Research on Node Control of Blockchain Network Based on Reputation Model

Weiping Zeng

zwp15697895052@163.com

Institute of Logistics Science and Engineering, Shanghai Maritime University, Shanghai 201306, China

Abstract: The rapid development of the Internet has driven the network technology to all walks of life, and the generation of massive data flow has caused huge pressure on the traditional centralized data management platform. The data information management system built can provide a better solution for data control nowadays. To this end, this paper researches the consensus algorithm to make the nodes of blockchain network reach consistency, addresses the lack of node behavior control problem of practical Byzantine fault tolerance (PBFT) algorithm, quantitatively evaluates the node reputation by combining the custom reputation model with PBFT algorithm, optimizes the selection of master nodes in the consensus process, and completes the real-time update and full monitoring of node reputation, which is essential for It has a good role in improving the security and reliability of blockchain system consensus. The scheme has certain theoretical and practical significance to solve the problem of safe storage of data in the market and improve the governance system of data.

Keywords: Block chain; Consensus mechanism; Trust model; Node Control

1 Introduction

Blockchain, as a distributed database technology, forms a series of data blocks by continuously growing records, each of which records transaction information within a certain time frame and is protected using encryption technology. In the blockchain, each node has a complete copy of the record, and the consistency, security and reliability of the data are ensured by certain consensus algorithms between different nodes. In the consensus algorithm, node control refers to a series of management tasks such as controlling the node entry conditions and selecting the set of nodes. The purpose of node control is to ensure the operation of the entire consensus algorithm and to protect the security and reliability of the entire network. It is usually managed by the core team or community of the blockchain project, and they can screen the appropriate nodes by certain rules and criteria.

Practical Byzantine Fault Tolerance (PBFT), as a Byzantine fault tolerance algorithm, is widely used in federated chains and private chains[1]. In PBFT algorithm, the node control includes two aspects, one is the node selection condition, which usually includes: the working status requirement of the node, the capability requirement of the node, and the normality requirement of the node. The PBFT algorithm can effectively reduce the waste of resources, support high transaction throughput, and provide high security and reliability of the system. However, the PBFT algorithm lacks credibility evaluation of nodes; there is no corresponding punishment mechanism for nodes with malicious behaviors in the consensus process; and it cannot meet the

ICBBEM 2023, May 19-21, Hangzhou, People's Republic of China

DOI 10.4108/eai.19-5-2023.2334350

demand for the corresponding increase in the number of dynamic nodes in the system due to the growth of network scale. Therefore, in order to solve the problem of the lack of node control mechanism in the existing consensus algorithm and improve the success rate of blockchain network consensus, this paper takes PBFT algorithm as the entry point to optimize the selection of blockchain nodes for the network node control mechanism to ensure the efficient operation of the blockchain network system.

2 Research on relevant theories

The data information management system built by blockchain technology can truly record the historical behavior data of nodes at the technical level and provide a detailed and reliable data source for the process of node reputation evaluation in the text.

2.1 Theoretical Study of Consensus Algorithms

PBFT algorithm is the focus of scholars' research.In 1999, Miguel Castro and Barbara Liskov from MIT lab proposed a state machine replication protocol that can tolerate Byzantine errors in asynchronous networks and called it Practical Byzantine Fault-Tolerant PBFT Consensus [2]. In terms of fair and secure selection of master nodes, Lei et al. proposed an improved algorithm based on reputation, which focuses on the behavioral performance of nodes during the consensus process and uses a reputation model to bind the reputation value to the node discourse power, thereby improving the security of master node selection [3].Wang et al. proposed an improved algorithm based on credit delegation, which designs the evaluation and reward and punishment mechanisms of reputation, and classifies nodes according to their trustworthiness differences into trustworthy, normal, abnormal, and failed four trust states to reduce the number of untrustworthy nodes in consensus nodes [4]. Chu et al. proposed a double-cluster improvement algorithm that uses a voting election mechanism to select the consensus master node, optimize the view switching process, and ensure the consistency of message order and views. The PBFT algorithm consistency consensus protocol is simplified to reduce the amount of communication between nodes to achieve reduced latency [5]. Fang Luo et al. designed a custom node performance evaluation and election mechanism, while simplifying the consistency protocol of the original PBFT algorithm and using a two-stage consensus protocol to complete the work and shorten the consensus latency in the blockchain system [6].

