2019 2nd International Conference on Electronics Technology

A Blockchain Consensus Mechanism for Educational Administration System

Baocheng Wang, Yafei Hu, Shan Li, Jiahao Niu
School of Computer Science
North China University of Technology
Beijing 100144 China
e-mail: wbaocheng@ncut.edu.cn, huyafei3@126.com, 865936806@qq.com, 1149603878@qq.com

***Abstract*—Applying the blockchain to the school's educational system can provide credible educational information and ensure the reliable recording and maintenance of student qulifications, grades and other information. The blockchain-based educational system has many nodes, and the fast and accurate blockchain consensus mechanism is the key to system implementation. To this end, this paper proposes an improved consensus mechanism of equity authorization proof for the educational system. The paper constructs the consensus framework of group-based educational system, refines the node state and gives the state transition mechanism. On this basis, the paper proposes a voting scheme based on credit reward and punishment to ensure the effectiveness of proxy node election and timly elimination of malicious proxy nodes. The simulation results show that the probability that the abnormal node becomes the proxy node again is reduced from 90% to 3%, and the number of voting rounds required for the abnormal node to be kicked out of the proxy node set is reduced from 3 rounds to 1 round, which can effectively guarantee the consensus efficiency and proxy node credibility, support the design and implementation of the educational system based on blockchain.**

Keywords-educational administration system; blockchain; consensus mechanism; DPOS; credit reward and punishmet

I. INTRODUCTION

Educational administration is the foundation of school teaching management and is closely related to the development of students [1]. Its management level directly affects the quality and efficiency of the entire school teaching system, and reflects the soft power of the school. The biggest problem facing the traditional educational administration system is the problem of data security credibility and easy to be tampered with, so that the information of the educational system cannot be trustedly shared among schools, students, education departments and even public groups. Applying the blockchain to the educational administration system can solve the problem and ensure that the educational information such as academic qualifications and achievements cannot be tampered with and the data is credible.

The educational system involves thousands of students and a certain size of teachers. If they become the blockchain consensus participants of the educational system, the network maintenance cost of the system will be greatly increased, which is not conducive to the effective operation of the school educational system and brings enormous challenges to the educational system. Therefore, according to the different roles of the objects involved in the educational system, selecting the nodes trusted by the users of the educational system to generate the information blocks of the educational system is the basic principle based on the consensus of the educational system of the blockchain. The DPOS consensus mechanism votes for a small number of proxy nodes in a large number of nodes to generate blocks. The data consensus rate is up to the second level, and the degree of matching with the blockchain-based educational system is extremely high. It is the primary choice for the consensus mechanism of the educational system based on blockchain.

The core idea of DPOS is that the participants have the right to elect any number of nodes they trust to generate new blocks [1]. The node with the top M number of votes has the right to be selected to create the block, and the creator of the new block is randomly selected from the previously selected nodes. In addition, the size of M is also determined by voting, the size of M is not fixed, it is not certain who chooses it. In addition, the size of M is also determined by voting. The size of M is not fixed. It is not certain who chooses it. However, there is a problem with DPOS. In order to quickly reach a consensus, the node will not be actively voting, and there is a lack of detection mechanism for abnormal nodes in the proxy node, which affects system security. To this end, DPOS needs to be improved to ensure the efficiency of the consensus and improve system security.

Based on the above analysis, the paper proposes an improved DPOS consensus mechanism for the educational system. We construct a consensus framework based on grouping educational system, refine the nodes state and give a state transition mechanism, and combine the methods of credit reward and punishment to improve the voting enthusiasm of nodes, ensure the validity of the election of the proxy node, remove the error proxy node in time, and ensure the credibility of the system data.

II. RELATED WORK

The blockchain consensus mechanism mainly studies the issue of accounting rights allocation and block verification. At present, a large number of scholars have studied the general blockchain consensus algorithm and the blockchain consensus mechanism applicable to various industry application characteristics, and achieved certain results.

