Journal of Network Intelligence
Taiwan Ubiquitous Information
 ISSN 2414-8105
Volume **8**, Number **1**, February **2023**

Decentralized Solution for Cold Chain Logistics Combining IoT and Blockchain Technology

Zhiying Wang*

The Engineering & Technical College of Chengdu University of Technology
Leshan, Sichuan, 614000, China
luna998103@163.com

Chenhao Zhang

The Engineering & Technical College of Chengdu University of Technology
Leshan, Sichuan, 614000, China
zhangchenhao1210@163.com

Xian Mu

Department of Computer Information Engineering
Nanchang Institute of Technology
Nanchang, Jiangxi, 330044, China
muxian@nut.edu.cn

Corresponding author: Zhiying Wang

Received July 16, 2022, revised September 10, 2022, accepted November 2, 2022.

Abstract. *At present, most of the cold chain logistics systems use centralized solutions, and data management is completed by the logistics enterprises alone, which will cause a series of trust problems. In response to these problems, a decentralized data sharing and storage scheme for cold chain logistics based on the Internet of Things (IoT) and blockchain technology is proposed. Using the unique characteristics of decentralization and trustlessness of blockchain, the consensus mechanism of proof of storage (PoS) is used to realize block consensus and distributed storage of shared data. Based on the Gossip protocol, a hierarchical block propagation mechanism is proposed between the consensus nodes and verification nodes of the blockchain network. The simulation results show that the block propagation delay increases with the increase of block size. In addition, when the block size remains unchanged, compared with the traditional block propagation scheme, the proposed block propagation mechanism successfully reduces the propagation delay significantly. The implementations of smart contracts and product tracking process prove that the proposed scheme effectively improves the reliability and data security of the cold chain logistics operations. To sum up, the proposed method combines the ubiquity of the IoT and the decentralized nature of the blockchain, which can meet the actual business needs and has important value for the development of the cold chain logistics industry.*
Keywords: Cold Chain Logistics; Blockchain; Smart Contract; Internet of Things; Data Sharing; Data Storage

1. **Introduction.** In recent years, with the continuous improvement of people's living standards and the popularization of e-commerce, the cold chain logistics market has also developed rapidly. The so-called cold chain logistics generally refers to the logistics and transportation mode that some special commodities (such as food and medicine) need to maintain a certain temperature at all times in their processing, storage, transportation, distribution, retail and other links, so as to ensure the quality of the commodities [1,2,3].

The Internet of Things (IoT) is a networking paradigm that connects objects in the real world with the Internet, allowing devices to collect, process, and communicate data without human intervention [4,5]. According to Ericsson's forecast, more than 24.9 billion devices will be connected to IoT networks by 2025. The growth in the number of smart devices has led to an explosive growth in the amount of network data [6]. Through the collection and analysis of IoT data, the potential value of IoT data can be further mined, but the data barriers between different IoT systems limit the further utilization [7]. In the era of the Internet of Everything, how to integrate the data collected from different IoT systems and realize data sharing among multiple IoT systems is still a challenge. Most of the current cold chain logistics systems use the IoT technology to improve the digitalization of the system.

If all data is sent to a centralized cloud platform for processing, it will bring huge data security risks. First, if the central server fails, the entire web server is at risk of being paralyzed, for example a denial of service (DoS) attack on the centralized server could lead to a single-point failure problem. Second, users have limited control over how and by whom personal data is used, and data stored in centralized servers may reveal personal privacy. Finally, data stored in a centralized cloud lacks reliability and traceability. Centralized IoT infrastructure requires trusted third parties for data processing, and data stored on centralized servers is at risk of being deleted or tampered [8]. Blockchain technology has attracted widespread attention in recent years due to its characteristics of decentralized autonomy, non-tampering, and traceability. Blockchain technology is considered a key decentralization technology to simplify network management and improve network performance [9]. The data stored on the blockchain is jointly maintained by the entire network, which can effectively transfer value between nodes that lack trust. Using blockchain technology, IoT data sharing that was previously only possible through trusted third-party platforms can now operate in a decentralized manner [10]. However, the research on IoT data sharing based on blockchain technology still faces many challenges, one of which is the storage of shared data.

Several approaches have been proposed in the past to combine blockchain technology and supply chain management. Rahmadika et al. [11] designed a blockchain-based food traceability system. Chen et al. [12] applied blockchain technology to supply chain management and used it as an important management tool. Tian et al. [13, 14] combined blockchain technology, HACCP technology and RFID technology to build a traceable logistics system. Xie et al. [15] designed some attack scenarios for the security of the blockchain to study whether the blockchain technology can ensure the data security in the agricultural product supply chain. Lu and Xu [16] applied blockchain technology to food traceability in consideration of the real-world scenarios, and explained how to manage the traceability information of food cold chain. In the IoT environment, the decentralized sharing and storage of data using blockchain technology is a huge challenge for the IoT itself. This is because most IoT devices are low-power devices and do not have the ability to participate in the distributed consensus of the blockchain network. In the consensus mechanism of the blockchain, the nodes participating in the consensus process need to be responsible for the formation of consensus, transaction verification, and block verification and packaging. The capabilities of devices in a blockchain network are one of the main factors to consider when designing a consensus mechanism. Resource-constrained nodes in IoT, such as sensors, cannot undertake consensus tasks. For nodes with relatively powerful computing and storage capabilities (such as gateways, etc.), they can still play an important role in the consensus process of the blockchain [17]. In addition, the proportion of consensus nodes will have an impact on the performance of the blockchain network. If the proportion of consensus nodes is too small, the degree of decentralization of the

entire blockchain network will be small, which is not conducive to the security of the entire system; If the proportion of nodes is too large, the block propagation delay will be very large. In scenarios that require a large amount of data interaction, the service requirements cannot be met. When a large amount of data needs to be shared between different IoT systems, a large consensus delay will lead to inefficient data sharing [18].