2.2 Nodal Control

Node control, as the main element of consensus algorithm, is created to ensure the legitimacy and trustworthiness of bookkeeping nodes in blockchain networks. In a decentralized blockchain network, how to select bookkeeping nodes and control their behavior are important issues. Without an effective node control mechanism, it may lead to malicious actors joining the node network and launching attacks, resulting in the failure of system consensus. For the good operation of the system, certain rules must be designed to select qualified nodes, and corresponding management measures must be carried out when nodes join and withdraw or are unable to perform node-related duties for other reasons[7].

The specific measures of node control are differentiated by different consensus algorithms, for example, the PoW algorithm usually requires the bookkeeping node to have sufficient

computing power and mining machines, while the PoS algorithm requires the node to hold a certain number of tokens, etc[8]. In the PBFT algorithm, nodes need to have sufficient business capacity to process transactions, etc. Therefore, the node control scheme will change with the development and update of consensus algorithms to cope with new security challenges and diverse application requirements. With the popularity and development of blockchain, node control will continue to be improved and optimized in practice.

3 Research on consensus mechanism scheme based on node control

In blockchain systems, reputation models can be used to assess the creditworthiness of nodes or users. The reputation model and node control are interrelated, and together they guarantee the stability, trustworthiness and security of the whole system[9]. The reputation degree of a node is calculated based on its historical behaviors and participation, which include the transactions in which the node has participated, the degree of contribution, and so on. The higher the reputation value, the higher the trustworthiness of the node or user, and the transactions or behaviors issued by it are more easily accepted by other nodes or users[10].

3.1 Node control analysis

When designing the reputation model, factors of node control need to be considered to ensure that the model has reliability and validity. Specifically, the following points need to be considered when designing a reputation model:

1. Determine the assessment metrics: The reputation model needs to assess the credibility of nodes based on certain assessment metrics, such as the number of participation, quality of participation, contribution, revenue and other indicators. These indicators should be representative and able to cover all aspects of node behavior.

2. Selection of evaluation algorithms: When designing the reputation model, it is necessary to select appropriate algorithms to calculate the reputation values of nodes and choose appropriate trade-offs and optimization strategies to balance the reputation among different nodes.

3. Integration with node control: The reputation model needs to be integrated with node control. For example, only nodes that pass the node control review can participate in the reputation evaluation, and also need to take corresponding optimization and punishment measures for malicious nodes or behaviors.

4. Design of incentives: The reputation model can be used to encourage nodes to participate in integrity activities and improve their contributions through incentives, which can help guide nodes to maintain good reputation and quality in the system.

To conclude, node control is a very important part to guarantee the success rate of consensus, and the legitimacy and stability of nodes determine the accuracy and effectiveness of reputation evaluation. Therefore, when designing the reputation model, we need to focus on the mutual cooperation of the node control of the reputation model to jointly improve the security and stability of the whole system. In response to the above problem this paper proposes a consensus algorithm based on Peer Trust reputation model (Trust PBFT), which can guarantee the good operation of consensus process of dynamic blockchain system by comprehensive evaluation of

node reputation value through the interaction behavior of nodes in the consensus process.

