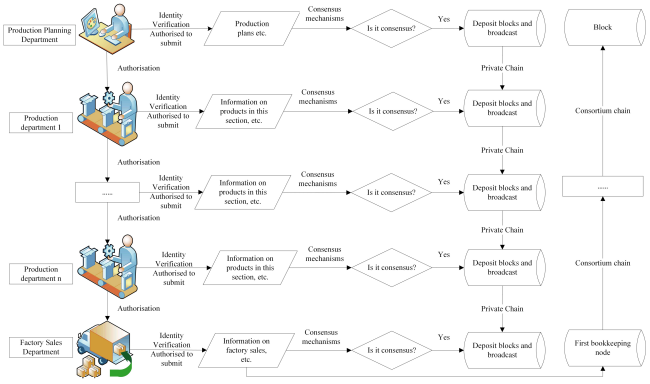
Step 3 Submitting step: The block is broadcast on the whole network if the leader node receives an approval message from a follower node that satisfies the predefined conditions

Step 4 Supervision step: The supervisor node records all nodes with feedback errors and supervises them. If a node has persistent problems, it needs to be further processed, and if the problem node is a candidate set node, it will be removed from the candidate set. If it is a follower node, it can be judged as a malicious node. Suppose the supervisor node receives an approval message from the follower node regarding the leader's request to validate the block that does not meet the predefined conditions or the leader's term expires. The election step is triggered in that case, and the leader node is re-elected

Compared with the traditional RAFT consensus algorithm, the private chain consensus algorithm categorises all consensus nodes into candidate and follower sets based on their reliability and stability. The nodes within the candidate set serve as the primary consensus nodes, as opposed to involving all consensus nodes in this role. This approach leverages the computational and processing capabilities of highly reliable nodes to enhance the stability and operational speed of the blockchain. Moreover, in scenarios where the leader consensus node experiences downtime or is identified as malicious, having a reduced number of candidate state consensus nodes streamlines the re-election process. This reduction in the number of nodes decreases the computational and transmission overhead, thereby accelerating the election process.

In addition, supervisory nodes have been added to receive feedback requested by the leader on the results of the validation blocks and to determine which nodes may be malfunctioning or behaving maliciously based on this feedback, thus increasing the tolerance of the consensus mechanism for malicious nodes. The specific steps of the private chain consensus algorithm are described in Algorithm 1.

Figure 1 Traceability route of food production process (see online version for colours)



3.2 Private chain-based traceability solution for food production processes

The private chain for tracing the food production process adopts an enhanced RAFT consensus algorithm for managing the production process. This process involves the production planning department, production department, management department, and factory sales department, all of which serve as consensus nodes on the private chain responsible for recording data related to food production. The management department generates a pair of public and private keys for each department within the enterprise, with the public key being public and the private key used for authentication and digital signatures. Any consensus node has the right to submit credibility assessment data to the chain and broadcast it to the entire network for verification by other nodes. Upon successful verification, the data block is stored in the local data storage centre, thus forming a consistent ledger. The route for tracing the food production

process based on the private chain is illustrated in Figure 1, with specific steps as follows:

1 The production planning department determines the production task order, signs it with its private key, and then submits all relevant information to the uplink. All consensus nodes verify the uploaded data and signatures according to the private chain consensus algorithm to reach a consensus and store the data blocks in the blockchain, which are then broadcast to form a consistent ledger.

2 The production department obtains the consensus-verified block containing the production task order. It executes the production program according to the task order, submitting the relevant information generated in the food production process, the private key signature of the information, etc., to the chain. Such information includes product traceability code, batch identification, person in charge of product production, origin information, etc. Again, all consensus nodes verify the uploaded data and signatures according to the private chain consensus algorithm to reach a consensus, store the data blocks into the blockchain, and then broadcast them to form a consistent ledger.

3 Food production needs to pass through multiple production departments, each of which can only continue under the authorisation of the previous department. During this process, the generated data and information must be verified by a consensus algorithm before they can be stored on the chain.

4 Upon completion of production, the factory sales department generates a unique food traceability code for each food item and submits the food production time, distributor-related information, and the transfer time and quantity of the food item to the chain. All consensus nodes again verify this information according to the private chain consensus algorithm to reach a consensus and then store it in the blockchain for broadcasting, thus forming a consistent ledger. The factory sales department participates in the consensus determination process as the first bookkeeping node in the consortium blockchain.