978-1-7281-1618-1/19/$31.00 ©2019 IEEE

Reference [3] presents the Proof-of-Work(POW). The POW performs the hash operation for each node to obtain the block accounting right. After the block is generated, it broadcasts to the whole network for verification by other nodes. The POW has higher security and strong anti-attack capability. Block generation consumes a lot of computing power and other resources, and the data is consistent for a long time. Usually, a block is generated every 10 minutes. There are currently applications in distributed P2P networks for distributed anonymous electronic cash payment systems [4]. In view of the waste of resources caused by POW and the fact that the mine pool occupies most of the computing power of the whole network, the Ethereum team conducted research on the POS consensus mechanism[5]. The core idea of the POS consensus mechanism is to reward the verifier to verify the equity and verify that the transaction is given a certain percentage of the reward to the verifier. The ratio is determined according to the number of tokens the certifier has. The more coins you have, the easier it is to get the billing rights. POS solves the problem of large energy consumption of the workload proof mechanism to a certain extent, shortens the generation time and confirmation time of the block, and improves the system efficiency. However, it still does not get rid of the mining job, and is not suitable for the practical application of blockchain with high efficiency requirements [6].

In order to enhance system efficiency while ensuring the rights of shareholders, Dan Larimer designs the equity authorization certification mechanism (DPOS) [7] and implements it for the first time in its BitShares project [8]. DPOS make a proper compromise to centralization, uses representative structure. All participating nodes vote to select a small number of proxy nodes to complete block generation. The number of nodes directly participating in the consensus is reduced, and the speed of reaching consensus is greatly increased. When the proxy node cannot correctly record the transaction information and synchronize the new block in time, other nodes can vote to replace it. The revenue generated by the generated block will prompt the selected proxy node to seriously perform the duties in the consensus process and maintain its own authority. The DPOS mechanism does not consume the computational mining process, which greatly reduces the number of nodes involved in the generation and verification of the block, and can achieve the second-level consensus verification [10]. However, in the specific application, the consensus participation nodes have their own characteristics. It needs further research that how to select the most suitable proxy nodes for the targeted application and determine the number of proxy nodes. At the same time, DPOS does not respond to error nodes in a timely manner, but only identifies the status, and there is a phenomenon that the node voting is not active, the system security has loopholes.

The contribution of the paper is to propose a DPOS consensus mechanism based on credit reward and punishment. Based on the application of the blockchain in the educational administration system, we design a consensus framework based on grouping educational system. Using the idea of credit reward and punishment improve the enthusiasm of the node voting and solve the loopholes in the consensus mechanism that error nodes are not timely removed.

III. GROUP-BASED CONSENSUS SYSTEM FOR EDUCATIONAL SYSTEMS

The educational system based on the blockchain is shown in Figure 1. It can realize easy and controlled teaching information data sharing relying on the existing decentralized system framework and the decentralization of blockchain technology. The blockchain-based educational administration system adopts a time-based and non-tamerable protection scheme. From the beginning of the student admission certification, the data generated in the process of students'learning are input into the blockchain. In conjunction with the time source service of the National Time Service Center, the data is stamped with legally valid time stamps to demonstrate the time effectiveness of the data. Blockchain technology can establish peer-to-peer trust in the transparent education system. Schools, the Ministry of Education, students and enterprises will have real-time records no matter what changes are made. When an objection occurs, it can be traced back to the source and cannot be denied. It implements a distributed trust infrastructure that ensures the credibility of student teaching information, and is evidence-based and law-abiding. The multi-private key and high redundancy of blockchain technology can help enterprises, students, schools and the Ministry of Education to solve the current problem of full information authentication, in order to achieve access and trusted sharing of various student teaching information data in different departments.