3.2 Consensus program process planning

In the design of the specific scheme of this paper, the blockchain system network consists of N nodes, introducing the credibility evaluation model, calculating the credibility value of nodes through the credibility model, considering other influencing factors in the system, evaluating the consensus behavior of each node on the chain composed of multiple participants, and quantifying the credibility of nodes; adding the node hierarchy based on the evaluated credibility value, grading the nodes, and correlating them with the system authority At the same time, a node reputation incentive system is introduced to reward and punish nodes with reputation value after each round of consensus, so that node reputation can be updated and monitored in real time. The overall process of this scheme is a three-stage cycle of "evaluation-monitoring-execution", including credibility evaluation, node level differentiation, time-out monitoring, credibility update, restoration, and reward and punishment.

Considering the relevant points about the design of reputation model, the specific steps of the node control scheme based on reputation model in this paper mainly include the following parts:

(1) Node evaluation, quantitative evaluation of the reputation of the nodes on the chain based on the customized reputation model, and classification of the nodes into four levels: candidate, trusted, regular and untrustworthy according to the final node ranking.

(2) Node selection, the node with high reputation is selected to be the master node on the chain according to the reputation level, and the node with bad reputation is screened out and consensus is conducted.

(3) Real-time update of reputation, based on the behavioral feedback between nodes in the historical consensus process, based on the reputation incentive evaluation model, the nodes are incentivized to different degrees, and the reputation of nodes is updated in time when new transactions are generated based on the reputation real-time evaluation model.

(4) Reputation restoration and reward and punishment, establishing a certain reputation threshold, when the node's reputation is greater than the reputation threshold, the node's excess reputation is recovered before the next round of consensus; when the node's reputation is insufficient to participate in the previous round of consensus process, then the node's reputation is partially restored before the next round of consensus, so that it has the minimum reputation value for the next round of consensus. Then the system enters the reputation reward and punishment, and rewards and punishes the nodes on the chain based on the behavior of the nodes in the previous round of consensus and the reputation reward and punishment system.

(5) Update view, after the last round of consensus, before entering the next round of consensus, repeat the first step to grade the nodes, and then select the updated master node based on the new node grade classification result, and so on and so forth until the enterprise client ends the consensus request.

4 System node management based on Peer Trust reputation model

The Peer Trust reputation model evaluates the interaction behavior of all nodes involved in data sharing on the chain in each round of the system, provides quantifiable indicators for the reliability of nodes' behavior, and divides all nodes into levels according to the needs of the system, and gives different powers to nodes of different levels as the main basis for the selection of master nodes in the consensus process, and the reputation modeled master node selection method can guarantee the fairness and correctness of the system to a greater extent and improve the trust of nodes on the blockchain system.

4.1 Node reputation evaluation

The behavioral interactions of nodes in the on-chain consensus are the basis for node reputation evaluation, and the behaviors of each node in the consensus are uncertain in terms of the direction of influence on the system consensus, specifically in terms of positive and negative behaviors that have different degrees of influence on the consensus results. Relying on the node control scheme built on the blockchain, the behavioral information of all nodes in the consensus process is recorded in the independent client logs, which can provide a credible data source for node reputation evaluation, mainly including the historical consensus process in which nodes participate, the number, time and amount of transactions conducted between nodes, the success rate of consensus in which they have participated, the transaction environment, etc.

In the blockchain system of this section, assuming that the system contains n ($n \in N+, n \geq 3$) nodes as the object of study, the various types of variables used for node evaluation are defined according to the Peer Trust custom reputation model, as shown in the table 1 below:

Table 1. Credit model variables table

Parameters	Definition
n	Total number of nodes participating in consensus ($n \in N+, n \geq 3$)
R_i	The final reputation value of node i calculated by the reputation model
S_i	Historical reputation value of node i
D_{it}	Real-time reputation value of node i
I_{ik}	The incentive reputation value of node i
k	Weight values assigned by the system to credibility evaluation indicators
Ai	Historical behavior factor of node i
C_i	Historical activity factor of node i
γ	Weight values of the engagement factor and the behavior factor
T_i	Total number of rounds in which node i participated in the historical consensus process