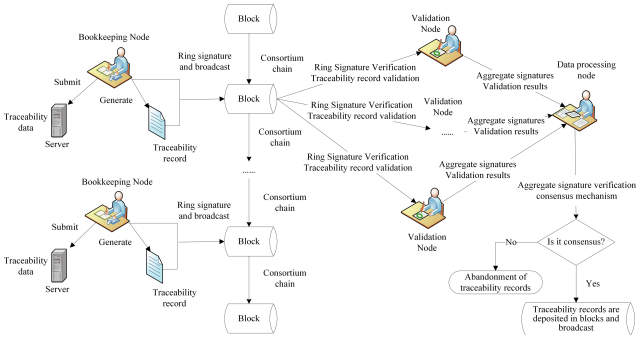
4 Consortium chain-based food distribution process traceability program

4.1 Consortium blockchain consensus algorithm

The consortium chain consensus algorithm (Lee et al., 2021) is a fusion of PBFT with aggregate signature and ring signature technologies. Each consensus round randomly selects a validation node to act as the speaker. The speaker can be determined according to the block height, and other verification processing nodes are councillors. Let p be the current speaker number and the member number i. Each consensus generates a block with signatures of at least $n–f$ validation nodes, where n is the number of validation nodes, and f is the number of validation nodes that do not pass the current record. Suppose the system requires that the time interval for each block generation is t, the current block height is h, the current data number is v, and the current data is recorded as a block.

Compared with the traditional PBFT consensus algorithm, the consortium chain consensus algorithm supports nodes' dynamic joining and exiting by forming a ring when the bookkeeping nodes perform ring signatures and simultaneously enhances privacy protection. The performance of the traceability system is improved by reducing the number of signature verifications through the aggregated signature technique. The consortium blockchain consensus algorithm is shown in Algorithm 2.

Figure 2 Traceability route of food circulation process (see online version for colours)



Algorithm 2 Consortium chain consensus algorithm

Step 1	The bookkeeping node forms a ring with itself and some or all of the other bookkeeping nodes and broadcasts to the whole network the submission of the up-linked data with the sender's ring signature
Step 2	All validation points listen independently to the up-linked data submitted by the whole network
Step 3	After the time t, the Speaker sends ‹Request, h, v, p, block, ‹block›$_{\sigma p}$›, where Request is the initiating request and ‹block›$_{\sigma p}$ is the aggregated signature of the Speaker verified by block in the aggregated signature algorithm
Step 4	When councilor i receives the proposal, if it passes the verification, it sends ‹Response, h, v, i, ‹block›$_{\sigma i}$ ›, where Response represents the message feedback and ‹block›$_{\sigma i}$ is the aggregated signature of councillor i that passes the block verification in the aggregated signature algorithm.
Step 5	Data processing node receives at least n-f ‹block›$_{\sigma i}$ and reaches consensus, performs aggregated signature verification, and if it passes the verification, publishes the complete block to the consortium blockchain; confirms the next Speaker based on the block height and starts the next round of consensus

4.2 Consortium chain-based food distribution process traceability program

For tracing the food distribution process based on the consortium blockchain, an enhanced PBFT consensus algorithm is employed for tracing the delivery process.

Food distribution encompasses the entire process of transferring food from production to consumption, involving various stakeholders such as manufacturers, distributors, regulatory agencies, retailers, and consumers. The registration authority plays a pivotal role in managing the consortium chain network by overseeing the admission and departure of manufacturers, distributors, and retailers. It creates comprehensive profiles for authorised participants, including corporate information, addresses, qualifications, and certifications, and assigns two pairs of public and private keys. One pair facilitates aggregate signatures, reducing communication in the consensus process, while the other pair enables ring signatures to maintain the anonymity of bookkeeping node addresses. Consumers only have query privileges in the food distribution process.

Apart from the registry and consumer nodes, the remaining nodes are categorised into bookkeeping, verification, and data processing nodes. Bookkeeping nodes generate food traceability data and traceability records and submit them to the blockchain for storage. Verification nodes are used to verify the traceability records submitted by bookkeeping nodes. The data processing node then uses a consensus algorithm to detect the validation result of the validation node to obtain the consensus result. In addition, the data processing node is responsible for receiving food label query requests sent by the client and returning the queried traceability record results.

The traceability route based on the consortium blockchain for the food distribution process is shown in Figure 2, and the following are the specific steps:

1 After evaluating the trustworthiness metric, the bookkeeping node generates traceability data containing the food traceability code and uploads it to the corresponding server for storage. The traceability data includes the food traceability code, the identity information of the food transferring party and its Ethernet account address, the time and quantity of the food transfer, etc. The food producer (factory sales department) is the first bookkeeping node.

2 The bookkeeping node generates a traceability record based on the traceability data, and some bookkeeping nodes in the consensus network generate ring signatures to confirm the traceability record and then submit it to the chain and broadcast it across the network. The traceability records include timestamps, server address identifiers, identity information of the food transferring party and Ethernet account address, and hash values generated from the traceability data. The ring signature ensures the anonymity of the bookkeeping node address.

3 The verification node checks and verifies whether the ring has signed the tracking and tracing record, and if it passes the verification, it obtains the corresponding food tracking and tracing data according to the corresponding server address identification recorded in the tracking and tracing record.

4 The verification node obtains all historical tracking and tracing records related to the food on the chain based on the food traceability code in the tracking and tracing record, obtains the corresponding data storage server based on the historical tracking and tracing record, and then obtains the tracking and tracing data related to the food and verifies its validity.

5 In the verification process, the authenticity of the food traceability data is judged based on the identity information of the food transferring party and the Ethernet account address, digital signature, timestamp, and other information.

