applied sciences

MDPI

Article

Design of Supply Chain System Based on Blockchain Technology

Jing Li [1,2] and Yafei Song [3,*]

[1] Equipment Management and Unmanned Aerial Vehicle Engineering School, Air Force Engineering University, Xi'an 710051, China; lijing6@eurasia.edu
[2] School of Finance, Xi'an Eurasia University, Xi'an 710065, China
[3] Air Defense and Antimissile School, Air Force Engineering University, Xi'an 710051, China
* Correspondence: yafei_song@163.com

Abstract: As the interaction between companies becomes more and more complex, the problems of asymmetric information, weak traceability, and low collaboration efficiency in the traditional centralized supply chain are becoming increasingly prominent. To solve these problems, this paper designs a supply chain system based on blockchain. With the help of trade chain and information chain platforms, an overall framework of the supply chain system is constructed. By formulating platform interaction rules, the system information exchange format is standardized to ensure the stability and efficiency of system interaction. Smart contracts are used to manage supply chain system transactions and information interactions to achieve efficient and convenient information sharing, ensuring the security and reliability of supply chain information. The comprehensive performance of the system is evaluated through experiments. Experimental results indicate that while the system realizes the basic functions of the supply chain, it can promote the sharing of information between participants and improve its efficiency.

Keywords: supply chain; blockchain; information sharing; smart contract; alliance chain

Citation: Li, J.; Song, Y. Design of Supply Chain System Based on Blockchain Technology. *Appl. Sci.* **2021**, *11*, 9744. https://doi.org/10.3390/app11209744

Academic Editor: Gianluca Lax

Received: 15 September 2021
Accepted: 15 October 2021
Published: 19 October 2021

1. Introduction

The concept of the supply chain [1] first appeared in the late 1980s and was first widely used in the 1990s. The supply chain is a functional network chain centered on core enterprises, including logistics, capital flow, and information flow among raw material suppliers, manufacturers, distributors, end consumers, and supply chain members. It contains links such as product production, processing, transportation, and storage. By participating in different stages of the supply chain with roles of both producer and consumer, enterprises promote the operation of the supply chain network [2]. The supply chain integrates information flow, capital flow, and logistics between enterprises, emphasizing information sharing, risk sharing, exchanges, and cooperation, so as to strengthen collaboration and maximize the overall benefits.

Since the beginning of the 21st century, with the development of the global market and the advent of the digital economy, supply chain capabilities have gradually become a key factor in corporate competition. The market environment is developed rapidly, and various kinds of interactions between supply chain enterprises are becoming more frequent and complex. The centralized supply chain model has been unable to meet the increasing needs of enterprises. It is inevitable for the entire supply chain to be informationalized. With the help of barcode technology and radio frequency data communication technology, Walmart improved the replenishment system and greatly improved the gross profit margin of goods [3]. In 2017, the marine carrier Maersk and IBM jointly established a digital trade platform to manage and track container transportation [4]; and GE Aviation Group is cooperating extensively with Microsoft, using its Azure platform to promote the digital transformation of airlines [5].

Blockchain is a decentralized and tamper-resistant distributed ledger based on multiple technologies [6]. It is characterized by a reliable database, security and trust, collective

maintenance, transparent transactions, and tamper-resistance. It was first used as the underlying technology of Bitcoin [7–12]. Its distributed storage and tamper-resistance can effectively protect data integrity while ensuring its credibility and maximizing sharing. The prospect of applying blockchain in data interaction and storage is good. The Ethereum platform [13] added the Turing complete programming language and smart contracts [14] to the blockchain. Through smart contracts, users can develop and deploy decentralized applications on the Ethereum platform to complete more complex and smarter functions [15]. The application of smart contracts in the blockchain has greatly expanded the application pattern of blockchain technology, extending it from the original simple transaction function to non-financial fields. Xie [16] and others designed the MeDShare system through smart contracts and access-control mechanisms to provide traceability and audit services for medical data. Zyskind et al. [17] proposed a distributed computing framework for secure data protection. Based on blockchain technology, the framework manages data through online indices, with data storage performed at off-chain nodes. McCorry [18] proposed an E-voting electronic voting scheme based on smart contracts, using blockchain technology to ensure the transparency of the voting process and the authenticity of its results. Faisal et al. [19] designed a smart drug supply chain management system based on blockchain. The system records the full-cycle information of drugs in a decentralized manner to ensure medication safety for patients.

There are three main problems with the traditional supply chain [20].

(a) Data is isolated. Enterprises usually establish a dedicated data platform to manage their relevant information. However, in the traditional supply chain, the lack of an open sharing platform between enterprises causes information asymmetry. In addition, the traditional way of information exchange cannot guarantee the security and reliability of data transmission, which makes it difficult to exchange data in the supply chain.

(b) Collaboration efficiency is low. Due to poor information flow in the supply chain and for other reasons, enterprises cannot grasp the relevant conditions in the supply chain in a timely fashion, and it is difficult to form a good cooperation mechanism between them. At the same time, as more enterprises are designed for the supply chain, the core enterprises exert less control, resulting in a lack of coordination among supply chain enterprises and the inability to form a good complementary mechanism, which affects efficiency.

(c) Product information tracing is challenging. This requires full life-cycle tracking. Difficulties sharing data in traditional supply chains, and the inability to guarantee the security of information in transmission and storage, have made it difficult and costly to establish tracing systems.

In response to these problems, we designed a supply chain system based on the blockchain. The overall architecture of the supply chain and trading system is based on smart contracts, which can record trading information while implementing trading functions. All kinds of information of supply chain products can be shared on a distributed information sharing platform through smart contracts and alliance chain technology. The comprehensive performance of the system is experimentally evaluated.

The rest of the paper is organized as follows. Section 1 introduces the basic concepts and operating mechanisms of blockchain and related technologies. In Section 2, a supply chain system model is designed based on the blockchain. Section 3 formulates system interaction rules, writes and deploys smart contracts, and builds a supply chain system. Section 4 tests the comprehensive performance of the system. Section 5 summarizes this work.

2. Related Technology

2.1. Blockchain Technology

The concept of blockchain was first proposed by a scholar named as Satoshi Nakamoto. He described the blockchain as a distributed ledger based on a chain structure. In the blockchain, data blocks are linked in order of generation time, and cryptography [14] and a consensus algorithm [21] are used to ensure the consistency of and lack of tampering

with the distribution of ledger data. Blockchain technology uses peer-to-peer networks to achieve communication between distributed nodes. It uses smart contracts to complete complex business logic functions to achieve automated operations, and a consensus mechanism to realize distributed verification of data results. It uses a chain structure to store data blocks. Cryptography ensures that data cannot be tampered with, to ensure distributed data storage in a trusted environment.

Blockchain platforms are implemented by various methods, but are generally divided into data, network, consensus, contract, and application layers [22], as shown in Figure 1. The data layer records and stores information on the chain, and uses a Merkel tree, asymmetric encryption algorithm, and a timestamp to ensure that data cannot be tampered with and are traceable. Through the peer-to-peer network, the network layer achieves communication between nodes. The consensus layer uses consensus algorithms to achieve a stable consensus between distributed nodes, ensuring data consistency and authenticity. The contract layer provides a smart contract development environment, including the sandbox environment of the blockchain platform and the corresponding programming language. The application layer employs various combinations of programmable currency, finance, and society, according to different application scenarios [23].

