TSINGHUA SCIENCE AND TECHNOLOGY
ISSN 1007-0214 07/14 pp500–510
DOI: 10.26599/TST.2022.9010030
Volume 28, Number 3, June 2023

A Review of Blockchain Solutions in Supply Chain Traceability

Xiaofeng Zhang and Li Ling*

Abstract: The supply chain plays an important role in daily life, and its traceability ensures product quality and safety. Therefore, an efficient and reliable solution to improve supply chain traceability is urgently needed. Because of its advantages of being decentralized, tamper-proof, and transparent, the emerging blockchain technology should address the problems of unreliable data and low tracking efficiency in traditional traceability systems. This paper explores blockchain-based supply chain traceability solutions, reviews recent research, and identifies challenges. First, the basics of blockchain are introduced, and the traditional traceability model and stakeholder needs are described. Then, the existing publications and enterprise applications are reviewed and analyzed in detail. Using blockchain is found to bring many benefits. It is also found that the current academic solutions are mostly based on mainstream blockchain platforms and lack specific and comprehensive evaluation. Finally, challenges and future research questions are discussed. Future research could focus on designing targeted consensus mechanisms, designing appropriate access control, the role of regulators in the supply chain, etc. This review shows that blockchain has great potential to address traceability issues, but many challenges remain.

Key words: blockchain; supply chain; traceability

1 Introduction

A supply chain is a chain structure composed of many nodes, such as suppliers, manufacturers, and customers. The nodes of a supply chain may be distributed worldwide because of globalization, and the chain structure can become highly intricate. The traceability of supply chains is crucial to each node. For instance, consumers can ensure product quality and safety by knowing the source of food, medicine, and other products. Therefore, the demand for efficient and reliable supply chain traceability is strong. The existing traceability methods are primarily based on centralized systems, and each enterprise node in a supply chain traditionally maintains its product information database. Such methods usually lack transparency and are vulnerable to data manipulation. In addition, the traced information becomes unreliable because of the low transparency and high susceptibility to tampering. Moreover, the traditional traceability system is inefficient and slowly realizes product recall because of its complicated procedures.

Blockchain technology with traceability and transparency provides a path for addressing traceability issues. After the seminal paper on Bitcoin by Nakamoto[1], blockchain, as the key underlying technology of Bitcoin, has received extensive attention from scholars. Blockchain is a distributed ledger technology that uses cryptographic algorithms to construct data blocks and links the blocks together through hashing, making the blockchain tamper-proof and traceable. Recently, blockchain technology has boosted the development of many nonfinancial sectors, including the Internet of Things[2, 3], healthcare[4, 5], and energy[6, 7]. The global investment in blockchain increases annually and is expected to reach 12.4 billion US dollar by 2022, among which the expenditure in the supply chain area should account for the largest

• Xiaofeng Zhang and Li Ling are with the School of Information Science and Technology, Fudan University, Shanghai 200433, China. E-mail: 20210720070@fudan.edu.cn; lingli@fudan.edu.cn.
∗ To whom correspondence should be addressed.
Manuscript received: 2022-02-17; revised: 2022-08-02; accepted: 2022-08-08

portion[8]. Research on blockchain-based supply chains has recently been booming. For example, Gurtu and Johny[9] studied the potential contribution of blockchain in supply chain management. Högberg et al.[10] discussed the driving factors of blockchain applications in supply chains, including security and data traceability. Pournader et al.[11] showed a series of applications of blockchain in supply chains. Kamilaris et al.[12] explored the impact of blockchain technology on agriculture and food supply chains.

Although some academic explorations have been conducted, most people, including supply chain stakeholders, remain unaware of blockchain technology and its value in supply chain traceability. To provide a clearer picture of the current applications and possible further research questions, this paper reviews the existing literature and industrial examples using blockchain technology to achieve supply chain traceability and explores the related challenges. To our best knowledge, this review is the first with a specific focus and detailed analysis of blockchain applications in supply chain traceability. Hence, we believe this paper can substantially contribute to this strand of research. The rest of this paper is organized as follows. Section 2 introduces the basis and characteristics of blockchain. Section 3 presents the traditional traceability model and the specific needs of supply chain participants for traceability. Section 4 analyzes a series of academic solutions and industrial cases that use blockchain to achieve traceability in supply chains. Section 5 discusses the current challenges in implementing blockchain and possible research interests. Section 6 provides a summary and outlook.

2 Blockchain Basics and Features

2.1 Blockchain basics

A blockchain is a data chain that can extend infinitely on a timeline. It constructs data blocks to record and store information using cryptographic algorithms and links the blocks to form a distributed ledger through hash pointers. The block structure is shown in Fig. 1, where the block header is associated with the block body to form a complete block, and two blocks are linked through the block headers to form a blockchain. The "T" and "H" in Fig. 1 stand for the transaction and hash value, respectively. The underlying technologies of blockchain include cryptography, consensus mechanisms, and smart contracts.