6 The verification node signs the traceability data and its verification results.

7 The data processing node receives and verifies traceability data using private key signatures from various verification nodes. The aggregated signatures will be performed as the number of validated nodes reaches the specified threshold. All the consensus network nodes will determine the obtained verification results and the signature by consensus according to the consensus algorithm of the consortium chain.

8 When the collected verification results and the number of signatures meet the consensus requirements, consensus is achieved. The traceability record is then stored on the chain, consensus results are broadcasted, and all other bookkeeping nodes update the traceability record to their data ledgers. Conversely, if consensus cannot be reached, the traceability record will be discarded.

9 Upon receiving a query request from the consumer, the traceability records related to the food are obtained based on the food traceability code. Then, all relevant traceability data is finally obtained. In addition, the data processing node needs to compare the hash value of each historical traceability data obtained with the relevant data and judge whether the obtained traceability data has been falsified.

The food circulation process entails recording extensive information, including the distributors and retailers involved, the logistics routes traversed, and timestamps for incoming and outgoing activities at various points. Given the substantial volume of data, uploading all information to the blockchain would significantly impact system performance. Therefore, only essential data is uploaded to the chain, while supplementary data such as videos and photos are stored offline on servers. The blockchain maintains specific mappings to these offline resources rather

than storing the data directly, ensuring efficient management of information while maintaining traceability.

5 Food quality and safety traceability system based on trusted dual chain

5.1 System architecture

Blockchain can be categorised into public, consortium, and private chains according to the participation access mechanism. In public chains, anyone can read and send transactions, However, due to the requirement for a strict consensus mechanism, the consensus process directly impacts the data processing speed, leading to lower efficiency. In consortium blockchains, the consensus process is managed by several major nodes, which ensures the organisation's operational efficiency while considering the system's security and the common maintenance characteristics of its members. Private chains limit participants to individuals or within companies. While they exhibit centralised control externally, they possess high internal decentralisation capabilities. This allows for fully customisable policies and excellent processing speed.

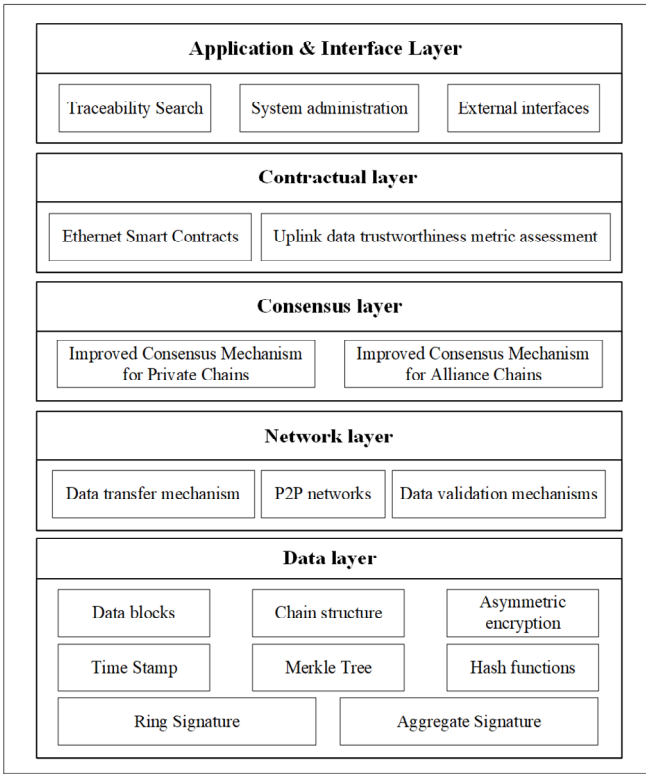
The food quality tracking and traceability system encompasses all stages of food production and distribution. Due to the proprietary nature of food production processes, research in private chain-based systems predominantly centres on tracing the food production process itself. Conversely, the food distribution process involves various stakeholders such as logistics providers, distributors, retailers, and consumers. Hence, research based on consortium blockchains is more suitable for tracing the intricacies of the food distribution process.

The trusted dual-chain-based food quality and safety tracking and traceability system includes an application and interface layer, contract layer, consensus layer, network layer, data layer, and other components, as shown in Figure 3.

In the contract layer, functions such as on-chain user management, smart contract management, and data management services are realised. Upstream user management authorises relevant users to join or leave the consensus network, which includes all individuals or organisations involved in the entire supply chain, from food production to sales. Smart contract management includes writing the corresponding smart contract according to the actual business requirements and realising the deployment and update of the smart contract and other operations. Only smart contracts can access the underlying data ledger. In addition, the contract layer allows the writing of various scripts and codes, which will automatically execute the smart contract or script code when specific agreed conditions are met. At the same time, the contract layer also needs to assess the trustworthiness of the uplinked data to allow data that passes the assessment to be uplinked. Otherwise, it will be rejected for uplinking.

In the consensus layer, an improved private chain-based consensus mechanism and an improved Consortium Blockchain-based consensus mechanism are included for reaching consensus in the food production and distribution process.

