Multi-Agent System for E-commerce Security Transaction with Block Chain Technology

XU Hao[1+], SHI Xiao-Hong[2], YI Dian[3]

[123](Information engineering College, Shanghai Maritime University, Shanghai 201306, China)
xuhao14@stu.shmtu.edu.cn,

Abstract—**In recent years, Agent technology has become a powerful tool for the e-commerce systems. Applying Agent technology to e-commerce systems can overcome the shortcomings of traditional e-commerce, meet the needs of users' intelligence and individuation, and greatly increase online transaction efficiency. Aiming at the development difficulties of multi Agent e-commerce system, such as information insecurity, unfair transaction and so on.Based on the technical characteristics of block chain technology: decentration, and unfo rgeability, this paper proposes a multi-agent e-commerce system based on blockchain technology.Firstly, the application of Agent technology in e-commerce is introduced, the hidden dangers are clarified.Secondly,from the perspective of data storage, transacti on information, executive scheme is put forward. Finally, the verification algorithm of verification node in agent transaction process is verified.The experimental results show that the proposed method can be applied to multi-agent e-commerce systems.**

Keywords—***Multi-Agent;blockchain;consensus algorithm;smart contract; secure transaction***

I. INTRODUCTION

With the rapid development of the Internet, the explosive growth of business information and the increasingly complex network environment, the traditional e-commerce processes and supporting technologies are facing new challenges, and their defects have become increasingly obvious. It is almost impossible for customers to search all shopping websites, analyze related information and make reasonable decisions. To solve this problem, mobile agents are considered to be a useful e-commerce solution[1]. With its mobile and autonomic capabilities, mobile agents can travel from one host to another over the network. Mobile agents can perform a variety of tasks, such as searching for data, analyzing business information, shopping on behalf of users, making necessary reservations, and so on. Obviously, agent-based e-commerce applications are more attractive, especially for wireless mobile users. In addition, it can save a lot of time for users and ultimately significantly reduce transaction costs and time. Related mobile agent systems have been developed for different applications [2][3][4][5],However, the multi-agent based e-commerce system is still under centralized control of the centralized, failed to achieve true fairness and justice and mutual trust, the legitimate rights and interests of users and information security can not be well protected, so there is an urgent need for both to avoid the centralized authority The method of interfering with e-commerce transactions and ensuring the security of user information The blockchain technology is exactly in line with the needs of e-business transformation. First of all, the blockchain technology and e-commerce markets are decentralized. The smart contract features of the blockchain can ensure that e-commerce users can freely trade anywhere and anytime. Second, the e-commerce market needs all users to maintain together, and blockchain technology in all areas. The block can achieve efficient collaborative autonomy; again, there is no need for a third-party trust mechanism in the blockchain to meet the demands for the diversified development of the e-commerce market.

At present, domestic and foreign research institutions show a growing trend in the study of block chains. Domestic research mainly focuses on financial, medical, shared economy, education and energy fields. Zhang Bo cited the PHILPS medical case to show that the block chain technology can realize the authentication of patient's medical records and privacy protection [6]; Li Qing and so on have realized the distributed learning record storage and credit bank service through the block chain technology, and provided the certificate authentication system for online education[7]. Looking at foreign literature, the application research based on block chain technology presents a hundred flowers and a hundred schools of thought contending. As far as the field of e-commerce is concerned, the research of block chain is focused on the innovation of e-commerce specific things. Richard Dennis has constructed the platform merchant credit rating system based on block chain technology, and put an end to the untrue [8] of the network rating information; Alexander Schaub and so on expanded the block chain in the business credit rating system. The application of [9] realizes the true online comment on merchant's information privacy. Based on the characteristics of block chain technology, such as central, difficult tampering and traceability, this paper proposes a multi-agent e-commerce system based on block chain technology. It does not need any intermediate trust mechanism to solve the security risks in the multi Agent e-commerce system.

978-1-5386-5638-9/18/$31.00 ©2018 IEEE

II. E-COMMERCE SYSTEMS BASED ON MAS

There are several e-Commerce systems based on MAs [2-5]. Our e-Commerce architecture is based on cooperative multi-agent negotiation [2].Figure 1 presents the system architecture and the scenario of buying goods using the MAs.