The blockchain-based educational administration system advances the data management time point and monitors and manages the entire life cycle from the data generation stage. The content changes and information transmission of each student's teaching information data need to be verified and recognized by other nodes of the system. Each node is both a participant and a supervisor. At the same time, the blockchain cannot be modified to ensure that the educational information data cannot be illegally modified; the authenticity and credibility of the educational system information data are effectively ensured.

The DPOS consensus is only reached between a small numbers of proxy nodes selected by the node. The speed of consensus verification can reach the second level, and the degree of matching with the educational system is extremely high. Under normal circumstances, it can meet the business requirements of the educational system. However, the educational system is faced with different departments, these departments have different rights and responsibilities, and there are differences in participation links and timings. The number of nodes is huge. Inevitably, when the DPOS consensus mechanism is elected at the proxy node, there is a problem that the voting is not positive, which not only affects the efficiency of the consensus, but also is not conducive to the timely elimination of the malicious proxy node. The application of DPOS in the educational administration system needs to solve three problems: (1) the

problem of the management and classification of the role of the educational system in the process of consensus; (2) the problem of not voting actively when electing the proxy node; (3) how to quickly eliminate error nodes from proxy nodes. In addition, statistical optimization of the voting results is considered while solving the above problems.

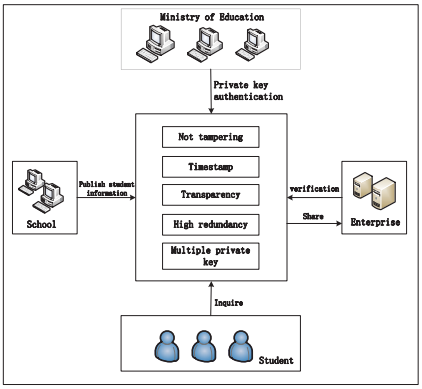

Figure 1. V2G scheduling network.

In order to solve the above problems, this paper proposes a group-based educational system consensus framework, as shown in Figure 2. We divide all the nodes of educational administration system into four node sets by grouping method, which are: the education administration node set, the school node set, the student node set and the enterprise node set. Each node set separately performs proxy node election voting. At least one proxy node is selected for each set to exercise the proxy rights of the set. The proxy nodes selected from the four groups form a set of proxy nodes to generate and validate executing blocks, which can solve the problem of large number of nodes and high cost of system consensus.

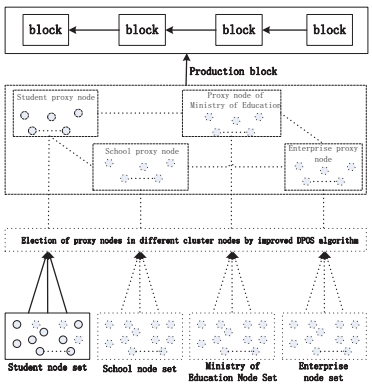

Figure 2. Group-based educational system blockchain consensus framework.

At this time, the DPOS consensus process is divided into three parts: the intra-collection proxy node election, the inter-set proxy node checksum, and the proxy node functions execution. The first two parts need to be solved emphatically. The core of the problem is how to ensure the validity of the election of proxy nodes. That is how to ensure the rationality of the voting scheme and how to guarantee the timely removal of error proxy nodes. Specifically, when selecting a proxy node, the node state and the change of the node states are considered, etc. the participating and rewarding mechanisms are used to drive the participating nodes to actively vote. Finally, the voting results of the proxy nodes in the educational administration system are counted and optimized to ensure that there are no abnormal nodes in the proxy nodes.

IV. DPOS Consensus Algorithm Based on Credit Reward and Punishment

In this section, we propose a DPOS consensus mechanism based on credit reward and punishment. The mechanism mainly includes two parts: node state transition based on voting behavior analysis and DPOS consensus voting method based on credit reward and punishment.

A. Node State Transition

In order to accurately diagnose and eliminate error nodes, the node status is refined. In addition to the normal state and the abnormal state, a good state and an error state are introduced. At same time, in order to enhance the timeliness of malicious node culling, in addition to the support ticket, the node voting process can also vote against the voting node itself. The use of voting behavior affects node state changes to accurately and timely eliminate malicious proxy nodes.