Figure 3 Architecture diagram of the system



In the network layer, the networking method between blockchain nodes is specified. A P2P network is used to interconnect the nodes to ensure that any node in the system can participate equally in the whole data operation process. The network layer also includes data transmission and authentication mechanisms.

In the data layer, the data storage function is mainly realised to ensure the security of accounts and transactions. Specifically, it includes data blocks, digital signatures, chain structure, asymmetric encryption, hash functions, time stamps, Merkle trees, and other related technologies.

5.2 System module

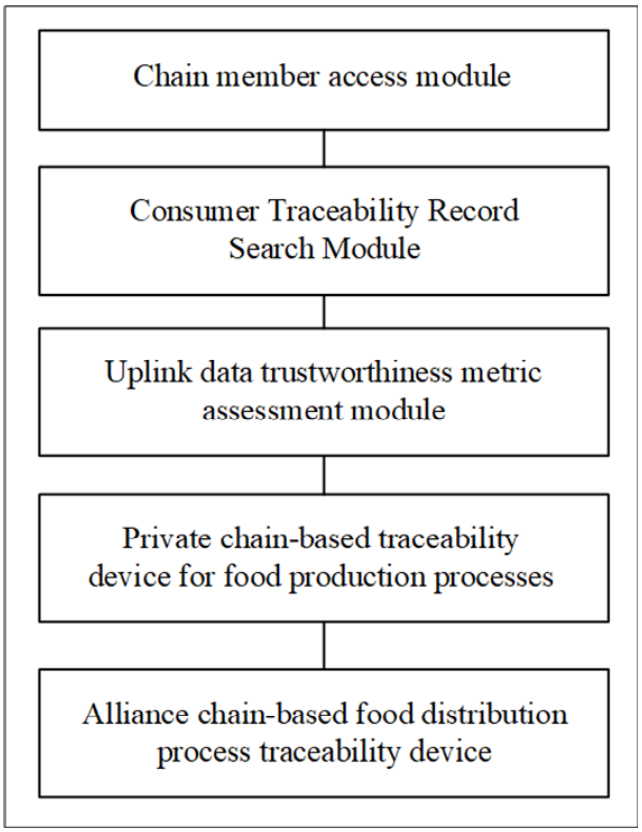
The trusted dual-chain-based food quality and safety tracking and tracing system are divided into five modules, as shown in Figure 4: on-chain member access module, on-chain data credibility metric assessment module, private chain-based food production process traceability module, consortium blockchain-based food distribution process traceability module, and consumer traceability record query module.

In the on-chain member access module, the on-chain members (including food-related organisations or individuals) are comprehensively assessed by a third-party certification organisation to obtain their initial creditworthiness. Then, according to the consensus degree of their uploaded data, the creditworthiness of the on-chain

members is updated, and the credit metric model of the on-chain members is finally formed.

The uploaded data credibility metric assessment module is used to assess the tracking and tracing data that needs to be submitted for uploading. This evaluation is based on the uplinked data credibility metric model and is used to determine the credibility of the uplinked data. If it passes the assessment, the data will be submitted to the uplink, and a consensus judgment will be made on the traceability data according to the consensus mechanism.

Figure 4 Schematic diagram of system modules



Finally, in the consumer traceability record query module, when the system receives a traceability code query request message from the user, it will query the data block based on the code to obtain all historical record information of the food products related to the traceability code, and then feedback the query results to the user.

Table 1 System configuration

CPU	Intel(R) Core (TM)i7-9750H CPU@2.60GH
RAM	4.00 GB
Operating systems	Ubuntu 20.04.1
Hard disk	50 GB
IDE	Geth1.9.24-stable, IPFS 0.7.0

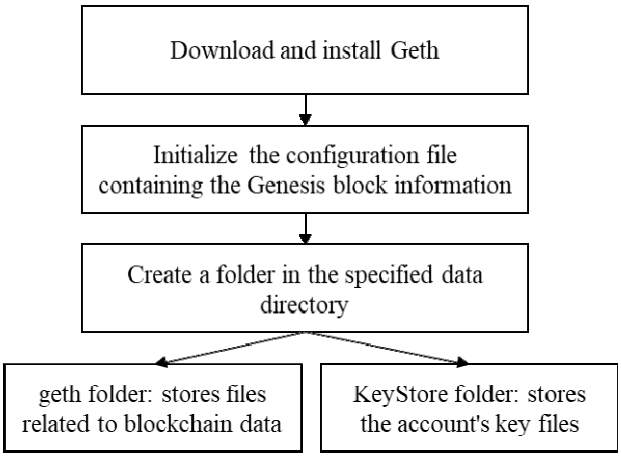
5.3 System implementation

The system is based on the Ethernet blockchain platform, and the hardware configuration and software platform used to build the system are shown in Table 1.

The specific implementation steps of the blockchain tracking and tracing system and data storage are as follows:

Step 1 Build the private chain

Figure 5 Build the private chain



Step 2 Mining

- Enter the command Geth console.
- Execute miner.start(1) to mine.
- Wait for the DAG file to be generated and start mining.

Step 3 New nodes join the private chain

New nodes joining can link to the private chain network through the Ethernet client to synchronise and update the block information.

