IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received November 7, 2018, accepted December 13, 2018, date of publication January 8, 2019, date of current version January 29, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2891065

Study of Blockchains's Consensus Mechanism Based on Credit

YUHAO WANG, SHAOBIN CAI, CHANGLONG LIN, ZUXI CHEN,
TIAN WANG, ZHENGUO GAO, AND CHANGLI ZHOU
College of Computer Science and Technology, Huaqiao University, Xiamen 361021, China

Corresponding authors: Yuhao Wang (947887638@qq.com) and Shaobin Cai (caishaobin@hqu.edu.cn)

This research was supported by the Natural Science Foundation of China under Grant 61571150 and Grant 61671169. The authors are grateful to the anonymous reviewers for their valuable comments.

ABSTRACT Practical Byzantine fault tolerance (PBFT) is one of the most popular consensus protocols of the blockchain. However, in the PBFT, the enthusiasm of reliable nodes cannot be stimulated effectively, and a large amount of communication resources are used for data consistency. Therefore, a new consensus protocol—credit-delegated Byzantine fault tolerance (CDBFT)—is proposed in this paper. The CDBFT works as the following: 1) a voting rewards and punishments scheme and its corresponding credit evaluation scheme are proposed not only to stimulate enthusiasm of reliable nodes but also to reduce the participation of abnormal nodes in the consensus process, and the virtuous circle of the system can be founded and 2) consistency and checkpoint protocols based on PBFT are proposed to improve the efficiency and flexibility of system. From the simulation results, a conclusion can be drawn, the participation probability of abnormal nodes in the consensus process can be reduced to 5%, and the efficiency and stability of the system are improved greatly in the long-time running.

INDEX TERMS Consortium blockchain, consensus mechanism, credit, PBFT.

I. INTRODUCTION

Blockchain technology [1] is a reliable, decentralized, de-trusted, tamper-resistant, and collectively maintained database. The long-standing Byzantine failures [2], [3] of digital cash were effectively solved by the data encryption, data link hooking, multi-copy storage, and distributed consensus of blockchain technology [4]. In 2008, the Blockchain technology was firstly proposed, and a decentralized trusted trading platform is founded [5], [6], on which no trusted third party is needed for the transactions. After the benefits of blockchain technology being reported by the "Economist", "Harvard Business Review", and other magazines in 2015, the potential value of blockchain was gradually realized. In 2016, the blockchain technology jumped beyond the Peak of Inflated Expectations according to The Hype Cycle of Gartner; In 2017, the blockchain technology was on the list of Gartner's Top 10 Strategic Technologies of 2018 [7]. So, more and more attentions of researchers in various fields are drawn by blockchain technology.

The public and the Consortium are two main forms of blockchains. The public blockchain is completely decentralized without any supervision nor management. Anyone can take party in public chain, and access all data freely. So, it is difficult for public chain to be applied to digital assets [8]. The Bitcoin is the most famous example of public blockchain.

For better both privacy protection of user and supervision of data, the consortium chain was proposed. In the consortium blockchain, only specifically allowed nodes can access the network, and the Sybil attack [9] is effectively eliminated. Hence, the consortium blockchain can support enterprise-level applications well, and is wildly adopted in public and governmental services.

The consensus algorithms are the core of blockchain technology, and the PoW (Proof of Work), PoS (Proof of Stake), DPoS (Delegated PoS), BFT (Byzantine Fault Tolerance), PBFT (Practical BFT) and some other consensus mechanisms have been proposed for blockchain. The computation cost, security and consensus efficiency of the above are different [10].

PoW was used by many early digital cash systems. In PoW, all nodes compete their computing power for the block accounting rights, and guarantee the decentralization and trust-worth of the system [11], [12]. That is, any participant competes like a miner by solving SHA256 mathematical problems, which are complex but easy to verify [13]. Although the data consensus can be guaranteed by PoW to some extent, about ten minutes is needed to produce a block, and too much computing and power resources are wasted for the competition. So, PoS [14] has been proposed. In PoS, the difficulty of mining is determined by the stock right

TABLE 1. Performance comparison of consensus algorithms.

	PoW	PoS	DPoS	PBFT
Applicable Form	public	public	public	consortium
Degree of decentralization	complete	complete	complete	incomplete
Accounting nodes	Whole network	Whole network	Elect	Dynamic decision
Response time	10 minutes	1minutes	3 seconds	second
Throughput capacity	7TPS (Bitcoin)		above 300TPS	above 1000TPS
Fault tolerance rate	49%	49%	10/21	33%(m/3m+1)

of miner. Hence, the used resources are reduced, and the speed of block generation is improved. However, the mining cost of PoS is still high, and it is not suitable for commercial applications.

In order to reduce the cost of computing, a representative election scheme, which based on the stakes of nodes, is used by DPoS [15] to abolish the mining, and the efficiency of block generation is enhanced. However, DPoS has a lower enthusiasm of participant, more uneven coin distribution, weaker defense of malicious nodes, and weaker security of the system [15].

Although the reliability of the blockchain can be guaranteed by the above algorithms to a certain extent, the throughput, delay and block generation etc cannot be solved well simultaneously. In these schemes, the data security depends on computing power. So, it is difficult for consortium blockchain to be applied widely. BFT is a classical consistency algorithm for distributed systems. PBFT (Practical Byzantine Fault Tolerance) are widely used by consortium blockchain now.