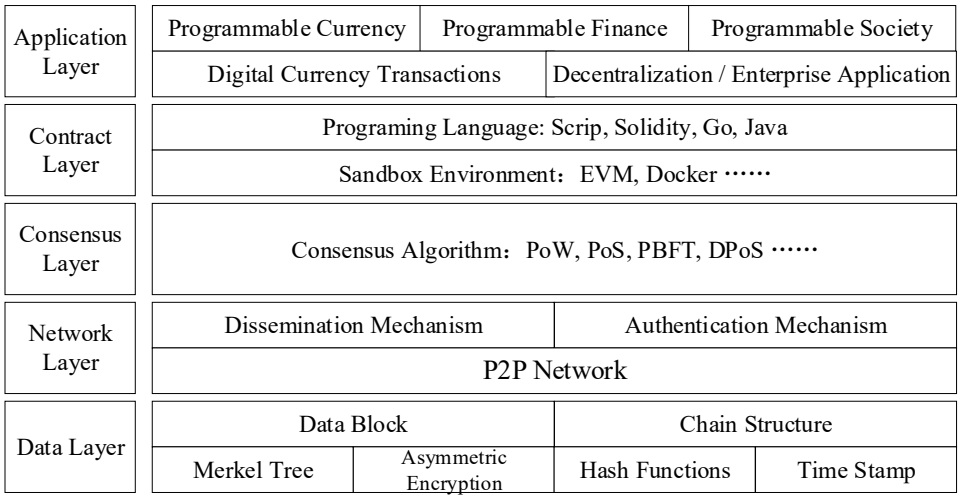

Figure 1. Blockchain platform architecture.

2.2. The Smart Contract

Smart contract is a series of computer program with state and conditional response deployed in a distributed database. The concept of smart contract was proposed by Nick Szabo in the 1990s, with the purpose of converting contract terms to a computer agreement. In a trusted third-party environment, this serves as a trust agent for all parties to a contract so as to fulfill it efficiently and securely. In the early days, subject to the level of computer technology, the concept of smart contracts failed to attract much attention. Blockchain technology provides a trusted execution environment for smart contracts, whose development has ushered in a new age [24].

A smart contract is not just a simple computer program, it also can be a participant in a system [25]. It can proactively respond to received commands; perform judgment, value acceptance, storage, and transmission operations; and process and send information. Figure 2 shows the smart contract model in the blockchain, where it has its own independent states and assets. When receiving assets or information from the outside world, a smart contract performs operations according to the established rules. After the execution is completed, the corresponding information or assets are sent to the target accounts.

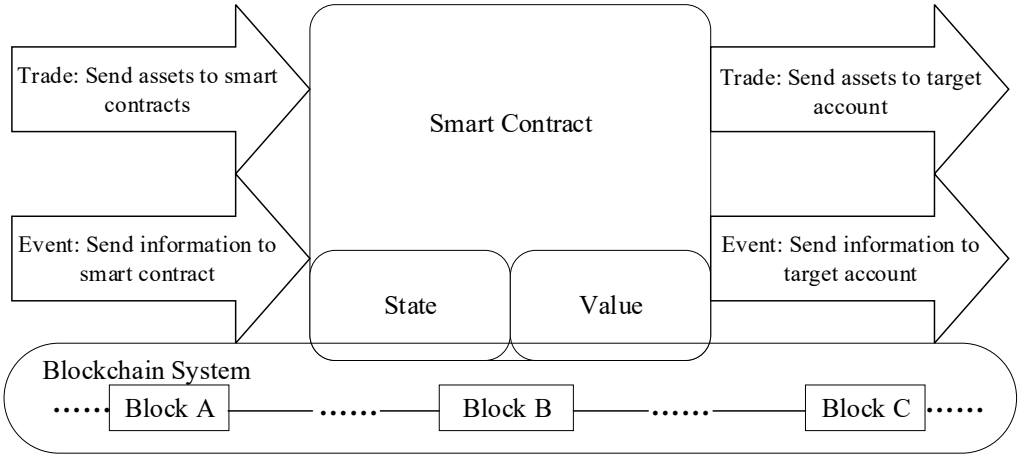

Figure 2. Smart contract model.

3. Blockchain-Based Supply Chain System

3.1. Overall System Architecture

The supply chain system has high requirements for the real-time nature of the trading process, while information sharing is mainly concerned with availability, reliability, and security. Combining the characteristics of the supply chain system and blockchain technology, we divided the system into a trade chain and information chain platforms, as shown in Figure 3.

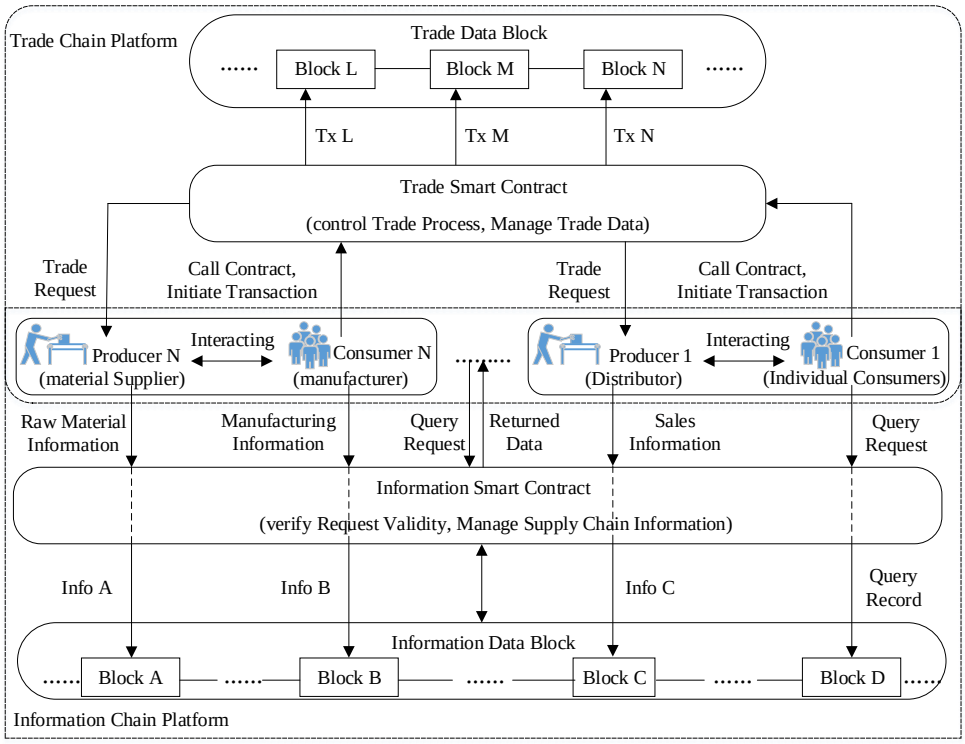

Figure 3. Overall framework of supply chain system.

(a) The trade chain platform is responsible for the trading functions of the supply chain system. Its main participant is the blockchain-based trading alliance chain, where trade smart contracts are deployed. The trade chain platform has two main roles. First, it achieves an efficient and convenient trading process. It controls the trading process between supply chain enterprises, during which a trade smart contract will verify a transaction's legitimacy, completion, and other information, reducing the steps in manual verification, improving the

efficiency and security of supply chain transactions, and reducing supply chain costs. Second, it makes transaction information transparent and traceable. When the trade chain platform executes a transaction, it records the initiation time, parties to the transaction, completion status, and other information, and makes it available to supply chain enterprises.

(b) The information chain platform is responsible for information management. Its main participant is the information alliance chain based on the blockchain, where information smart contracts are deployed. The information chain platform stores relevant data of supply chain products. Enterprises can share their product information here, and can obtain information about their supply chain. The information chain platform can also be used as a product cycle management system. Through recorded product information, the full life cycle of a product can be traced. If a product has a problem, then consumers and the core enterprise can trace through the information chain platform to locate the step where the problem occurred.

3.2. Trading Alliance Chain Based on Blockchain

The trading alliance chain is the basis for the supply chain system to realize the trading function. It adopts the alliance chain model: nodes are given different permissions, individual consumers and other users are connected to the trade chain platform through free nodes, and supply chain enterprises must be authorized by the core enterprise to access the trade chain platform. Individual consumers have fewer permissions and usually can only conduct product transactions; supply chain enterprises have transaction permissions and transaction data permissions.

