



Article

A Novel Decentralized E-Commerce Transaction System Based on Blockchain

Yuanyuan Xiao ¹, Chuangming Zhou ¹, Xinpeng Guo ^{1,*} , Yafei Song ^{1,*}  and Chen Chen ²

¹ College of Air and Missile Defense, Air Force Engineering University, Xi'an 710051, China; x15545577162@163.com (Y.X.); afeu_zhcm@163.com (C.Z.)

² Xi'an Satellite Control Center, Xi'an 710043, China; chenchen2020@163.com

* Correspondence: xinpeng_guo@163.com (X.G.); yafei_song@163.com (Y.S.)

Abstract: With the rapid development of e-commerce systems, the centralized service model gradually fails to meet the needs of SMEs. In the existing centralized e-commerce system, users' transaction data and reputation scores are stored in a centralized cloud server, which has high storage cost, low processing efficiency, and the data is vulnerable to attacks and leaks. However, the existing decentralized e-commerce systems more than its reputation system to store the average credit score evaluation are receiving unfair evaluations against risk. The system of malicious nodes and no disciplinary measures, is not conducive to system development. To solve this problem, this paper proposes a blockchain-based decentralized e-commerce transaction system. The system commodity information is stored in the Interplanetary File System (IPFS) and the returned commodity addresses are stored in the blockchain to enhance the service performance. This paper proposes a reputation evaluation model based on multi-criteria decision making (MCDM), which can effectively resist unfair evaluation and collusion attacks, and proposes an incentive mechanism based on reputation value to reward and punish nodes, thus promoting the good circulation of the system. We implement the proposed system based on Ethereum. The experimental results show that the system has a small communication cost, accurately reflects the user's reputation value, and has good availability and reliability.

Keywords: blockchain; e-commerce; IPFS; MCDM; reputation value



Citation: Xiao, Y.; Zhou, C.; Guo, X.; Song, Y.; Chen, C. A Novel Decentralized E-Commerce Transaction System Based on Blockchain. *Appl. Sci.* **2022**, *12*, 5770. <https://doi.org/10.3390/app12125770>

Academic Editors: Zheng Chang, Jun Wu and Shancang Li

Received: 5 May 2022

Accepted: 3 June 2022

Published: 7 June 2022

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2022 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

With the increasing popularity of Internet technology, commodity exchange has undergone profound reforms and innovations, gradually transforming from traditional offline exchange to online real-time transaction [1]. The sales volume of retail e-commerce achieved totally USD 4.89 trillion in 2021 and is expected to grow to USD 6.39 trillion in 2024 [2]. E-commerce has fundamentally changed people's way of life, shopping, office, medical, education, entertainment and other necessities of people's lives can be perfectly solved through the e-commerce system. The third-party network payment platform driven by the e-commerce industry has fundamentally overturned the original capital flow and brought greater convenience to people. However, current e-commerce platforms face some problems. For example, (1) the third-party organization (logistics party) is supervised by the platform only, probably leading to false logistics information and advanced signature [3]; (2) commodity data and buyer information are stored in enterprise servers centrally, which are vulnerable to be maliciously attacked, resulting in data leakage or theft; (3) Lack of incentive mechanism, buyers have an inactive enthusiasm for comments, and there are numerous false praise and comments, influencing buyers' judgment towards sellers.

Blockchain is a distributed ledger consisting of encryption algorithm, consensus mechanism and smart contract, featured by authenticity, unforgeability and traceability [4,5], whose core value lies in establishing the open and transparent rules of the algorithms,

constructing a trust network [6], and ensuring the security and privacy of transactions [7]. The combination of blockchain and e-commerce transaction systems can enhance the trust between users and platforms, protect the privacy of users and ensure that their evaluation cannot be modified, improving the reliability, security and credibility of the system [8,9].

In recent years, decentralized reputation systems (DRSs) have been proposed. However, researchers focus on decentralized reputation management for simple transactions rather than online shopping, and do not sufficiently consider transaction factors such as transaction time, transaction amount, and user's previous reputation score to prevent common attacks when performing reputation assessment. Therefore, this paper proposes an e-commerce transaction system based on blockchain and IPFS as well as a reputation value calculation model based on Multi-Criteria Decision Making (MCDM). Specifically, the seller stores the detailed information (name, price, etc.) of commodity in the IPFS system and obtains the return address in the chain. The buyer concludes the transaction through the smart contract [10]. The logistics party updates the logistics information on the blockchain, which is then signed by the seller for evaluation. The platform can calculate and update the reputation value according to the transaction records. The main contributions of this paper are as follows.

1. This paper proposes a new e-commerce transaction system based on blockchain. The buyer and seller temporarily store the deposit in a smart contract, and the logistics service provider updates the logistics information on blockchain [11]. When the buyer receives the goods, the deposit will be automatically transferred to the seller.
2. Unlike most decentralized e-commerce systems, this paper proposes to store the item details in IPFS and then store the item address in the blockchain. To reduce IPFS storage space, commodity records are periodically cleaned up.
3. By investigating the common attacks on reputation evaluation, this paper proposes a reputation evaluation scheme based on simple weighting (SAW) and MCDM. By combining different factors (transaction completion time, reputation value of trading partners) to evaluate the reputation value of the participants, it can effectively defend against various attacks, such as collusion attacks and unfair evaluation attacks against reputation value.
4. We propose a blockchain-based incentive for e-commerce system to promote stable operation of the system. A good reputation is a reflection of the quality of the seller's service. Buyers with good reputation value can pay less deposit in the transaction. On the contrary, if the reputation value is low, there is a penalty.

The rest of this paper is organized as follows. Section 2 introduces the relevant work. In Section 3, the blockchain framework of the electronic transaction system and the system architecture of the paper are presented, and the proposed system is demonstrated in detail. Section 4 presents and analyzes the experimental results. Section 5 summarizes the research and puts forward the future research direction.

2. Related Work

Blockchain was proposed by Satoshi Nakamoto, which is a distributed ledger consisting of encryption algorithm, consensus algorithm and smart contract [12]. As illustrated in Figure 1, It is a chained storage structure [13]. Each block stores transaction data for a period of time, which is linked by the Hash value of the previous block and all blocks involved in the transaction can be traced. Therefore, blockchain data will not be easily changed and is applicable to be traced and is stored in tamper proof supply chain systems [14].

Smart contract is an executable program whose instances and statuses are stored in blockchains. Blockchains are trusted, traceable and tamper-proof without the need for trusted third parties that usually constitute a single point of failure [15]. There is some explorations on the combination of blockchain and e-commerce. For example, the decentralized market Open Bazaar 1.0 for transaction with bitcoin was officially launched in April 2016, providing ideas to develop a secure e-commerce transaction system. Gao proposed a cross-border e-commerce system based on blockchain, which solved the problem of the

difficult traceability of cross-border commodity sales by combining the blockchains features of credibility and traceability on transactions [16]. Zhang et al. proposed a traceability system of agricultural product supply chain based on master-slave alliance chain. The master chain is the agricultural product supply chain, and the slave chain is the third-party organization supervision chain that is connected with the master chain by smart contract, which solved the problems of small storage capacity and low storage efficiency of a single blockchain [17]. Zhang et al. proposed an efficient storage method based on cloud storage and dual blockchain, which encrypts and stores high-capacity data in the cloud, and saves the index in the blockchain, avoiding the limited storage capacity of blockchain and improving the speed of data chaining [18]. Jiang and Chen designed a Blockchain-Supported E-Commerce Platform (BS-EP) for small-and medium-sized enterprises, which provides trust guarantee for transactions between small-and medium-sized enterprises. It also proposed three applications to solve the trade problems of enterprises based on the traceability and tamper proof characteristics of blockchain [19]. Zhou et al. proposed a Decentralized Reputation System (BC-DRS) based on blockchain in e-commerce environment [20]. The system stores users' comments in Interplanetary File System (IPFS), returns them to the corresponding address, and calculates the reputation value weighted by actual transaction factors. A monetary incentive mechanism was also proposed. The experimental results showed that the proposed decentralized reputation system has good usability and reliability. However, most of the proposed decentralized e-commerce systems are still focused on the transactions between buyers and sellers. That mean, they fail to record the information of third-party institutions in the chain, and there is no available corresponding reputation system to effectively prevent the attacks.