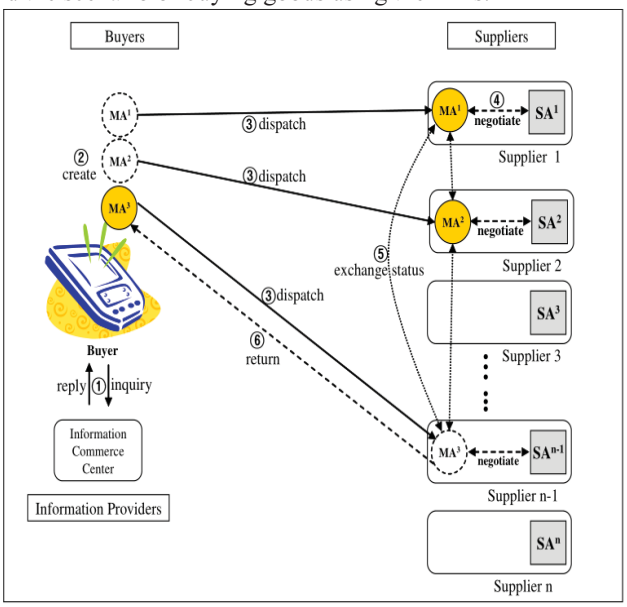

Fig.1 e-Commerce architecture and the scenario of buying goods

It is assumed that the e-marketplace consists of buyers, supplier sites, and a commerce center providing the supplier information. All supplier sites have their own supplier agents. If a buyer requests a quotation of certain goods, an inquiry is transmitted to the supplier section of the commerce center and the commerce center responds with a list of supplier sites for the buyer. The buyer composes multiple buyer agents and dispatches each agent to each supplier site in the list.The buyer agents retrieve quotations of the products from the supplier agents at each supplier site and exchange this information with each other. The most suitable item is then determined.For supplier Agent, you can recommend products to customers Agent at this stage and negotiate with customers who are interested in their products. When Agent has reached an agreement between the two parties, the buyer, Agent, "fills out" the order according to the agreement reached. After the supplier Agent receives the order, the buyer requires the buyer's Agent to authorize it and obtain the money from the buyer's Bank after the buyer's authorization is obtained. After that is the sending and receiving of goods (physical goods are distributed by logistics).

In this case, there are still some security risks in the multi-agent e-commerce system, such as : Information leakage,Tampering,Identification ,nformation destruction

Using the characteristics of blockchain technology such as decentralization, hard to falsify, and traceability, a multi-Agent e-commerce system based on blockchain technology is proposed. It does not require any intermediary trust mechanism and can solve the above mentioned security risks.

III. APPLICATION OF BLOCKCHAIN IN MULTI-AGENT E-COMMERCE SYSTEM

A. Multi-Agent Electronic Commerce System model Based on Block Chain Technology

A multi-Agent e-commerce system based on blockchain technology is proposed. It is composed of three entities: user, e-commerce platform, and blockchain. Figure 2 shows the blockchain-based e-commerce platform transaction process.