In the supply chain, consumers conduct transactions by calling trade smart contracts, as shown in Figure 4. The consumer sends a trading request to the trade smart contract account, and the trade smart contract verifies the content of the request and sends it to the corresponding producer, who proofreads the request and executes the trade. The logistics information of the product is sent to the trade smart contract, which forwards the information to the consumer. After receiving the product, the consumer sends confirmation information to the trade smart contract, and transaction funds are paid to the producer. Information on the completed transaction is packaged by the trade smart contract and uploaded to the information alliance chain.

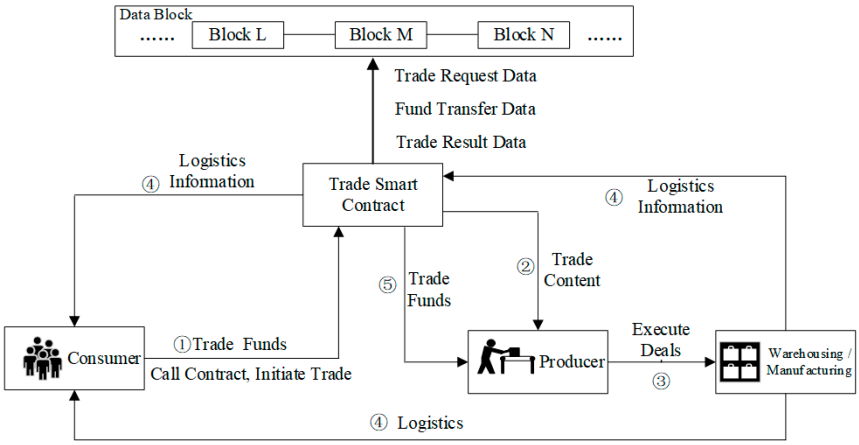

Figure 4. Trade smart contract workflow.

3.3. Information Alliance Chain Based on Blockchain

The information alliance chain manages information in the supply chain, using the alliance chain model. Individual consumers and supply chain companies access the information alliance chain in different ways, and have different permissions. Supply chain enterprises can share information about supply chain products through the information alliance chain, and have different information acquisition permissions, depending on their stage of participation in the supply chain. Individual consumers can usually only obtain information on specific products, and generally lack information upload permission.

After the supply chain enterprise accesses the information alliance chain, it can upload information on supply chain products in the enterprise's intranet to the information alliance chain, which manages the received information, and nodes such as supply chain enterprises, individual consumers, and regulatory agencies can obtain information according to their permissions. When a node obtains information, an information smart contract will verify the legitimacy of the request, and the information will be sent to the requesting node. The structure is shown in Figure 5.

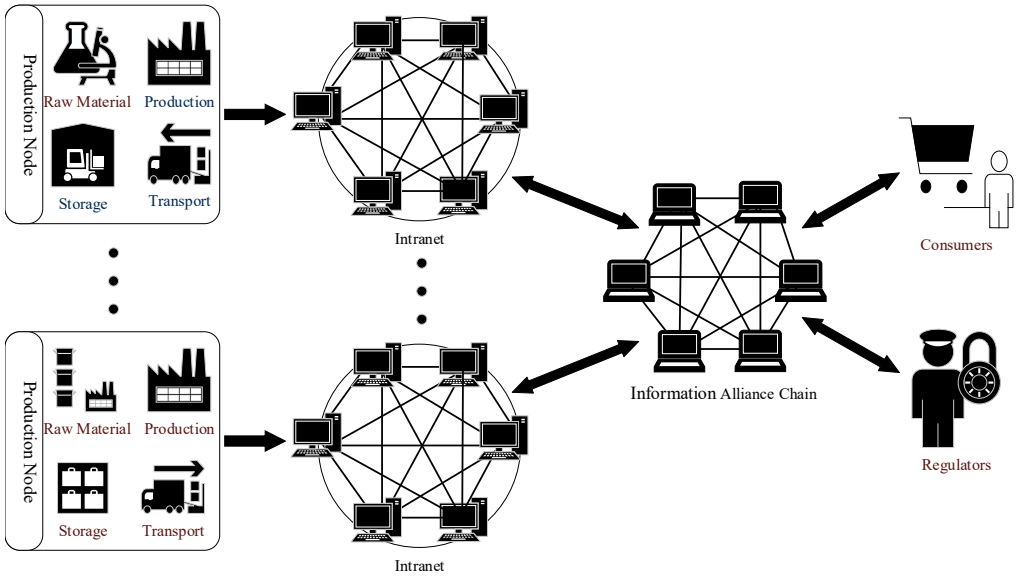

Figure 5. Overall structure of info alliance chain.

4. System Construction

4.1. Currency System in Supply Chain System

Currency is the foundation of transactions. Realizing the functions of a trade chain platform requires an appropriate digital currency system. The currency in the supply chain system is issued by a core enterprise. Digital currency is a value medium for transactions and can be used as a credit certificate between enterprises and between enterprises and financial institutions to achieve reliable trust transfer.

A core enterprise can issue digital currency more conveniently in a supply chain system based on blockchain technology, and by setting relevant parameters, can obtain suitable digital currency, whose issuance is relatively simple. The parameters of digital currency must be combined with actual demand, so the processes of issuing digital currency and setting-related parameters are not repeated.

4.2. Node Permissions

To prevent abuse of the normal operation of the supply chain and related information, nodes in the supply chain system must verify permissions when a requestor asks for information or initiation of a transaction. A node's permissions are assigned by the core enterprise when the node applies for access to the supply chain system. There are three types of nodes.

(a) The core enterprise is the core node of the supply chain system, with the highest permissions, and it is responsible for the overall coordination of the supply chain. It prepares a table of permissions corresponding to each node, and stores it for smart contract verification.

(b) Upstream and downstream enterprises are authorized nodes. When accessing the supply chain system, they must go through the audit of the core enterprise and obtain the corresponding permissions.

(c) Individual consumers are free nodes that can be added to the supply chain system without review by the core enterprise, but their permissions are relatively limited.

4.3. Rules for System Interaction

Various types of interactions between supply chain enterprises are relatively frequent and complex. The system is based on a distributed architecture, and communication pressure is relatively heavy. Therefore, we formulate interaction rules to ensure stable and efficient operation of the supply chain system.

4.3.1. Trade Chain Platform Interaction Rules

The interaction of the trade chain platform involves the roles of producer, consumer, and trade smart contract. A complete transaction process has three stages: 1. The consumer calls a trade smart contract to initiate the transaction; 2. The trade smart contract verifies the request, and the transaction information is sent to the producer's account; 3. After the transaction is completed, the trade smart contract determines the results.

We next analyze the information interaction of the trading process.

(a) Transaction initiation phase. When initiating a transaction, consumers must send the transaction product, corresponding producer, transaction funds, and expected completion time to the smart contract account. The interaction content is as follows: $[id_C, jur_C, C \rightarrow P, tab_C(w, v, a, dl)]$, where id_C is the consumer account information, jur_C is the consumer transaction permission information, $C \rightarrow P$ indicates that the transaction is initiated by consumer C and executed by producer P, tab_C is the information of the transaction, w is the consumer's target product, v denotes the funds for the transaction, a is the agreement for the transaction, and dl is the transaction completion period given by the consumer.

(b) Smart contract verification phase. The trade smart contract verifies the transaction content upon receiving the request. After verification, the trade smart contract sends the transaction content to the producer account. The interaction content is $[T \rightarrow P, inf_T(tab_C, st)]$, where $T \rightarrow P$ indicates that the information is sent to the producer by the trade smart contract; and $infT$ is the content of the transaction information sent by the trade smart contract to the producer, where tab_C is the transaction information sent by the consumer to the trade smart contract, and st is the time when the smart contract receives the request.

(c) Transaction result determination phase. After the transaction is completed, the trade smart contract must determine the transaction completion status. If the producer delivers the product on time, then the trade smart contract forwards the funds to the producer's account and sends the transaction result information to the producer. The content of the information is $[T \rightarrow P, tab_T(v, ct, N)]$, where $T \rightarrow P$ indicates that the information is sent by the trade smart contract to the producer, tab_T is the content of the information, v is the amount of funds, ct is the transaction completion time, and N indicates that the transaction is completed on time and is normal.