The four states of the nodes are as follows:

Normal state (NS): the initial state of all nodes. At the same time, it indicates that the proxy node does not produce invalid blocks and does not vote against the normal and good nodes.

Good State (GS): the proxy node exceeds the cumulative number of thresholds to continue to generate valid blocks and does not vote against proxy nodes with states NS and GS.

Abnormal State (AS): The proxy node generates an invalid block but does not exceed the accumulated value or vote against the NS and GS nodes.

Error state (ES): Proxy nodes produce invalid blocks many times, or the number of rounds voting against normal and good state nodes exceeds the cumulative value. Malicious nodes will not be able to vote for a period of time.

After refinement of node state, state identifier is added to each node, and node behavior is judged according to certain conditions and state transition is carried out. In order to ensure that the block generated by the proxy node is a valid block and there is no error behavior (such as voting against the NS and GS nodes), the node state transition is mainly judged according to two conditions: whether the node generates a valid block and whether the node vote against NS and GS nodes. Combining the number of votes and the node state, the conditions for state transition are as follows: (1) consecutively generating multiple valid blocks exceeding the cumulative value N, and no vote against the NS and GS nodes; (2) generating an invalid block or voting against the NS and GS nodes; (3) Multiple invalid blocks are generated more than the cumulative value N or the NS and GS nodes are voted more than N.

As shown in Figure 3, all nodes of the educational system are initialized to the NS state. Each new node is added, the

system sets it to the NS state by default, and the new node participates in the proxy node election activity normally. When the NS node generates multiple valid blocks and there is no error voting behavior, which means that the working state of the NS node is good, the state is changed to GS, and the GS node is selected as the proxy node as much as possible. When the NS and GS nodes generate an invalid block or have an error voting behavior, their status will be changed to AS, which means that the node behavior has been detrimental to the system work, The AS node will have certain disadvantages in the election process of the proxy node. If the proxy node generates an invalid block multiple times and exceeds N, and performs an error vote multiple times, it can be determined that the node has a negative effect on the system work and needs to be culled, its state is changed from AS to ES. The ES node will not be allowed to participate in voting and proxy node elections for a period of time. When the system votes at the node, it will prompt the node status so that the node can vote effectively. In order to improve the timeliness of eliminating malicious nodes, we can start eliminating malicious nodes when they are in AS state.

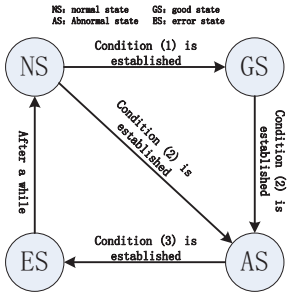

Figure 3. Node state transition.

B. Voting Method Based on Credit Rewards and Punishments

1) Credit reward and punishment model

The credit value is the credit parameter given by the system when the node joins the network. According to the consensus mechanism and the characteristics of the nodes in the administration system, the credit value of each node is calculated by percentage system, and the initial credit value of each node is 70.

The voting method based on credit rewards and punishment involves three basic factors: black, credit penalty and credit reward.

a) Negative vote

In the process of proxy node election, the system gives each node the opportunity to vote against each node. The purpose is to quickly remove the AS node and ensure the security of the educational system if it appears in the proxy node. For this purpose, the node has the right to vote for the votes and the right to vote for the negative votes, the two voting processes are basically similar. For the AS node, the system will give a prompt when voting, so that it can vote against it, in this way, the AS node can be quickly removed from the proxy node set according to the corresponding changes in the credit value when the voting results are counted.

b) Credit punishment

The credit value of each node is calculated according to its vote. We set a time t, which represents the time interval from the last vote to the next vote. $C_i(t)$ represents the credit value of the i-th node. In order to prevent the node from voting negatively and encouraging the node to vote, the credit value will decrease as the node's two voting intervals t increase, and credit penalty will be imposed. T represents a time constant. When t<T, that is, when the two voting time intervals are less than T, the credit value of the node does not change. Conversely, the credit value will decrease, and the node will reset the time t after the vote is successful, that is, let t=0, which encourages the node to participate in the voting. At the same time, in order to punish the error voting behavior, if the node votes against the node with the status of NS and GS, the credit value of the node is lowered.