In this paper, an improved consensus algorithm based on PBFT, called CDBFT (Credit-Delegated Byzantine Fault Tolerance), is proposed for consortium blockchain. Inspired by DPoS, a vote system, based on credit rewards and punishments, is defined for the representative election scheme of CDBFT, and the cycle of the system can be well maintained for a long time. By this scheme, the enthusiasm of participants, the elimination of malicious node, the security and efficiency of system can be improved greatly.

The remainder of the paper is organized as follows. The PBFT is introduced in section 2; CDBFT is introduced in Section 3; the experiment analyses is done in section 4; and a conclusion is drawn in Section 5.

II. THE DEFINITION OF PBFT

PBFT was proposed by Miguel Castro of MIT in 1999 [16]. PBFT is a general solution to ensure the consistency of a distributed system with the Byzantine failures nodes. PBFT is mainly composed of a consistency protocol, a view-change protocol, and a checkpoint protocol. Normally, there can be up to f Byzantine failure nodes in a system with $3f + 1$ replica nodes, which runs a copy of a finite state machine that supports reading, writing, modifying permissions, etc. In the PBFT consensus process, a block is generated by the unique primary node, and no bifurcation is created. PBFT works without tokens. It is high efficiency and low consumption.

A. CONSISTENCY PROTOCOL

The consistency protocol is the core of PBFT. In the blockchain system, the transactions are packaged into blocks periodically. The consensus and integrity of the blocks, generated and recorded by the nodes, are guaranteed by the consistency protocol in the whole network. There are two types of nodes, primary and replica, and three stages, "Pre-Prepare", "Prepare", and "Commit", in the consistency protocol.

a) "Pre-Prepare" stage: the primary node sends out a "Pre-Prepare" message; a replica node enters the "Prepare" stage when it accepts its received "Pre-Prepare" message.

b) "Prepare" stage: a replica node sends out a "Prepare" message; a replicated node changes its state to "Prepared", and enters the "Commit" stage after its receiving a "Prepare" message from other replica nodes.

c) "Commit" stage: a "Prepared" node sends a "Commit" message to announce that a "Prepared" authentication certificate is available. A replica node enters the "Commit" state after receiving 2f+1 "Commit" acknowledgments (including its own), and writes the block information into the blockchain.

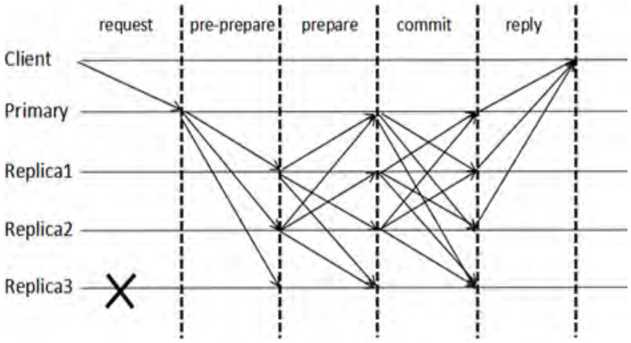


FIGURE 1. Interaction process of consistency protocol.

As shown in Fig.1, "Primary" is the primary node. "Replica 1", "Replica 2" and "Replica 3" are three replica nodes. Replica 3 has Byzantine failures, and cannot broadcast messages. However, the protocol can still work correctly by the consistency protocol.

B. VIEW-CHANGE PROTOCOL

The primary node is replaced by the View-Change protocol to guarantee the stability of the system when it fails. The relationship among nodes in the consistency protocol is defined by view "v". The View-Change protocol works as following:

a) "View-Change" stage: a replica node enters view v+1 and broadcasts the "View-Change" certification to all nodes when it determines that the primary node is inactive.

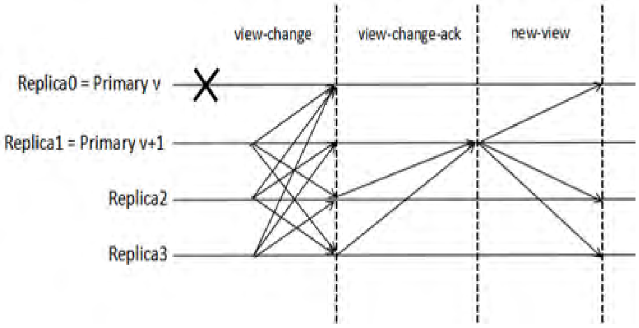


FIGURE 2. Interaction process of the view-change protocol.

b) "View-Change-Ack" stage: a node sends the "View-Change-Ack" certificate to the primary node of view v+1 when it receives a $2f+1$ View-Change certificate (including from itself). The new primary node enters the New-View stage after its receiving the "View-Change" and the "View-Change-Ack messages".

c) "New-View" stage: The new primary node selects a checkpoint as the starting state of the "New-View" request, and then executes the consistency protocol according to the local block-chaining data.

In "View-Change" processes, in order to guarantee the data consistency, the nodes communicate with each other, and the confirmation of transactions are stopped. In View-Change protocols, the block generation of the primary node is monitored by a timeout monitoring scheme. That is, the "View-Change" will be executed when the primary node fails to complete the block generation in a given time threshold T.

C. CHECKPOINT PROTOCOL

In the consensus process, a lot of logs are generated by nodes. More and more of memories are need by logs when the system runs. However, some of the log messages are already recorded by the certification message of consensus. So, in order not only to save memory but also to prevent the system fault, caused by the accumulation of node inconsistency, the checkpoint scheme is introduced. The Checkpoint protocol is a periodic protocol. It clears the verified certifications after confirming consistency of the node.