ContinuedTable 1. Credit model variables table

Parameters	Definition
T_{is}	Number of rounds of positive behavior in the historical consensus process in which node i participated
T_{if}	Number of rounds of negative behavior in the historical consensus process in which node i participated
μ	Weighting values for positive and negative rounds
τ	Historical activity factor of node i
i	The consensus cycle in which node i participates
m	A total of m rounds of consensus in the consensus cycle
k	denotes the kth round consensus process
$D_{ij}^{t_k}$	denotes the reflective evaluation of node j on node i in the kth round of consensus process
f(k)	Time recession factor set by the system

Definition 1, Reputation evaluation of a node. When evaluating the reputation indicator of node i, the reputation value of node i is defined as R_i in the custom reputation model, and the R_i value in the computational equation of reputation value consists of three components: the historical reputation value S_i, the real-time reputation value D_{it} and the incentive reputation value I_{ik} of this node. Considering that different elements have different degrees of influence on the reputation value of a node, a certain weight value k is assigned to the above three elements in this calculation formula, and the combination of the three sets of reputation measures and preset weights is used to comprehensively measure the reputation of a node on the chain. The specific computational equation is as follows:

$$R_i = k_1 * S_i + k_2 * D_{it} + k_3 * I_{ik} \quad (1)$$

Definition 2, the historical reputation evaluation of nodes. Define this historical reputation evaluation index as S_i, which is calculated by the interaction of this node with other nodes in the historical consensus process as the main influence factor, and its core basis is divided into two parts, one is the positive and negative behaviors of node i in the historical consensus process, which is defined as the historical behavior factor A_i in the model; the second is the high or low participation of this node in conducting the consensus process, which is defined as the historical activity factor C_i, while assigning weights γ to the two behavior factors to balance the differences in the influence of different factors on the total reputation value results, which are calculated as follows:

$$S_i = \gamma_1 * A_i + \gamma_2 * C_i \quad (2)$$

Definition 3, node historical behavior factor. Determined by the interaction behavior of node i with other nodes in the historical consensus process, as part of the node's historical reputation evaluation, which is reflected in the consensus process as the positive behavior of the node will have a positive impact on the consensus result and the negative impact of the negative behavior

on the consensus result, the nodes with more positive behavior are selected in preference, and the state of these nodes is relatively stable. The calculation of the formula is defined by the total number of historical consensus T_i that node i has participated in, the number of positive behaviors T_{is} and the number of rounds of negative behaviors T_{if} in the historical consensus process of that participation and the corresponding weight factor μ. The specific calculation equation is as follows:

$$A_i = \frac{\mu_1 * T_{is} - \mu_2 * T_{if}}{T_i} \tag{3}$$

Definition 4, Node historical activity factor. This index is determined by the node's historical activity in the consensus process, and the specific value is expressed as the number of times the node has participated in the consensus. Based on the consensus process under Byzantine consensus mechanism, nodes need to broadcast and receive messages among themselves, and different nodes have different reaction processing time for messages. When a low active node participates in the consensus process as the master node, there may be a delay in broadcasting causing other nodes on the chain to have to wait, thus making the consensus process stall in a certain part and reducing the efficiency and success rate of the system consensus. In the calculation of the specific historical participation factor in the equation, the purpose of designing the activity factor τ is to ensure that the final reputation value of the node varies within a certain value range.

$$C_i = \left(\frac{1}{2}\right)^{\frac{\tau}{T_i}} \tag{4}$$

Definition 5, real-time reputation evaluation of nodes. This evaluation index is defined by node i and node j in the consensus cycle t, defined in the cycle of m rounds of consensus, in the consensus cycle of the kth round of consensus process, nodes according to the established rules for a certain interaction behavior, node j then to make a certain reflection of the behavior of node i evaluation $D_{ij}^{t_k}$, taking into account the impact of time on the reputation evaluation, in the calculation of the model to add a time recession factor f (k), calculated as $f(k)=\rho^{(m-k)}$ ($0<\rho<1, 1\leq k\leq m$), the time recession factor has a positive correlation for the impact of reputation evaluation, which is reflected in the fact that the closer the node's performance in time in the evaluation process of the node is for its reputation evaluation, as shown in the following equation.