Step 4 Write the smart contract

According to the business logic and compile the smart contract on Remix-IDE with the help of an Ethernet wallet (the Kovan test network is used in this paper).

Step 5 Executing the smart contract

Load and execute the content of the contract through EVM to realise the interactive application with the outside world.

Step 6 File upload and storage using IPFS

Installation and startup of IPFS nodes, uploading files in video, text, image, and other information formats via IPFS.

Figure 6 New nodes join the private chain

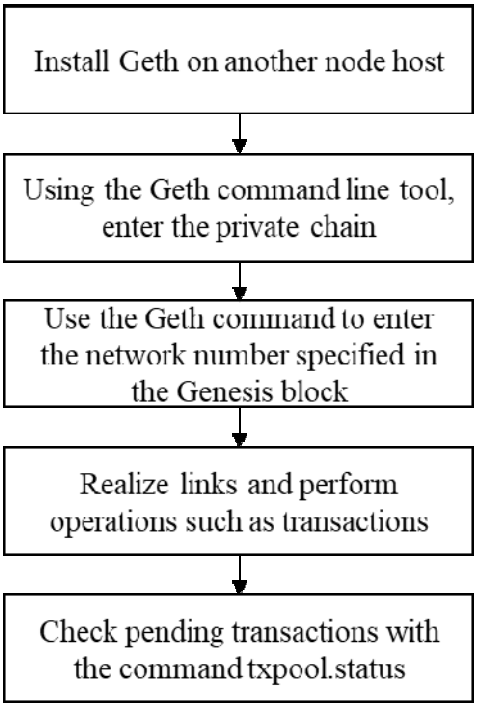
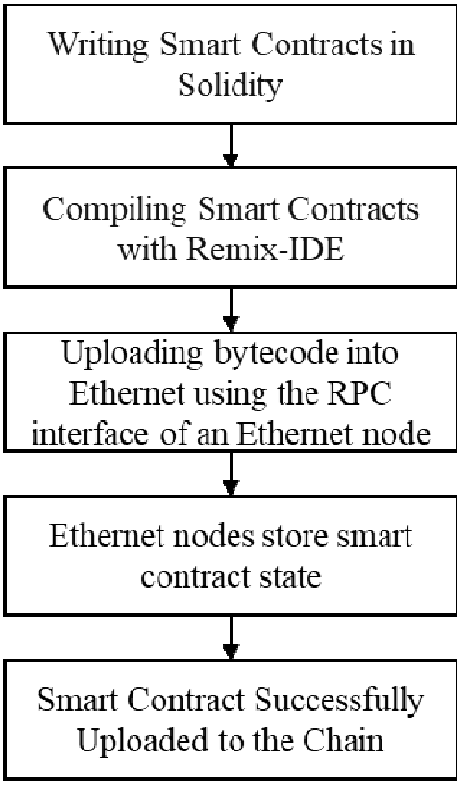


Figure 7 Write the smart contract



6 System advantage analysis

6.1 Analysis of system complexity

In the food quality and safety traceability system proposed in this paper, an enhanced RAFT algorithm is used to trace the food production process on a private chain, while an improved PBFT consensus algorithm is employed to trace the food flow process on a consortium chain. Therefore, in analysing the complexity of the proposed methods, our main focus is on the enhanced RAFT algorithm and the improved PBFT consensus algorithm.

Firstly, concerning the improved RAFT algorithm for tracing the food production process on a private chain, the communication complexity of the traditional RAFT algorithm is generally low. Its consensus process includes leader election and log replication steps. Assuming the total number of nodes in the cluster is n, the communication count during the log recording phase is n–1, and during the data submission phase is also n–1. Therefore, the total communication count is $2n$–2. Thus, the complexity of the traditional RAFT algorithm is $O(n)$.

Our enhanced RAFT algorithm divides the consensus nodes into candidate sets and follower sets, with consensus nodes in the candidate set acting as candidate-state nodes. This improvement may reduce the complexity of leader election, especially when highly reliable consensus nodes participate in the candidate group. In cases where leader-state consensus nodes fail or are detected as malicious, the re-election process may become faster due to the relatively fewer candidate-state consensus nodes, thereby reducing the time required for computation and transmission. Additionally, the introduction of supervisor nodes to validate block feedback results and identify node issues or malicious nodes, while increasing communication overhead, maintains the complexity of the improved RAFT algorithm at $O(n)$.

For the improved PBFT algorithm tracing the food flow process on a consortium chain, the communication complexity of the traditional PBFT algorithm is relatively high. In the PBFT algorithm, the consensus process consists of three stages: pre-prepare, prepare, and commit, with corresponding communication counts of n, n^2, and n^2 respectively. Therefore, for the PBFT algorithm, the total communication count required for a complete consensus process is $l_1 = 1 + n + n^2 + n^2 + n = 2n^2 + 2n + 1$. The complexity of the improved PBFT algorithm is $O(n^2)$.