III. AN EFFICIENT CONSENSUS MECHANISM BASED ON CREDIT

Although the performance of blockchain's consensus were greatly improved by PBFT, the overhead of message transmission is still extensive, which scales $O(N^2)$ in the network with N nodes [17]. So, the performance of the PBFT protocol decreases dramatically when number of nodes over a certain amount because of the complexity of communications. The Blockchain based on PBFT does not work well in the consortium blockchain system with lots of nodes [18].

Now, many schemes are proposed to improve PBFT. The "layered" schemes are the mostly used. In these "layered" schemes, some of the reliability evaluations are done by PoW, PoS, or DPoS firstly, and the rest are done by PBFT. The complex problem is solved by two parts, and only a part of nodes take part in the consensus process like the representative democracy, where some representatives are selected to take part in the final consensus verification by the elections or other means. The performance of consensus algorithms is improved by a PoW + PBFT hybrid consensus mechanism, based on the random fragmentation [19]. however, It still cannot guarantee that the malicious node is less than 1/3 even when it is assumed to be used in fair environment by default. So, there are still some shortcomings in this scheme.

To reduce not only the participation probability of abnormal nodes in consensus but also the communication resources wasted by PBFT, an improved consensus mechanism, CDBFT (Credit-Delegated Byzantine Fault Tolerance), is proposed based on PBFT scheme in this paper. The main improvements of the CDBFT mechanism include:

1) A credit evaluation system is defined to describe the states of nodes, referring to the system model of Ethereum and Hyperledger Fabric.
2) A vote mechanism, based on the above credit and node states, is proposed to reward the right nodes and punish the wrong nodes. So, the initiative of the credible node can be enhanced, and the participating of abnormal nodes can be reduced.
3) A privilege classification mechanism of node is founded in the consistency protocol, and a privilege class is assigning to a primary node according to the credit states of the nodes.
4) In the checkpoint protocol, the certificates clearance, based on block times tamp, is proposed instead of that based periodic negotiation, to reduce the usage of communication resources.

A. CDBFT CONSENSUS PROCESS

The process of the CDBFT is shown in Fig.3. Firstly, the proxy nodes are selected out to participate in the consensus according to the results of the voting. Secondly, the primary node is selected out to generate blocks according to the credit-based consistency protocol. The consistency protocol is monitored to determine whether the primary node is timed out or not. The primary node is changed via the View-Change protocol when the timeout occurs, otherwise a new block is written into the blockchain. Finally, the checkpoint protocol is executed according to the times tamp of the new block to clear the remaining validated certificate information in memory.

B. BLOCKCHAIN MODEL BASED ON CREDIT

To manage the status of nodes, participating in consensus mechanisms, a credit mechanism is defined to describe the states of node, referring to the system model of Ethereum and Hyperledger Fabric. The improved blockchain model is shown in Fig. 4. The relevant definitions are as follows:

Definition 1 (Organization): $Org_i \in \{Org_1, \ldots, Org_N\}$ is defined to represents different participants in the blockchain network, such as e-commerce trading platforms,

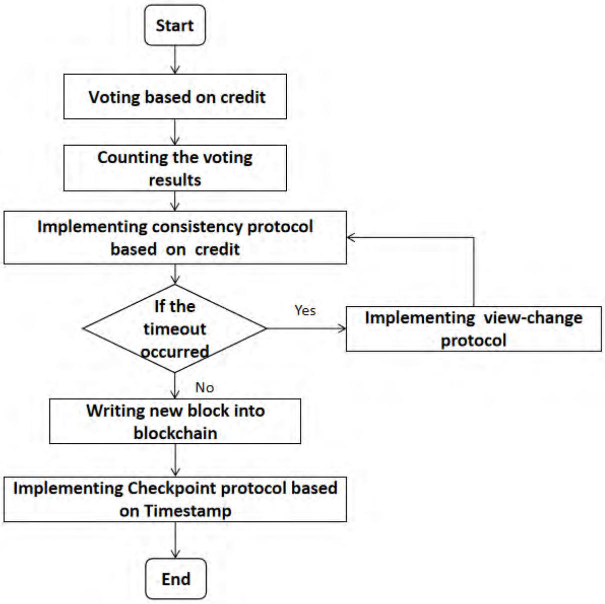

Start
Voting based on credit
Counting the voting results
Implementing consistency protocol based on credit
If the timeout occurred
Yes
Implementing view-change protocol
No
Writing new block into blockchain
Implementing Checkpoint protocol based on Timestamp
End

FIGURE 3. The flow chart for the process of the CDBFT.

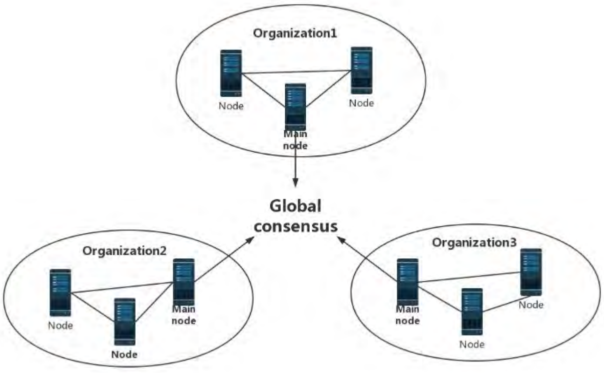


FIGURE 4. Blockchain model.

logistics platforms, supply chain platforms, and governmental regulatory authorities. In above definition, N represents the number of organizations in the block chain network. The organization is identified by its public key address, and can be identified each other. An organization Org_i has n_i blockchain nodes $Node_{ij}$, $1 \leq j \leq n_i$.