Based on the above problems, this paper proposes a cold chain logistics solution based on blockchain technology and the IoT. The main contributions are as follows:
1) The blockchain smart contract scheme for product management in the logistics system is designed and implemented. Using input data from IoT devices, many different functions can be successfully implemented, such as role-based access control, product tracking and traceability, and semi-automated clearance procedures. The proposed solution proves that some problems faced in the logistics industry can be solved by utilizing the decentralized features of the blockchain technology.
2) A data sharing and storage framework based on blockchain technology is proposed to realize the decentralized sharing and storage of cold chain IoT data. Through the consensus mechanism of Proof of Storage (PoS), the concepts of block consensus and distributed storage of shared data are combined.
3) Based on the Gossip protocol, a hierarchical block propagation mechanism is proposed. Through the analysis of the capabilities of IoT devices, the block propagation delay model of the blockchain network are derived, and the simulation results prove that the performance of the proposed protocol is better than the traditional Gossip protocol.

The rest of this paper is organized as follows. Section II explains the overall design of the proposed cold chain logistics solution based on blockchain and IoT technology. Section III presents the blockchain data storage and sharing mechanism. Section IV analyzes the performance of the proposed method through simulation experiments, and demonstrates the implementation process of product tracking. Finally, Section V summarizes the full text.

2. **Block and IoT-enabled cold-chain logistics.**

2.1. **Overall Architecture.**

The proposed blockchain system aims to promote the tracking and traceability of products in the cold chain circulation process. The proposed smart logistics method enables the registration of important product tracking data into a decentralized ledger, and implements an identity verification and access control system, incorporating certificate authentication, customs/quality control, and IoT sensor device data in the process. The conceptual diagram of cold chain logistics tracking based on blockchain and smart contracts is shown in Figure 1. The tracking data of the products are continuously updated through the IoT device, and the products are traced from the origin, where the information about the condition, location or status of the products is measured and registered on the blockchain using the IoT sensor devices.

2.2. **Product Tracking.**

The main object of the smart contract system is product tracking and traceability, so the system development process focuses on the product object itself, which represents a single item or a container of items in the blockchain. Figure 2(a) presents the attribute categories of products and the associated data points: 1) Labels: Products in the logistics system can use different types of labels to support different industry standards, and users need to register a set of keys to access this data from an external smart contract system. 2) Holder: As the product circulates in the supply chain, the list of entities that physically hold the product. Any changes of handover need to be registered with a timestamp. 3) Location: Like the holder, changes in product location

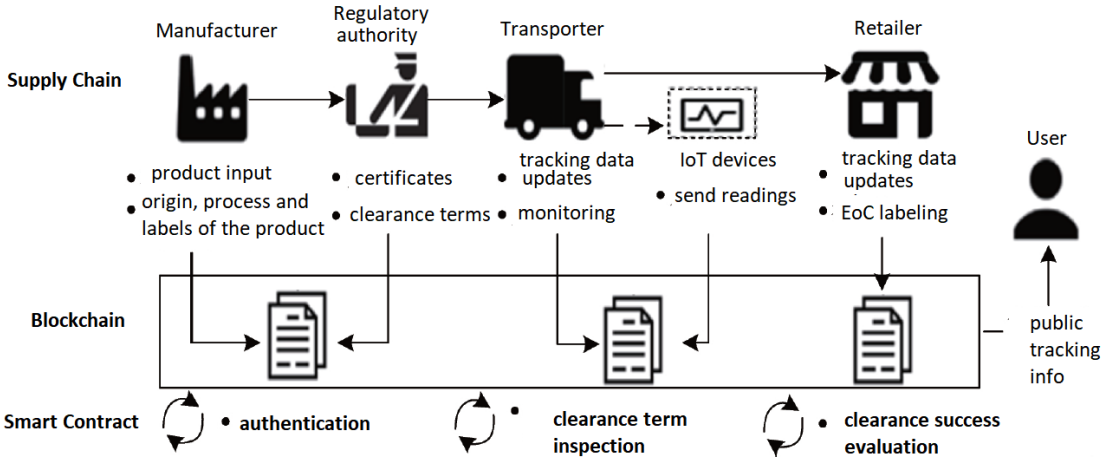


FIGURE 1. Overall architecture of the proposed cold chain logistics scheme.

will also be registered and time stamped. 4) Status: Changes in product state codes during shipping or handling are registered and time stamped. 5) Readings: The sensor data readings of IoT devices are registered to the blockchain, such as temperature, humidity, etc. The "Clearance" term in Figure 2(b) records the product certificates and successfully

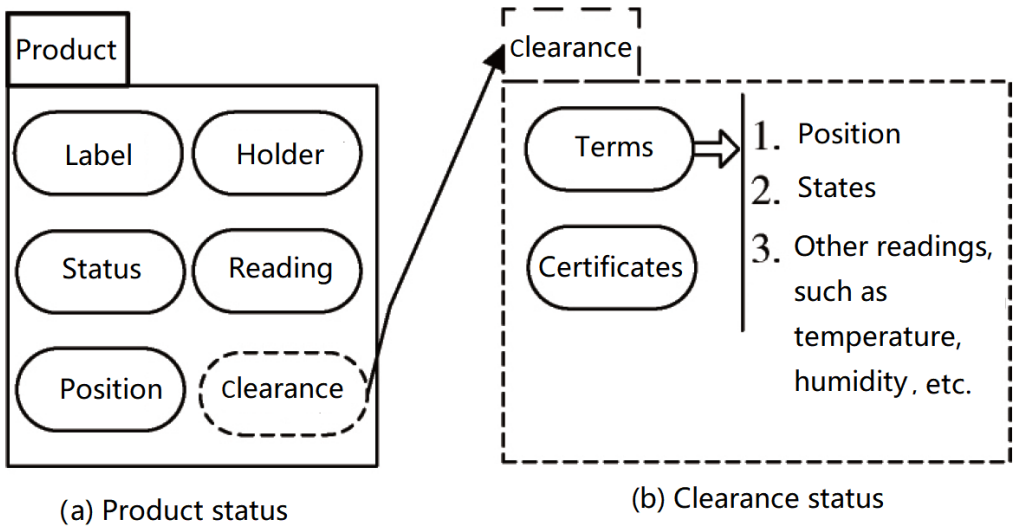


FIGURE 2. Product and clearance state records.