The formula for calculating the credit value of the i-th node is:

$$C_i(t) = C_i(t) - \lfloor t / T \rfloor * U - R_i(U) \tag{1}$$

$$R_i(U) = \begin{cases} U & \text{Vote against NS or GS nodes} \\ 0 & \text{No vote against NS or GS nodes} \end{cases} \tag{2}$$

U indicates the speed at which the credit value is reduced. It is a constant and can be adjusted in combination with specific services. $R_i(U)$ represents a penalty for a node that has an error vote during the voting process.

c) Credit award

In order to ensure that the AS node is present in the agent system node set, it can be removed from the agent node as soon as possible, and the node that voted against the AS node is given a credit reward. In order to prevent malicious increase in credit, it is stipulated that each node has only one chance to vote against each time. At the same time, in order to improve the accuracy of the credit reward, it will be judged whether the AS node that was voted against becomes a proxy node after each round of voting results. If not, the node that voted against the AS receives a credit reward, as shown in (3), and vice versa, the credit value does not change.

The formula for calculating the credit value of the i-th node is:

$$C_i(t) = \begin{cases} C_i(t) & \text{No vote against the AS node} \\ C_i(t)+U & \text{Vote against the AS node} \end{cases} \tag{3}$$

2) Voting result statistics and optimization

After the nodes in the educational administration system vote according to the credit reward and punishment model, they need to count the results to obtain a new set of proxy nodes, and judge the abnormal proxy nodes according to this. The system assigns each node a node attribute table and updates it in real time. The node attribute table includes: node ID, node state, credit value, votes and negative votes. The voting result statistics are calculated according to node state, credit value, votes and negative votes. The statistical

results are calculated by considering the degree of influence on the results. The statistical formula of the n-th round of the i-th node voting result is as follows. V indicates the number of votes, N indicates the number of negative votes, M indicates the number of nodes with voting rights in the round, A is the proportion of the number of nodes in the voting rights node. B and C are the statistical weights of the number of votes and the number of negative votes. The basic values are taken as 0.5.

$$\Omega_{nj}=\begin{cases} M_{nj}(C_i(t))+H_{nj}(V) & nodestate=='NS' \| nodestate=='GS' \\ M_{nj}(C_i(t))+H_{nj}(V)-\Psi_{nj}(N) & nodestate=='AS' \end{cases} \quad (4)$$

$$M_{nj}(C_i(t))=A*C_i(t) \quad (5)$$

$$H_{nj}(V)=B*V \quad (6)$$

$$\Psi_{nj}(N)=C*N \quad (7)$$

$$A=V/M \quad (8)$$

$$B=0.5*V/M \quad (9)$$

$$C=0.5*(1+N/M) \quad (10)$$

After the calculation of equation (4), a node with a lower node credit value needs more support votes to become a proxy node. The node voting statistics are positively correlated with the votes they receive, and negatively correlated with the negative votes they receive. The more support votes a node obtains, the higher the positive statistical coefficient, the more the statistical result data increases, and the higher the statistical ranking; the less the negative votes obtained by the node, the smaller the negative statistical coefficient and the decrease of the statistical result data. The less the statistics, the less the statistical ranking are.