Definition 2 (Node): The $Node_{ij}$ represents the j^{TH} node in the organization $Org_i.\{Node_{ij}, 1 \leq i \leq N, 1 \leq j \leq n_i\}$. The public keys are used by nodes to identify each other, and P2P asynchronous communications are used. A node in the organization Org_i have a private key of Org_i. When a block is signed by a node, the private keys of that node and $\mathrm{Org_iOrg_i}$ Org are used for double signatures. The nodes, which maintain the normal operation of the blockchain network, are labeled "honest" nodes. The nodes, which maliciously tamper and attack the network to destroy the trusted consensus mechanism, are labeled "malicious" nodes.

Definition 3 (Credit): The credit C_{ij} is the credit of the j^{TH} node of organization $Org_i.\{C_{ij}, 1 \leq i \leq N, 1 \leq j \leq n_i\}$. $C_{ij} \in [C_{\min}, C_{\max}]$. C_{max} and $C_{\min}$ are the upper and lower limits of the credit respectively. C_{good}, C_{bad} and C_{init} satisfy $C_{\min} < C_{bad} < C_{init} < C_{good} < C_{\max}$. C_{good} is the credible credit threshold. C_{bad} is the untrusted credit threshold. C_{init} is the initial credit of a node. The state of node and permissions of the node in the blockchain is directly affected by the credit. The credit changes dynamically according to the behavior of nodes. The credit of a new node is initialized with the value C_{init}. The credit is combined with the actual businesses in different fields, and can be converted to represent digital physical products, electronic information according to the needs of the specific business.

Definition 4 (Credit Rewards and Punishments): credit rewards and punishments is assigned according to the impact of the behavior of the node on the system.

The reward formula is:

$$C_{ij} = C_{ij} + X \tag{1}$$

The punishment formula is:

$$C_{ij} = C_{ij} - X \tag{2}$$

In the above formulas, C_{ij} is the credit of the j^{TH} node in the organization Org_i. X is the change of the rewards (punishments) credit, and can be adjusted according to the specific business.

Definition 5 (Credit Recovery): Credit recovery is used to define how node credit gradually reinstate to its initial value over a time. In some specific businesses, credit recovery is defined as the consumption or growth to a certain value over a time. The credit recovery follows a certain rule at the beginning of each vote, which is defined as following:

$$C_{ij} = C_{ij} - \lfloor t/T \rfloor \times X(C_{ij} > C_{init}) \tag{3}$$
$$C_{ij} = C_{ij} + \lfloor t/T \rfloor \times X(C_{ij} < C_{init}) \tag{4}$$

where C_{ij} is the credit of the j^{TH} node of the organization Org_i; C_{init} is the initial credit of the node; t is the period from the last vote to the beginning of this vote; T is a constant, presenting the recovery cycle period, and is adjusted according to the specific business. X is the credit recovery ratio and is customized according to the specific business.

Definition 6 (Node Credit States): $\mathrm{State_{ij}}$ represents the credit state, which are determined by the credit, of the j^{TH} node in the organization Org_i. there are four kinds of credit states.

$$\sigma(\mathrm{Node_{ij}}) = \{\mathrm{Credible, Normal, Excepted, Invalid}\}.$$

The "Credible" state indicates that the node $\mathrm{Node_{ij}}$ does not produce any invalid blocks during a period T, and its credit C_{ij} exceeds the threshold C_{good}; The "Normal" state presents that the node $Node_{ij}$ work normally; The "Excepted" state indicates that the node $Node_{ij}$ has produced invalid blocks during the period T, but its credit score C_{ij} is not lower than the threshold C_{bad}; The "Invalid" state indicates that the node $Node_{ij}$ has produced invalid blocks during the period T, and its credit score $\mathrm{C_{ij}}$ is lower than the

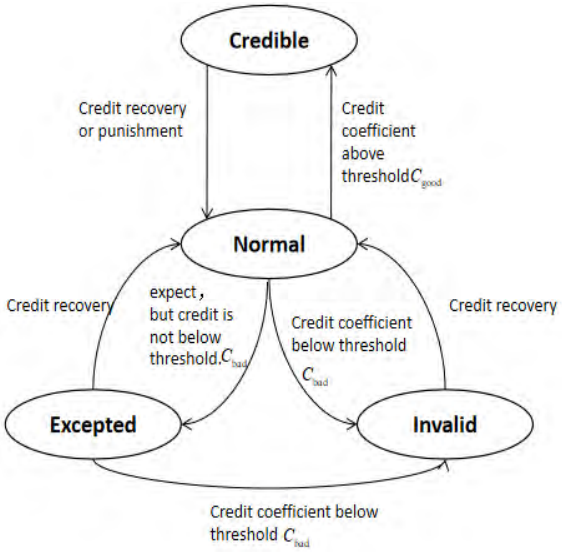

Credible
Credit recovery or punishment
Credit coefficient above threshold C_{good}
Normal
Credit recovery
expect, but credit is not below threshold C_{bad}
Credit coefficient below threshold C_{bad}
Credit recovery
Excepted
Invalid
Credit coefficient below threshold C_{bad}

FIGURE 5. **Transition diagram of node credit states.**

credit threshold C_{bad}. The transition of node credit states is described in Fig.5.