If the producer fails to deliver a product on time, then the trade smart contract returns part of the funds to the consumer according to the agreement between the parties, sends the remaining funds to the producer's account, and sends the transaction result information to the producer. The content of the information is $[T \rightarrow P, tab_T(v', ct, od)]$, where v' is the remaining part of the original funds after deducting part, and od indicates that the transaction is overdue.

4.3.2. Information Chain Platform Interaction Rules

The interactive process of the information chain platform has two types of information upload and acquisition. The trade smart contract verifies a received request and the permissions of the requestor, and the next operation is performed. We describe the two types of interaction.

(a) Information upload. When uploading product information, a supply chain enterprise indicates the product type and product information type. Based on the identity of the enterprise, the system analyzes its permissions and sends the corresponding information to the information smart contract. The interaction content is as $\left[id_{up}, jur_{up}, inf_p(tar, ti, c)\right]$, where id_{up} is to upload enterprise identity information, jur_{up} is to upload enterprise in-

formation upload permission, inf_p is the content of the uploaded information, *tar* is the product type, *ti* is the product information type, and *c* is the brief product information.

(b) Information acquisition process. A supply chain enterprise or individual consumer information acquisition request must indicate the target product and the type of information required, at which time it is possible to give necessary conditions such as time intervals to narrow the scope of information. The system analyzes the requestor's permissions and sends it to the information smart contract. The interaction content is $\left[id_{up}, jur_{up}, inf_p(tar, ti, c)\right]$, where id_d is the identity information of the requestor, jur_d is the requestor's information acquisition permission, con_p is the content of the information to be acquired, *tp* is the target product, ti_d is the target information of the product, and *res* denotes the limiting conditions set by the requestor.

The information smart contract verifies the content of the request. If the upload content matches the requestor's permissions, then the corresponding operation will be performed and the operation record will be uploaded to the information alliance chain; if it does not match, then the request is rejected.

4.4. Smart Contract Design

4.4.1. Trade Smart Contracts

The trade smart contract has two functions: to verify the transaction information and to confirm the transaction results and complete the fund transfer.

When a consumer initiates a transaction, the request is sent to the trade smart contract, which verifies the request content and consumer permissions. After verification, the transaction information is sent to the corresponding producer account. Upon accepting the transaction, the producer sends a confirmation message to the trade smart contract, which begins to follow up. The process to verify the legality of transaction information is shown as Algorithm 1.

Algorithm 1. Verify the legality of transaction information

Input: Consumer con1 sends a transaction request: [id_{con1}, jur_{con1}, $con1 \rightarrow pro1$, $tab_{con1}(w, v, a, dl)$]

Output: If the transaction request is legal, the trade smart contract sends the transaction information to producer pro1: [$T \rightarrow pro1$, $inf_T(tab_C, st)$]; if the request does not meet the conditions, then the trade smart contract rejects the request.

Consumer con1 calls the trade smart contract and sends [id_{con1}, jur_{con1}, $con1 \rightarrow pro1$, $tab_{con1}(w, v, a, dl)$] to the trade smart contract;

The public key address of consumer con1 is obtained, consumer = msg. sender;
If con1 != legal user []
return;
else
If the target product w = = p of con1 []
then
If commodity w matches agreement a
then
The trade smart contract sends [$T \rightarrow pro1$, $inf_T(tab_C, st)$] to producer pro1;
else return;
end If
else return;
end If
Producer pro1 verifies the information in Inf_T (tab_{con1},st);
end If
If the transaction request meets the requirements
then
Confirmation information is returned to the trade smart contract;
else
Reject this transaction;
end If

When the transaction is over, the trade smart contract determines the transaction completion and sends funds to the producer. If the transaction is completed on time, then the trade smart contract will normally transfer the funds to the producer pro1 account; if the transaction is overdue, then the trade smart contract will pay part of the funds to the producer according to the agreement, and the remaining funds will be returned to the consumer. The identification of the transaction result can be implemented by Algorithm 2.

Algorithm 2. Transaction result identification

Input: transaction completion status (transaction completion time *ct*);
Output: Confirmation of the transaction result, and funds are sent to the producer according to the transaction result.
If ct $\leq$ dl
then
transfer (address _ pro1, v);
Send [$T \rightarrow P$, $tab_T(v, ct, N)$] to the producer account;
else
v' = v − m;
transfer (address _ pro1, v');
Send [$T \rightarrow P$, $tab_T(v', ct, od)$] to the producer account;
end If

4.4.2. Information Smart Contract

The information smart contract is the basis of information exchange in the supply chain. It has two main tasks: to check whether information uploaded by the enterprise and its permissions meet requirements; and to check the legality of the information acquisition request of each node. To ensure the accuracy and availability of data information in the supply chain, the information smart contract must verify the information uploaded by an enterprise, i.e., whether it is consistent with the enterprises' permissions. Algorithm 3 shows the process of information uploading.

Algorithm 3. Upload information

Input: enterprise part a uploads product information message a [];
Output: If the uploaded information matches the permissions, then the information will be stored in the information alliance chain; if it does not match, then the request will be rejected.
The enterprise part a calls the information smart contract and sends message a [] to the information smart contract;
Information smart contract obtains the public key address of enterprise part a, *pkA a* = msg. sender;
Retrieve tag a = message a [$inf_p(tar,ti)$];
If tab a = = lab of massage a []
then
Verify the data format of form a in message a [];
If form a = = stand [tag a]
then
The information smart contract classifies message a by label and stores it in the information chain;
else Return error message;
end If
else return;
end If

After the information is stored in the information alliance chain, other enterprises in the supply chain can obtain it. However, this information is not completely open to all users, as nodes have different permissions. Users needing to obtain information from the information chain platform must send an information acquisition request to the information

smart contract, which determines whether the request is legal based on the requestor's permissions and the requested information. Such information acquisition process can be described in Algorithm 4.

Algorithm 4. Information acquisition

Input: enterprise part b sends an acquisition request application b [];

Output: If the content of the request matches its permissions, then the information smart contract sends the corresponding information to the requestor's account; if it does not match, then the request is rejected.

Enterprise part b calls the information smart contract and sends an information query request application b [];

The information smart contract obtains the public key address of the participant part b, pkA b = msg. sender;

Purview b = purview [*pkA b*];

If application b [$con_p(tp,ti_d)$] = = purview b

then

Smart contract retrieves request content con_p, checks the availability of information;

If con_p = = 0

then return;

else

con_p [] → part b, and saves the request record in the information alliance chain;

end If

else return; end If

4.5. Contract Deployment

A smart contract can be compiled and deployed after the smart contract design is completed. This paper uses the Solidity programming language [26], kernel version 0.4.22, and an EthFiddle-Solidity compiler. The compilation results are shown in Figures 6 and 7.