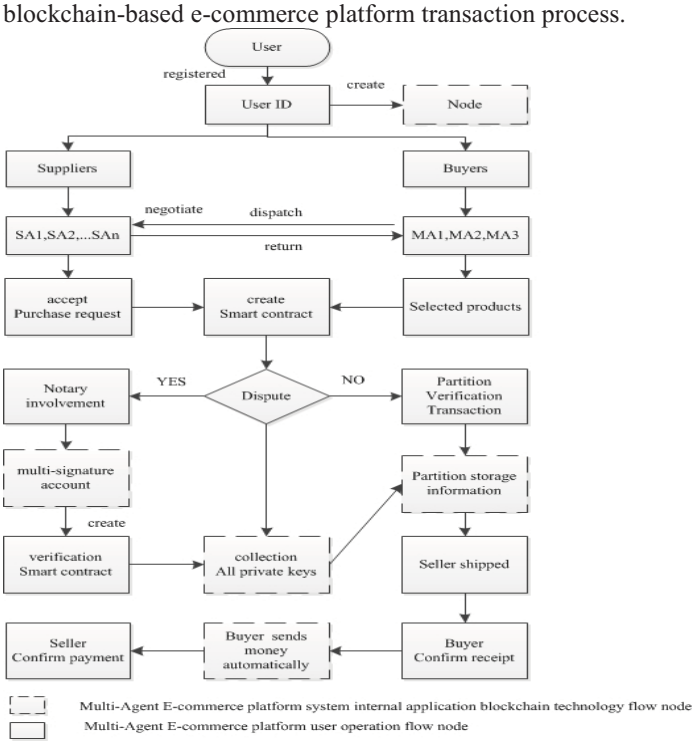

Fig.2 Blockchain based Mulit-Agent e-commerce platform transaction process model

When users want to sell products on the platform, they need to create a supplier agent that contains the product's price, model number, quantity, and other detailed information. If the buyer requests quotations for certain items, the query is sent to the supplier portion of the business center, and the business center responds to the buyer's list of supplier websites. The buyer creates multiple buyer agents and sends each agent to each vendor site in the list. The buyer agent retrieves the product quote from the supplier agent of each supplier site, and selects the merchant with which to deal according to the price comparison principle and the like. After selecting the desired product, the buyer agent can communicate with the seller agent about the price, quantity, and mode of transportation. Until the agreement is reached, the e-commerce platform will create a smart contract based on the digital signature of the buyer and seller. The smart contract will be sent to the corresponding product attribute block for verification. If all the blocks are verified successfully, they can be shipped according to the agreed terms. When the buyer receives the goods and the verification is correct, the digital currency will be automatically paid to the seller's account from the address of the buyer's digitally signed account. All

the information of the entire transaction process is stored in the flow node of the blockchain.

If the buyer and seller have a dispute during the transaction, they can choose to have the third party notary involved to solve the problem. In order to ensure the fairness and credibility of the notaries, the e-commerce platform has established a reputation scoring system for all users, allowing each user to anonymously score feedback on the overall situation of users who have traded with them. The users with higher credit standing can apply to become notaries, and the higher the credibility of the notary, the more rewards the digital currency will have, but if the notary is reported abused by other users and it is true, it will be blacklisted. And impose a high fine. The notary of each transaction must be jointly chosen by both the buyer and the seller to avoid situations where the notary favors either side.

In the case of disputes over the transaction amount, the notary will verify the smart contract and create a digital currency account based on a multi-signature technique. The notary and the buyer and the seller each have a private key. Only when all three parties agree to collect the three private accounts. In the key, the buyer will send the corresponding digital currency to the multi-signature address according to the terms of the contract. When the seller receives the notice that the buyer has paid, it can deliver the goods, and the buyer will also receive a notification that the goods have been shipped. After the buyer confirms the goods receipt, the e-commerce platform will automatically release the payment from the multi-signed address to the seller.

IV. System Implementation Core Technology

A. *data storage*

The blockchain data data is different from the previous relational database's key-value pair storage format. It uses blockchain storage. Each block contains a header and a body. Each block contains the previous one. The hash value of the block and the hash value of the block, and the link between the blocks is achieved through a hash value. The data block header structure designed in this paper is shown in Table 1.

Table 1 block header structure

Head information	Meaning	Bytes
version number	Indicates version information	4
Parent hash	Record the hash value of the previous block	32
Header hash of this block	Record the hash value of this block	32
Merkle Tree Root	Record the hash value of the Merkle number of all transactions in the current block	32
Timestamps	Record the generation time of this block	4

The block body mainly contains: the number of transactions and the details of the transaction. The detailed structure is shown in Table 2.

Table 2 Block structure

Body information	Meaning	Bytes
Number of transactions	Record the number of current block transactions	4
Transaction Details	Record all transactions in the current block	No fixed value

Each block contains the hash value of the previous block and the hash value of the block. The link between the blocks is completed by the two hash values. This block can pass the hash value of the previous block. Link to the previous block, and so on, you can create a complete data chain, as shown in Figure 3.