$$D_{it} = \begin{cases} \dfrac{\sum_{j=1}^{n} \dfrac{\sum_{k=1}^{m} f(k) * D_{ij}^{t_k}}{m}}{n} & m \neq 0 \\ 0 & m = 0 \end{cases} \tag{5}$$

Definition 6, Node incentive reputation evaluation. Reputation incentive evaluation is a metric that the system rewards and punishes the node for the behaviors it exhibits in this round of consensus after the consensus is completed, first classifying the behaviors as normal, faulty, and malicious behaviors, and then assigning different scores to different behaviors according to the scoring rules corresponding to the behavior rule table, and the specific reward and punishment values are determined by the following equation, in which R_{k-1} is expressed as the updated Reputation degree.

$$I_{ik} = \begin{cases} \sin\dfrac{(1-R_{k-1})\pi}{2} & \text{(Positive behavior)} \\ \sin\dfrac{(-R_{k-1})\pi}{2} & \text{(Negative behavior)} \end{cases} \tag{6}$$

The above evaluation model can evaluate the node credibility more correctly and comprehensively, and when a node(s) on the chain behaves maliciously, it can also be punished by incentivizing the credibility evaluation, which guarantees the real-time update of node credibility, and can significantly improve the credibility of nodes participating in the consensus process through the preferred node selection method, which has a great positive effect on improving the consensus success rate. At the same time, since the reputation model is based on the historical behavior data of nodes, these historical evaluation data are stored separately on the chain, and the client cannot tamper with them, which greatly ensures the objectivity and credibility of the evaluation results under the reputation model.

4.2 Consensus master node selection

In the evaluation of node interaction behaviors the behaviors exhibited by nodes in the consensus process are classified into three categories: normal, faulty and malicious, as shown in Table 2. In the Peer Trust reputation model, nodes can rate other nodes based on their behavior in the previous consensus round through scoring rules. The score will be used as a reference element for the final reputation value of that node.

Table 2. Rules for node behavior

Behavior classification	Scoring Rules	Become a master node
Normal behavior	+1	Send messages normally and with low message error rate
Fault behavior	0	Messages not sent or not processed from other nodes within the system specified period
Malicious behavior	-1	High error rate in the content of sent messages

After evaluating the node reputation based on the reputation model, we obtain the reputation index value of each node, and divide certain reputation thresholds based on the ranking ratio of the values, so as to complete the grading process of all nodes, and classify the nodes into four levels: candidate, credible, conventional and untrustworthy, and the thresholds of the four node states are R_{good} for the candidate state, R_{normal} for the credible state, R_{bad} for the conventional state, and 0 for the untrustworthy state. The threshold lower limit Rbad for the regular state, and the threshold lower limit 0 for the loss of trust state, and the specific grading is shown in Table 3. Nodes of different grades have different powers, candidate nodes have the priority to become master nodes, and discredited nodes are prohibited from participating in the next round of consensus. The grading of reputation can prevent nodes with negative behavior from participating in the consensus process, reduce the consensus failure due to subjective factors of nodes, and improve the consensus efficiency.

Table 3. Node reputation level table

Reputation Value Ranking	Credit Value Range	Node Type	Node Permissions		
			Consensus Master Node	Consensus Nodes	Candidate Consensus Nodes
Top 25 percent	（Rgood,1）	Candidate nodes	√	√	√
Top 50 percent	(Rnormal, Rgood)	Trusted nodes	×	√	√
Top 75 percent	(Rbad, Rnormal)	Regular nodes	×	×	√
The last 25%	(o,Rbad)	Breach of trust node	×	×	×

The PBFT algorithm based on the Peer Trust reputation model selects the master node by taking the modal operation, based on the node reputation value calculated in the previous part of the reputation model, and correlates the selection of the master node before consensus with the reputation value of the node, the larger the node reputation value the higher the priority it has in being elected as the master node, this selection method has greater fairness, and all the nodes in the system nodes in the system have the same probability of being elected as a master node. The pseudo code of the algorithm is shown in Table 4.