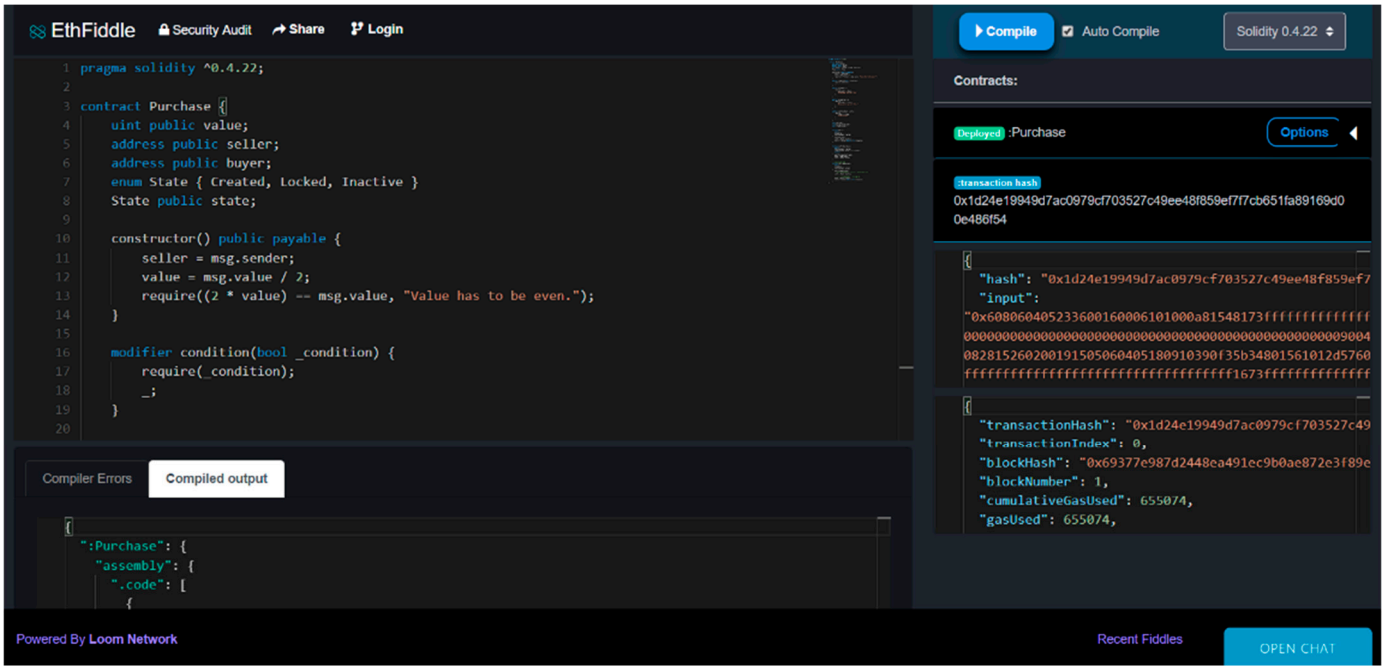

Figure 6. Trade smart contract compilation results.

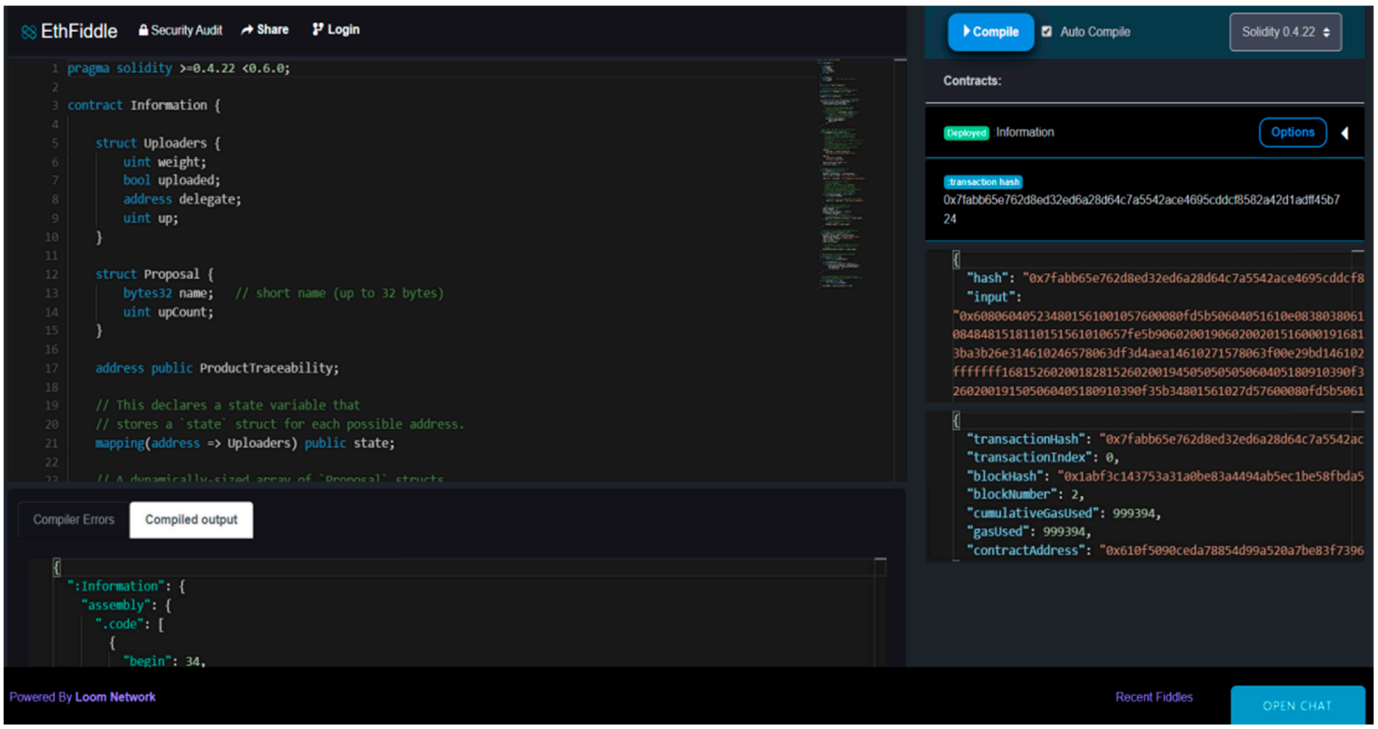

Figure 7. Info smart contract compilation results.

A smart contract can be deployed after compilation, and a user can implement the corresponding operation by calling a smart contract. The deployment results are shown in Figures 8 and 9. We use EthFiddle pre-stored accounts; the main account is the transaction initiation account, and the remaining accounts are the main participants of the supply chain.

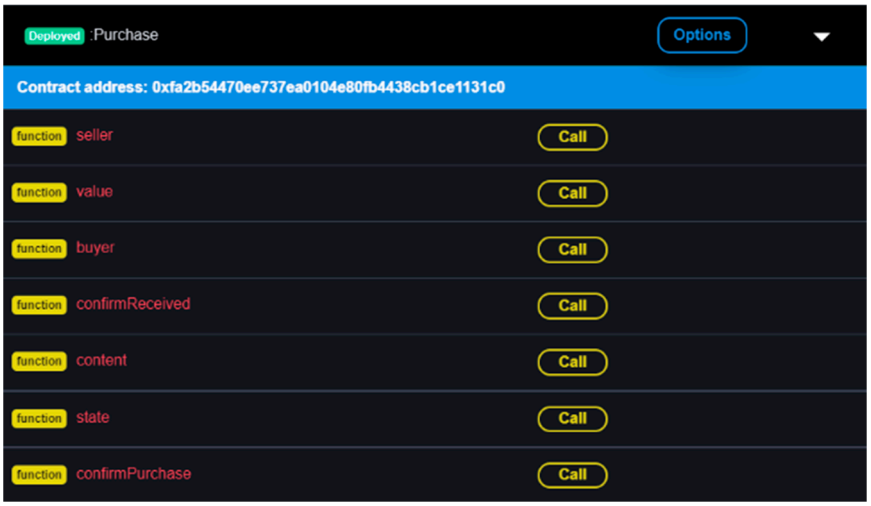

Figure 8. Trade smart contract deployment results.

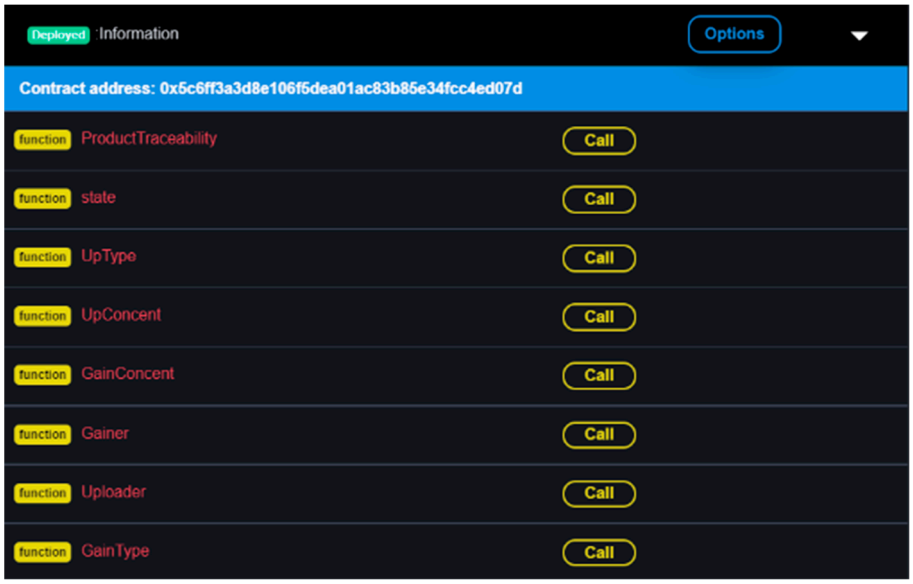

Figure 9. Info smart contract deployment results.