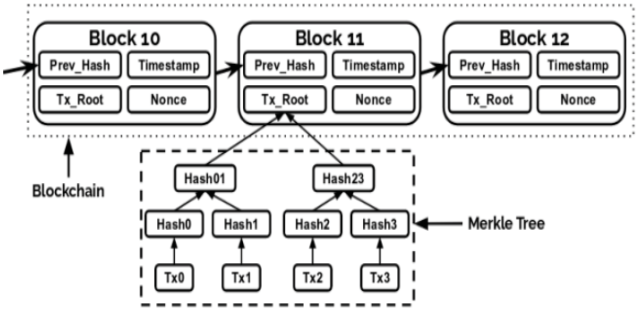

Fig.3 Schematic of a blockchain

The use of this structure can prevent transaction information from being maliciously tampered with. We assume that the k block data has been tampered with, because the k+1 block stores the hash value of the k block, and the calculated k block The hash value of the block data is compared and an exception can be found. It is immediately dethat the transaction information of the k block has been tampered with.

The storage of data in the blockchain uses the data structure of the Merkle Trees[12]. The most common and simple form of Merkle trees is the Binary Merkle Trees. In this Merkel tree data structure, all data blocks are divided into two groups, and these data blocks are the nodes of the tree. The hash pointer corresponding to each data block is stored in the parent node of the upper layer, and the hash pointers of these pointing nodes are again grouped by two. Repeat this process until you get a single block, the Merkle Root. Finally, the Merkle Root Hash is generated through the Merkle Tree algorithm and stored as a summary of the transaction list in the Block Header. The binary Merkle tree structure is shown in Figure 3.

If the data block of the tree node is tampered with, the parent node's hash value will not match it. Layers are passed upwards, and the eventual change of data is passed to the top of the Merkle tree. Therefore, as long as the hash value of the root node is saved, any attempt to modify the data block in the node can be detected.

B. *SHA -256 and RSA encryption algorithm*

In this article's digital asset security transaction method, dual SHA256 hash function is used in conjunction with RSA encryption algorithm to verify the authenticity of transaction information and prevent falsification. This method uses the dual SHA256 of Bitcoin blockchain system. The Greek

function converts the original data into two 256-bit (32-byte) binary digits after two SHA256 hash operations.

1) SHA-256 algorithm

The message, M, is padded by Appending the bit"1"to the end of the message, followed by k zero bits, so that its length is congruent to 448mod512. The padded message is parsed into N 512-bit message blocks, $M^{(1)}$, $M^{(2)}$,.., $M^{(N)}$, by appending 64-bit block . The initial hash value, $H^{(0)}$ =IV is set, consist of eight 32-bit words, in a hexadecimal form .

SHA-256 uses a message schedule of sixty-four 32-bit words .The words of the message schedule are labelled W_0 , W_1 ,…, W_{63} .

The following steps describe the algorithm:

a) Prepare the message schedule,{Wt }

$$W_t = \begin{cases} M_t^{(t)} & 0 \le t \le 15 \\ \sigma_1^{\{256\}}(W_{t-2}) + W_{t-7} + \sigma_0^{\{256\}} + W_{t-16} & 16 \le t \le 63 \end{cases}$$

Where

$$\sigma_0^{\{256\}} = POTR^7(x) \oplus POTR^{18}(x) \oplus SHR^3(x)$$

$$\sigma_1^{\{256\}} = POTR^{17}(x) \oplus POTR^{19}(x) \oplus SHR^{10}(x)$$

b) Initialize the eight working variables, a, b, c, d, e, f, g, and h, with the (i-1)st hash value:

For t=0 to 63

{

$T_1 = h + \sum_1^{\{256\}}(e) + ch(e,f,g) + k_t^{\{256\}} + W_t$

$T_2 = \sum_1^{\{256\}}(a) + Maj(a,b,c)$

h = g, g = f, e = d+T1, d = c, c = b, b= a,

a= T1+T2

}

Where

Ch(x, y, z) = (x^ y)□(x^ z)

Maj(x, y, z) = (x^ y)□(x ^z)□(y^ z)

$K_t^{\{256\}}$is a sequence of sixty-four constant 32-bit words

$$\sum_0^{\{256\}}(x) = ROTR^2(x) \oplus ROTR^{13}(x) \oplus ROTR^{22}(x)$$

$$\sum_0^{\{256\}}(x) = ROTR^6(x) \oplus ROTR^{11}(x) \oplus ROTR^{25}(x)$$

c) After repeating steps one through four a total of N times (i.e., after processing M(N)), the resulting hash function is $H_0^{(N)} \| H_1^{(N)} \| H_2^{(N)} \| H_3^{(N)} \| H_4^{(N)} \| H_5^{(N)} \| H_6^{(N)} \| H_7^{(N)}$.