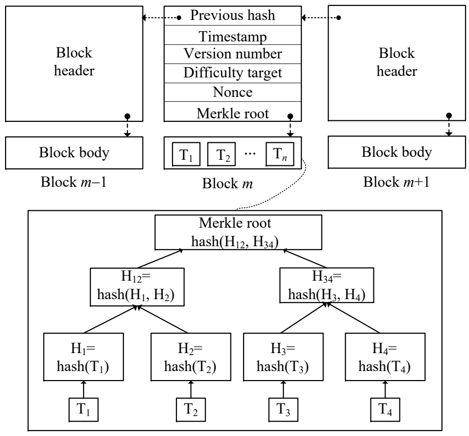

Fig. 1 Blockchain structure.

(1) Cryptography technologies are used to construct the blockchain and guarantee the security of the blockchain network. They mainly include asymmetric key cryptography and hash functions[13]. More specifically, asymmetric key cryptography includes Rivest-Shamir-Adleman cryptography (RSA)[14], ellipse curve cryptography (ECC)[15], and Elgamal[16]. Additionally, the Bitcoin blockchain uses the ECC algorithm. The rationale of how the ECC algorithm transmits confidential data is explained as follows. Denoting the private and public keys as k and K, respectively, we have $K = kG$, where G is the base point. When encrypting with the public key, the plaintext is encoded to point M on the elliptic curve, and a random number r is generated. The ciphertext C_1 and C_2 are calculated according to Eqs. (1) and (2), respectively. In decryption, $M' = C_1 - kC_2$ is calculated, and the proof of principle of decryption operation is shown in Eq. (3), so the plaintext can be obtained after M' decoding. A hash function can be used to convert the input data with flexible length into a message digest with a fixed length, and the link between the two blocks can be established through the message digest and the hash pointer.

$$C_1 = M + rK \tag{1}$$

$$C_2 = rG \tag{2}$$

$$C_1 - kC_2 = M + rK - k(rG) = M + r(K - kG) = M \tag{3}$$

(2) Common consensus mechanisms include proof of work (PoW)[1], proof of stake (PoS)[17], and practical byzantine fault tolerance (PBFT)[18]. The PoW mechanism compares the computing power of mining nodes. Only by attacking more than 51% of the computing power of the entire network can the validity of

the blockchain be destroyed. The corresponding process is shown in Fig. 2. On the other hand, creating new blocks in the PoS mechanism is related to the number of tokens owned by nodes and does not require much computing power, so it is less effective. The PBFT algorithm emphasizes that even if f failed nodes are in the network, the data consistency can still be safeguarded as long as the total number of nodes is not less than $3f+1$.

(3) A smart contract is a set of digitally defined engagements and a protocol on which contract participants can enforce these engagements. After smart contracts are deployed to the blockchain, once a transaction meets predetermined conditions, the relevant contract terms are automatically executed without third-party involvement[19].

2.2 Classification

Blockchains can be classified into public blockchains, private blockchains, and consortium blockchains according to their degree of decentralization, as shown in Table 1. A public blockchain, also called a permissionless chain, achieves true decentralization, while a private blockchain and a consortium blockchain belong to a permissioned chain. Currently, the mainstream blockchain platform prototypes include Bitcoin, Ethereum, and Hyperledger Fabric. Except for the Bitcoin blockchain, the prototypes support the deployment of smart contracts.

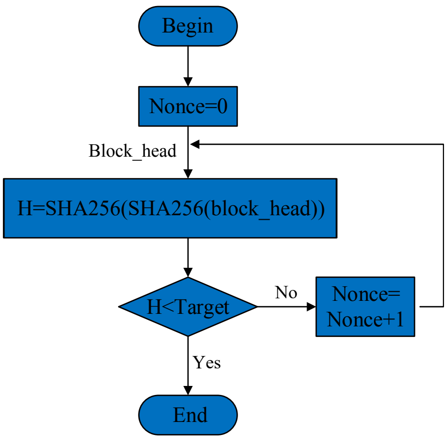

Fig. 2 PoW algorithm flowchart.

Table 1 Blockchain classification.

Content of comparison	Public blockchain	Private blockchain	Consortium blockchain
Participant	Anyone	Internal members of the organization	Consortium members
Degree	Decentralization	Weak centralization	Multiple centralization
Mechanism	PoW	An endorsement on their own	Consensus mechanisms

2.3 Feature

Blockchain is suitable for achieving reliable and efficient traceability in supply chains because it has the following characteristics.

(1) Decentralization: Blockchain is a distributed ledger in which each full node in the system holds the same copy of the ledger, and each node has equal status. A decentralized blockchain will not be affected by the failure of some nodes and is more resistant to malicious access.

(2) Traceability: Block information can be traced using timestamps, Merkle trees, and links between blocks, so blockchain is suitable for the traceability field.

(3) Transparency and tamper-proofness: The nodes in the blockchain system have the right to view the transactions recorded on the chain in real time, and network activities have extremely high visibility. In addition, the hash entanglement between blocks and the consensus mechanisms make tampering with the records on the chain exceptionally difficult.