5. Experiment and Analysis

After system construction is completed, the performance of this system will be tested and analyzed. Basic performance of the supply chain system will be firstly tested, including the transaction, information upload, and information acquisition functions. Similar programs are compared to analyze the advantages and disadvantages of the system. The second test is to analyze the system performance, i.e., the security and throughput.

The test environment is as follows: Windows 10 operating system, Intel Core i5-9400 processor, main frequency 2.90 GHz, 8 GB memory.

5.1. Basic Functions of the System

The system function test was divided into tests of the trade chain and information chain platforms. We tested the trading function of the trade chain platform and the information upload and acquisition functions of the information chain platform.

A test was performed on the trading function of the trade chain platform. During the transaction process, the trade chain platform must complete legality verification, result confirmation, and fund transfer. The test simulated the transaction process through virtual transactions between any two nodes in the system. The details of the transaction process were controlled by the trade smart contract. The system functions were analyzed by the transaction information stored in the corresponding block after the transaction was completed. The block information is shown in Figure 10. According to the test results, the trade chain platform could realize the transaction legality verification, transaction result identification, and transaction fund transfer functions, and could store transaction information, which meets the basic requirements of supply chain transactions.

The function test of the information chain platform was then carried out. When a node uploads or obtains information, the information chain platform must verify the node's identity, permissions, and operation objects. After the operation is completed, the information chain platform stores relevant records in the information alliance chain for later verification. The test simulated the workflow of an information chain platform by uploading virtual information through a node and obtaining the information from another node. Figure 11 shows the product information uploaded by an enterprise to the information alliance chain, and Figure 12 shows the operation record of the information smart contract after a user obtained product information. It can be seen that the information chain platform could realize basic information upload and information acquisition functions.

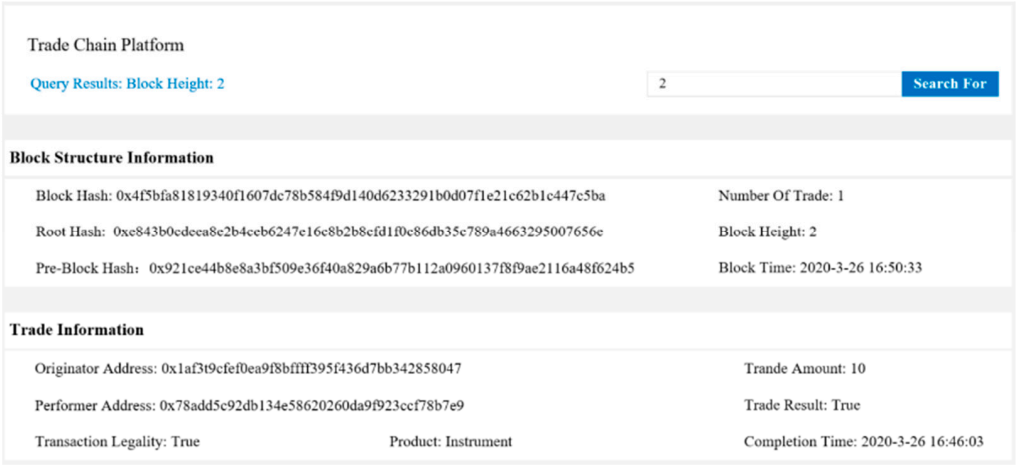

Figure 10. Trading block information.

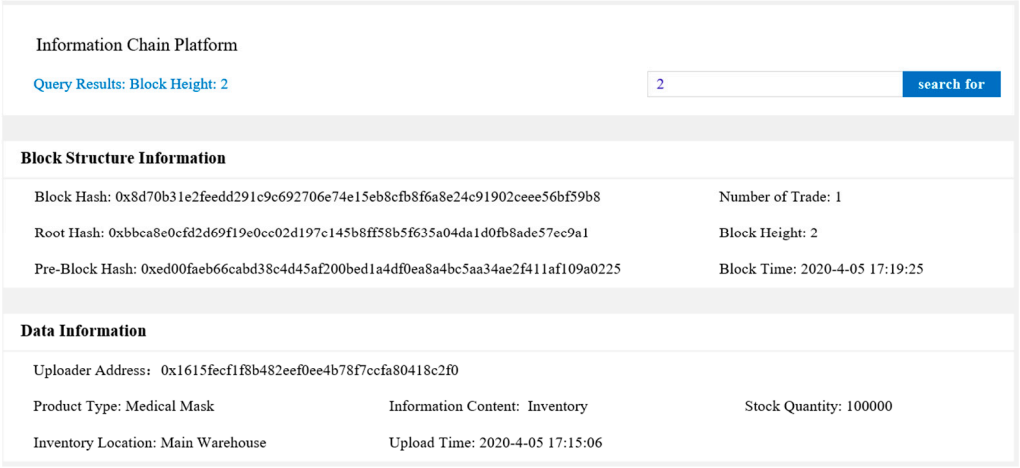

Figure 11. Product information block.

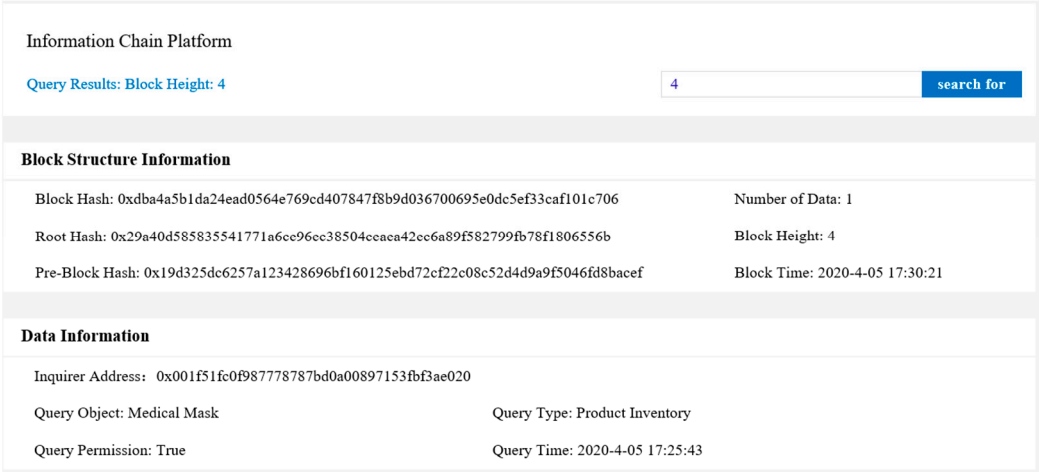

Figure 12. Records fetched.

Following the performance test, we compare the program with those proposed in the literature [27–30], which are applied in medical data management [27,28], information management in the construction industry [29], and the beef supply chain [30]. They are compared from five aspects, including the contribution of block chain, information

traceability, search, third-party access and access control. The results are shown in Table 1. Through comparison, it can be noticed that this program had certain advantages as a whole, but compared to other research results, each of its functions has not been fully perfected. For example, the search function does not support keyword search, and the access control mechanism is relatively simple. It is necessary to continue improving the system functions in future research.

Table 1. Functional comparison.