Definition 7 (Main Node of Organization): The main node of organization is the node with the highest credit score in a organization, and runs for the proxy nodes of global consensus as delegate of its organization. After a round of consensus, a new main node is selected out according to the new credit values of nodes.

C. VOTING MECHANISM BASED ON CREDIT

In PBFT, all nodes usually run for primary node. So, the "Exception" nodes are selected as primary node frequently, "View-Change" operations happen frequently. The performance of PBFT drops rapidly with the number increase of nodes. In order to eliminate "Exception" nodes and prevent them from being primary nodes, a credit-based vote mechanism, based on the credit state of nodes, is proposed. The vote mechanism is defined as follows:

Definition 8 (Election): The "election" is the process via which all eligible nodes vote for the main node of their organization, and elect them to participate in the final global consensus. The votes include "support", "oppose", and "abstain" choices. In each election, nodes can support(oppose) a node, or abstain from vote. A node has one chance to oppose a node during a period of time T, which is consistent with the constant T of credit recovery (Definition 5).

Definition 9 (Eligible Nodes): Eligible nodes are those nodes whose credit states are not Invalid.

Definition 10 (The Vote Result): The vote result is the primary node for which all eligible nodes of a organization vote for. According to the credit states and values of the nodes, the statistical formula is as follows:

$$Result_{ij} = State_{ij} \times C_{ij} + \sum\nolimits_{k=1}^{N} \sum\nolimits_{l=1}^{n_k} State_{kl} \times Vote_{kl} \tag{5}$$

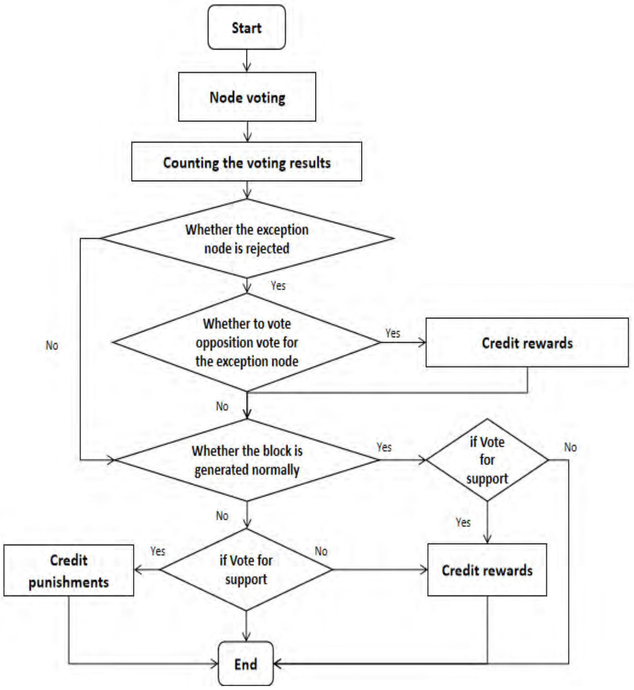

Start
Node voting
Counting the voting results
Whether the exception node is rejected
Yes
No
Whether to vote opposition vote for the exception node
Yes
Credit rewards
No
Whether the block is generated normally
Yes
if Vote for support
No
Yes
No
Credit punishments
Yes
if Vote for support
No
Credit rewards
End

FIGURE 6. **Flow chart of voting and credit rewards and punishments.**

In above formula, the $state_{ij}$ is the credit state of $Node_{ij}$; C_{ij} is the credit ratio of the $Node_{ij}$; N is the number of organizations, participating in the election; n_k is the number of nodes, participating in the election, of the organization; $Vote_{kl}$ is the vote of the $Node_{kl}$, The values corresponding to "support", "abstain" and "oppose" are 1, 0, and, -1, respectively.

Definition 11 (Vote Rewards and Punishments): According to the vote and the involvement in the consensus of proxy nodes, the reward and punishment of a vote is defined as following:

a) A credit reward is assigned to the node, who opposite the "Excepted" node, which fails in the proxy node election.
b) A credit reward is assigned to the nodes, who support the proxy node, which generates the block successfully.
c) A proxy node becomes an "Excepted" node when it acts maliciously or fails. And then, a credit punishment is assigned to the node, who supports the proxy node. Otherwise, a credit reward is assigned to the nodes, who opposites the proxy node.

The work flow of vote and its corresponding credit rewards and punishments is described in figure 5. Firstly, a node votes; secondly, the vote result is counted out; at last, the rewards and punishments are assigned to the nodes, who take part in the vote, according to Definition 11.

D. CONSISTENCY PROTOCOL BASED ON CREDIT

To avoid a node with low credit serving as a primary node, the privilege of a node is classified according to its credit state in the consistency protocol of CDBFT (shown in Table 2).

TABLE 2. **Node classification.**

credit states	Permissions		
	Priority as primary node	Serving as primary node	Serving as replica node
Credible	√	√	√
Normal	×	√	√
Excepted	×	×	√
Invalid	×	×	×

The "Credible" nodes are prior in election of the primary node. "Normal" nodes can be elected as primary nodes after all "Credible" nodes have been elected, or after no "Credible" nodes is eligible for vote. "Expected" nodes cannot serve as primary nodes, but can work as replica nodes. The "Invalid" nodes cannot participate in consensus at all. The privilege classification effectively prevents a "Expected" node from being a primary node, and reduces not only the frequency of "View-Change" operations but also the communication consumption among nodes. The system efficiency is improved.