3) Design of voting algorithms

This section proposes a proxy node voting election algorithm based on credit rewards and punishments. The algorithm steps are as follows:

Algorithm 1

Step 1: initialize

Step 2: all nodes in the educational administration system vote to elect the proxy node;

Step 3: Judging whether a node votes or not, the voting node performs the step 4, the node without voting performs step 5;

Step 4: Using the formula (4) to perform voting result statistics; and resetting the time t of the voting node, t=0;

Step 5: Calculate the credit value penalty of the unnoted node by using formula (1), and wait for the next round of voting;

Step 6: Judging whether the abnormal node loses the proxy right; if the proxy right is not lost, the program ends, waiting for the next round of voting, if the proxy is lost, Step 7 is performed;

Step 8: Judging whether the node voted against the abnormal node. If yes, use the formula (3) to credit the node. If the program ends, wait for the next round of voting.

The algorithm flow is shown in Figure 4:

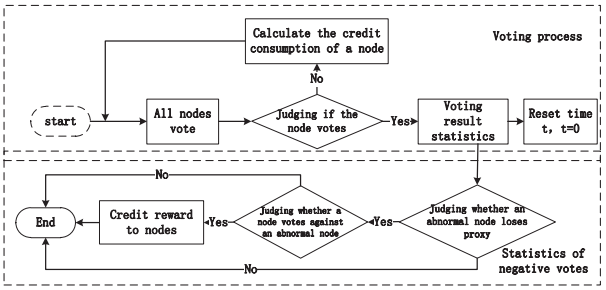

Figure 4. Voting process based on credit rewards and punishments.

V. SIMULATION RESULTS

In this section, a simulation experiment is conducted for a group, and the experimental analysis is performed using a school node set. Comparing the effects of the algorithm before and after the improvement, verifying whether the node still has negative voting behavior in the proposed algorithm, whether the node with the state AS can obtain the identity of the proxy node with high probability, and realize the timely elimination of the AS node.

A. Comparison of Voting Results

The simulation experiment is based on a distributed network with 20 nodes. The number of proxy nodes that need to be elected is four. After a round of voting, the voting results are shown in Table 1.

TABLE 1 VOTING RESULTS TABLE

Node ID	Node state	Credit value	Votes	Negative Votes
N5	NS	70	35	0
N4	NS	70	16	0
N10	AS	70	11	0
N7	NS	70	6	0
N1	NS	70	3	0
N11	NS	70	0	0
N14	NS	70	0	0
N18	NS	70	0	0
N19	NS	70	0	0
N20	NS	70	0	0
N6	NS	70	0	0
N9	NS	70	0	0
N2	NS	70	0	0
N3	NS	70	0	0
N8	NS	70	0	0
N12	NS	70	0	0
N15	NS	70	0	0
N13	NS	70	0	0
N16	NS	70	0	0
N17	NS	50	0	0

In Table 1, the first four nodes are calculated as proxy nodes according to the voting result statistical formula. We assume that the state of the node N10 is changed to AS, the second round of voting is based on the result, and the voting results of the second round before and after the algorithm improvement are compared. The statistical abnormal node ranked the number of votes after the second round of voting, and carried out 30 repeated experiments. The experimental results are shown in Figure 5.

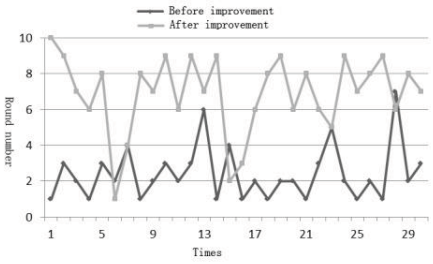

Figure 5. Comparison of abnormal node votes before and after DPOS improvement.

As shown in Figure 5, AS nodes rank significantly lower than before, before improvement, the number of times that a AS node obtains the identity of the proxy node in the third round is 27 times, the times is 90% of the total. The improvement is only 4 times, which accounts for less than 3%. This experiment shows that the probability that the AS node becomes a proxy node is significantly reduced.