3 Traditional Traceability Model and Traceability Demand Analysis

3.1 Traditional traceability

A supply chain mainly consists of suppliers, producers, distributors, and customers, as shown in Fig. 3. Supply chain traceability refers to tracking and obtaining information on the history, state, and location of products, involving a series of processes from raw materials to final products[19]. The traceability of supply chains should ensure the high quality of products. Hence, consumers are increasingly concerned about product traceability. Meanwhile, relevant enterprises can improve management and decision-making through

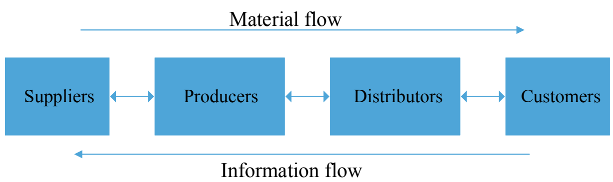

Fig. 3 Supply chain network.

an efficient traceability system. For example, in the event of a food safety incident, members of the food supply chain can quickly find the source of the problem and recall the relevant products using an efficient traceability system, thus contributing to public health.

Figure 4 shows the traditional authentication model of a supply chain. In this model, only the certified central authority authenticates transactions. Because this central organization has too much power, it needs a certain level of authority and independence. During supply chain operation, each node in the link stores the product traceability information in its system. For example, the supplier's item information is stored in the supplier's warehouse database, and the delivery information is maintained by the logistics company, forming multiple centralized systems. Currently, the traditional traceability system can be divided into three types: enterprise-built systems, third-party platforms, and government-built systems. Compared with the other two types, the enterprise self-built one requires more investment, and its operation and maintenance management are more difficult. Third-party systems usually lack pertinence and are generally not sufficiently authoritative to be trusted by enterprises and consumers. The systems established by the government are mainly used to supervise agricultural products and lack the flexibility for diverse applications. The above three types are based on centralized information management and are exposed to the following weaknesses in practice:

(1) Vulnerability to data tampering: The traceability information is stored in a centralized system. When the recorded information conflicts with the enterprise's interest, the enterprise is likely to manipulate the product's information. In addition, even when the government or a third party supervises the central database, the data security depends heavily on the institutions and is vulnerable to network attacks.

(2) Information asymmetry: All kinds of information generated during the operation of supply chains are recorded dispersedly in the respective systems of each node, resulting in the problem of information silos[20]. To make supply chain data complete, extra human and material resources are needed to integrate the data. The traceability information is connected with difficulty, and the traceability process is complicated and can be easily interrupted.

(3) Difficulty in identifying the responsible body: Because of the complex structure of the existing traceability system, quickly identifying the source of the problem and pinpointing the responsible department are difficult when quality issues arise[21].

3.2 Demand analysis

The demand for traceability systems varies between stakeholders in the supply chain and can be roughly divided into three categories: consumer, enterprise, and regulator demand. The specific needs are as follows:

(1) Consumers

Consumers expect the traceability system to be convenient, rapid, and simple for products. The traceability information should process with integrity and be tamper-proof so that users can acquire detailed information on product quality.

(2) Enterprises

The system should be easy to deploy, implement, and maintain. Moreover, restricted access to the information shared by enterprises should be ensured to prevent the leakage of sensitive information.

(3) Regulators

The information provided by the traceability system is a critical support for managing and supervising product

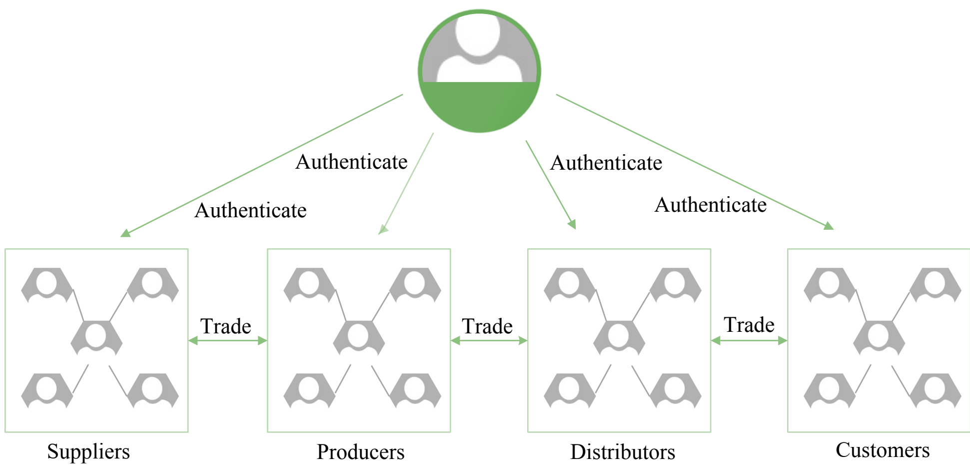

Fig. 4 Traditional authentication model of a supply chain.

quality and safety. Therefore, the regulatory authorities should have the highest access to the system to acquire timely and comprehensive information on any link in the supply chain. The traceability system should allow regulators to exactly determine the responsible nodes in the event of a defective product.