In the consistency protocol, a credit reward is assigned to a node when it generates a block successfully; otherwise, a credit punishment is assigned to a node when it fails or hinders the generation of block by its malicious attacks. a node changes its state to "Excepted" when it is punished. The definition of rewards and punishments is given by **Definition 4**.

E. CHECKPOINT PROTOCOL BASED ON TIMESTAMP

In PBFT, the checkpoint protocol is periodically executed to prevent system faults caused by inconsistencies among nodes. To protect the security of the system, it must be ensured that the contents must be executed by at least $f + 1$ other nodes before they being deleted. Hence, the synchronous communications among nodes are needed, and lots of communication resources are used in the checkpoint protocol of PBFT.

To avoid the waste of communication resources, based on PBFT, the checkpoint protocol of CDBFT is proposed, which is time-stamp-based instead of periodicity-based. The blockchain is verified in chronological order. According to the characters of blockchain, the contents and the order, written on blockchain, are integrated and cannot be distorted in whole network. The previous verification messages have already been executed and recorded on the blockchain when a block is written into the blockchain. And then, the previous messages in the local memory is redundant, and can be safely deleted. Therefore, in the proposed checkpoint protocol based on timestamp, the communications among nodes are not necessary. So, the memory accumulation is omitted, the communication overhead is reduced, and the system operation efficiency is improved.

IV. PERFORMANCE ANALYSIS AND EXPERIMENT

To analyze the performance of CDBFT, a simulation platform, which is composed of fifteen computers, running Linux operating system, with 8GB memory, I7-6700 CPU and GTX960 graphics card, is founded. The version of Linux system is Ubuntu 16.04. A computer is an Org., marked as Org_1 to Org_{15}. All computers are in the same LAN. The system environment is configured according to the requirements of Hyperledger fabric V1.1, and the network of blockchain infrastructure is founded. There are five to twenty numbered nodes in a Org. The transactions are continuously initiated by the $Node_{11}$ in the simulation to test TPS (Transactions per second).

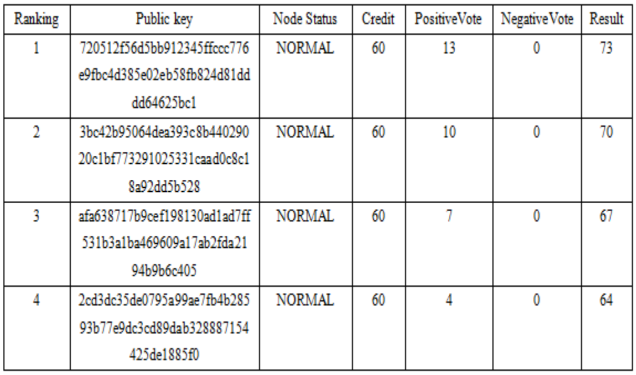
In the following experiments, the performance of PBFT and CDPBFT is compared by their second-round participation of the exception node, the relationship between the number of nodes and the efficiency, and the relationship between the running time and the efficiency.

A. EXCEPTION NODE PARTICIPATION IN CONSENSUS

In PBFT, all nodes take part in consensus, and the probability, that an exception node becomes a primary node, is very high. In CDBFT, a vote mechanism is used to reduce this probability drastically, and four proxy nodes are selected out per round to participate in the final consensus

The vote result of CDBFT is calculated by Formula (5), in which, C_{ij} is the credit score of the elected node, and C_{init} is set 60. The $state_{ij}$ is the credit state of corresponding node. The states for "Credible", "Normal", "Excepted", or "Invalid" nodes are set to 1.1, 1.0,0.9, or 0.0 respectively. The result of the first-round vote is shown in Table 2.

TABLE 3. **The results of the first four nodes in the first round.**



Ranking	Public key	Node Status	Credit	PositiveVote	NegativeVote	Result
1	720512f56d5bb912345ffccc776 e9fbc4d385e02eb58fb824d81dd dd64625bc1	NORMAL	60	13	0	73
2	3bc42b95064dea393c8b440290 20c1bf773291025331caad0c8c1 8a92dd5b528	NORMAL	60	10	0	70
3	afa638717b9cef198130ad1ad7ff 531b3a1ba469609a17ab2fda21 94b9b6c405	NORMAL	60	7	0	67
4	2cd3dc35de0795a99ae7fb4b285 93b77e9dc3cd89dab328887154 425de1885f0	NORMAL	60	4	0	64

In this simulation, the election classes of excepted nodes after the second-round consensus are analyzed by 100 repeated experiments. The first node in table 3 is supposed to be a "Excepted" node after the first round of consensus. From the simulation results (Shown in Fig.7), only one "Excepted" node was ranked in the top four once in 100 elections, and the probability is less than 5%, which far lower than that of PBFT. So, the participation probability of exception node in consensus is reduced effectively by CDBFT, and the security of system is improved.