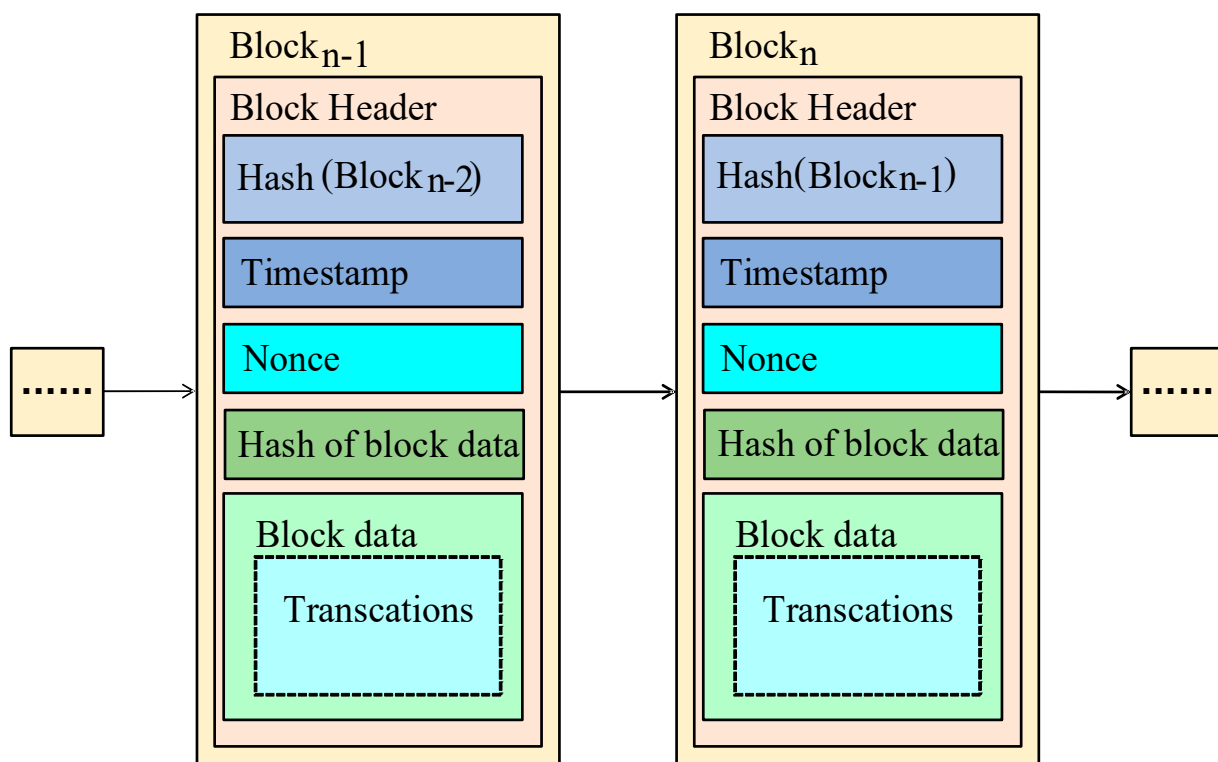


Figure 1. Block structure.

In this paper, we propose an e-commerce transaction system based on blockchain and IPFS, and establish a decentralized reputation model based on multi-criteria decision making (MCDM) method. In this system, merchants store the commodity details in the IPFS system and update the returned addresses to the blockchain to improve the efficiency of commodity data on the chain. To reduce the storage space of IPFS, we propose a mechanism

to clean up the records periodically. The logistics party updates the logistics information to the blockchain for easy inquiry and supervision. In this system, a reputation evaluation scheme that fully considers transaction factors such as transaction time, transaction amount, and user reputation is proposed, and a monetary incentive mechanism is designed to promote the smooth operation of the e-commerce system.

3. Platform Design

Firstly, a framework combining blockchain and e-commerce system are proposed, including the node types in the system. Then, the platform architecture of e-commerce system is demonstrated and the procedure to implement it with smart contract is described in detail.

3.1. Node Types

The node types in the system are as follows:

Seller: The seller is the party who sells the commodity, mainly involving retailers or enterprises. When registering identity information, the seller needs to upload relevant qualification information to blockchain. After successful registration, the seller can upload the details of commodity into the IPFS system, obtain the return address and upload it to the blockchain. Meanwhile, the status of commodity can be updated to saleable, and the buyer can be evaluated after completing the transaction.

Buyer: The seller is the party who is consuming and capable of viewing the commodity description from the platform, then confirming the purchase and changing the commodity into a lock status, as well as signing for the commodity and evaluating the seller.

Logistics: The logistics party collects the storage and logistics information of commodity and publicizes it to the blockchain for future accountability [21].

3.2. Conceptual Framework

The frameworks of blockchain are consisted of six layers, including the data layer, network layer, consensus layer, actuator layer, contract layer and application layer. Based on this framework, this paper proposes a conceptual framework of blockchain that can be applied to e-commerce system, as shown in Figure 2.

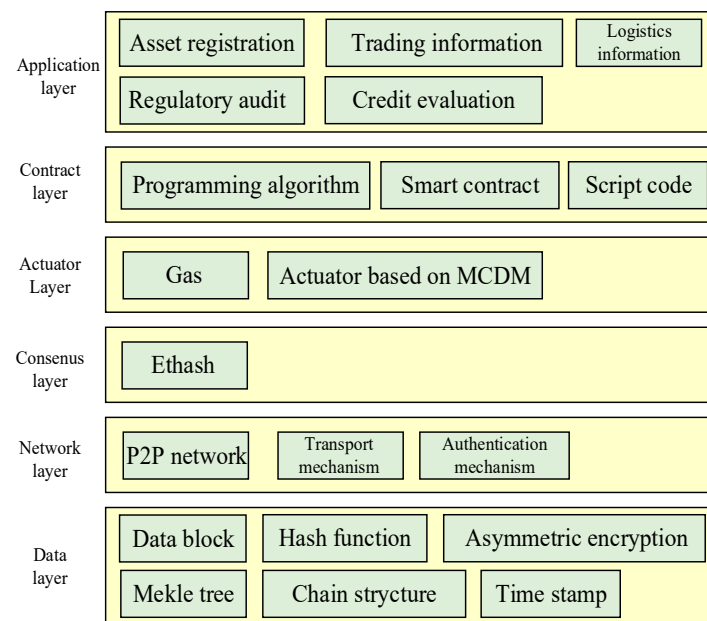


Figure 2. E-commerce system framework based on blockchain.