4 Supply Chain Traceability Under Blockchain Technology

As discussed in Section 2, blockchain is decentralized, traceable, transparent, and tamper-proof, which makes it a reliable and efficient solution to supply chain traceability. This section reviews and analyzes relevant research and industrial applications using blockchain technology to enable traceability in supply chains.

Tian[22] proposed using blockchain technology to guarantee the credibility of shared information in the traceability system of the agricultural supply chain. In terms of local citations, Tian is popular among researchers who apply blockchain to supply chain management. His article described a conceptual model of a blockchain-based supply chain traceability system for agricultural products. In his model, the information of the entire supply chain process, ranging from production, processing, storage, and distribution to sales, is collected via radio frequency identification (RFID) technology. This mechanism prevents manual operations from destroying data integrity and uses blockchain technology to ensure data reliability. The system design also considers the government and third-party organizations. As the nodes in the traceability system, the government and third-party organizations need to verify the authenticity of the information uploaded on the chain. Although the system described in this paper is conducive to enhancing the trust and traceability of agricultural products management, it is only based on qualitative elaboration without the support of a practical application effect. Later, Tian[23] proposed another traceability system based on blockchain and the Internet of Things (IoT), which included many improvements compared with the previous model. It introduced BigchainDB to keep the traceability information in the food supply chain, which has the decentralization feature of blockchain and the high-capacity feature of a distributed database. After registration, supply chain members are given public and private key pairs and can view the relevant information on BigchainDB. When the product is in a certain supply chain process, only the node in that link can use the private key to update the configuration file of the product. In addition, third-party institutions can check the identity and behavior of members, and the verification results are stored in BigchainDB for publication, improving the transparency of the supply chain. The system allows registered members to obtain real-time information about food safely and reliably. However, the study still focuses on describing the conceptual model and lacks empirical evidence. After presenting a description and many advantages of blockchain-based supply chain traceability, Tian called for more scholars to get involved in promoting the application in practice.

Although the studies of Tian[22, 23] mainly focused on the conceptual construction of the traceability system model, they also showed a path for blockchain implementation in nonfinancial fields. Increasingly more scholars have started studying blockchain's implementation in supply chain traceability. At present, there are two main efforts: reconstructing blockchain-based traceability systems independently from the bottom level and designing and implementing them based on the mainstream platforms.

4.1 Reconstructing the blockchain system

Leng et al.[24] designed an agricultural supply chain system based on a double-chain structure. The double-chain consists of a transaction chain for storing the transaction data and a user information chain for storing the enterprise information. The storage of transaction records in the transaction chain is based on the Merkle Patricia tree structure because this structure provides the key-value query to obtain complete and true transaction results more conveniently. The storage in the user information chain is based on the Merkle tree structure, which mainly realizes the privacy, security, and integrity protection of information. To design the consensus algorithm, this paper proposed a consensus mechanism based on the weighted PoS mechanism. The equity value of each node is calculated according to the weight, and the highest equity value is used as the accounting node to calculate the block value of the node that needs to be updated. Their results showed that the double-chain design can consider the privacy of user information and the authenticity and transparency of the traced transaction data. The split-chain storage of the two data types improves the system's efficiency to a certain extent. Although the consensus algorithm is specifically designed, its speed and efficiency are still not ideal.

4.2 Design based on mainstream platforms

Most of the current blockchain-based supply chain traceability projects are on Ethereum or Hyperledger Fabric. Founded in 2014, Ethereum is a permissionless blockchain. Hyperledger provides several distributed ledger frameworks for enterprise-scale blockchain development, including Sawtooth and Fabric.

4.2.1 Design based on permissionless blockchain systems

Benčić et al.[25] were the first to apply blockchain technology and the IoT to implement a supply chain management system with traceability and privacy protection. Unlike Tian's scheme[23], Benčić et al.'s scheme does not require all users in the supply chain to register accounts in the system, and it also has real-life applications. In this scheme, producers in the initial link of the supply chain apply to the TagItSmart (TIS) platform to create a smart tag for a product. The information related to this transaction, including the owner, the stakeholders, and the hash of the product item, is encrypted by the private key of the TIS and then recorded in the Ethereum blockchain. This design excludes information fraud. When the product is transferred to the next link node, information on the new owner's ID and transaction details need to be recorded on the blockchain. Then, the new owner votes on the validity of the product item based on whether the scanned smart tag matches the information recorded on the blockchain. Ultimately, the product information available to the consumer is validated by all supply chain participants, and the entire process of product transmission can be supervised. However, the results of an implementation test in the wine industry showed that the cost could be up to 128.12 US dollar during the 2018 testing period, which is slightly too high.

Helo and Hao[26] built a logistics monitoring model based on Ethereum. The system consists of an IoT layer, a data layer, a business layer, and a user layer. Only registered users can record transactions. Transaction information includes operator information, a timestamp, and packet information. When a new transaction is created, a new block must be verified by all participants in the network, and the verified block is added to the chain. Operators and customers can effectively enjoy a full view of logistics history. The blockchain and application layers are separated, with Web services responsible for caching transactions, the ledger's maintenance, and the queries' execution. This solution also has shortcomings: It is not compatible with applications on other platforms, and the transaction processing speed needs further improvement because it is based on Ethereum.