completed quality control clauses. A government agency or other certification body may grant certification for a specific product or shipment, and these events will be recorded in the clearance record for that product. In addition, the governing body may establish special shipping terms or conditions that will be validated when tracking data is available in the system. These terms can be related to location or shipping status, and logistics companies must implement these terms to meet quality requirements or standards (including measurable sensor reading requirements, i.e. temperature, humidity, etc.). At the same time, a check for time constraints can be implemented. To monitor the products in the cold chain, the use of IoT devices is integrated in the proposed system, and a user account is set up for each device to allow it to interact with the blockchain. When the product reaches the End of the Chain (EOC), the completion of all terms and conditions

related to product quality control and clearance is verified, so as to judge whether the overall shipping process of the product is successful or not.

2.3. **Role-Based Access Control.** To ensure that the tracking update process is resistant to malicious access, the proposed blockchain application is a permissioned chain that is only accessible to authorized parties. To this end, role-based access control (RBAC) is implemented in the smart contract system, and the permissions of blockchain users are determined according to their roles [19]. Different roles and corresponding permissions are shown in Table 1, and almost all system privileges listed in the table also depend on whether the user is the current holder of the product. The current holder of the product means that the item is physically being held by the entity, so that it can update the tracking status of the product. the roles defined in Table 1 are meaningful only when the entity is the current holder of the product.

Roles	Permissions							
	Authorized holder	Change position	Change states	Create product	User management	EoC labeling	Clearance/ transport terms	Certification
Manufacturer	x	x	x	x	✓	✓	x	✓
Transporter /Warehouse	x	x	x	✓	✓	✓	✓	x
Regulatory authority	x	x	x	✓	✓	✓	x	✓
Retailer	x	x	x	✓	✓	x	✓	✓
Registered service provider	✓	✓	✓	✓	x	✓	✓	✓

TABLE 1. List of permissions for different roles.

2.4. **Smart Contract.** The overview and code structure of smart contract implementation are shown in Figure 3, developed using Truffle and Ganache - cli [20]. Truffle is a smart contract testing tool and Ganache-cli is an Ethereum blockchain simulator. The proposed scheme uses the "inheritance" feature of Ethereum smart contracts, which allows future smart contracts to access the data structures of their parent contracts. In the example in Figure 3, the last contract launched in the blockchain is the "Product Manager", which also integrates all the structures of the previous contracts.

The functions included in each smart contract module are as follows.

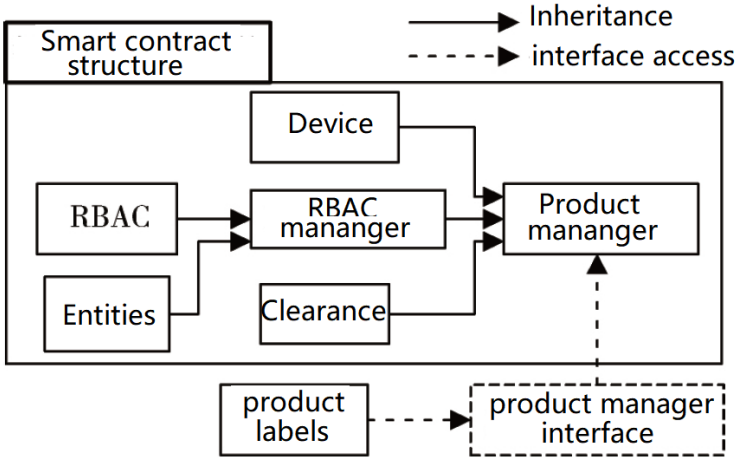


FIGURE 3. Smart contract implementation based on inheritance or interface.

1)RBAC and RBAC Manager: RBAC is taken from the open source library OpenZeppelin and contains basic methods for assigning user roles and performing authentication. The RBAC Manager utilizes this code to implement the roles required in the proposed logistics system.
2) Entity and device: they are used to store and manage user and device data, respectively.
3) Clearance: it contains methods and structures for evaluating the processes of product quality control and clearance.
4) Product Manager: The core smart contract in the system. It implements product classification and related tracking and clearance management, as well as RBAC authentication and authorization.
5) Product labels and interfaces: It contains data structures and methods for storing label data of different standards related to products. This smart contract is launched separately from the main smart contract system and interacts through an interface.

3. **Blockchain-based IoT data sharing and storage.** The data sharing and storage process between IoT devices is as follows: When the data requester needs to obtain data from other devices, the data requester will publish the data request transaction on the blockchain through a smart contract. After the data holder listens to the data requester's transaction on the blockchain network, if it holds the required data, it will perform the following operations:
1) Rent storage resources from consensus nodes through smart contracts;
2) After getting the response from the consensus nodes that provide storage resources, it sends the encrypted data, description of the data, storage time and the number of copies to be stored to the consensus nodes, and the consensus nodes send the address of the shared data along with a description of the data to the blockchain.
By storing the shared data storage address on the chain and storing the actual data off the chain, the data holder can decide the time when the shared data is stored at the consensus nodes according to the actual needs. After the data requester obtains hashed key from the data holder, it can obtain the required data from the corresponding data address.

3.1. **Consensus mechanism.** A core concept in blockchain is decentralization, so there is no central database in the blockchain network. Every node is equal, so a consensus mechanism is needed to ensure that all peer nodes can cooperate effectively. The consensus mechanism is an algorithm for blockchain transactions to achieve distributed consensus. Both Bitcoin and Ethereum use the proof-of-work (PoW) concept that relies heavily on computing power. There are a large number of low-power devices in the IoT, and the lack of computing resources makes the PoW algorithm unsuitable for IoT data sharing scenarios. Hyperledger Fabric uses traditional Byzantine fault tolerance algorithms, such as practical Byzantine fault tolerance (PBFT). In IoT scenarios with a large number of nodes, the communication complexity of PBFT will increase significantly [21].