2) RSA encryption algorithm

The RSA encryption algorithm generates public and private key flows as shown in Figure 4.RSA involves a public key and private key. The public keycan be known to everyone, it is used to encrypt messages.Messages encrypted using the public key can only bedecrypted with the private key. The keys for the RSA encryption algorithm are generated the following way:

Key Generation Process:

1) Choose two different large random prime numbers p and q ,and Calculate n=p*q

2) n is the modulus for the public key and the private keys

3) Calculate the totient: f=(p-1)(q-1)

4) Choose an integer e such that 1<e<f , and is co prime to f i.e.: e and f share no factors other than 1; gcd(e,f) = 1.

5) e is released as the public key exponent

6) Compute d to satisfy the congruence relation d*e=1(mod f) i.e.: d*e=1+kf for some integer k.

7) d is kept as the private key exponent

Encryption:

1) Consider the device A that needs to send a message to B securely.

2) Let e be B's public key. Since e is public, A has access to e.

3) To encrypt the message M, represent the message as an integer in the range 0<M<n.

4)Cipher text C = M^e mod n, where n is the modulus.

Decryption:

1) Let C be the cipher text received from A.

2) Calculate Message M = C^e mod n, where d is B's private key and n is the modulus.

In practical applications, the sender A of the transaction initiates a new transaction, for example, transferring a voucher worth 100 yuan to the user B. At this time, the SHA256 hash algorithm is invoked to sign the message to obtain a digest after the hash. The RSA asymmetric encryption algorithm generates a pair of public and private keys. The public key is used to encrypt the signature. The sender sends the RSA-encrypted signature and the message together to the receiver. The receiver uses the sender's public key to decrypt the signature and restore a hash value. Check whether the hash value is consistent with the result of the packet processed by the SHA256 hash algorithm. Check whether the message originates from the sender and whether the information is tampered with. The specific process is shown in Figure 4.

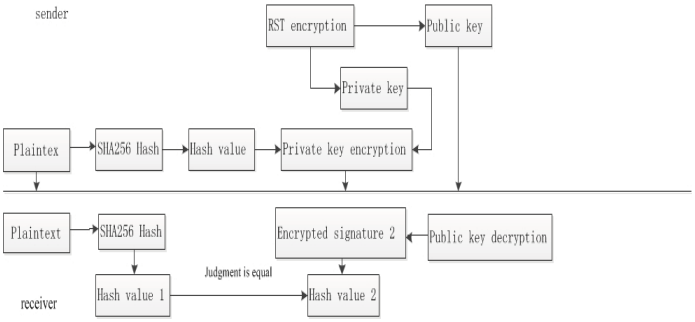

Fig.4 transaction information encryption and verification process

C. consensus algorithm

In this method, each node jointly maintains a ledger, and a consensus mechanism is reached between the nodes. The consensus mechanism is mainly applied in the consensus process of the transaction information recorded by the verification node in the overall architecture Fig.4 above. Commonly used consensus mechanisms in blockchain technologies currently include: Pow (workload proof), Pos (equity proof), DPos (share authorization certificate), and

distributed consensus algorithm. Due to the high efficiency and simplicity of the RAFT distributed consensus algorithm, this paper uses the RAFT consensus algorithm. However, the RAFT consensus algorithm belongs to non-Byzantine algorithm and does not consider the existence of Byzantine node malicious operation. In order to apply to multi-agent e-commerce system transaction applications, this paper borrows the idea of Byzantine consensus algorithm, adds message signature verification mechanism to RAFT algorithm, and uses RAFT based on improvement. Consensus algorithm in the multi-agent e-commerce system security transaction method.

The improved RAFT consensus algorithm process is shown in Figure 5. The verification node has three states: leader, follower, candidate.