Salah et al.[27] achieved soybean traceability based on the Ethereum blockchain, which could be applied to almost all agricultural supply chains. Participants are required to create their own Ethereum accounts corresponding to an address, and each participant interacts with the smart contract. For example, farmers store records of crop growth in the interplanetary file system (IPFS) as timestamped images or moving picture experts group (MPEG) files and then hash the records and store the digests in the smart contract. All uploaded data require the digital signature of the participant so that each piece of data has its responsible person. The smart contract can penalize dishonest nodes. Although cooperative storage based on blockchain and IPFS makes supply chain traceability dependable and highly transparent, relevant testing and evaluation are lacking.

4.2.2 Design based on permissioned blockchain systems

In Ref. [28], Perboli et al. presented a tracking use case for an e-commerce fresh food supply chain using blockchain technology. They considered a network involving producers, warehouse managers, distributors, certifiers, and users. Product certification documents are embedded in transactions to ensure compliance with regulations. Blockchain is used to store supply chain data and track products, but the project currently only covers part of the system. Only relevant information, such as authentication and documents created by smart contracts, will be kept on the blockchain. The remaining information will stay in the traditional systems of network participants. On the basis of Hyperledger Fabric, the solution was implemented in a food company. The empirical results showed that the cost of applying blockchain can be offset by the savings it brings. They also showed that the traceability accuracy was improved, the brand image was enhanced, and the occurrence of counterfeit goods was reduced.

Caro et al.[29] designed a blockchain-based traceability system called AgriBlockIoT for the agricultural supply chain, where data from IoT sensors throughout the supply chain are stored directly on the blockchain. The traceability system consists of three main modules: a blockchain, a controller, and an application programming interface (API). The representational state transfer (REST) API integrates with existing software systems, and the controller is used to inquire and transform information on the blockchain. The blockchain, a key module of the traceability system, is used to implement various operations through smart contracts. In particular, if any anomalies are in the supply chain process, the smart contracts automatically create a record of them. An analysis of the performance of the traceability system using Ethereum and Hyperledger Sawtooth showed that the Ethereum-based implementation had a higher latency of 16.55 s compared to Hyperledger Sawtooth's blockchain set-up time of 0.021 s. Moreover, the central processing unit (CPU) load on the Ethereum-based implementation was 40% higher, which imposes limitations on computationally constrained microdevices. However, Ethereum is more mature than Sawtooth and supports more node participation. Additionally, the solution lacks considerations in privacy protection and regulator settings.

Wu et al.[30] proposed a food supply chain traceability system built on the Hyperledger Fabric platform. Their model includes network, data, consensus, contract, and application layers. The PBFT consensus algorithm is used to select nodes for block generation. Transactions and events are recorded in the blockchain after encryption. In the system, customers, members, and regulators have different access rights, and smart contracts control the access. For example, the full nodes in the network are created by the regulators, so only the regulators can review all the data; a member can submit the data but can only view the data from adjacent links. The customer can obtain information mainly on the food manufacturer and the place of origin. Therefore, the solution not only realizes traceability but also has the function of privacy protection. Their test results showed that 10 queries could be completed in 0.3 s, but 50 queries would take approximately 1 s, mainly because the processing was not parallel, and instead, transactions were validated one by one.

In the construction supply chain field, Wang et al.[31] proposed an information management scheme for the supply chain based on consortium blockchain and smart contracts, which achieves information sharing and traceability. Their system is based on Hyperledger Fabric. A series of related operation information of precast components (PCs) is stored in the blockchain. In addition, all participants, namely, construction contractors, factories, owners, and logistics companies, have copies of ledgers to share information and track operations on PCs. This design has a few limitations: It does not address the throughput and latency issues associated with the adoption of blockchain; the approval of transactions requires consensus among stakeholders; and the construction company may be reluctant to disclose business information to other participants.

Complex supply chains have relatively large amounts of data. To reduce the load of blockchain and alleviate data explosion, some scholars proposed the mechanism of multiple storages of blockchain plus database. The general structure is shown in Fig. 5. For example, Zhang et al.[32] proposed a grain supply chain traceability system, including data acquisition, cloud service, blockchain, and application layers. The cloud service layer is the data storage, which is divided into a node database and an information database. The node database stores the complete data uploaded by the node and the corresponding relationship between the data and the blockchain. In addition, to achieve data reliability and security, the data backup is stored in the two nonadjacent node databases of the node. The hash of the entire data is stored in the blockchain. The information database is used to hold information that does not require consensus. The system also differs from the traditional coding design. When the product is passed between links, the code is replaced with a new one to record the organization and link information. The authors also deploy smart contracts that are compliant with the regulations and design extended contracts that cater to the specific needs of different enterprises. Hence, product information can be tracked and traced with high efficiency through blockchain and the coding of each link. However, their design has issues in trusted data collection, and the credibility of data needs more consideration before being uploaded. Yang et al.[33]