As can be seen from Figure 2, the data layer is the underlying data structure of the blockchain, including data block, chain structure, Hash function, asymmetric encryp-

tion [22], timestamp and Merkel tree [23], which is capable of realizing data storage and ensuring the security of accounts and transactions. The network layer is composed of point-to-point (P2P) network [24], transmission mechanism and authentication mechanism to maintain the communication between blockchain. The consensus layer is composed of consensus algorithm and consensus mechanism, promoting the nodes to reach a consensus in the chain. This paper adopts Ethereum ethash consensus mechanism [25]. The contract layer encapsulates various codes and smart contracts to ensure the automatic execution of instructions. In the incentive layer, this paper proposes a reputation value incentive mechanism based on MCDM to reward and punish the nodes and improve chain operation efficiency based on Ethereum Gas incentive mechanism. As the most important layer in the framework, the application layer provides services for nodes through the application layer blockchain, including information storage, logistics information chaining and credit evaluation.

3.3. Platform Architecture

Figure 3 shows the architecture established for e-commerce platform, including four stages, i.e., information upload stage, purchase confirmation stage, logistics stage and evaluation stage.

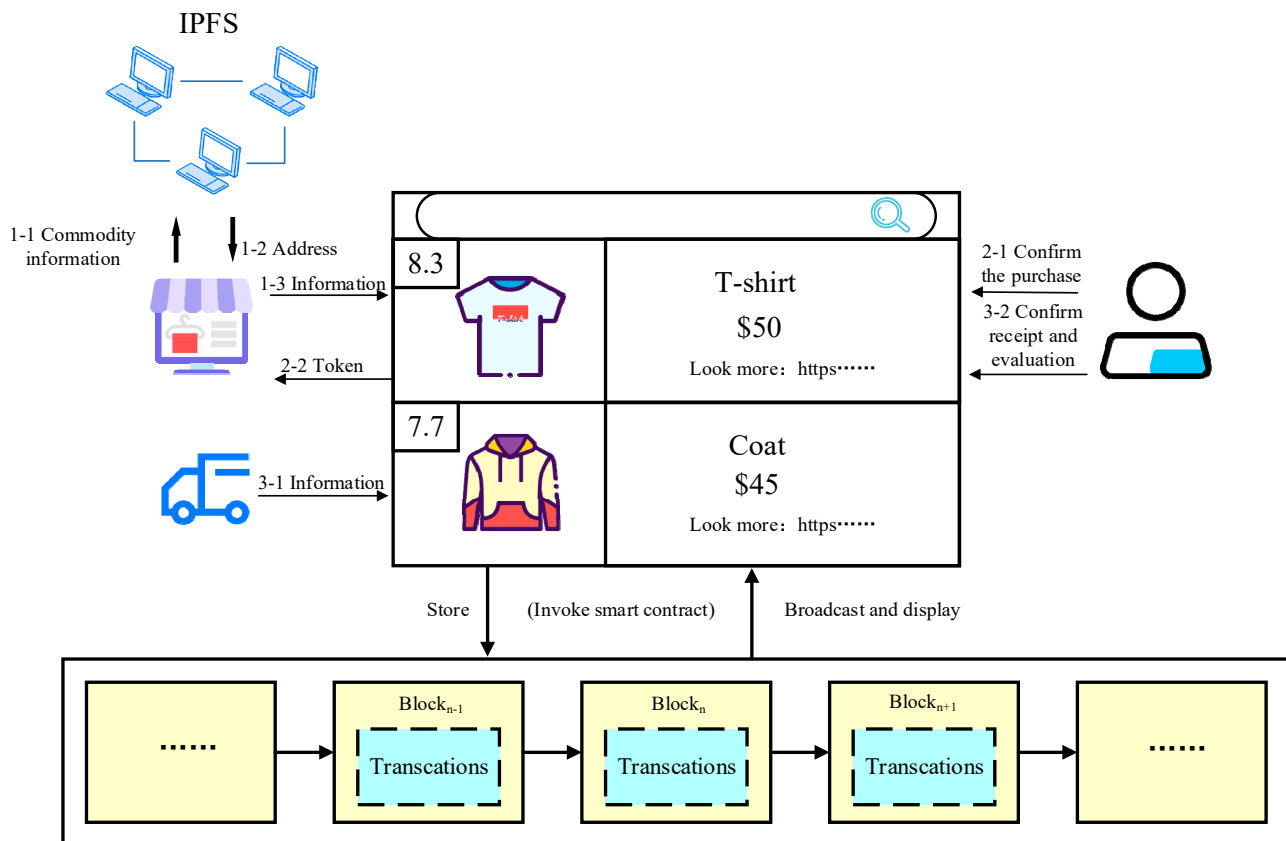


Figure 3. E-commerce system platform architecture.

3.3.1. Information Upload Stage

1. The seller sends the detailed information of commodity to IPFS, including the name, country of origin, specifications, and then IPFS returns an address.
2. The seller launches the address and basic information of the commodity into the platform, including the name, unit price, and pay a certain deposit.
3. The smart contract uploads the address and information to the blockchain, and the deposit is stored in the smart contract.

4. Blockchain feeds back the upload status information. Based on the price adjustment of commodity, the deposit is deposited in the smart contract. If an accident happens during the transaction, the buyer can get compensation from the deposit first. During the sale of commodity, if the commodity needs to be taken off from platform due to selling out, the seller can take the initiative to cancel the smart contract with uncompleted-transaction, and the rest of the deposit will be returned to seller's account except for the gas consumed. The introduction of deposit mechanism increases the cost of false transactions of sellers and effectively prevent the false transactions.

3.3.2. Purchase Confirmation Stage

1. The buyer can view commodity's information and status through the interface on the platform, and decide whether to buy by referring the reputation score of seller.
2. The buyer confirms the purchase and pays a certain deposit (the deposit will be transferred to the seller's account as the fund for purchasing commodity after the completion of the contract) and deposited in the smart contract.
3. The smart contract sends the transaction action to blockchain.
4. Blockchain feeds back the upload status information.

3.3.3. Logistics Stage

1. The logistics party checks the status of commodity. If the transaction is completed, the commodity will be transported.
2. The logistics party uploads the transportation status to the platform and calls the smart contract to store in the chain.
3. After receiving the commodity, the buyer can confirm the acceptance. At this time, the deposit stored in smart contract will be transferred to seller and the contract will be closed. User can also refuse to accept the commodity. Then, the deposit will deduct the cost of gas and returned to each account.
4. The smart contract sends the transaction action to blockchain.
5. Blockchain feeds back the upload status information.

3.3.4. Evaluation Stage

During the evaluation stage, the buyer and the seller can submit comments and evaluations to platform.

1. After completing the transaction, the buyer and the seller can upload their evaluation of transaction to platform.
2. The platform calls the smart contract and publishes the reputation score to blockchain.
3. The blockchain stores reputation score and feeds back the successful evaluation to platform.

As shown in Figure 4, the system completes the transaction through four stages [26].

3.4. Reputation Evaluation Scheme

The definition on reputation is an opinion on intentions and norms of past behavior of one party [27]. Assuming that the transactions of users in a cycle period are sufficient to reflect his reputation value, and the rest transactions have little influence on them, this paper proposes a reputation model. The model can reflect users' reputation value based on their transactions in a cycle. The platform can give higher priority to sellers with good reputation in the search process and supervise and sanction buyers with low reputation, and its incentive mechanism based on reputation value is conducive to the formation of a virtuous online shopping cycle.

3.4.1. Calculation of Node Reputation Value

After completing the transaction, the buyer and the seller can evaluate mutually according to smart contract. However, it is unreasonable to calculate the node reputation

value by only relying on this evaluation. In the process of transaction, in addition to the subjective feelings of the buyer, time of transaction, amount of transaction and reputation score of both parties also play important roles. Therefore, this paper proposes a method based on SAW and MCDM. The proposed method calculates the node reputation value according to the difference between period of node transaction and time of transaction completion, amount involved in transaction, reputation value of transaction partner and the evaluation of buyers [28]. Obviously, the earlier the transaction is completed, the higher reputation value of participating users. The more transaction amount, the higher reputation value of transaction user. In addition, the reputation of transaction partners is also a positive evaluation standard.