Considering the data sharing and storage requirements in IoT scenarios, the PoST (Proof of Space and Time) consensus mechanism is adopted in the paper. Let Nc be the number of consensus nodes in the network, and is p_i^t the proof of capacity provided by the consensus node i in the t-th consensus cycle, then the proportion of effective storage space pos_i^t provided by consensus node i for the network in t consensus cycles can be calculated

as:

$$\mathrm{pos}_i^t = \frac{p_i^t}{\sum_{j=1}^{N_c} p_j^t} \tag{1}$$

The greater the storage power p_i^t , the greater the probability that the consensus node will successfully add a block to the blockchain. Compared with PoW, the consensus process between consensus nodes in the PoS consensus mechanism does not need to waste a lot of computing power to complete meaningless hash calculation tasks. At the same time, the PoS consensus mechanism can also promote the storage of shared data by consensus nodes, because in a consensus cycle, the more data a consensus node stores, the greater the probability of obtaining consensus rewards. In order to increase the degree of decentralization of the blockchain network, the consensus result of the blocks is determined not only by the consensus nodes, but also by the verification nodes. When a consensus node generates a block, it needs to propagate the generated block to all consensus nodes and some verification nodes for verification, and the verified block can be added to the blockchain.

Considering that there are a large number of low-power devices and a small number of high-capacity devices in the IoT, the Pareto distribution [22] is used to describe the computing power and storage capacity of IoT devices. Let the computing power of the IoT devices be $\{X_1, X_2, \ldots, X_N\}$, and X_i is subject to the Pareto distribution with parameters ζ and σ_c, where $\sigma_c = \min\{X_i\}$; let the storage capacity of the IoT devices be $\{Y_1, Y_2, .., Y_N\}$, and Y_i is subject to the Pareto distribution with parameters ζ and σ_s, where $\sigma_s = \min\{Y_i\}$. N is the total number of IoT devices ($N \gg N_c + N_v$). The survival function of computing capability X of IoT devices can be expressed as:

$$F_c(x) = \Pr(X > x) = \left[\frac{x}{\sigma_c}\right]^{-\zeta}, x \geq \sigma_c > \zeta \tag{2}$$

The probability density function of the computing capability X of the IoT devices is:

$$f_X(x) = \begin{cases} \dfrac{\zeta \sigma_c^{\zeta}}{x^{\zeta+1}}, & x \geq \sigma_c \\ 0, & x < \sigma_c \end{cases} \tag{3}$$

The survival function of storage capability Y of IoT devices can be expressed as:

$$F_s(y) = \Pr(Y > y) = \left[\frac{y}{\sigma_s}\right]^{-\zeta}, y \geq \sigma_s > \zeta \tag{4}$$

Let the computing power threshold of consensus nodes be X_c, and the storage capacity threshold of consensus nodes be Y_c. When the computing power of a node is greater than X_c and the storage capacity of the node is greater than Y_c, the IoT node can be used as a consensus node. The probability that the IoT node is a consensus node can be determined as:

$$F_{\mathrm{con}} = F_c(X_c)F_s(Y_c) = \left[\frac{X_c}{\sigma_c}\right]^{-\zeta}\left[\frac{Y_c}{\sigma_s}\right]^{-\zeta}, X_c \geq \sigma_c > \zeta, Y_c \geq \sigma_s > \zeta \tag{5}$$

the larger the parameter ζ, the smaller the proportion of consensus nodes in the total number of IoT devices. Let $N_c = NF_{con}$ be the number of consensus nodes, and the capacity expectation of the consensus nodes can be calculated as:

$$\mathrm{E}(X)_{\mathrm{con}} = \int_{X_c}^{+\infty} \frac{\zeta X_c^{\zeta}}{x^{\zeta}} \mathrm{d}x \tag{6}$$

Let the computing capacity threshold of the verification nodes be X_v, and the storage capacity threshold of the verification nodes be Y_v. When the computing capacity of a node is greater than the threshold X_v and less than the threshold X_c, and the storage capacity of the node is greater than the threshold Y_v and less than the threshold Y_c, the IoT node can be used as a verification node, and the probability that the IoT node is a verification node can be calculated as:

$$\begin{aligned}\Pr(X_v < X < X_c)\Pr(Y_v < Y < Y_c) &= [\Pr(X > X_v) - \Pr(X > X_c] \cdot [\Pr(Y > Y_v) - \Pr(Y > Y_c)] \\ &= \left[\left(\frac{X_v}{\sigma_c}\right)^{-\zeta} - \left(\frac{X_c}{\sigma_c}\right)^{-\zeta}\right]\left[\left(\frac{Y_v}{\sigma_s}\right)^{-\zeta} - \left(\frac{Y_c}{\sigma_s}\right)^{-\zeta}\right] \quad , X_c > X_v \geq \sigma_c > \zeta, Y_c > Y_v \geq \sigma_s > \zeta\end{aligned} \tag{7}$$

The computing capacity expectation of the verification nodes can be expressed as:

$$\mathrm{E}(X)_{\mathrm{ver}} = \int_{Xv}^{X_c} \frac{\zeta X_v^{\zeta}}{x^{\zeta}} \mathrm{d}x \tag{8}$$

where $X = \beta_1 f_m$ is the computing capacity of the IoT node, and f_m represents the CPU frequency of the node, $Y = \beta_2 e$ is the storage capacity of the IoT node, and e represents the memory size of the node. The number of verification nodes is expressed as $N_v = NF_{ver}$.