B. THE RELATIONSHIP BETWEEN THE NUMBER OF NODES AND EFFICIENCY

The system perform of PBFT is affected greatly by the number of nodes, and decreased greatly when the number of node

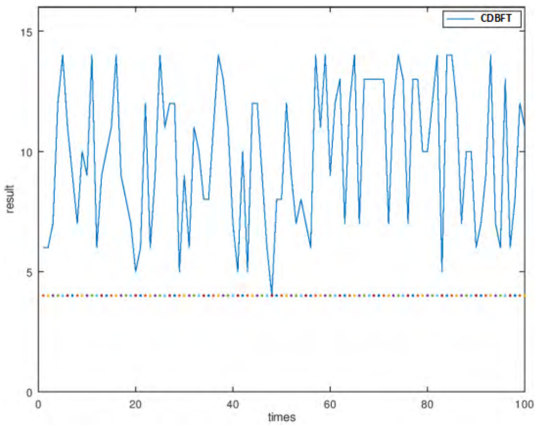


FIGURE 7. Rank of exception nodes of CDBFT in the second round.

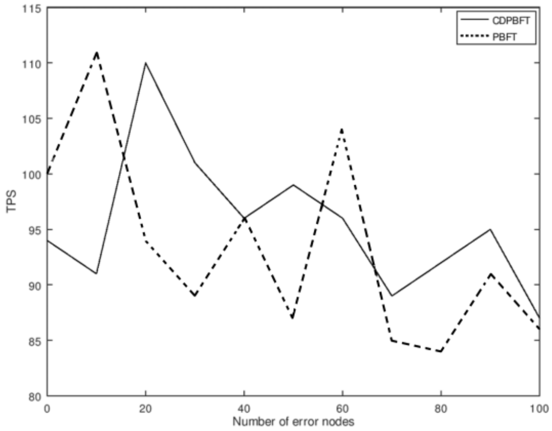


FIGURE 8. The relation between TPS and number of nodes in PBFT and CDBFT.

exceeds a threshold. In CDBFT, only a certain proportion of nodes are selected out to participate in consensus by vote, and the consensus can run stably when there lots of nodes. In simulation, the TPS of both PBFT and CDBFT were tested with 0, 20, 40, 60, 80, 100, 120, 140, 160, 180, 200 nodes respectively. As shown in Fig. 8, the efficiency of PBFT decreases significantly, and the performance of CDBFT remains stable when there are more than 100 nodes.

C. THE RELATIONSHIP BETWEEN RUNNING TIME AND EFFICIENCY

Within the range of fault tolerance, the efficiency of PBFT is stable throughout the simulations, and is increased with the system running because of its credit and vote mechanism. A conclusion can be drawn from the simulation results that the participation probability of "Exception" nodes in the consensus is greatly reduced, and the error rate of the primary node decreases. In the long run, the efficiency of block generation of CDBFT is higher than that of PBFT. The TPS changes of both PBFT and CDBFT is described in Fig.9. It can be seen that the "Exception" nodes are eliminated, the error rate of primary node is reduced by CPBFT, and the throughput of system is improved significantly.

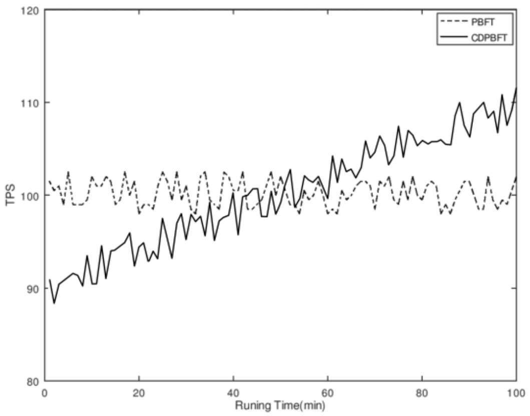


FIGURE 9. Comparison of TPS between PBFT and CDPBFT over time.

V. CONCLUSION

In recent years, the blockchain technology has been applied in lots of fields. As the core of blockchain, the consensus mechanism has been studied widely, and different consensus mechanisms are required to support the blockchain systems in different application backgrounds [20]. In consortium blockchain, the computing overhead is reduced, and the centralization trend is avoided by the consensus of PBFT effectively. However, it performs poorly in the system with a large number of nodes due to the frequent view change and huge network communication.

To solve these problems, a new efficient consensus mechanism, CDBFT, based on credit evaluation, has been proposed. The simulation results show that the communication overhead and the participating probability of exception nodes are reduced greatly, and the efficiency of system is improved by credit, vote, reward and punishment mechanisms of CDPBF in the consensus process.

REFERENCES

[1] M. Swan, *Blockchain: Blueprint for a New Economy*. Newton, MA, USA: O'Reilly Media, 2015.

[2] A. M. Antonopoulos, *Mastering Bitcoin: Unlocking Digital Cryptocurrencies*. Newton, MA, USA: O'Reilly Media, 2014.

[3] J. Fan, L. T. Yi, and J. W. Shu, "Research on the technologies of Byzantine system," (in Chinese), *J. Softw.*, vol. 24, no. 6, pp. 1346–1360, 2013. [Online]. Available: http://www.jos.org.cn/1000-9825/4395.htm

[4] W. Qian, Q. Shao, Y. Zhu, C. Jin, and A. Zhou, "Research problems and methods in blockchain and trusted data management," (in Chinese), *J. Softw.*, vol. 29, no. 1, pp. 150–159, 2018. [Online]. Available: http://www.jos.org.cn/1000-9825/5434.htm

[5] S. Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*. 2008.

[6] U. Mukhopadhyay, A. Skjellum, O. Hambolu, J. Oakley, L. Yu, and R. Brooks, "A brief survey of cryptocurrency systems," in *Proc. Privacy, Secur. Trust*, Dec. 2016, pp. 745–752.