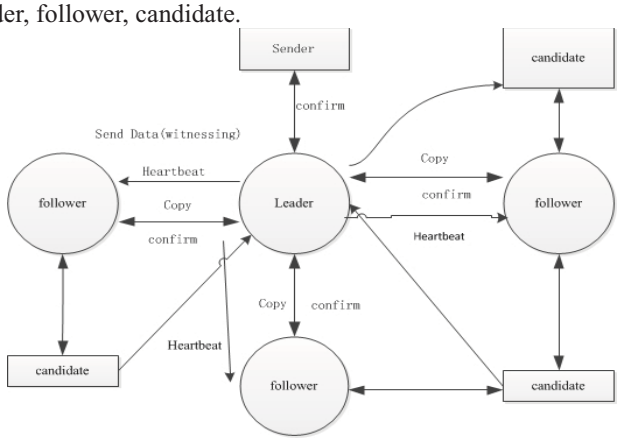

Fig.5 RAFT Consensus algorithm

RAFT Consensus algorithm:

1 Input: Message signature x+p Message number h
2 Begin
3 (x+p, n)→Leader
4 Leader→(Verficationn)(x+p, n)
5 (x, n)→Follower /*Leader copied to follower*/
6 Leader←Verify from follower
7 If leader is bad /*If the leader is down, re-election*/
8 Leader→Candidate
9 Follower→Candidate
10 Voting(follower)→New leader
/*The follower node verifies whether the leader node is down due to the leader timeout. If the leader node is down, all nodes are candidate state, and the new leader is re-elected. */
11 End

D. Smart contract

The blockchain and smart contract technology can solve the above problems of Multi-Agent System for E-commerce Security Transaction.Smart contracts are the code for executing contract terms. It was first proposed by cryptographer Nick Szabo in 1994. The replacement of traditional paper contracts with smart contracts can greatly reduce contract development, control protocols and performance. Labor costs and calculation costs.

The blockchain formulates the rules of the transaction of the multi-agent e-commerce system into smart contract codes, records the code and project status in the blockchain, and executes the project code by the blockchain. The smart contract on the blockchain can be directly Controlling funds and their transfer, not only ensures the authenticity, reliability and compulsory of the transaction, but also makes the execution of the transaction evidence-based, greatly improving the credibility of the multi-agent e-commerce system.

The blockchain adds the rules of contract execution to the consensus algorithm of the blockchain, and the code and state of the contract itself are also stored in the blockchain. When the contract is triggered, the contract code is directly read and executed, and the result of the execution is executed. Return to the contract state, so that the blockchain becomes a trusted environment for contract calculations. At the same time, the blockchain lays the foundation for the recording and transfer of fully digital assets. With fully digital assets, smart contracts on the blockchain can control assets. Therefore, the blockchain makes the smart contract a trusted system. It is not limited to the function of the database, but also a distributed computer that can execute code and record asset ownership.

In the blockchain, the Agent transaction process and payment process are automatically completed in the form of smart contracts. The user and the platform manager convert the transaction rules of the Agent transaction item into project contracts. When the buyer and the seller reach a transaction, a transaction contract is generated according to a preset rule, and the transaction contract is used to execute the payment and delivery plan.

V. EXPERIMENT AND RESULT ANALYSIS

A. consensus algorithm verification

The consensus algorithm proposed in this paper requires a minimum of 4 nodes, so there are 4 verification nodes in this experiment. To verify that the consensus algorithm can be well applied in the digital asset security transaction business, artificially simulate leader node downtime and verify whether the algorithm can trigger automatic election at this time. The experimental steps are as follows:

(1) Analog leader node downtime;

(2) Record the time taken from the leader to the completion of the election;

(3) Repeat the above steps 50 times.

From Figure 6, we can see that when the leader fails to election success rate is 100%, the average execution time is 14s. The consensus algorithm can automatically elect new leader nodes when failures such as downtime occur to complete the consensus.

Fig.6 Time taken by Leader to take the opportunity to complete the election

B. Safety effectiveness assessment

This method uses blockchain technology to record transaction data in the blockchain to ensure the security and effectiveness of transaction data. Use Table 3 to assess the effectiveness of the system.