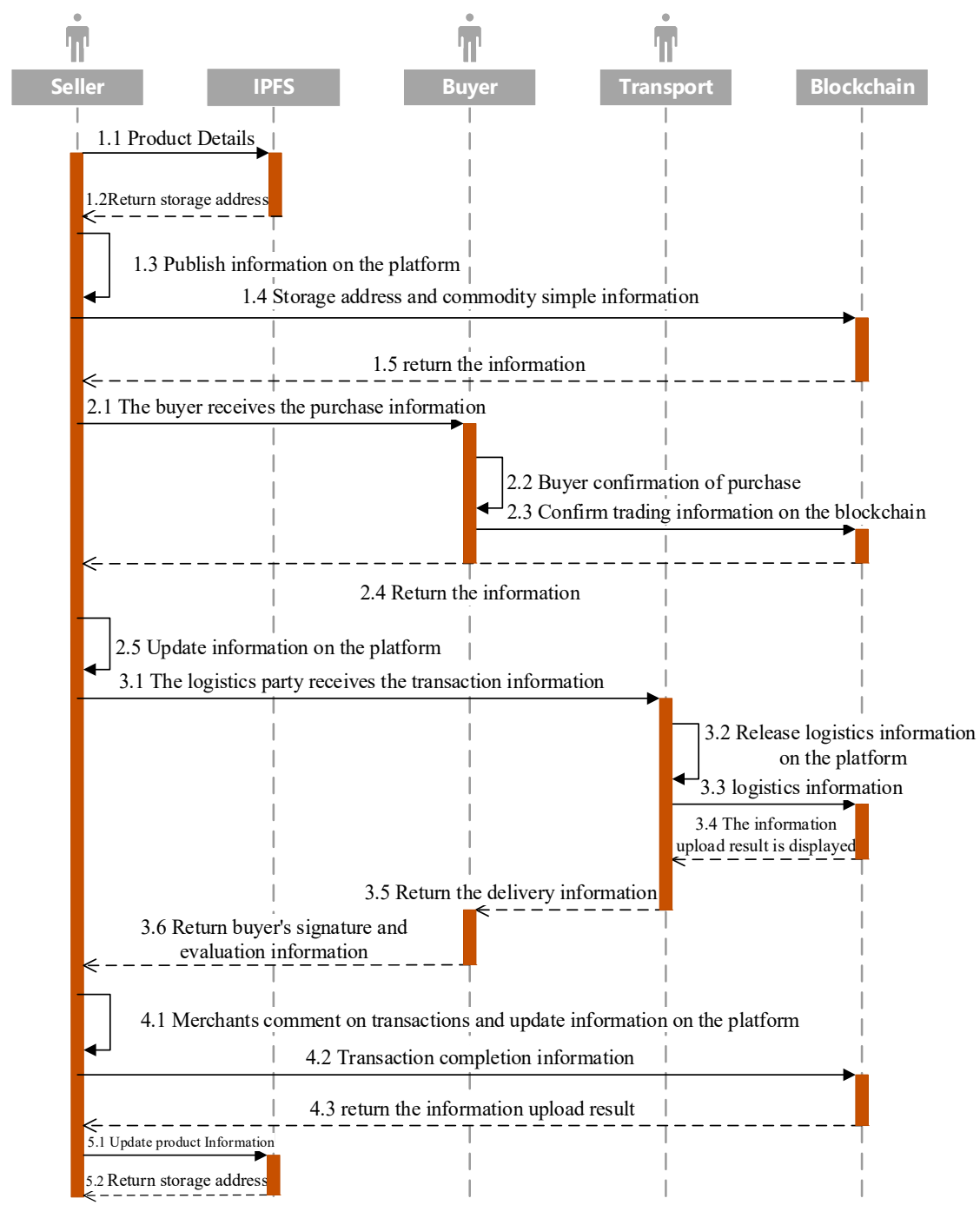


Figure 4. The UML Sequence diagram of e-commerce transaction system.

For a cluster with n^* nodes ($y_1, y_2, y_3, \dots, y_n$), each node has a_i ($i \in 1, 2, 3, \dots$) transactions. For transaction j record of y_i has the time interval t_{ij} and the transaction amount c (the difference between the transaction period and the actual transaction time, t_1 is the deadline of each transaction, t_2 is the sign-off time of the transaction, $t_{ij} = t_1 - t_2$), which can be normalized by:

$$t'_{ij} = \frac{t_{ij} - t_{ij}^{\min}}{t_{ij}^{\max} - t_{ij}^{\min}} \quad (1)$$

$$w'_{ij} = \frac{w_{ij} - w_{ij}^{\min}}{w_{ij}^{\max} - w_{ij}^{\min}} \quad (2)$$

where t_{ij}^{\max} and t_{ij}^{\min} represent the maximum and minimum value of the historical transaction time difference of node y_i in the cycle period, respectively; w_{ij}^{\max} and w_{ij}^{\min} represent the maximum and minimum value of historical transaction amount of node y_i in the cycle period, respectively. If the transaction time exceeds the time limit, the transaction is cancelled and the deposit is returned to each account, meaning that t'_{ij} cannot be negative.

Recording c_{ij} as the reputation value of the other party node in the j th transaction, we perform the normalization operation by:

$$c'_{ij} = \frac{c_{ij}}{c_{\max}} \quad (3)$$

where c_{\max} is the historical maximum reputation value of a node. If there is no historical maximum reputation value with node of transaction partner, then c'_{ij} is recorded as 1.

Recording s as the score of the other party node in the j th transaction (the score value is within 0–10), we have:

$$s'_{ij} = \frac{s_{ij}}{10} \quad (4)$$

Recording the reputation value of node as R_i , and φ_{ij} as the influence of a single transaction on reputation value of the node, we have:

$$R_i = \sum_{j=1}^{a_i} \varphi_{ij} \quad (5)$$

$$\varphi_{ij} = (\alpha C'_{ij} + \beta w'_{ij} + \gamma t'_{ij} + \delta s'_{ij}) T_{ij} \quad (6)$$

where α, β, γ and δ are the weights that are adjusted according to the actual needs, which satisfies $\alpha + \beta + \gamma + \delta = 1$; T_{ij} is a collusion factor, whose function is to prevent excess influence on the reputation of transaction partners from one node, and to prevent two nodes from colluding with each other to update a higher reputation. Therefore:

$$T_{ij} = \left(\frac{1}{num_{ij}} \right)^{\theta} \quad (7)$$

where θ is the adjustment coefficient, and num_{ij} is the same transaction number of node i in the j th transaction in the cycle period. If the two parties have the same transaction users and the same transaction commodity, it will be judged as the same transaction. By taking Equation (7) into Equation (6), the reputation value of the node can be obtained. The pseudo-code for calculating reputation value is shown in Algorithm 1.

3.4.2. Incentive Mechanism of Reputation Value

As shown in Figure 3, sellers with higher reputation value are more likely to be recommended by the platform and have more advantages in the competition. To obtain higher reputation value, sellers will choose faster logistics and better commodity quality to improve buyer's evaluation. For buyers, buyers with higher reputation need to pay

less deposits stored in smart contracts, whose reputation value incentive mechanism is beneficial to form a positive online shopping cycle.