Our improved PBFT algorithm enhances the consistency protocol process by introducing aggregate signatures, despite adding consensus process stages (including pre-prepare, prepare, pre-commit, and commit, totalling four stages), it reduces the communication complexity. The total communication count required for a complete consensus process is $l_2 = 1 + n + n + \mathrm{n} + n + 1 = 4\,n + 2$. Therefore, the complexity of the improved PBFT algorithm is $O(n)$.

Based on the analysis above, it can be concluded that the overall complexity of the methods we proposed is $O(n)$, which demonstrates significant advantages in improving system performance and efficiency.

6.2 Compared to traditional traceability systems

6.2.1 A shared distributed ledger

Traditional food traceability often adopts the form of paper or electronic documents, recording the relevant information from the origin of food to the hands of the final consumer in all aspects. However, this form of information recording is often more dispersed. The recording process is simple and requires a large workforce and time to maintain, while the opacity of the information can easily lead to delayed and timely information recording. The blockchain has decentralised characteristics, which can ensure that all participants in the entire consensus network themselves have a copy of the same data ledger (Pilkington, 2016). The relevant participants jointly negotiate to generate, verify, and maintain the data ledger. If the data in the distributed ledger undergoes update or write operations, real-time data synchronisation is carried out through the network to maintain the distributed ledger's consistency and solve the trust crisis problem.

6.2.2 Tamper-proof

Traditional traceability system records are stored in a centralised database, and unauthorised access or data leakage may lead to leakage of sensitive information and malicious tampering. Blockchain technology can ensure that once the data is uploaded to the chain, it will generate a unique hash value corresponding to the data. The authenticity and reliability of data information are effectively guaranteed.

6.2.3 High efficiency and low cost of traceability

The flow of information in traditional systems is usually not transparent enough and lacks traceability. It is not easy to realise real-time monitoring of the food circulation process. Once a food safety problem occurs, the traceability system often cannot quickly locate the source of the problem, and it is not easy to trace it back to the specific responsible link and responsible person. The introduction of blockchain technology traceability system can be produced from food production until the sale of the relevant information, including production, circulation, and other aspects of the relevant responsible person and other specific time information all on the chain record preservation (Lu, 2019), once a food safety accident occurs, it can quickly lock the food safety problems related to the person responsible for the relevant food and food-related information, and timely sort out the source of the food safety accidents, to avoid the occurrence of more people's lives and properties caused by the losses.

6.3 Compared to existing blockchain traceability systems

6.3.1 Trustworthiness assessment of on-chain data

Most of the existing blockchain traceability systems emphasise the benefits of blockchain technology and the organisation's value, but little attention is paid to the trustworthiness of the uplinked data. This paper introduces the trustworthiness metric model of uplinked data (Tao et al., 2022) as an important module of the food quality and safety tracking and traceability system. By assessing the trustworthiness of the uplinked data, any data that fails the assessment will be rejected for uplinking. This process enhances the overall trustworthiness of the uplinked data, fostering greater reliance from the public on the information within the system. Consequently, reliance solely on information from third-party quality inspection organisations is diminished.

6.3.2 Improve the consensus mechanism and enhance the system performance of the traceability system as a whole

Most existing blockchain traceability systems adopt the consortium chain and use the Kafka consensus model (Meng and Zhanc, 2021) or PBFT consensus algorithm (Wang et al., 2019). In order to improve the overall performance of the system, this paper improves the RAFT and PBFT. In comparison to the traditional RAFT consensus algorithm. The improved RAFT consensus algorithm categorises all consensus nodes into candidate and follower sets based on their reliability and stability. Nodes with high reliability are further segregated into candidate groups, leveraging their computational and processing capabilities to enhance the stability, computational efficiency, and transmission speed of the blockchain. In scenarios where a consensus node in a leader state fails or is identified as a malicious node, the reduced number of nodes in the candidate state accelerates the re-election process, minimising the time required for computation and transmission. Additionally, the introduction of a supervisor node enhances the fault tolerance of the consensus mechanism by receiving block feedback results related to the leader's verification request and identifying nodes with issues or malicious intent. Compared to the traditional PBFT consensus algorithm, the improved PBFT consensus algorithm facilitates dynamic node joining and exiting. This is achieved through the nodes forming their own rings during the signing of ring signatures by the bookkeeping nodes. Simultaneously, the algorithm reinforces privacy protection and reduces the number of signatures checking times using aggregation signature technology, thereby enhancing the performance of the traceability system. The application of the improved consensus mechanism to the food quality and safety tracking and tracing system better aligns with the actual requirements of food quality and safety tracking and tracing.

6.3.3 A comprehensive food traceability system is constructed

Most of the previous implementations of food safety traceability systems on blockchain platforms are based on the consortium chain alone, such as in the food traceability chain proposed by Li et al. (2019), which selects the consortium chain to reduce the problem of resource wastage and at the same time, simplifies the recording ledger and reduces the bandwidth required for system operation. Zeng et al. (2018) also adopts the alliance chain model and the super ledger dual chain development platform to realise food traceability. This paper proposes a food quality and safety tracking and tracing system based on dual chains (private chain and consortium chain). In this system, the private chain is used to trace the food production process, and the consortium chain is used to trace the food distribution process. Aggregate signature technology improves the system performance, while ring signature enhances the privacy protection of the system. This system covers all aspects of the food industry chain, which not only improves the privacy protection and data security reliability of the food quality and safety tracking and tracing process but also improves the scalability and traceability efficiency of the system, and at the same time protects the commercial interests of all parties in the chain.