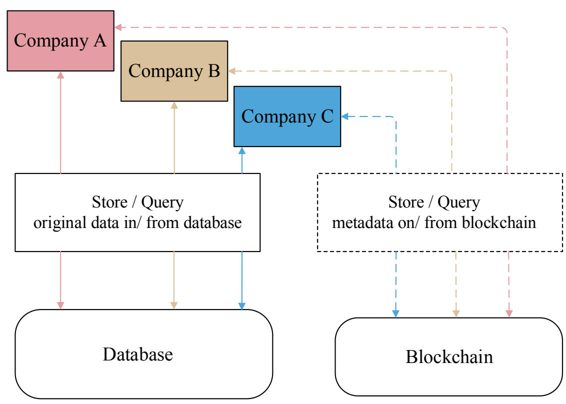

Fig. 5 Example diagram of the storage mechanism.

designed a fruit and vegetable traceability system based on blockchain and encryption technology. Information uploaded by members is classified as public information or private information. The public information is stored in the MySQL database. In contrast, the ciphertext of the private information encrypted by the cipher block chaining (CBC) algorithm and the digests of the public information are stored in the blockchain. This design can reduce the storage pressure of the blockchain and protect privacy. Users can obtain the information stored in the database and block number by scanning the quick response (QR) code and can tell if the information has been tampered with by checking whether it matches the hash value stored in the blockchain. The system is designed with a smart contract that gives credit to members when they submit traceability information, thus providing an incentive to upload the required information. The system is built based on Hyperledger Fabric. The test results showed that the read delay was approximately 0.02 s and the write delay was approximately 0.12 s, both of which met the requirements of practical applications. After the system was applied to an apple company in Shandong, the cost of system software increased by 24.9%, so more money was spent on the development and maintenance of the new system.

4.3 Analysis

Some traceability solutions are stuck in the conceptual stage or lack specific and comprehensive effectiveness evaluation in terms of processing speed, cost, and overall efficiency to prove which design is the most suitable for real-life scenarios[22, 23, 27]. At present, few studies build the system from the bottom level up[24], most of which are based on the mainstream blockchain platform. However, the transaction speed on the Ethereum blockchain is low. Ethereum and Hyperledger Fabric are general frameworks supporting various applications, and the proposed solutions lack redesign of the consensus mechanism and optimization for throughput, which are points that can be further improved.

In addition to academic studies, some cases of effective supply chain traceability solutions using blockchain are also found in the industry. For example, Alibaba partnered with Australia Post, Blackmores, New Zealand's Fonterra, and New Zealand Post to design a blockchain-based food trust framework to improve supply chain traceability and reduce food fraud. Tmall Global uses blockchain and product labels with QR codes to track food[34]. In May 2017, Walmart announced the result of its project on using blockchain technology to track and monitor mangoes in the United States and pork in China. The report showed that the blockchain-based supply chain traceability system reduced the traceability time from a few weeks to 2.2 s, substantially improving the efficiency[35]. Maersk and IBM used blockchain's transparency and traceability features to solve cross-border supply chain problems[36]. In March 2018, JD.com initiated its blockchain project for meat tracking and traceability, with high-quality Australian beef as its initial focus. Everledger, a London-based company, designed a blockchain-based traceability scheme to verify the origin of diamonds[37].

In the exploration and implementation of blockchain-based supply chain traceability solutions, the industry mostly prefers high-value products, such as diamonds and the above-mentioned high-end beef. The reason is that enterprise applications inevitably involve cost-effective analysis. However, most current academic studies[24, 27, 29, 32, 33, 38, 39] focus on agricultural supply chain traceability, and some lack cost application evaluation.

5 Challenges and Development

Four main challenges are encountered in applying blockchain technology to supply chain traceability: scalability, cost, excessive transparency, and regulation. Accordingly, some areas can be studied and improved; that is, some future research paths are apparent.

Scalability: Each node in the decentralized blockchain has equal rights and obligations, and nodes with maintenance functions jointly maintain data blocks across the entire network. Consequentially, transaction data are stored and verified in full size to meet security requirements. However, this design also means that system performance is limited to the upper limit of a single node. Thus, the system throughput is usually not ideal for the supply chain, which contains much data. Taking the performance of the mainstream blockchains as an example, the maximum throughput of Bitcoin is approximately seven transactions per second, and approximately 1 h are needed to confirm that the committed transaction is in the blockchain; Ethereum processes approximately 15 transactions per second. Designing a consensus algorithm according to the characteristics of the supply chain, rather than directly using the existing PoW, PBFT, and other untargeted algorithms, may improve the performance. In addition, a multi-chain design may be an alternative solution to boost scalability.

Cost: For example, every operation executed by a smart contract and each transaction on Ethereum costs gas, which may not be economical for a data-intensive system. Moreover, many managers do not well recognize the value of blockchain, and they are concerned with the reduction in returns resulting from excessive operation and transaction costs. Therefore, in future studies, more attention should be paid to designing a less expensive and risky system.

Excessive transparency: The immutability and permanent visibility of blockchain data may jeopardize privacy. Hence, appropriate access controls should be designed to alleviate the concerns of the entities involved.