Table 3 Safety Effectiveness Assessment

NO.	Evaluation conten	Test result
1	During transaction data entry process,transaction information is maliciously modified	Signature and encryption mechanism to distinguish authenticity
2	Network abnormality occurs on one of the leader verification nodes	Consensus mechanism re-election
3	Impersonation of data	not pass

VI. CONCLUSION

In this paper, a multi-Agent e-commerce system based on blockchain technology is designed. The innovation of this system is mainly reflected in the adoption of distributed data storage method. The verification node in the system completes the data storage through a consensus algorithm and uses dual SHA256. The hash function is combined with the RSA encryption algorithm to process transaction information. To ensure the authenticity of transaction information, prevent tamper. To achieve a safe and reliable trading process. At the same time, the key technologies and core algorithms involved in this method are analyzed and verified. The experimental results show that blockchain technology can effectively solve the security risks in multi-agent e-commerce systems.

The system designed in this paper has some shortcomings. To achieve complete decentralization of the system will make the system less efficient. For example, each distributed node has to store a large amount of data redundantly, which not only occupies a large storage space, but also causes inefficiency for information traversal query and verification. Therefore, on the basis of ensuring data security, a "partial decentralization" or "multi-centered" network structure can be formed, so that the efficiency of the system will be greatly improved. There is also a blockchain data security problem. This paper uses an improved RAFT consensus algorithm. Although the message signature verification mechanism is added to the RAFT algorithm, the data security is greatly improved, but the possibility of this security threat still exists. Therefore, the safety and effectiveness of the consensus mechanism needs further research and improvement.

ACKNOWLEDGMENT

We thank Prof. Shi Xiaohong for discussing some issues about this paper.

REFERENCES

[1] M.StraBer, K.Rothermel, C.Maihöfer.Providing Reliable Agents for Electronic Commerce[J].Proceedings of International IFIP/GI Working Conference, TREC'98,Hamburg, Germany, June 1998, pp. 241-253.

[2] F. C. Lin , C.N. Kuo. Cooperative Multi-Agent Negotiation for Electronic Commerce Based on Mobile Agents[J]. Proc. of the IEEE Int'l Conf. on Systems,Man and Cybernetics, Oct. 2002.

[3] P.Dasgupta,N.Narasimhan,L.E.Moser,P.M.Melliar-Smith.MAgNET:Mobile Agents for Networked Electronic Trading[J]. Proc. of the IEEE Int'l Conf. on Transactions on Knowledge and Data Engineering, Jul./Aug. 1999.

[4] J.J.Jong, S.J.Geun.Brokerage Between Buyer and Seller Agents using Constraint Satisfaction Problem Models[J]. Proc. of the Decision Support Systems,Vol. 28, Issue 4, Elsevier Science, Jun. 2000.

[5] T. Sandholm, Q. Huai.Nomad: Mobile Agent System for an Internet-Based Auction House[J]. Int'l Journal of the IEEE Internet Computing, Mar./Apr. 2000.

[6] Zhang Bo. Utilization of foreign blockchain technology and related inspiration [J]. Financial Technology Times, 2016 (5): 35-38.

[7] Li Qing, Zhang Xin. Blockchain: Promoting Education through Technology Openness and Public Trust [J]. Distance Education Magazine, 2017 (1): 36 -44.

[8] Dennis R,Owenson G. Rep on The Roll: A Peer to Peer Reputation System Based on a Rolling Blockchain[J]. International Journal of Digital Society,2016,7 (1): 1123 -1134.

[9] Schaub A, Bazin R, Hasan O, et al. A Trustless Privacy-Preserving Reputation System[C] . Ghent , Belgium: IFIP International Information Security and Privacy Conference. 2016.

[10] NAKAMOTO S.Bitcoin : a peer-to-peer electronic cash system[EB/OL]. [2017-12-05].

[11] Yuan Yong, Wang Feiyue. Status and Prospects of Blockchain Technology Development[J].Acta Automatica Sinica,2016,42(4):481-494.

[12] Hu Changping,Huang Shushu.User Rights Protection in Public Cloud StorageServices[J],InformationStudies:Theory&Application,2016,39(11):17-21.

XU Hao was born in 1994. He is a Postgraduater of Shanghai Maritime University. His current research interests include Bayesian network and Mobile Agent.

SHI Xiaohong was born in 1963. He is a Associate Professor and graduate advisor of Shanghai Maritime University. His current research interests include Mobile Agent, Mobile Agent Group Communication and System reliability research etc.

YI Di an was born in 1993. He is a Postgraduater of Shanghai Maritime University. His current research interests include Convolutional Neural Network and Deep Learning.