Algorithm 1: Reputation Assessment

Input: Transaction Records

Output: Reputation

```

1: for  $i = 1$  to  $y_n$  do
2:   for  $i = 1$  to  $a_i$  do
3:      $C'_{ij} \leftarrow \frac{C_{ij}}{C_{\max}}, T_{ij} \leftarrow (\frac{1}{num_{ij}})^\theta$ 
4:   end for
5:    $R_i \leftarrow \sum_{j=1}^{a_i} \varphi_{ij}$ 
6: end for
7: return  $R_i$ 

```

4. Experimental Results and Analysis

This section analyzes the functionality and performance of the proposed system, and explains its function integrity and performance by the comparison with other similar systems. Also, the reliability and security of the proposed e-commerce system are analyzed. The experimental configuration information is shown in Table 1.

Table 1. Experimental configuration information.

Object	Configuration Information
CPU	Intel i7-6300HQ
Operating System	Windows 10
Ram	8 GB DDR4
Hard Disk	256 GB SSD

This paper adopts Geth to build and test private blockchain. The system proposed in this paper was arranged in the private Quorum, written in Solidity language and with version 0.8.4, which was tested by Remix.

4.1. Basic Function Test of the Trading Systems

4.1.1. Test and Analysis of Smart Contract

Before testing, it is necessary to compile and arrange the smart contract. The smart contract on Remix platform was compiled and tested. The smart contract was deployed as soon as being compiled. The account in Ganache was applied to imitate the transaction account. The compilation result is shown in Figure 5. With the transaction, the currency of transaction account would change, and the transaction could be concluded normally.

After completing the transaction, the transaction information was stored in the chain. As shown in Figure 6, the logistics information was stored in the chain through hash encryption.

The proposed transaction system could realize the function of chaining and storage of transaction and key information, and meet the general requirements of e-commerce transaction system.

4.1.2. Functional Comparison of the State-of-Art E-Commerce Systems

The proposed system was compared with the state-of-art systems. The results are shown in Table 2.

Gao et al. proposed a cross-border e-commerce-driven foreign trade research based on blockchain [16]. However, the operation speed was slow due to the processing of large amount of data to be stored on chain.

Jiang et al. describes an e-commerce platform for small-and medium-sized enterprises without an incentive mechanism [19].

```

61 //This structure can indicate the name and price of the item
62 struct Product {
63     string name;
64     uint price;
65 }
66
67 Product[] public products;
68
69 //This function declares the price and name of an item
70 function declare(string memory name,uint price)public onlySeller inState(State.Created) returns(uint){
71     products.push(Product(name,price));
72     return products.length;
73 }
74
75 //This function can terminate the transaction and retrieves the token
76 //This function can only be called by the seller before the transaction is locked
77 function abort() public onlySeller inState(State.Created)
78 {
79     emit Aborted();
80     state = State.Inactive;
81     seller.transfer(address(this).balance);
82 }
83
84 //Buyer confirmation of purchase
85 //Tokens are locked until the "confirmReceived" function is called
86 //Buyers need to enter the corresponding item name
87 function confirmPurchase(string memory goods) public inState(State.Created) condition(msg.value == (2*value)) payable
88 {

```

Search with transaction hash or ad...

listen on all transactions

block:1 txIndex:0 from: 0x3B6...c88E3 to: Commerce. (constructor) value: 1000000000000000000 wei data: 0x608...70033 logs: 0
hash: 0x717...d12d1

status true Transaction mined and execution succeed

transaction hash 0x0148c54e6b220c96544fdd3ccb00312884acffe05834ad19c9371c3e29e2b550

(a)

ACCOUNTS									
BLOCKS									
TRANSACTIONS									
CONTRACTS									
EVENTS									
LOGS									
SEARCH FOR BLOCK NUMBERS OR TX HASHES									
CURRENT BLOCK 1 GAS PRICE 20000000000 GAS LIMIT 6721975 HARDFORK MURGLACHER NETWORK ID 5577 RPC SERVER HTTP://127.0.0.1:8545 MINING STATUS AUTOMINING WORKSPACE WARY-SCARECROW SWITCH									
MNEMONIC slab shrimp auto ten bird odor replace remove muscle flock clerk infant HD PATH m/44'/60'/0'/0'/0/account_index									
ADDRESS	BALANCE				TX COUNT		INDEX		
0x3B61Cfd359E5C71F48D61f406380d88d0fDc88E3	89.97 ETH				1		0		
ADDRESS	BALANCE				TX COUNT		INDEX		
0x128F7fAAB6aFcAa7Df00b5292304a919f3D6C4ee	100.00 ETH				0		1		
ADDRESS	BALANCE				TX COUNT		INDEX		
0x3Aa291C74Fa33A549D9995D900f319ad4a4C83bD	100.00 ETH				0		2		
ADDRESS	BALANCE				TX COUNT		INDEX		
0x61f4B6995191738AAfc52eAd96df4795b585C395	100.00 ETH				0		3		
ADDRESS	BALANCE				TX COUNT		INDEX		
0x0cAb74bFb25d14FbB68c99A02cFB0F449Ce7C12E	100.00 ETH				0		4		
ADDRESS	BALANCE				TX COUNT		INDEX		
0xfd670D60A3e0038E31e0B62f925cCE6754542ddf	100.00 ETH				0		5		
ADDRESS	BALANCE				TX COUNT		INDEX		
0xbE1C93Fcb89022F7D47964455Fd9154269502935	100.00 ETH				0		6		
ADDRESS	BALANCE				TX COUNT		INDEX		
0x83a7b91b8761fB26A8B82c8743981769A041B19b	100.00 ETH				0		7		
ADDRESS	BALANCE				TX COUNT		INDEX		
0xb3Fe42Ed74d9c069553EAf648B9eE46ffDe57684	100.00 ETH				0		8		
ADDRESS	BALANCE				TX COUNT		INDEX		
0x803Bd8b3cd52716A07238E9499bA746CaCd533b0	100.00 ETH				0		9		

(b)

Figure 5. Smart contract compilation and testing: (a) Smart contract compilation tests; (b) Ganache simulates account token changes.

```

decoded input      {
                    "string name": "Transporter",
                    "uint256 _biddingTime": "36000"
                  }

decoded output     {}

logs               [
                    {
                      "from": "0xD7ACd2a9FD159E69Bb102A1ca21C9a3e3A5F771B",
                      "topic": "0x463832c8e4407b3ae4188e09718792e05dce9f4f98f14cdd4f54a7ec42921cfb",
                      "event": "Transports",
                      "args": {
                        "0": "Transporter",
                        "name": "Transporter"
                      }
                    }
                  ]

```

Figure 6. Logistics information encryption on the chain.

Table 2. Functional comparison of e-commerce system.

Functional Characteristic	Ref. [16]	Ref. [19]	Ref. [20]	Ref. [29]	This Paper
Storage Optimization	×	×	✓	✓	✓
Logistics Chaining	✓	✓	×	✓	✓
Incentives Mechanism	✓	×	✓	✓	✓
Credit Evaluation	✓	✓	✓	×	✓

Zhou et al. describes a decentralized e-commerce system in an e-commerce environment based on blockchain, with no introduction on third-party institutions except buyers and sellers, and more improvements are required for supply and logistics [20].

Lahkani et al. proposed a supply chain finance based on blockchain, while fails to perform credit evaluation. By comparison, the system proposed in the paper could satisfy the above requirements and show a good functionality [29].

4.2. Performance Analysis and Test of the Proposed System

This section presents the testing of the communication overhead of the proposed system, and analyzes the gas consumption and time cost of the system to evaluate its performance.