3.2. **Block propagation mechanism.** The proposed block propagation mechanism is shown in Figure 4. When consensus node i generates a new block $block_i$, consensus node i needs to transmit $block_i$ to other consensus nodes for verification, and it also needs to recruit some verification nodes for verification. Other consensus nodes that receive this block also need to recruit validator nodes for verification. The block propagation in the proposed system adopts the hierarchical propagation mechanism based on the Gossip protocol, including the consensus node layer and the verification node layer. That is, the Gossip protocol is used for block propagation between different consensus nodes, between consensus nodes and verification nodes, and between different verification nodes. The Gossip protocol was first proposed in [23] and is mainly used for data synchronization between replica nodes in a distributed database system. The basic idea is that nodes randomly select some other nodes for information transmission, and the node that receives the information will transmit the information to other nodes in the same way. Wireless multicast is used for block propagation among nodes. The propagation process of blocki is as follows: 1) between consensus nodes: Consensus node i transmits $block_i$ to other consensus nodes; 2) between consensus nodes and verification nodes: consensus node i transmits $block_i$ to its recruited verification nodes; 3) between verification nodes : $Block_i$ is transmitted between validation nodes recruited by consensus node i.

Let the set of consensus nodes be $C = \{c_1, c_2, \ldots, c_{|C|}\}$, where $|C| = N_c$; and let the set of verification nodes as $V = \{v_1, v_2, \ldots, v_{|V|}\}$, where $N_v > N_c$. Assuming that the number of verification nodes recruited by each consensus node is the same and it's equal to $\alpha N_v (0 < \alpha < 1)$, so the total number of times that $block_i$ needs to be verified is $N_c(\alpha N_v + 1) - 1$.

During the process of block transmission, the block transmission protocol between node A and node B adopts the traditional block propagation protocol [24], and the implementation process is shown in Figure 5. Before sending the block, node A sends an Inventory information to node B to verify whether node B has recorded the block. If node B does not have the block, it will reply to node A with a Getdata message, and wait to receive block information. By using a block propagation protocol, unnecessary information transfer between nodes can be reduced [25]. The propagation delay of the block includes three parts: the transmission delay of the block, the verification delay of the block, and the delay of exchanging Inventory and Get data information between nodes. The average

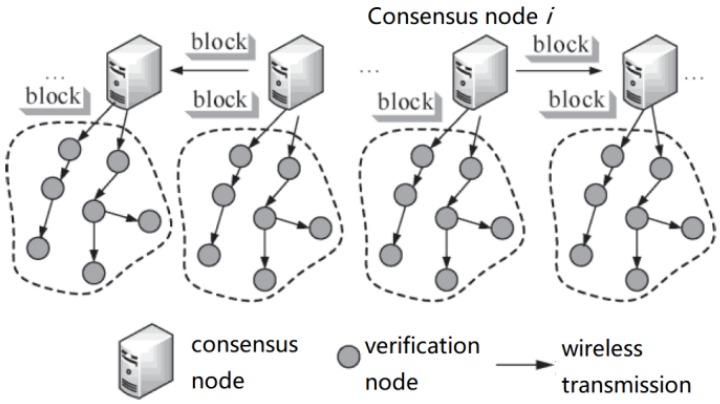


FIGURE 4. Block propagation mechanism.

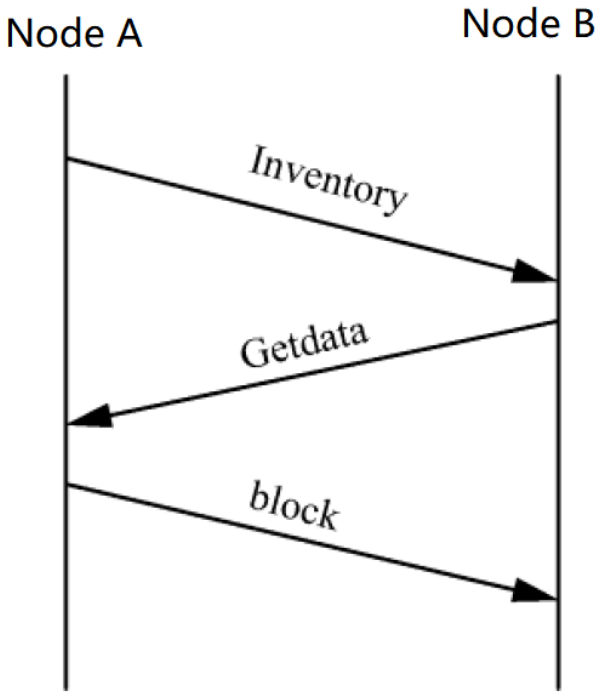


FIGURE 5. Block transmission between Node A and Node B.

round-trip time for exchanging Inventory and Get data information is denoted as τRTT [26]. The block transmission between nodes adopts the Gossip protocol. For a network of N nodes, assuming that in each Gossip cycle, the node that receives the block can transmit the block to at least one more node, then the number of cycles for the block to be transmitted to N nodes is log(N). Let the block size be s, the transmission delay of the block can be expressed as:

$$\tau_{p,b} = \frac{s}{c} \log(N) \tag{9}$$

where c is the average effective channel capacity of the links.

4. **Experiment and Analysis.** In this section, through simulation experiments, the differences in block propagation delay between the proposed Gossip protocol and the traditional Gossip protocol are compared. At the same time, the relationship between block

size and block propagation delay is analyzed under different proportions of verification nodes.Then the impacts of the parameter ζ and the capacity threshold of consensus nodes on the block propagation delay are analyzed. Finally, For cold chain logistics scenarios, the implementation of product tracking in cold chain logistics are carried out based on the Ethereum development platform.

4.1. **Numerical simulation results.** Firstly, the performance difference between the proposed improved Gossip protocol and the traditional Gossip protocol in terms of block propagation delay is compared, and the relationship between block size and block propagation delay under different proportions of verification nodes is analyzed. Then, the influence of parameter ζ and consensus node capability threshold on block propagation delay is analyzed. The simulation parameters are shown in Table 2.

parameters	values
Block size , s	213 s /bit
channel capacity , c	100 /(bit /s)
Average round trip time , τRTT	100 /ms
proportion of verification nodes recruited by each consensus node, α	0.3
minimum computing capacity of IoT node , σ_c	1 000 /Hz
minimum storage capacity of IoT node , σ_s	32 GB
storage threshold of consensus node , Y_c	100 GB
storage threshold of verification node , Y_v	60 GB
total number of IoT nodes , N	10 000
CPU cycle required for each bit , U	1/64

TABLE 2. parameter configuration in the simulation.