Table 4. Master node selection algorithm pseudo-code

Master node selection algorithm
Input: node number i, node reputation value Ri
Output: master node number p
1： for i=1,2 3,…,N do
2： Sort Ri to get the descending order of Ri
3： if Ri is the current maximum value
4： i is elected as the master node, p = i
5： else
6： i becomes a slave node
7： end if
8： end for

4.3 Reward and punishment of node reputation

After the node reputation evaluation, a certain reward and punishment system should be designed to reward and punish the nodes with high reputation and low reputation in real time, the purpose of which is to prevent the nodes with high reputation in the first round of consensus from acting negatively in the subsequent consensus, and to give a certain degree of reward to the nodes with low reputation in the first round of evaluation to promote the positive behavior of these nodes in the subsequent consensus.

1) Node reputation reduction

The node reputation reduction is mainly used to balance the node reputation value in the consensus system that is lower or higher than the threshold value. When the reputation value of node i is higher than the upper limit of candidate node reputation initially specified in the consensus after the evaluation and update of the reputation model, the system automatically performs the credibility restoration of the node according to the preset algorithm, so that the reputation of the node is replaced with the credible node reputation threshold; when the updated node reputation value is in the discredited node interval, the node does not participate in the consensus process, and before the next round of consensus starts the The credibility is restored so that it is transformed into a regular node and has the right to join the next round of consensus to prevent the continuity of this type of node in the consensus negatively. The algorithm of reputation reduction under consensus mechanism is shown in Table 5.

Table 5. Node reputation reduction algorithm

Credit Reduction Algorithm
Inputs：Ri，Ni ，K
Outputs：Ri，Ni
1：for k ← 1 to K do; Check the K-round consensus list
2：if Ri > 1；
3：then Ri ←Rnormal；
4：Ni ← Nnormal； Reputation reset for nodes whose reputation is above the threshold
5：else if Ri < Rbad;
6：then Ni banned from taking part in the next round of consensus; Nodes with credibility below the threshold are banned from the next consensus round
7：Ri ←Rbad after the next round of consensus;
8：Ni ← Nbad; Reputation restoration for nodes whose reputation is below the threshold after the next consensus round
9：else keep the Ri in Ni; Nodes that do not meet the above credibility restoration conditions Ni keep their credibility unchanged
10：return Ri、Ni;
11：end for

2) Reward and punishment of node reputation

In the consensus mechanism about the node rewards and punishments, mainly based on the interaction behavior of different levels of nodes in the last round of consensus process, through the supervisory judgment of each type of node initiating behavior and the assessment of each node's credibility in the node credibility model, the nodes with positive and negative behavior are given certain level conversions, the specific conversions are shown in Figure 1 below. If the node that participated in the previous round of consensus, i.e., the non-defaulted node, behaves positively in the consensus, the system gives it a certain reputation reward after the consensus is over, which enables the defaulted node judged in the previous round of consensus to improve its reputation value by performing positive behaviors in the next round of consensus, so as to obtain the opportunity to become a candidate node and master node; if the participating node

behaves negatively in the consensus, the system automatically deducts a certain If a node behaves negatively during the consensus, the system automatically deducts a certain amount of reputation as a penalty; if the consensus fails due to the subjective factors of the master node in the previous round, the node's right to become the master node in the next round will be withdrawn.