4.2.1. Analysis of Gas Consumption

Ethereum executes commands step by step according to smart contract during the transaction. To perform each step, there exists the consumption called gas [30]. Gas Limit is the maximum available amount of gas for a transaction execution. However, if a transaction execution requires more gas than the gas Limit, the System will emit an out-of-gas exception immediately, and all executed operations will be reverted [31]. The user loses all of Gas. For users, smart contracts with low gas consumption are more popular. This research arranged the smart contract on Remix to predict the consumption of gas, and compared the proposed system with the BC-DRS and BS-EP. The results are shown in Figure 7.

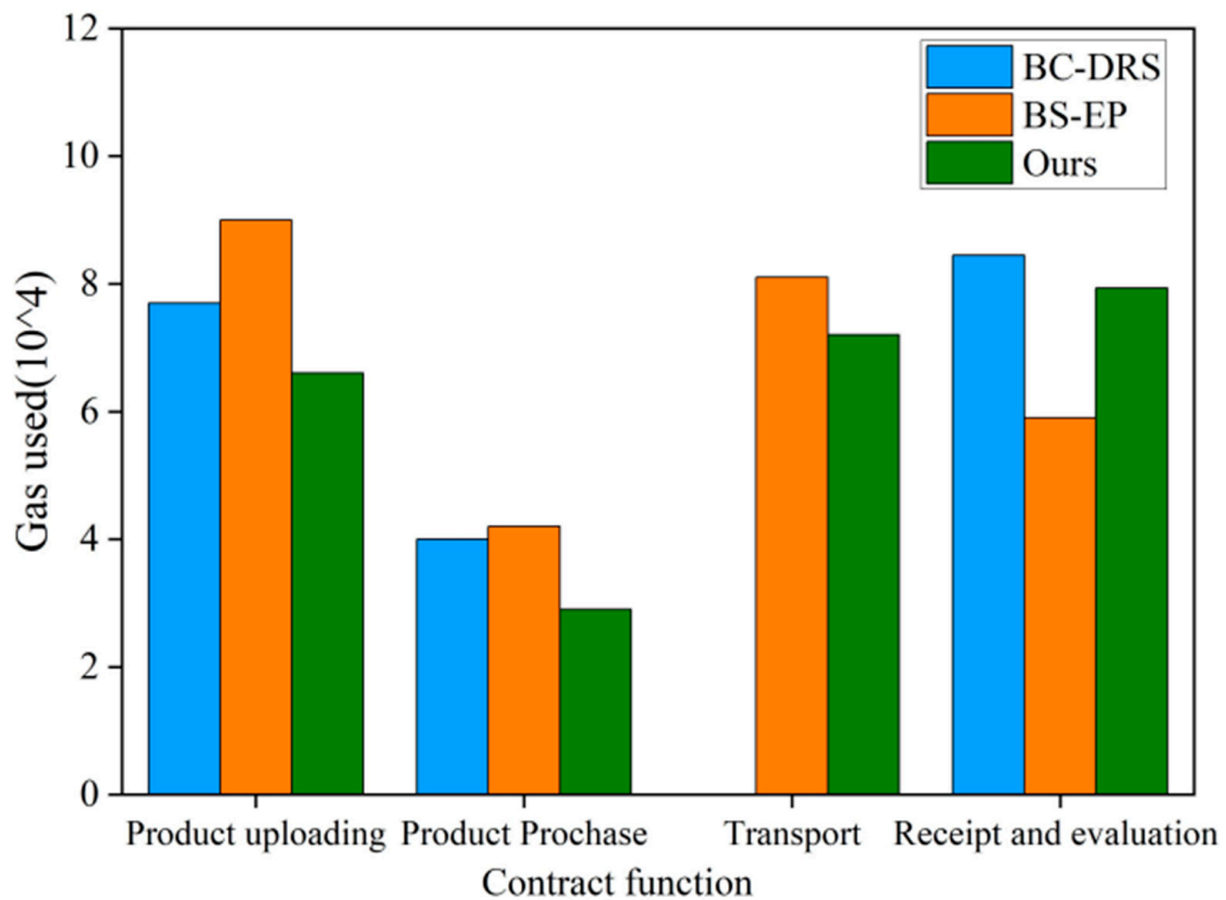


Figure 7. Comparison of gas consumption in smart contract.

As can be found from Figure 7, the gas value consumed by our contract confirmation purchase functions was minimum. For smart contracts, upload numerous data consumed more gas than simply signing the transactions. The systems of Literature BC-DRS and BS-EP shall upload numerous data in upload stage of commodity, so that the cost of gas was high. The proposed system stored the IPFS address of commodity information on blockchain. The address was a fixed size bitstream. Therefore, the cost of gas processing address data would not increase, so that the upload time of commodity information was less. the gas costs for loops are higher than that for other functions in smart contracts [31,32]. In this paper, the smart contract used is optimized so that it still has good functionality and reduces gas consumption even with fewer loop functions. The BC-DRS had no evaluation function, so that it consumed less gas. In general, the proposed system had more comprehensive functions and less gas consumption.

4.2.2. Analysis of Time Consumption

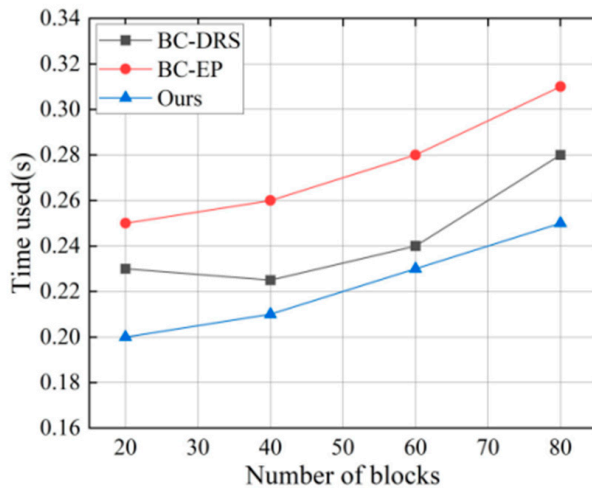
This paper takes the time taken by Ethereum blockchain to call smart contract as dependent variable and different block length as independent variable, and compares it with the BC-DRS and BS-EP. The results are shown in Figure 8.

Through analyzing the experimental results, we can draw the following conclusions.

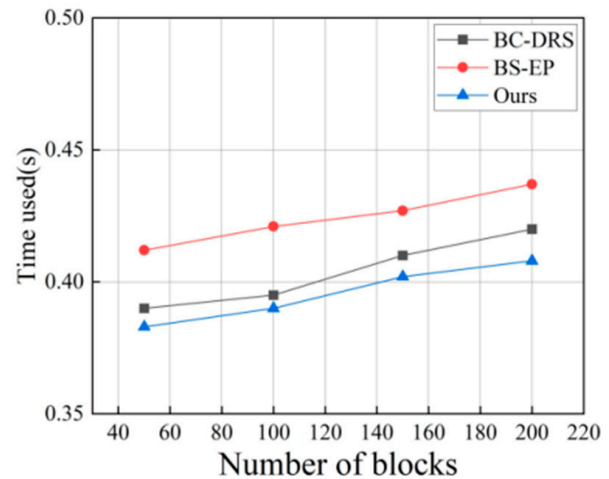
1. The time cost of the three functions of the proposed system increases slightly as the increase in the number of blocks. Smart contracts need to upload information to the blockchain. Therefore, as number of blocks increase, the consumption of the proposed system increases.
2. The proposed system consumes the most time in accepting and evaluation function. The accepting and evaluation function of the system needs to call smart contract to realize accepting in function and upload the information to blockchain. Therefore,

compared with the information upload and transaction completion functions, it consumes the most time.