Figure 6 shows the relationship between the block propagation delay τ and the block size s with different proportion α of validator nodes recruited by consensus nodes. At the same time, the proposed hierarchical block propagation scheme based on Gossip protocol is compared with the traditional Gossip protocol-based block propagation scheme. In this simulation, $\zeta = 2$, $X_c = 10000Hz$, and $X_v = 8000Hz$. The block size s refers to the number of bytes stored in each block. As can be seen from Figure 6, when the block size s is constant, compared with the traditional block propagation scheme, the block propagation delay of the proposed scheme is greatly reduced. In the block propagation scheme proposed in this paper, the consensus node is not only responsible for the block transmission in the consensus node layer, but also responsible for the block transmission in the verification node layer, so as to reduce the block propagation delay. At the same time, the simulation results show that the block propagation delay τ increases with the increase of α. Because when α increases, the number of verification nodes recruited by consensus nodes during the block verification process will increase, and the number of times the block is verified will also increase, resulting in increased block propagation delay. When α remains constant, the block propagation delay τ increases with the increase of block size s.

Figure 7 shows the relationship between the block propagation delay τ and the consensus node capability threshold under different values of the parameter ζ , in which the capability threshold of the verification nodes and the computing capability threshold of the consensus nodes increase at the same rate. It can be seen from Figure 7(a) that when ζ remains unchanged, the block propagation delay τ decreases as the computing power

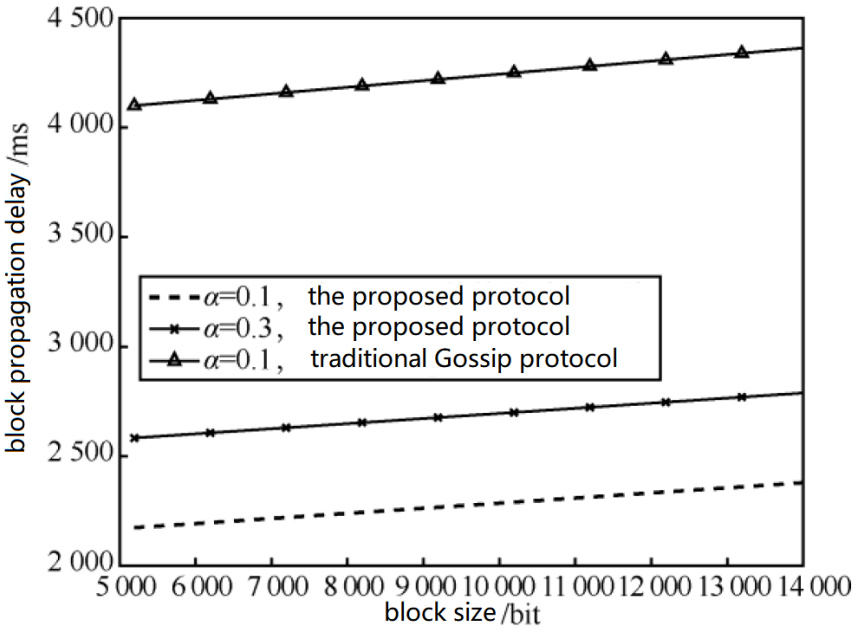
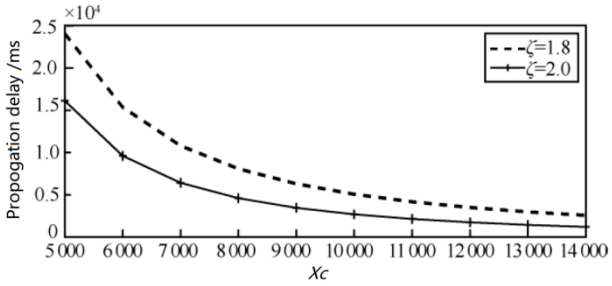


FIGURE 6. Block propagation delay as a function of block size.

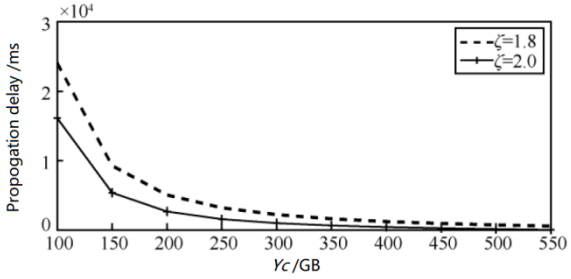
threshold X_c of the consensus node increases. This is because when the computing power thresholds X_c and X_v of the nodes increase, the ratio between the consensus nodes and the verification nodes in the network will decrease, and the number of verifications required to reach a consensus on a block will decrease, thereby reducing the total delay of block propagation. When X_c remains unchanged, the block propagation delay τ decreases with the increase of ζ. This is because when ζ increases, the ratio between consensus nodes and verification nodes in the network decreases, and the number of verifications required for a block to reach consensus decreases, thereby reducing the total propagation delay. It can be seen from Figure 7(b) that when ζ remains unchanged, the block propagation delay τ decreases with the increase of the storage capacity threshold Y_c of the consensus nodes. When Y_c is constant, the block propagation delay τ decreases with the increase of ζ.

4.2. **Analysis of cold chain transportation scheme.** Figure 8 shows how product tracking works throughout the cold chain logistics in 3 different views: (1) At the supply chain level, the method used by each holder entity to bring data into the blockchain can be found. Changes in states, positions and holders are marked with diamonds, circles, and squares, respectively. (2) At the tracking level, the data entered by the holders can be used to reconstruct a timeline of events for changes in states, locations, holders, and readings received from IoT devices. (3) At the clearance inspection level, the transport terms formulated by the manufacturer or the regulatory body can be found. It will also reveal the data points for which data brought into the blockchain is checked against these terms, and whether quality requirements have been met.