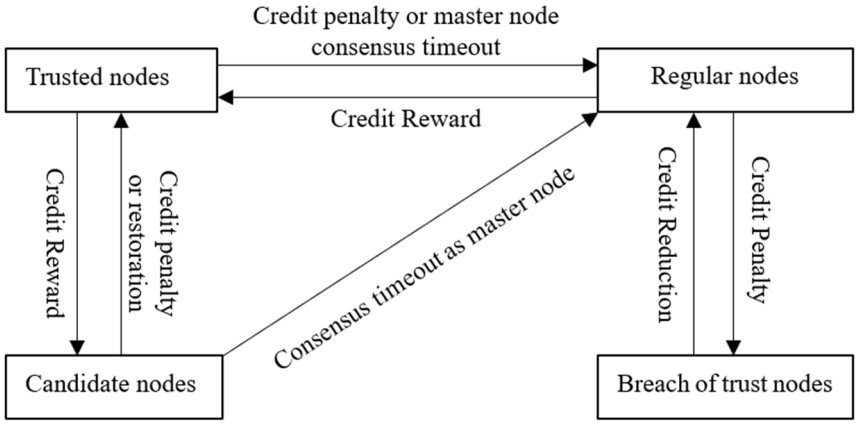

Fig. 1. Conversion of nodes

4.4 Joining and exiting of nodes

Since the blockchain network is dynamic, nodes do not remain unchanged, and there may be node entry and exit in the system consensus process. In order to ensure that the consensus process can be successfully completed when a node exits the consensus stage, a certain dynamic node entry and exit mechanism needs to be designed.

(1) New node joining: When a node on the chain chooses to withdraw and the number of nodes after withdrawal does not meet the minimum number of nodes for the consensus process, the new node joining needs to be verified by the master node and other slave nodes on the chain. Firstly, the system needs to select the node with the highest reputation value from the candidate consensus node set to replace the withdrawn node, and the selected node needs to send a join request message to the master node and other slave nodes, which mainly contains its own node reputation value, node number and node signature. After verification, the master node broadcasts the request information of the node to other nodes on the chain, and if more than 2/3 of the nodes on the chain send their own information to the node for preservation, the node is considered to have officially joined the system to participate in the subsequent consensus work.

(2) Withdrawal of the old node: When the old node chooses to withdraw from the blockchain system, it needs to send a withdrawal confirmation message to the master node and other slave nodes on the chain, and the withdrawal condition is satisfied when the withdrawal message is permitted by more than 2/3 of the nodes on the chain, and then the withdrawing node needs to delete the relevant node information and records of the system stored in the local client, and formally withdraw the power of the node after system verification. successfully exits the system.

5 Conclusions

This paper constructs an optimization scheme for the consensus mechanism of blockchain system under custom reputation model for the problem of lack of control over network nodes in practical Byzantine fault-tolerant consensus mechanism (PBFT) in blockchain system, taking into account the behavior of nodes, and incorporating the historical activity degree of nodes in the consensus process and the consensus success rate of their participation into the node reputation evaluation process, in order to infer the future behavior of the node based on the historical behavior, so as to achieve a comprehensive evaluation of the system node reputation, promote the active and positive behavior of nodes in the consensus process, and improve the consensus efficiency of the system.

5.1 Summary of the program

The proposed optimization scheme of consensus mechanism under reputation model, on the one hand, selects nodes with higher reputation value to participate in system consensus by means of reputation evaluation, gives more rights and interests to nodes with high trustworthiness, and has a good promotion effect on nodes' active honest behavior, on the other hand, the punishment mechanism of nodes' malicious behavior in this scheme makes the power of nodes with low trustworthiness be restricted to different degrees when When the nodes with low trustworthiness participate in the system consensus, it has a negative impact on the broadcast of system messages and the interaction between nodes, and the security of the system will be threatened. The reduction of the number of Byzantine nodes (untrustworthy nodes) in the consensus process has a significant impact on improving the success rate and efficiency of the system consensus and enhancing the system security. In order to more clearly express the advantages of the node control mechanism under the credibility model in this paper, the comparison with the consensus algorithms such as PBFT, DBFT and EPBFT in the traditional sense, which are set in the paper, is shown in Table 6 below.