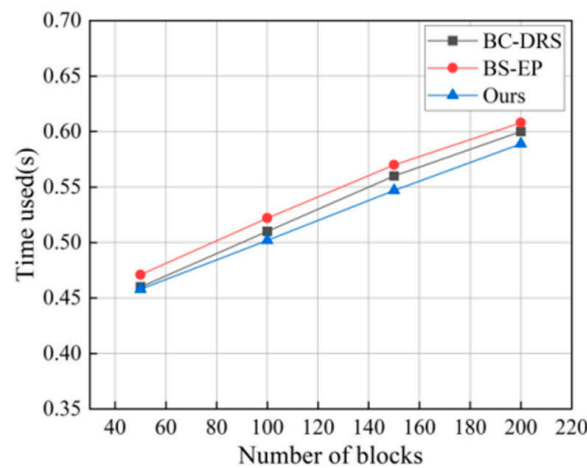
3. Compared to storing massive information data into blockchain, we only store fixed size addresses of product information. Therefore the time consumption of the proposed system is low. The amount of information in the confirmation of purchase and the signing and evaluation stages is relatively small. Therefore, the system time consumption is low. Therefore, according to the above results in cost and time cost, we can conclude that the proposed system has good usability for online shopping.



(a)



(b)



(c)

Figure 8. The time cost of invoking smart contracts: (a) Time cost of commodity upload function; (b) Identify the time cost of purchasing features; (c) Time overhead of sign-in and evaluation functions.

4.3. Reliability and Safety Analysis

The current reputation evaluation systems are mostly based on average score. There are numerous good and malicious comments in the system, which is difficult to resist collusive attacks and unfair attacks. To improve the reliability and security of the system, this paper proposes a reputation evaluation method based on SAW and MCDM, as demonstrated in Section 3.4.1. We randomly generated the transaction records of users a, b, c by Python, including transaction period, transaction completion time and transaction amount, The reputation of users was evaluated. The results are shown in Figure 9.

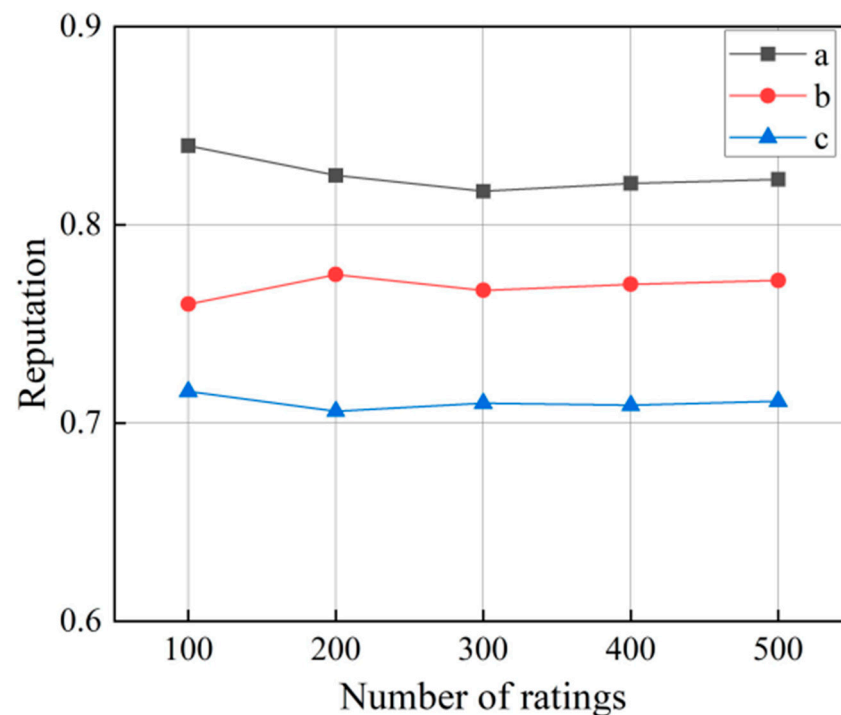


Figure 9. User reputation value.

Figure 9 suggests that with the increase in the number of transactions, the reputation value of user tends to be stable. That is, the proposed reputation value calculation model could effectively reflect the reputation value of user. Sellers with high reputation value have high priority in the search results and buyers with low reputation value will be supervised by the platform for unreasonable return behavior. In addition, the transaction system with the reputation evaluation scheme is capable of resisting the following attacks:

1. **Unfair evaluation attack.** The attack means that the malicious evaluator deliberately places an unfair evaluation to reduce the reputation value of transaction partner. In the reputation calculation model proposed in this paper, the reputation value is not only connected with the evaluation, but also related to the completion time of transaction, amount involved and reputation value of counterparty. The single malicious evaluation of malicious attacker has little influence, while the reputation value of malicious attacker will be influenced. When its reputation value is too low, malicious attacker will be subjected to system supervision and sanctions.
2. **Reputation accumulation attack.** To avoid the node accumulating rights and interests for a long time, the age of currency owned by the node will be limited generally in blockchain system. The proposed system selects transactions in a certain period according to the timeliness to reflect the current reputation value of the node, aiming at avoiding the node accumulating too high reputation value.
3. **Collusive attack.** It means that multiple users collusively give good comments to each other to obtain high reputation value. This paper proposes a collusion factor to avoid collusion attack, as shown in Equation (7). With the increase of node transactions, the interaction degree of nodes gets lower, effectively avoiding the collusion between malicious nodes.

5. Conclusions

In recent years, researchers have proposed blockchain-based decentralized e-commerce systems. However, no reputation value calculation method and incentive mechanism have been proposed to match it, and the motivation of nodes in the system is low, which is not conducive to the long-term and smooth development of nodes. In this paper, we propose a multi-criteria decision-based reputation evaluation scheme to evaluate merchants and

customers, which enables the system to effectively resist reputation accumulation attacks and collusion attacks, and to provide incentives to users based on reputation scores, which is conducive to the formation of a virtuous cycle of online shopping. In order to improve the operation efficiency of the system, this paper adopts IPFS system to store product details and output addresses to the blockchain, and regularly cleans up IPFS storage records. The system is simulated through Ethereum blockchain. Experimental results show that the proposed system has small communication cost and can accurately reflect the user reputation value, with good availability and reliability.

Considering the characteristics of small storage capacity and low storage efficiency of a single blockchain, We will apply the alliance chain between main chain and subordinating chain to construct the supply chain transaction system in the future. In this way, the transaction information between commodity raw material providers and sellers can be saved on subordinating chain, and the traceability of commodity is enhanced.

Author Contributions: Conceptualization, Y.X. and C.Z.; methodology, C.Z.; software, Y.X.; validation, Y.S., C.Z. and X.G.; formal analysis, C.Z.; resources, Y.X.; writing—original draft preparation, Y.S., Y.X. and C.C.; writing—review and editing, X.G.; supervision, C.Z. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the National Science Foundation of China, grant number 61703426.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: All data used in this paper can be obtained by contacting the authors of this study.