Regulation: Currently, the regulations related to blockchain are imperfect, and blockchain application requires certain supervision. Moreover, the supply chain traceability scheme's design should also consider regulators. When defective products are detected, the regulators should timely find the responsible node and implement a recall.

In addition to the above-mentioned challenges and the corresponding possible research interests, the analysis in Section 4 shows that the current blockchain-based supply chain traceability solutions mainly focus on storage mechanism design, and blockchain is mainly used for storage in the supply chain. Compared with the functions of blockchain in the financial field, such as bookkeeping and transaction, authorization, and rights confirmation, the supply chain currently only uses the most basic storage function of blockchain, which is not sufficiently perfect and mature. The most important contribution of blockchain is to digitalizing assets. Supply chain information should be treated as data assets to establish mutual relations, which can confirm rights and authorize access to give full play to the value of blockchain.

6 Conclusion

With its recent development, blockchain technology has been deployed in increasingly diverse scenarios. However, many supply chain participants still claim that they have little understanding of blockchain technology and the contribution it can bring to a supply chain. This paper introduces blockchain technology in the context of supply chains and summarizes the blockchain solutions in supply chain traceability, hoping to provide a good reference for supply chain managers and alleviate their concerns. Moreover, we also discuss the current issues in implementing blockchain for supply chain traceability to provide a practical agenda for researchers. Researchers could focus on the design of targeted consensus algorithms, the appropriate design of access control, and treating supply chain information as data assets to establish interrelationships and fully use the value of blockchain and so on. In conclusion, our review shows that blockchain improves the reliability and efficiency of traceability and has great value in the field of supply chain traceability, while some challenges need to be addressed by further research.

Acknowledgment

This work was supported by the National Key R&D Program of China (No. 2018YFB2101100).

References

[1] S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system, https://bitcoin.org/bitcoin.pdf, 2008.

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

[3] Y. Zhang, S. Kasahara, Y. Shen, X. Jiang, and J. Wan, Smart contract-based access control for the internet of things, *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1594–1605, 2019.

[4] K. Fan, S. Wang, Y. Ren, H. Li, and Y. Yang, Medblock: Efficient and secure medical data sharing via blockchain, *Journal of Medical Systems*, vol. 42, no. 8, pp. 1–11, 2018.

[5] Y. Chen, S. Ding, Z. Xu, H. Zheng, and S. Yang, Blockchain-based medical records secure storage and medical service framework, *Journal of Medical Systems*, vol. 43, no. 1, pp. 1–9, 2019.

[6] N. Z. Aitzhan and D. Svetinovic, Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams, *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 5, pp. 840–852, 2018.

[7] K. Gai, Y. Wu, L. Zhu, M. Qiu, and M. Shen, Privacy-preserving energy trading using consortium blockchain in smart grid, *IEEE Transactions on Industrial Informatics*, vol. 15, no. 6, pp. 3548–3558, 2019.

[8] B. Müßigmann, H. V. D. Gracht, and E. Hartmann, Blockchain technology in logistics and supply chain management—a bibliometric literature review from 2016 to January 2020, *IEEE Transactions on Engineering Management*, vol. 67, no. 4, pp. 988–1007, 2020.

[9] A. Gurtu and J. Johny, Potential of blockchain technology in supply chain management: A literature review, *International Journal of Physical Distribution and Logistics Management*, vol. 49, no. 9, pp. 881–900, 2019.

[10] F. Högberg, M. A. R. Othman, and C. Große, Blockchain in supply chains and logistics: Trends in development, in

Proc. 2020 IEEE International Conference on Industrial Engineering and Engineering Management (*IEEM*), Singapore, 2020, pp. 852–856.

[11] M. Pournader, Y. Shi, S. Seuring, and S. C. L. Koh, Blockchain applications in supply chains, transport and logistics: A systematic review of the literature, *International Journal of Production Research*, vol. 58, no. 7, pp. 2063–2081, 2020.

[12] A. Kamilaris, A. Fonts, and F. X. Prenafeta-Boldu, The rise of blockchain technology in agriculture and food supply chains, *Trends in Food Science and Technology*, vol. 91, pp. 640–652, 2019.

[13] Y. Wang, M. Singgih, J. Wang, and M. Rit, Making sense of blockchain technology: How will it transform supply chains? *International Journal of Production Economics*, vol. 211, pp. 221–236, 2019.

[14] R. L. Rivest, A. Shamir, and L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[15] V. S. Miller, Use of elliptic curves in cryptography, in *Proc. CRYPTO '85*: *Advances in Cryptology*, Santa Barbara, CA, USA, 1985, pp. 417–426.

[16] T. E. Gamal, A public key cryptosystem and a signature scheme based on discrete logarithms, in *Pro. CRYPT0 '84: Advances in Cryptology*, Santa Barbara, CA, USA,1984, pp. 10–18.

[17] V. Buterin, A next-generation smart contract and decentralized application platform, *Ethereum White Paper*, https://ethereum.org/en/whitepaper/, 2014.