6.4 Industrial significance of the system

1 Enhancing food safety: The improved RAFT and PBFT consensus algorithms, along with the dual-chain system based on blockchain technology, enable precise tracing of the entire process of food production and distribution. This aids in promptly identifying and addressing potential food safety issues, thereby enhancing the overall food safety of the supply chain.

2 Data reliability and tamper resistance: The introduction of reliability assessment modules and aggregated signature techniques effectively resolves issues regarding data reliability on the blockchain. Simultaneously, it ensures the authenticity and tamper resistance of tracing information, crucial for safeguarding the integrity and credibility of the traceability system.

3 Reducing business risks: The application of enhanced consensus algorithms and dual-chain systems helps mitigate information asymmetry and business risks within the food supply chain. By improving the performance and credibility of the traceability system, it reduces the occurrence of commercial disputes and losses arising from inaccurate or tampered information.

7 Conclusions and future work

In this paper, we propose a novel solution for food quality and safety traceability by introducing a dual-chain system, enhancing the efficiency and reliability of food safety management. In comparison to predominantly consortium-based blockchain tracing systems, our innovative approach not only aids regulatory bodies in better supervising production processes but also helps businesses respond promptly to food safety incidents, reducing potential risks and losses.

In the design of the traceability solution for food production and distribution processes, we introduce improved RAFT and PBFT consensus algorithms. Through the optimisation of consensus algorithms, we enhance system stability, scalability, and real-time performance, ensuring the accuracy and integrity of traceability data. Additionally, the introduction of a reliability index assessment module and aggregate signature technology further enhances the performance and security of the traceability system. The reliability index assessment module assists users in evaluating the credibility of on-chain data, reducing risks associated with information uncertainty. The aggregate signature technology reduces signature verification costs, improves system processing efficiency, protects user privacy, and strengthens system acceptability and utility.

In summary, our research brings significant innovation and improvement to the field of food safety traceability, providing stakeholders with a more reliable and efficient solution. We believe that this work will have a positive impact on the future of food safety management and regulation, contributing to the development of the industry and the well-being of the public.

Future work will focus on further optimising the implementation of the system prototype and completing on-site deployment to ensure the feasibility and effectiveness of the system. As product-related data and new product data are uploaded, the system will accumulate a large amount of data, which may affect the overall operational performance of the system. Therefore, further optimisation of consensus algorithms and storage technologies is necessary to improve the overall performance of the system.

Acknowledgements

This work was supported by the National Science Foundation of China under (Grant Nos. 61906175); the Academic Degrees & Graduate Education Reform Project of Henan Province (Grant No. 2021SJGLX115Y), the Key Research Project of Colleges and Universities of Henan Province (Grant No. 22A520013), and Zhengzhou University of Light Industry Doctoral Research Initiation Fund (Grant No. 2019BSJJ007).

References

Abeyratne, S. and Monfared, R. (2016) 'Blockchain ready manufacturing supply chain using distributed ledger', *International Journal of Research in Engineering and Technology*, Vol. 5, No. 9, pp.1–10.

Benaddi, A., Cohen, O., Matyjaszewski, O., Silverstein, K. and Raft, M.S. (2021) 'Polymerization within high internal phase emulsions: porous structures, mechanical behaviors, and uptakes', *Polymer: The International Journal for the Science and Technology of Polymers*, Vol. 213.1, No. 20, p.123327.

Bin, L. and Jiang, J. (2020) 'Security analysis of Paxos mechanism design based on game theory', *IEEE International Conference on Information Technology, Big Data and Artificial Intelligence IEEE*.

Chen, J., Luo, D., Tang, C. et al. (2022) 'Blockchain-based trusted traceability system for agricultural internet of things', *Journal of Information Security*, Vol. 7, No. 2, pp.139–149.

Chen, Y-Y. et al. (2016) 'Analysis and design of a food traceability system based on IoT technology', *Journal of Dongguan Institute of Technology*, Vol. 23, No. 1, pp.7–9.

Cortier, V. et al. (2017) 'Machine-checked proofs of privacy for electronic voting protocols', *2017 IEEE Symposium on Security and Privacy (SP) IEEE*.

Dai, F. et al. (2017) 'From Bitcoin to cybersecurity: a comparative study of blockchain application and security issues', *International Conference on Systems and Informatics*, pp.975–979.

Deng, C. (2008) *Research on Food Safety Regulatory Mechanism in China*, Zhongshan University.

Dixit, P. et al. (2020) 'An overview of blockchain technology: architecture, consensus algorithm, and its challenges', *Blockchain Technology and the Internet of Things*, p.26.

Feng, T. (2016) 'An agri-food supply chain traceability system for China based on RFID & blockchain technology. 13th international conference on service systems and service management (ICSSSM)', *Proceedings of 13th International Conference on Service Systems and Service Management (ICSSSM)*, Piscataway: IEEE, pp.1–6.