In the example shown in Figure 8, the manufacturer first uses the function createProduct to bring product data and product location into the system. From this, the producer becomes the first holder, representing the origin (original data point) of the product. The producer accesses the addState function to update the product state and creates a clearance term T1 related to the product state, which in this case is a requirement for a specific state the product needs to pass through before reaching the EOC. After that, the producer uses the function changeBearer to deliver the product to the first transporter,



(A) X_c vs τ



(B) Y_c vs τ

FIGURE 7. Relationship between the block propagation delay and the consensus node capacity

Transporter 1. Product tracking data is continuously updated and status changes are checked for compliance with T1 requirements. Thereafter, the governing body becomes the owner of the product and makes a status change in compliance with term T1. The governing body also created a new shipping term, which is the temperature requirement. As the product is delivered to the second transporter, Transporter 2, it uses the blockchain to send instructions to the IoT temperature sensor to initiate temperature recording. At the end of the transportation process, Transporter 2 sends an instruction to stop reading the data, and the value registered by the device is inserted into the blockchain as a Reading object to check whether the data meets the term T2. By the time the product reaches the EOC, the product has passed all clearance checks. In the form of transaction logs, the blockchain records the status, locations, changes of holders, equipment readings, certificates and the transportation terms that are met during the product transportation process. The timeline can be reconstructed using this information, as shown in the bottom half of Figure 8.

5. **Conclusion.** By combining blockchain and IoT technology, a cold chain logistics solution is proposed. Using input from IoT devices, role-based access control, product tracking and traceability, and semi-automated clearance procedures are successfully implemented. Through the proposed data storage and sharing mechanism, some nodes in the IoT are selected as consensus nodes and verification nodes according to the capabilities of IoT devices. Through the consensus mechanism of PoS, block consensus and distributed storage of shared data are realized simultaneously. Based on the Gossip protocol, a hierarchical propagation mechanism for the consensus node layer and the verification node layer is proposed, and the block propagation delay model of the blockchain network is deduced. Simulation analysis shows that the proposed hierarchical propagation scheme has a significant reduction in block propagation delay compared with the traditional protocol, and as the capability thresholds of consensus nodes and verification nodes increase, that is, the

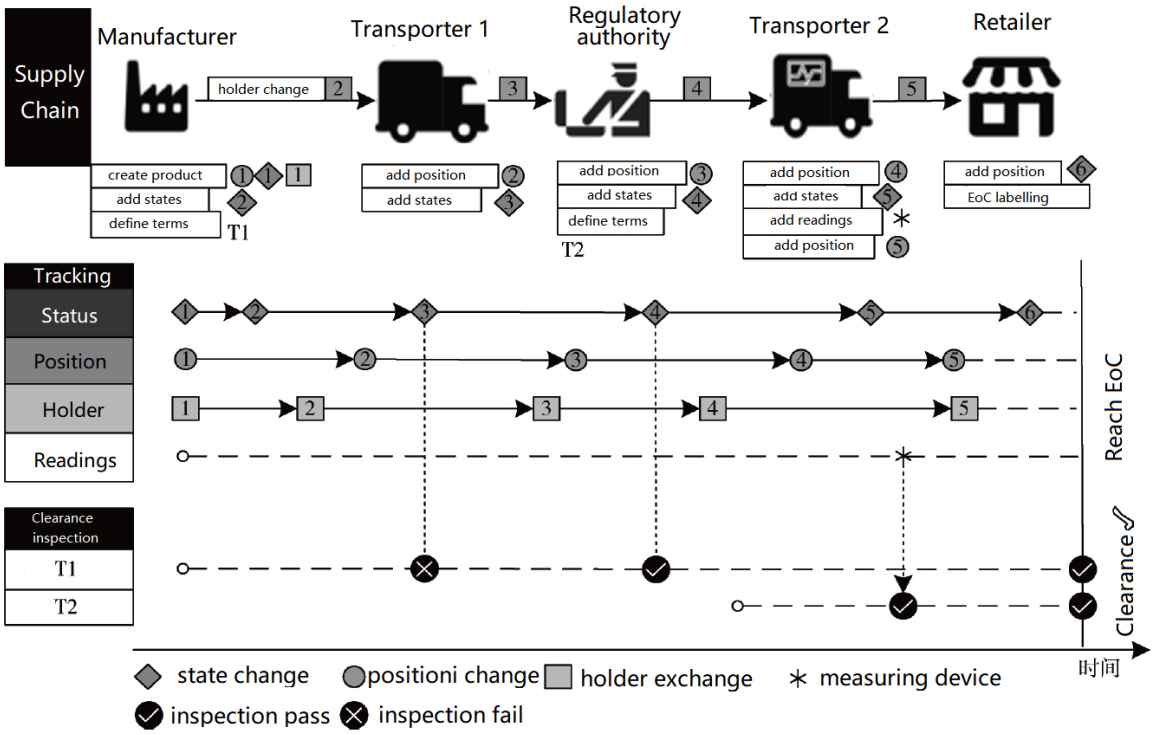


FIGURE 8. Implementation example of the proposed logistics scheme.

ratio between the consensus nodes and verification nodes decreases, the block propagation delay of the blockchain network is reduced accordingly.

The logistics industry is considered by industry insiders to be the one with the highest innovative application value other than the financial industry. The cold chain logistics industry is actively learning from blockchain technology to boost its industrial upgrading. This article is a preliminary exploration of applying blockchain technology to the field of cold chain logistics. In the next step, we will continue to improve the application in this field with improved system performance and more services provided, and further explore the application value of blockchain in the logistics industry.

Data Availability. The data used to support the findings of this study are included within the article.

Conflicts of Interest. The author declares that there is no conflict of interest regarding the publication of this paper.

Funding Statement. This work is supported by project of The Engineering & Technical College of Chengdu University of Technology 'Research on cold chain logistics structure scheme based on blockchain from the perspective of rural e-commerce'.