[18] M. Castro and B. Liskov, Practical byzantine fault tolerance, in *Proc. Third Symposium on Operating Systems Design and Implementation*, New Orleans, LA, USA, 1999, pp. 173–186.

[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 Generation Computer Systems*, vol. 92, pp. 399–406, 2019.

[20] Q. Jiang and G. Ke, Information sharing and bullwhip effect in smart destination network system, *Ad Hoc Networks*, vol. 87, pp. 17–25, 2019.

[21] Y. Zhang and U. Guin, End-to-end traceability of ICs in component supply chain for fighting against recycling, *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 767–775, 2019.

[22] F. Tian, An agri-food supply chain traceability system for China based on RFID & blockchain technology, in *Proc. 2016 13th International Conference on Service Systems and Service Management* (*ICSSSM*), Kunming, China, 2016, pp. 1–6.

[23] F. Tian, A supply chain traceability system for food safety based on HACCP, blockchain & internet of things, in *Proc. 2017 International Conference on Service Systems and Service Management*, Dalian, China, 2017, pp. 1–6.

[24] K. Leng, Y. Bi, L. Jing, H. C. Fu, and I. V. Nieuwenhuyse, Research on agricultural supply chain system with double chain architecture based on blockchain technology, *Future Generation Computer Systems*, vol. 86, pp. 641–649, 2018.

[25] F. M. Benčić, P. Skočir, and I. P. Žarko, DL-tags: DLT and smart tags for decentralized, privacy-preserving, and verifiable supply chain management, *IEEE Access*, vol. 7, pp. 46198–46209, 2019.

[26] P. Helo and Y. Hao, Blockchains in operations and supply chains: A model and reference implementation, *Comput. Ind. Eng.*, vol. 136, pp. 242–251, 2019.

[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] G. Perboli, S. Musso, and M. Rosano, Blockchain in logistics and supply chain: A lean approach for designing real-world use cases, *IEEE Access*, vol. 6, pp. 62018–62028, 2018.

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

[30] H. Wu, J. Cao, Y. Yang, C. L. Tung, S. Jiang, B. Tang, Y. Liu, X. Wang, and Y. Deng, Data management in supply chain using blockchain: Challenges and a case study, in *Proc. 2019 28th International Conference on Computer Communication and Networks* (*ICCCN*), Valencia, Spain, 2019, pp. 1–8.

[31] Z. Wang, T. Wang, H. Hu, J. Gong, X. Ren, and Q. Xiao, Blockchain-based framework for improving supply chain traceability and information sharing in precast construction, *Automation in Construction*, vol. 111, pp. 103063.1–103063.13, 2020.

[32] X. Zhang, P. Sun, J. Xu, X. Wang, J. Yu, Z. Zhao, and Y. Dong, Blockchain-based safety management system for the grain supply chain, *IEEE Access*, vol. 8, pp. 36398–36410, 2020.

[33] X. Yang, M. Li, H. Yu, M. Wang, D. Xu, and C. Sun, A trusted blockchain-based traceability system for fruit and vegetable agricultural products, *IEEE Access*, vol. 9, pp. 36282–36293, 2021.

[34] H. Zhang, T. Nakamura, and K. Sakurai, Security and trust issues on digital supply chain, in *Proc. 2019 IEEE Intl. Conf. on Dependable, Autonomic and Secure Computing, Intl. Conf. on Pervasive Intelligence and Computing, Intl. Conf. on Cloud and Big Data Computing, Intl. Conf. on Cyber Science and Technology Congress* (*DASC/PiCom/CBDCom/CyberSciTech*), Fukuoka, Japan, 2019, pp. 338–343.

[35] N. Kshetri, 1 Blockchain's roles in meeting key supply chain management objectives, *International Journal of Information Management*, vol. 39, pp. 80–89, 2018.

[36] Y. L. Chang, E. Iakovou, and W. D. Shi, Blockchain in global supply chains and cross border trade: A critical synthesis of the state-of-the-art, challenges and opportunities, *International Journal of Production Research*, vol. 58, no. 7, pp. 2082–2099, 2020.

[37] N. Kshetri and E. Loukoianova, Blockchain adoption in supply chain networks in Asia, *IT Professional*, vol. 21, no. 1, pp. 11–15, 2019.

[38] D. Prashar, N. Jha, S. Jha, Y. Lee, and G. P. Joshi, Blockchain-based traceability and visibility for agricultural

products: A decentralized way of ensuring food safety in India, *Sustainability*, vol. 12, no. 8, pp. 1–20, 2020.

[39] A. Shahid, A. Almogren, N. Javaid, F. A. Al-Zahrani, M. Zuair, and M. Alam, Blockchain-based agri-food supply chain: A complete solution, *IEEE Access*, vol. 8, pp. 69230–69243, 2020.

Xiaofeng Zhang received the bachelor degree from Nankai University, Tianjin, China, in 2020. She is pursuing the master degree at Fudan University in Shanghai, China. Her research interests include blockchain technology and smart contracts.

Li Ling received the master degree from Fudan University, Shanghai, China. He is a professor at the School of Information Science and Technology, Fudan University. His research interests include blockchain technology, cryptography, and information security.