B. The Verification of the Voting Rounds the AS Node Loses Proxy Rights

Further verifying whether the average number of voting rounds required by the AS node to lose the proxy identity before and after the DPOS mechanism is improved. Judging the timeliness of the mechanism proposed in this paper to eliminate abnormal nodes. The number of voting rounds that the AS node needs to be replaced from the set of proxy nodes is counted. In order to ensure the accuracy of the results, 30 repeated experiments are performed before and after the improvement of the mechanism. When the AS node is kicked out of the proxy, the statistics of the number of voting rounds are shown in Figure 6. The average of the experimental results before and after the improvement of the mechanism is calculated and compared. Before the mechanism is improved, it need the average of 3 rounds that the AS node is kicked out of the proxy set. After the mechanism is improved, it takes the average of 1round.

As can be seen from Figure 6, in the improved consensus algorithm, the probability that the AS node becomes the proxy node again is significantly reduced. The number of voting rounds required for the AS node to be kicked out of the proxy node set is also greatly shortened, from three rounds to only one round of voting. The negative impact of node anomaly on the system has been reduced, which enhances the security of the system.

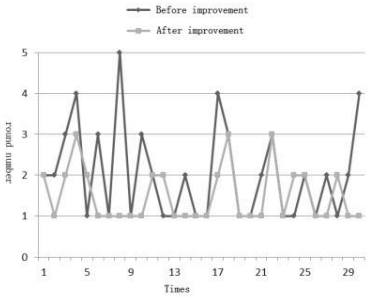

Figure 6. V2G scheduling network.

VI. CONCLUSION

In this paper, aiming at the problems of inactive voting and abnormal nodes in the blockchain consensus mechanism of educational administration system, we propose an improved DPOS blockchain consensus algorithm suitable for educational administration system. Firstly, all the nodes of the educational administration system are divided into different sets according to the roles, and a consensus framework of the group-based educational system is constructed. Secondly, aiming at the error behavior of nodes, the nodes state is refined and the state transition mechanism is given. On this basis, we design the node credit reward and punishment model, and the result statistics method is optimized. Then we propose the voting scheme based on credit reward and punishment. Using the idea of credit reward and punishment, the effectiveness of the election of the proxy node is guaranteed and the purpose of eliminating abnormal nodes in time is achieved.

REFERENCES

[1] Yaoyao Chen, Research on the Application of Incentive Mechanism in College Educational Administration [J], Yangtze River series, 2017(4):229-229.

[2] Yong yuan, Feiyue Wang. Blockchain: The State of the Art and Future Trends[J]. Acta automatica sinica, 2016, 42(4): 481-494

[3] NAKAMOTO S. Bitcoin: A Peer-to-Peer Electronic CashSystem[EB/OL].https://www.researchgate.net/publication/228640975_Bitcoin_A_peer-to-peer_electronic_cash_system,2017-6-11.

[4] Bin Liang. Viewing the Consensus Mechanism of Block Chain Technology from "Bitcoin Mining" [J]. Financial Computer of China, 2016(09):45-46.

[5] Zamfir V. Introducing Casper 'the Friendly Ghost'[J]. Ethereum Blog URL: https://blog.ethereum.org/2015/08/01/introducing-casper-friendly-ghost, 2015.

[6] Xuan Han, Yamin Liu. Research on the Consensus Mechanisms of Blockchain Technology [J]. Netinfo Security, 2017(9):147-152

[7] Larimer D. Delegated proof-of-stake white paper [J]. 2014

[8] Schuh F, Larimer D. BitShares 2.0: Financial SmartContract Platform[J]. 2015.

[9] Zhili Xu, Huamin Feng, Biao Liu. Study of highly efficient PBFT consensus mechanism based on credit [J]. Application Research of Computers, 2018, 36(10).

[10] Qiubo Huang, Qingwen An, Houqing Su. Study and Realization of Improved PBFT Algorithm As An Ethereum Consensus Mechanism [J]. Computer Applications and Software, 2017, 34(10).