Table 6. Comparison of Consensus Solutions

Consensus algorithm	Node Trustworthiness Assessment	Master node fairness selection	Reputation rewards and penalties for nodes	Communication Complexity	Degree of expansiveness
PBFT	No	No	No	High	Poor
DBFT	No	No	No	High	Good
EPBFT	No	Yes	Yes	Low	Good
TPBFT	Yes	Yes	Yes	Low	Excellent

5.2 Analysis of the problem

In the optimization scheme based on the reputation model in this paper, the selection of indicators for measuring the reputation of nodes, the selection of existing indicators may not be the best, and there may be more excellent evaluation indicators as the research proceeds. At the same time, in the calculation of historical behavior factor and historical reputation evaluation, it is necessary to give certain weights to the corresponding indicators to balance the degree of influence of different factors, but the specific weights given to the indicators for measuring node

reputation may not reach the optimal solution, and further in-depth exploration is needed in this regard. In addition, the underlying consensus optimization scheme proposed in this paper is still based on the PFBT algorithm, which cannot be improved for the problems of the algorithm itself, and the transaction speed may be affected in the application of multiple programs, and the occupied network communication will increase with the operation of the system.

The node control based on the reputation model takes into account the historical behavior of nodes and the transaction environment, and has high requirements for the data storage and governance system on the chain while taking a comprehensive consideration. As the data information in the blockchain exists in the form of blocks on the chain, the client needs to copy different blocks to complete the transmission of data information, making the amount of data written in the blocks more and more massive as the working time increases. In addition, due to the consensus process, the amount of historical data of nodes is increasing, but these historical data are not needed with time, but still occupy a large amount of storage space, these have higher requirements for computer network storage capacity, and each node is facing greater pressure.

Reference

[1] Wang Qun,Li Fujuan,Ni Xueli,Xia Lingling,Wang Zhenli,Liang Guangjun. Research on blockchain consensus algorithm and application [J]. Computer Science and Exploration,2022,16(06):1214-1242.

[2] Castro M, Liskov B. Practical byzantine fault tolerance and proactive recovery[J]. ACM Transactions on Computer Systems, 2002, 20(4):398-461.

[3] Lei Kai, Zhang Qichao, Xu Limei, et al. Reputation-based byzantine fault-tolerance for consortium blockchain[C]// 2018 IEEE 24th International Conference on Parallel and Distributed Systems (ICPADS). Singapore: IEEE Press, 2018: 604-611.

[4] Wang Yuhao, Cai Shaobin, Lin Changlong, et al. Study of blockchains's consensus mechanism based on credit[J]. IEEE Access, 2019, 7(1): 10224-10231.

[5] Chu, Lee. Research on multi-party dynamic consensus algorithms for permission chains [D]. Chengdu: University of Electronic Science and Technology, 2021.

[6] Luo Fang. Research on blockchain consensus algorithm based on dynamic reputation [D]. Dalian: Dalian University of Technology, 2021.

[7] Lu Kun, Wang Junlong, Li Mingchu. An eigentrust dynamic evolutionary model in P2P file-sharing systems[J]. Peer-to-Peer Networking and Applications, 2016, 9(3): 599-612.

[8] Xi Jing,Wang Yuan,Lu Jiande. Trust and recommendation based P2P reputation model[J]. Computer Engineering,2009,35(04):143-145.

[9] Li Xiong, Liu Ling. Peertrust: supporting reputation-based trust for peer-to-peer electronic communities[J]. IEEE Transactions on Knowledge and Data Engineering, 2004, 16(7): 843-857.

[10] Wang K, Wu M. A trustworthy global reputation model in P2P networks[J]. Journal of Applied Sciences,2010,28(03):237-245.