System Function	Literature [27]	Literature [28]	Literature [29]	Literature [30]	This Paper
Contribution of Blockchain	√	√	√	×	√
Information Traceability	√	×	√	√	√
Search	√	√	×	√	√
Third-party Access	×	√	√	√	√
Access Control	√	√	√	√	√

5.2. System Performance

5.2.1. Check on the Smart Contract

We start with the check on the vulnerability of smart contracts, using the ant blockchain BaaS platform for vulnerability detection. This platform integrates smart contract detection functions and can detect common security vulnerabilities such as unauthorized access and re-entrant attacks that may exist in smart contracts [31]. Figures 13 and 14 show the detection results of trade smart contracts and information smart contracts, respectively. The results reveal unauthorized access vulnerabilities in both, primarily because the user lacks the identity authentication step when triggering the state change operation to modify unrelated state variables. In the later stage of system improvement, it is necessary to add an identity authentication mechanism when calling unrelated state variables.

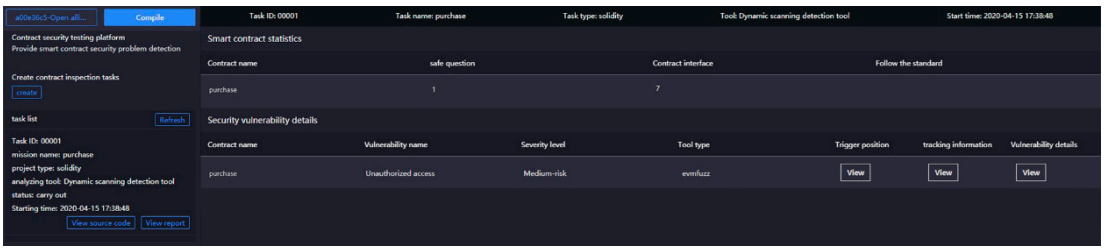

Figure 13. Test results of trade smart contract.

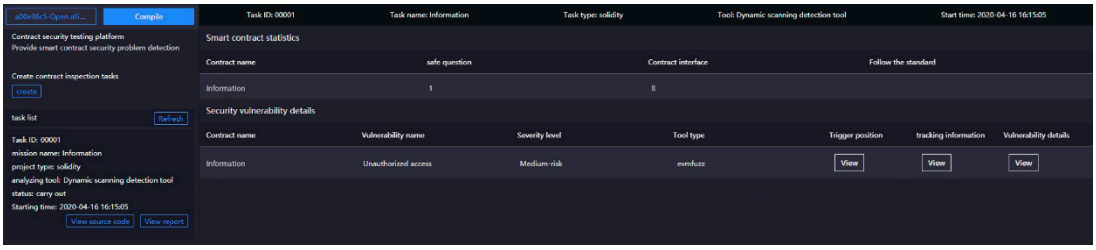

Figure 14. Test results of info smart contract.

5.2.2. System Fault Tolerance Test

We define the fault tolerance of the supply chain system as its ability to maintain stable operation when attacked by malicious nodes in a system with a certain number of access nodes. In the experiment, the probability of a certain number of malicious nodes successfully destroying the normal operation of the system was used as an indicator to evaluate fault tolerance performance.

Combining the results of the final experiment and equipment performance, we set the total number of nodes in the supply chain system to 60. The number of malicious nodes was increased from 1 to 40, with a step size of 3. Repeated experiments were conducted under different numbers of malicious nodes to obtain the corresponding attack success rates. The attack method of the malicious node was set to forge block information. When the normal node started to record the forged block, it was assumed that the malicious node attack had been successful. The experimental results are shown in Figure 15.

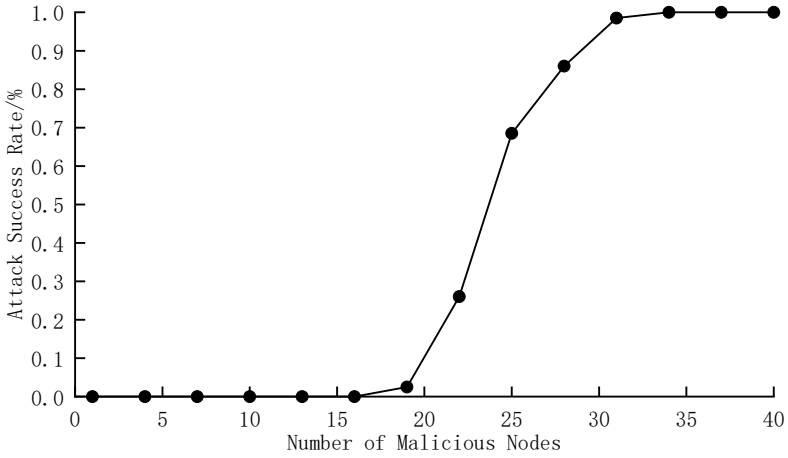

Figure 15. Attack success rate under different number of malicious nodes.

The experimental results show that the attack success rate of malicious nodes decreased as the number of malicious nodes decreased. When the number of malicious nodes was less than 32% of the total, the probability of successful attack approached zero. In the supply chain system, the core enterprise will audit each enterprise, so the probability of malicious nodes exceeding 1/3 of the total is usually low. This shows that the system has high fault tolerance performance, but there is still some room for improvement. Later, the system consensus algorithm and identity authentication mechanism can be improved.

5.2.3. System Throughput Test

System throughput refers to the amount of information that a system can handle per unit of time. We used the transaction throughput per second (TPS) to evaluate system throughput. Although the supply chain system has lower requirements on throughput, to ensure the stability of system operation and subsequent improvement, we tested the throughput through experiments.

We used the total number of nodes in the supply chain system as a variable, increasing it from 5 to 70, with a step size of 5. Repeated experiments were made under different numbers of nodes, and the average value of throughput in each state was calculated. The experimental results are shown in Figure 16. It can be seen that when the number of nodes was between 5 and 45, the throughput of the supply chain system showed a linear upward trend with the increase of the number of nodes. When the number of nodes was greater than 45, the system throughput decreased, and eventually remained around 36 TPS. This shows that even in a relatively simple experimental environment with a single request content, the throughput of the supply chain system is low. In follow-up research, the supply chain system architecture, consensus algorithm, and other aspects must be improved to increase the system throughput.

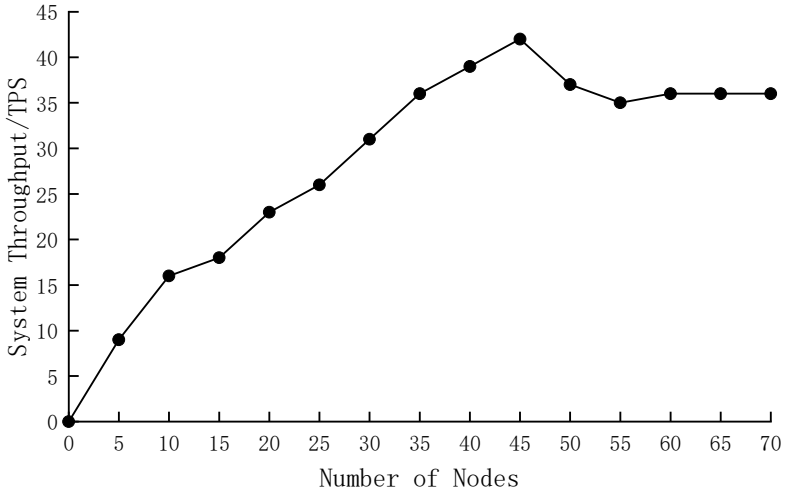

Figure 16. System throughput under different number of nodes.

6. Conclusions

With the rapid development of blockchain technology and the enormous attention it has received, it is being applied to more and more fields. We proposed a supply chain system based on blockchain technology and attempted to solve some of its problems. The system is based on a trade chain platform and information chain platform. The first is responsible for trading functions, and the second provides for convenient and reliable information sharing. Trade smart contracts are deployed to realize the management of transaction process information, including funds and results; information smart contracts are deployed in the information chain platform to enable participants to carry out convenient, efficient information interaction, and to manage the permissions of each participant for information security. The comprehensive performance level of the system was analyzed through experiments. The results show that the system can meet the basic requirements of the supply chain, but requires improvement in subsequent research in terms of throughput and security.