REFERENCES

[1] J.-W. Han, M. Zuo, W.-Y. Zhu, J.-H. Zuo, E.-L. Lu, X.-T. Yang, "A comprehensive review of cold chain logistics for fresh agricultural products: Current status, challenges, and future trends," *Trends in Food Science & Technology*, vol. 109, no. 3, pp. 536-551, 2021.

[2] T.-Y. Wu, Q. Meng, S. Kumari, P. Zhang, "Rotating behind security: A lightweight authentication protocol based on IoT-enabled cloud computing environments," *Sensors*, vol. 22, no.10, pp. 3858-3871, 2022.

[3] C.-M. Chen, X.-T Deng, W.-S. Gan, S.-K.-H. Islam, "A secure blockchain-based group key agreement protocol for IoT," *The Journal of Supercomputing*, vol. 77, no. 8, pp. 9046-9068, 2021.
[4] C.-M. Chen, X.-T Deng, S. Kumar, S. Kumari, S.-K. Islam, "Blockchain-based medical data sharing schedule guaranteeing security of individual entities," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 7, pp. 1-10, 2021.
[5] S. Pattar, R. Buyya, K.-R. Venugopal, S.-S. Lyengar, L.-M. Patnaik, "Searching for the IoT resources: Fundamentals, requirements, comprehensive review, and future directions," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 3, pp. 2101-2132, 2018.
[6] S. Verma, Y. Kawamoto, Z.-M. Fadlullah, H. Nishiyama, N. Kato, "A survey on network methodologies for real-time analytics of massive IoT data and open research issues," *IEEE Communications Surveys & Tutorials*, vol. 19, no.3, pp. 1457-1477, 2017.
[7] Y. Yang, "Multi-tier computing networks for intelligent IoT," *Nature Electronics*, vol. 2, no. 1, pp. 4-5, 2019.
[8] M.-S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, M.-H. Rehmani, "Applications of blockchains in the Internet of Things: A comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1676-1717, 2018.
[9] H.-N. Dai, Z. Zheng, Y. Zhang, "Blockchain for Internet of Things: A survey," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8076-8094, 2019.
[10] K. Christidis, M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," *IEEE Access*, vol. 54, no. 4, pp. 2292-2303, 2016.
[11] S. Rahmadika, B.-J. Kweka, C.-N.-Z Latt, K.-H. Rhee, "A preliminary approach of blockchain technology in supply chain system," in *International Conference on Data Mining Workshops (ICDMW 2018)*. IEEE, pp. 156-160, 2018.
[12] S. Chen, R. Shi, Z. Ren, J. Zhang, "A blockchain-based supply chain quality management framework," in *14th International Conference on e-Business Engineering (ICEBE 2017)*. IEEE, pp. 172-176, 2017.
[13] F. Tian, "A supply chain traceability system for food safety based on HACCP, blockchain & Internet of things," in *14th International Conference on Service Systems and Service Management (SSSM 2017)*. IEEE, pp. 1-6, 2017.
[14] F. Tian, "An agri-food supply chain traceability system for China based on RFID & blockchain technology," in *16th International Conference on Service Systems and Service Management (ICSSSM 2016)*. IEEE, pp. 1-6, 2016.
[15] C. Xie, Y. Sun, H. Luo, "Secured data storage scheme based on block chain for agricultural products tracking," in *Third International Conference on Big Data Computing and Communications (BIGCOM 2017)*. IEEE, pp. 45-50, 2017.
[16] Q. Lu, X. Xu, "Adaptable blockchain-based systems: A case study for product traceability," *IEEE Software*, vol. 34, no. 6, pp. 21-27, 2017.
[17] E. Regnath, S. Steinhorst, "LeapChain: Efficient blockchain verification for embedded IoT," in *18th International Conference on Computer-Aided Design (ICCAD 2018)*. IEEE, pp. 1-8, 2018.
[18] P. Danzi, A.-E. Kalor, C. Stefanovic, P. Popovski, "Delay and communication trade-offs for blockchain systems with lightweight IoT clients," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 2354-2365, 2019.
[19] J.-P. Cruz, Y. Kaji, N. Yanai, "RBAC-SC: Role-based access control using smart contract," *IEEE Access*, vol. 56, no. 6, pp. 12240-12251, 2018.
[20] S. Bistarelli, G. Mazzante, M. Micheletti, L. Mostarda, F. Tiezzi, "Analysis of ethereum smart contracts and opcodes," in *Second International Conference on Advanced Information Networking and Applications (AINA 2019)*. IEEE, pp. 546-558, 2019.
[21] L. Luu, V. Narayanan, C. Zheng, K. Baweja, P. Saxena, "A secure sharding protocol for open blockchains," in *29th ACM SIGSAC Conference on Computer and Communications Security (CCCS 2016)*, IEEE, pp. 17-30, 2016.
[22] M. Newman, "Pareto distributions and Zipf's law," *Contemporary Physics*, vol. 46, no. 5, pp. 323-351, 2005.
[23] A. Demers, D. Greene, C. Hauser, "Epidemic algorithms for replicated database maintenance," in *Sixth Annual ACM Symposium on Principles of Distributed Computing*, IEEE, pp. 1-12, 1987.
[24] Y. Shahsavari, K. Zhang, C. Talhi, "A theoretical model for block propagation analysis in bitcoin network," *IEEE Transactions on Engineering Management*, vol. 67, no.3, pp.1-18, 2020.
[25] Y. Aoki, K. Shudo, "Proximity neighbor selection in blockchain networks," in *Second International Conference on Blockchain (Blockchain 2019)*, IEEE, pp. 52-58, 2019.

[26] J. Misic, V.-B. Misic, X. Chang, S.-G. Motlagh, M. Zulfiker, "Block delivery time in Bitcoin distribution network," in *19th International Conference on Communications (ICC 2019)*, IEEE, pp. 1-7, 2019.