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

References

1. Liu, F. The Collaborative Development Model of Cross-border E-commerce Based on Ocean Transportation. *J. Coast. Res.* **2020**, *112*, 231–233. [\[CrossRef\]](#)
2. Treiblmaier, H.; Sillaber, C. The impact of blockchain on e-commerce: A framework for salient research topics. *Electron. Commer. Res. Appl.* **2021**, *48*, 101054. [\[CrossRef\]](#)
3. Deng, S.G.; Cheng, G.J.; Zhao, H.L.; Gao, H.H.; Yin, J.W. Incentive-Driven Computation Offloading in Blockchain-Enabled E-Commerce. *ACM Trans. Internet Technol.* **2021**, *21*, 1–19. [\[CrossRef\]](#)
4. 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. [\[CrossRef\]](#)
5. Yuan, Y.; Wang, F.Y. Blockchain: The state of the art and future trends. *Acta Autom. Sin.* **2016**, *42*, 481–494. [\[CrossRef\]](#)
6. Ghosh, A.; Gupta, S.; Dua, A.; Kumar, N. Security of Cryptocurrencies in blockchain technology: State-of-art, challenges and future prospects. *J. Netw. Comput. Appl.* **2020**, *163*, 102635. [\[CrossRef\]](#)
7. Swan, M. Blockchain Thinking The Brain as a Decentralized Autonomous Corporation. *IEEE Technol. Soc. Mag.* **2015**, *34*, 41–52. [\[CrossRef\]](#)
8. Zhuansun, F.; Chen, J.J.; Chen, W.L.; Sun, Y. The Mechanism of Evolution and Balance for e-Commerce Ecosystem under Blockchain. *Sci. Program.* **2021**, *2021*, 5984306. [\[CrossRef\]](#)
9. Song, Y.G.; Liu, J.; Zhang, W.; Li, J. Blockchain's role in e-commerce sellers' decision-making on information disclosure under competition. *Ann. Oper. Res.* **2022**, 1–40. [\[CrossRef\]](#) [\[PubMed\]](#)
10. Kim, S.I.; Kim, S.H. E-commerce payment model using blockchain. *J. Ambient Intell. Humaniz. Comput.* **2022**, *13*, 1673–1685. [\[CrossRef\]](#)
11. Yi, H.B. A secure logistics model based on blockchain. *Enterp. Inf. Syst.* **2021**, *15*, 1002–1018. [\[CrossRef\]](#)
12. Paulavicius, R.; Grigaitis, S.; Igumenov, A.; Filatovas, E. A Decade of Blockchain: Review of the Current Status, Challenges, and Future Direction. *Informatica* **2019**, *30*, 729–748. [\[CrossRef\]](#)
13. Ning, Z.T.; Xiao, L.J.; Liang, W.; Shi, W.Q.; Li, K.C. On the Exploitation of Blockchain for Distributed File Storage. *J. Sens.* **2020**, *2020*, 8861688. [\[CrossRef\]](#)
14. Dutta, P.; Choi, T.M.; Somani, S.; Butala, R. Blockchain technology in supply chain operations: Applications, challenges and research opportunities. *Transp. Res. Part E Logist. Transp. Rev.* **2020**, *142*, 102067. [\[CrossRef\]](#) [\[PubMed\]](#)
15. Kemmoe, V.Y.; Stone, W.; Kim, J.; Kim, D.; Son, J. Recent Advances in Smart Contracts: A Technical Overview and State of the Art. *IEEE Access* **2020**, *8*, 117782–117801. [\[CrossRef\]](#)

16. Gao, T.G. Study on the Intention of Foreign Trade Driven by Cross-Border E-Commerce Based on Blockchain Technology. *Secur. Commun. Netw.* **2021**, 2021, 9623672. [[CrossRef](#)]
17. Zhang, Y.; Li, B. Agricultural product supply chain traceability system design based on master-slave alliance chain structure. *Appl. Res. Comput.* **2022**, 1–8. [[CrossRef](#)]
18. Zhang, L.J.; Peng, M.H.; Wang, W.Z.; Su, Y.S. Secure and Efficient Data Storage and Sharing Scheme Based on Double Blockchain. *CMC Comput. Mater. Contin.* **2021**, 66, 499–515. [[CrossRef](#)]
19. Jiang, J.; Chen, J. Framework of Blockchain-Supported E-Commerce Platform for Small and Medium Enterprises. *Sustainability* **2021**, 13, 8158. [[CrossRef](#)]
20. Zhou, Z.L.; Wang, M.M.; Yang, C.N.; Fu, Z.J.; Sun, X.M.; Wu, Q.M.J. Blockchain-based decentralized reputation system in E-commerce environment. *Future Gener. Comput. Syst. Int. J. Esci.* **2021**, 124, 155–167. [[CrossRef](#)]
21. Li, M.; Shen, L.D.; Huang, G.Q. Blockchain-enabled workflow operating system for logistics resources sharing in E-commerce logistics real estate service. *Comput. Ind. Eng.* **2019**, 13, 950–969. [[CrossRef](#)]
22. Gao, F. Data encryption algorithm for e-commerce platform based on blockchain technology. *Discret. Contin. Dyn. Syst. Ser. S* **2019**, 12, 1457–1470. [[CrossRef](#)]
23. Hsiao, S.J.; Sung, W.T. Utilizing Blockchain Technology to Improve WSN Security for Sensor Data Transmission. *CMC Comput. Mater. Contin.* **2021**, 2, 1899–1918. [[CrossRef](#)]
24. Hao, W.F.; Zeng, J.J.; Dai, X.H.; Xiao, J.; Hua, Q.S.; Chen, H.H.; Li, K.C.; Jin, H. Towards a Trust-Enhanced Blockchain P2P Topology for Enabling Fast and Reliable Broadcast. *IEEE Trans. Netw. Serv. Manag.* **2020**, 2, 904–917. [[CrossRef](#)]
25. Wang, T.T.; Zhao, C.H.; Yang, Q.; Zhang, S.L.; Liew, S.C. Ethna: Analyzing the Underlying Peer-to-Peer Network of Ethereum Blockchain. *IEEE Trans. Netw. Sci. Eng.* **2021**, 8, 2131–2146. [[CrossRef](#)]
26. Górski, T. The 1 + 5 Architectural Views Model in Designing Blockchain and IT System Integration Solutions. *Symmetry* **2021**, 13, 2000. [[CrossRef](#)]
27. Wang, X.H.; Wu, Y. Platform-Based E-commerce Reputation Management Model:Based on the Collaborative Matching Perspective of Reputation Sharing Mechanism With Responsibility Recourse Strategy. *Res. Financ. Econ. Issues* **2020**, 92–100. [[CrossRef](#)]
28. Xu, X.L.; Zhu, D.W.; Yang, X.X.; Wang, S.; Qi, L.Y.; Dou, W.C. Concurrent Practical Byzantine Fault Tolerance for Integration of Blockchain and Supply Chain. *ACM Trans. Internet Technol.* **2021**, 21, 1–17. [[CrossRef](#)]
29. Lahkani, M.J.; Wang, S.Y.; Urbanski, M.; Egorova, M. Sustainable B2B E-Commerce and Blockchain-Based Supply Chain Finance. *Sustainability* **2020**, 12, 3968. [[CrossRef](#)]
30. Liu, C.; Gao, J.B.; Li, Y.; Wang, H.H.; Chen, Z. Studying gas exceptions in blockchain-based cloud applications. *J. Cloud Comput. Adv. Syst. Appl.* **2020**, 1, 12–24. [[CrossRef](#)]
31. Li, C.; Nie, S.; Cao, Y. Trace-Based Dynamic Gas Estimation of Loops in Smart Contracts. *IEEE Open J. Comput. Soc.* **2020**, 12, 46–58. [[CrossRef](#)]
32. Li, C.M. Gas Estimation and optimization for smart contracts on ethereum. In Proceedings of the 36th IEEE/ACM International Conference on Automated Software Engineering (ASE), Melbourne, Australia, 15–19 November 2021; pp. 1082–1086. [[CrossRef](#)]