[7] A. D. Liu, X. H. Du, N. Wang, and S. Z. Li, "Research progress of blockchain technology and its application in information security," (in Chinese), *J. Softw.*, vol. 29, no. 7, pp. 2092–2115, 2018. [Online]. Available: http://www.jos.org.cn/1000-9825/5589.htm

[8] X.-P. Min *et al.*, "Permissioned blockchain dynamic consensus mechanism based multi-centers," *J. Comput. Sci.*, vol. 41, no. 5, pp. 1005–1020, 2018.

[9] J. R. Douceur, "The Sybil attack," in *Proc. 1st Int. Workshop Peer-Peer Syst. (IPTPS)*, Cambridge, MA, USA, Mar. 2002, pp. 251–260.

[10] Z. Yan, G. GuoHua, D. Di, J. Feifei, and C. Aiping, "Security architecture and key technologies of blockchain," *J. Inf. Secur. Res.*, vol. 2, no. 12, pp. 1090–1097, 2016.

[11] M. Pilkington, *Blockchain Technology: Principles and Applications*. Rochester, NY, USA: Social Science Electronic Publishing, 2016.

[12] L. Lee, *New Kids on the Blockchain: How Bitcoin's Technology Could Reinvent the Stock Market*. Rochester, NY, USA: Social Science Electronic Publishing, 2016.

[13] S. Underwood, "Blockchain beyond bitcoin," *Commun. ACM*, vol. 59, no. 11, pp. 15–17, 2016.

[14] S. King and S. Nadal, "PPCoin: Peer-to-peer crypto-currency with proof-of-stake," Tech. Rep., 2012, p. 19.

[15] D. Larimer, "Delegated proof-of-stake (DPoS)," Bitshare whitepaper, 2014.

[16] M. Castro and B. Liskov, "Practical Byzantine fault tolerance," in *Proc. 3rd Symp. Oper. Syst. Design Implement.*, New Orleans, LA, USA, Feb. 1999, pp. 173–186.

[17] Q.-F. Shao, C.-Q. Jin, Z. Zhang, W.-N. Qian, and A.-Y. Zhou, "BlockChain: Architecture and research progress," *J. Comput. Sci.*, no. 5, pp. 969–988, 2018.

[18] T. T. A. Dinh, J. Wang, G. Chen, R. Liu, B. C. Ooi, and K.-L. Tan, "Blockbench: A framework for analyzing private blockchains," in *Proc. ACM Int. Conf. Manage. Date (SIGMOD)*, Chicago, IL, USA, 2017, pp. 1085–1100.

[19] L. Luu, V. Narayanan, C. Zheng, K. Baweja, S. Gilbert, and P. Saxena, "A secure sharding protocol for open blockchains," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, 2016, pp. 17–30.

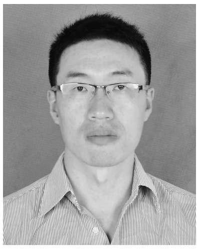
[20] Z. Yong and L. Xiao-Hui, "The research and implementation of an improved blockchain's consensus mechanism," *Electron. Des. Eng.*, vol. 26, no. 1, pp. 38–47, 2018.

YUHAO WANG was born in 1993. He received the B.S. degree in computer science and technology from Huaqiao University, in 2015, China, where he is currently pursuing the M.S. degree in computer science and technology.

His primary research interest is the blockchain technology.

SHAOBIN CAI was born in 1973. He received the Ph.D. degree in computer system architecture from the Harbin Institute of Technology, in 2005. He is a Minjiang Scholar of Fujian Province. He is currently a Professor of computer science and technology with Huaqiao University. His primary research interests include ad hoc networks, wireless sensor networks, underwater acoustic sensor networks, and the blockchain technology. He is a member of the Wireless Sensor Network Committee of the Chinese Computer Society.

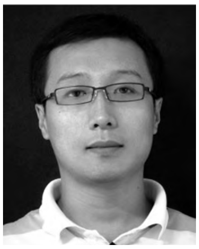
CHANGLONG LIN received the Ph.D. degree in pattern recognition and intelligent system from the University of Chinese Academy of Sciences, Beijing, China, in 2011. He is currently a Lector with the College of Computer Science and Technology, Huaqiao University. He has authored about 20 articles. His current research interest includes the control and navigation of unmanned underwater vehicles.



ZUXI CHEN was born in 1981. He received the Ph.D. degree in software theory from Tongji University, Shanghai, China, in 2015. He is currently a Lector with Huaqiao University. His current research interests include program analysis, software testing, and formal verification.

TIAN WANG received the Ph.D. degree in computer science from the City University of Hong Kong, China, in 2011. He is currently a Professor of computer science and technology with Huaqiao University. He has published more than 150 papers at well-known international conferences, of which more than 60 were indexed by SCI, and the total number of citations exceeded 1800. His current research interests include the Internet of things, cloud computing, fog computing, and other new network areas.

ZHENGUO GAO was born in 1976. He received the Ph.D. degree in computer system architecture from the Harbin Institute of Technology, in 2006. He is currently a Professor with Huaqiao University. He has published more than 100 articles in the IEEE Transactions and other international journals and conferences, and dozens of them are indexed by SCI. His current research interests include wireless network (underwater acoustic networks and vehicle networking) technology, communication technology, image processing, and artificial intelligence.



CHANGLI ZHOU was born in 1985. He received the Ph.D. degree from Harbin Engineering University, China, in 2015. He is currently a Lector with Huaqiao University. His primary research interests include privacy protection network and information security.