Gang, H. et al. (2022) 'Blockchain-based attribute-based keyword searchable encryption for health cloud system', *International Journal of Embedded Systems*, Vol. 15, No. 6, pp.493–504.

Gao, K., Liu, Y., Xu, H.Y. et al. (2020) 'Design and implementation of food supply chain traceability system based on hyperledger fabric', *International Journal of Computational Science and Engineering*, Vol. 23, No. 2, pp.185–193.

George, R.V., Harsh, H.O., Ray, P. et al. (2019) 'Food quality traceability prototype for restaurants using blockchain and food quality data index', *Journal of Cleaner Production*, Vol. 240, No. 10, p.118021.

Kentaroh, T., Mathiopoulos, P.T., Iwao, S. et al. (2017) 'A novel blockchain-based product ownership management system (POMS) for anti-counterfeits in the post supply chain', *IEEE Access*, Vol. 13, No. 1, pp.17465–17477, DOI: 10.1109/ACCESS.2017.2720760.

Lee, W-K. et al. (2021) 'Post-quantum blockchain for secure communication in IoT-based smart home services', *International Journal of Embedded Systems*, Vol. 14, No. 5, pp.509–524.

Li, J., Yu, Y., Hu, S., Yang, S., Zhao, S. and Zhang, C. (2021) 'A blockchain-based authority management framework in traceability systems', *International Journal of Computational Science and Engineering*, Vol. 24, No. 1, pp.42–54.

Li, M., Wang, D., Zeng, X. et al. (2019) 'Food safety tracing technology based on block chain', *Food Science*, Vol. 40, No. 3, pp.279–285.

Liu, S., Lei, M.R., Xu, L. et al. (2022) 'Development of reliable traceability system for agricultural products quality and safetybased on blockchain', *Transactions ofthe Chinese Society for Agricultural Machinery*, Vol. 53, No. 6, p.11.

Lu, Y. (2019) 'The blocckchain: state-of-the-art and research challenges', *Journal of Industrial Information Integration*, Vol. 15, No. 10, pp.80–90.

Meng, W. and Zhanc, D. (2021) 'Optimization scheme for hyperledger fabric consensus mechanism', *Acta Automatica Sinica*, Vol. 47, No. 8, pp.1885–1898.

Onireti, O., Zhang, L. and Imran, M.A. (2019) 'On the viable area of wireless practical byzantine fault tolerance (PBFT) blockchain networks', *IEEE Global Communications Conference*, pp.1–6.

Pilkington, M. (2016) 'Blockchain technology: principles and applications', *Research Handbook on Digital Transformations*, pp.225–253, DOI: 10.4337/9781784717766.00019.

Ramos, L.F.M. and Silva, J.M.C. (2019) 'Privacy and data protection concerns regarding the use of blockchains in smart cities', *The 12th International Conference*.

Shi, L., Zhang, F. and Liu, W. (2019) 'Research on blockchain-based traceability system of fruit and vegetable agricultural products', *Rural Economy and Science-Technology*, Vol. 30, No. 15, pp.166–169.

Tao, H.W. et al. (2022) 'The credibility measurement method of food safety on-chain data based on blockchain', *Journal of Internet Technology*, Vol. 23, No. 4, pp.719–725.

Wang, Y., Cai, S., Iin, C. et al. (2019) 'Study of blockchains's consensus mechanism based on credit', *IEEE*, Vol. 7, No. 1, pp.10224–10231, DOI: 10.1109/ACCESS.2019.2891065.

Wang, Z., Liu, P., Song, C. et al. (2020) 'Research on flexible and trusted traceability system for agricultural products based on blockchain', *Computer Engineering*, Vol. 46, No. 12, pp.313–320.

Xu, R. et al. (2018) 'Progress in the application and research of food safety traceability system based on blockchain technology', *Journal of Food Safety and Quality*, Vol. 11, No. 20, pp.7610–7616.

Xu, S. et al. (2023) 'A privacy-preserving and efficient data sharing scheme with trust authentication based on blockchain for mHealth', *Connection Science*, Vol. 35, No. 1, pp.1–23, DOI: 10.1080/09540091.2023.2186316.

Xu, X.W., Lu, Q.H., Liu, Y. et al. (2019) 'Designing blockchain-based applications a case study for imported product traceability', *Future Generation Computer Systems*, Vol. 92, No. 1, pp.399–406, DOI:10.1016/j.future.2018.10.010.

Zeng, S-Q., Huo, R., Huang, T. et al. (2021) 'A review of blockchain technology application areas and problems', *Technology Innovation and Application*, Vol. 11, No. 12, pp.134–136 + 139.

Zeng, X., Peng, Y. and Wang, Q. (2018) 'Research on food safety traceability system based onloT and blockchain technology', *Food and Machinery*, Vol. 34, No. 9, pp.100–105.

Zhao, W. (2019) 'Research on agri-food safety traceability system based on blockchain technology', *Research on Technical Economy and Management*, Vol. 40, No. 1, pp.16–20.