Author Contributions: Conceptualization, J.L. and Y.S.; methodology, J.L.; software, J.L.; validation, J.L. and Y.S.; writing—original draft preparation, J.L.; writing—review and editing, Y.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Major theoretical and practical research project of Philosophy and social Sciences in Shaanxi (2021ND0267).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Wible, B.; Mervis, J.; Wigginton, N.S. Rethinking the global supply chain. *Science* **2014**, *344*, 1100–1103. [CrossRef]
2. Simon, C.; Pietro, R.; Mihalis, G. Supply chain management: An analytical framework for critical literature review. *Eur. J. Purch. Supply Manag.* **2000**, *6*, 67–83.
3. Shin, S.; Eksioglu, B. An empirical study of RFID productivity in the U.S. retail supply chain. *Int. J. Prod. Econ.* **2015**, *163*, 89–96. [CrossRef]
4. White, M. A Global Trade Platform Using Blockchain Technology Aimed at Improving the Cost of Transportation, Lack of Visibility and Inefficiencies with Paper-Based Processes. 2018. Available online: https://www.ibm.com/blogs/blockchain/2018/01/digitizing-global-trade-maersk-ibm/ (accessed on 26 August 2021).

5. Allison, I. Codename 'TRUEngine': GE Aviation, Microsoft Reveal Aircraft Parts Blockchain. 2019. Available online: https://www.coindesk.com/codename-truengine-ge-aviation-and-microsoft-reveal-aircraft-parts-certification-blockchain (accessed on 26 August 2021).
6. Nakamoto, S. A Peer-To-Peer Electronic Cash System. 2008. Available online: https://nakamotoinstitute.org/bitcoin/ (accessed on 27 August 2021).
7. Du, M.; Chen, Q.; Chen, J.; Ma, X. An Optimized Consortium Blockchain for Medical Information Sharing. *IEEE Trans. Eng. Manag.* **2021**, *68*, 1677–1689. [CrossRef]
8. Boubeta-Puiga, J.; Rosa-Bilbaob, J.; Mendling, J. CEPchain: A graphical model-driven solution for integrating complex event processing and blockchain. *Expert Syst. Appl.* **2021**, *184*, 115578. [CrossRef]
9. Kyzy, I.E.; Song, H.; Vajdi, A.; Wang, Y.; Zhou, J. Blockchain for consortium: A practical paradigm in agricultural supply chain system. *Expert Syst. Appl.* **2021**, *184*, 115425. [CrossRef]
10. Leng, J.; Ye, S.; Zhou, M.; Zhao, J.L.; Liu, Q.; Guo, W.; Cao, W.; Fu, L. Blockchain-Secured Smart Manufacturing in Industry 4.0: A Survey. *IEEE Trans. Syst. Man Cybern. Syst.* **2021**, *51*, 237–252. [CrossRef]
11. Liao, H.; Mu, Y.; Zhou, Z.; Sun, M.; Wang, Z.; Pan, C. Blockchain and Learning-Based Secure and Intelligent Task Offloading for Vehicular Fog Computing. *IEEE Trans. Intell. Transp. Syst.* **2021**, *22*, 4051–4063. [CrossRef]
12. Singh, M.; Aujla, G.S.; Singh, A.; Kumar, N.; Garg, S. Deep-Learning-Based Blockchain Framework for Secure Software-Defined Industrial Networks. *IEEE Trans. Ind. Inform.* **2021**, *17*, 606–616. [CrossRef]
13. Buterin, V. A Next-Generation Smart Contract and Decentralized Application Platform. 2014. Available online: https://cryptorating.eu/whitepapers/Ethereum/Ethereum_white_paper.pdf (accessed on 27 August 2021).
14. Nick, S. Smart contracts: Building blocks for digital markets. *J. Transhumanist Thought* **1996**, *18*, 16.
15. Dezfoulian, H.R.; Afrazeh, A.; Karimi, B. A new model to optimize the knowledge exchange in industrial cluster: A case study of Semnan plaster production industrial cluster. *Sci. Iran.* **2017**, *24*, 834–846. [CrossRef]
16. Xie, C.; Sun, Y.; Luo, H. Secured data storage scheme based on block chain for agricultural products tracking. In Proceedings of the 2017 3rd International Conference on Big Data Computing and Communications (BIGCOM), Chengdu, China, 10 August 2017; pp. 45–50.
17. Tian, F. A supply chain traceability system for food safety based on HACCP, blockchain & Internet of things. In Proceedings of the 2017 International Conference on Service Systems and Service Management, Dalian, China, 16–18 June 2017; pp. 1–6.
18. Rahmadika, S.; Kweka, B.J.; Latt, C.N.Z.; Rhee, K. A preliminary approach of blockchain technology in supply chain system. In Proceedings of the 2018 IEEE International Conference on Data Mining Workshops (ICDMW), Singapore, 17–20 November 2018; pp. 156–160.
19. Ye, X.; Shao, Q.; Xiao, R. A supply chain prototype system based on blockchain, smart contract and Internet of Things. *Sci. Technol. Rev.* **2017**, *35*, 62–69.
20. Reijers, W.; Coeckelbergh, M. The blockchain as narrative technology: Investigating the social ontology and normative configurations of cryptocurrencies. *Philos. Technol.* **2016**, *31*, 1–28. [CrossRef]
21. Nach, H.; Ghilal, R. Blockchain and smart contracts in the logistic and transportation industry: The demurrage and mar-itime trade use case. In Proceedings of the 1st Annual Toronto FinTech Conference, Toronto, ON, Canada, 20–21 October 2017; pp. 1–9.
22. Ghadge, A.; Dani, S.; Chester, M. A systems approach for modelling supply chain risks. *Supply Chain. Manag.* **2013**, *18*, 523–538. [CrossRef]
23. Saberi, S.; Kouhizadeh, M.; Sarkis, J.; Shen, L. Blockchain technology and its relationships to sustainable supply chain management. *Int. J. Prod. Res.* **2019**, *57*, 2117–2135. [CrossRef]
24. Wu, J.-N.; Tran, N.K. Application of blockchain technology in sustainable energy systems: An overview. *Sustainability* **2018**, *10*, 3067. [CrossRef]
25. Ruffing, T.; Moreno-Sanchez, P.; Kate, A. CoinShuffle: Practical decentralized coin mixing for bitcoin. In Proceedings of the 19th European Symposium on Research in Computer Security, Wroclaw, Poland, 7–11 September 2014; pp. 345–364.
26. Shao, Q.-F.; Jin, C.-Q.; Zhang, Z.; Qian, W.-N.; Zhou, A.-Y. Blockchain: Architecture and research progress. *Chin. J. Comput.* **2018**, *41*, 969–988.
27. Karame, G.; Capkun, S. Blockchain security and privacy. *IEEE Secur. Priv.* **2018**, *16*, 11–12. [CrossRef]
28. Ouyang, L.-W.; Wang, S.; Yuan, Y.; Ni, X.-C.; Wang, F.-Y. Smart contracts: Architecture and research progresses. *Acta Autom. Sin.* **2019**, *45*, 445–457.
29. Gatteschi, V.; Lamberti, F.; Demartini, C.; Pranteda, C. Blockchain and smart contracts for insurance: Is the technology mature enough? *Future Internet* **2018**, *10*, 20. [CrossRef]
30. Sandhu, R.S.; Coyne, E.J.; Feinstein, H.L.; Youman, C.E. Role-based access control models. *IEEE Comput.* **1996**, *29*, 38–47. [CrossRef]
31. Ferraiolo, D.; Sandhu, R.; Gavrila, S.; Kuhn, R.; Chandramouli, R. Proposed NIST standard for role-based access control. *ACM Trans. Inf. Syst. Secur.* **2001**, *4*, 224–274. [CrossRef]