BW-PBFT: Practical Byzantine Fault Tolerance Consensus Algorithm Based on Credit Bidirectionally Waning

Zhen-Fei Wang
School of Computer and Artificial Intelligence
Shi-Qi Liu
School of Computer and Artificial Intelligence
Pu Wang
School of Computer and Artificial Intelligence
Li-Ying Zhang (zlyzzu2017@126.com)
School of Computer and Artificial Intelligence

Research Article

Keywords: Blockchain, Consensus, Analytic Hierarchy Process, PBFT, DBFT

Posted Date: May 10th, 2023

DOI: https://doi.org/10.21203/rs.3.rs-2900100/v1

Additional Declarations: No competing interests reported.

Version of Record: A version of this preprint was published at Peer-to-Peer Networking and Applications on September 25th, 2023. See the published version at https://doi.org/10.1007/s12083-023-01566-x.

BW-PBFT: Practical Byzantine Fault Tolerance Consensus Algorithm Based on Credit Bidirectionally Waning

Zhen-Fei Wang[1†], Shi-Qi Liu[1†], Pu Wang[1], Li-Ying Zhang[1*]

[1*]Zhengzhou University, School of Computer and Artificial Intelligence, Kexuedadao, Zhengzhou, 450001, Henan, China.

*Corresponding author(s). E-mail(s): zlyzzu2017@126.com;
Contributing authors: iezfwang@zzu.edu.cn; qq693186625@outlook.com;
pwang928@outlook.com;
†These authors contributed equally to this work.

Abstract

The consensus algorithm, as one of the cores of blockchain technology, plays a very critical role. As one of the mainstream consensus methods, PBFT has the advantages such as low energy consumption and large throughput. However, the traditional PBFT algorithm also has disadvantages, such as high network bandwidth occupation, for PBFT needs broadcasting information for all nodes in stage 3 and 4; limited expandability. With the increase of nodes, the bandwidth overhead of the blockchain network will increase significantly, which leads to a decrease in throughput, so that cause a crash of the blockchain network. We proposed an improved PBFT consensus based on a credit value bidirectionally waning, named BW-PBFT. The algorithm first elects some nodes to form a committee according to the ballot and the credit value, and then the committee nodes use the PBFT algorithm for consensus, and calculate the credit value of the nodes according to the performance in the consensus process. If nodes do not get punishment anymore, their credit value will approach 50 with the increase of the blockchain height. Theoretical analysis and experiments prove that the proposed algorithm can effectively improve the quality of the nodes involved in the consensus.

Keywords: Blockchain, Consensus, Analytic Hierarchy Process, PBFT, DBFT

1 Introduction

At the beginning of this article, this part will briefly introduce the aims of this article, the contributions of us, and the structure of this article.

1.1 Motivation

Blockchain is one of the core technologies of Bitcoin [1], a blockchain is a data chain that uses the hash value as a pointer [2]. It has tamper-proof, programmable, time-sequence data and other characteristics [3]. Beside of this, blockchain support many technical extension, such as smart contract [4], cross chain [5]. Due to its advantages, the blockchain has been using in a lot of area [6], like financial [7], healthcare [8], artificial intelligence(AI) [9], network security [10], internet of things(IoT) [11], and so on. The consensus algorithm is one of the hinges of blockchain. The consensus algorithm determines the blockchain's security, throughput, resource consumption, degree of decentralization, and so on [12]. At present, the mainstream consensus methods are mainly divided into Proof of X(PoX) algorithms and Byzantine Fault Tolerance(BFT) algorithms [13]. In PoX algorithms, nodes compete to become a committer peer by proving themselves; BFT algorithms mainly refer to Practical Byzantine Fault Tolerance algorithms (PBFT) and related improved algorithms based on PBFT.

The proof-of-work algorithm (PoW) used by Bitcoin [1]. In the PoW algorithm, the consensus nodes compete to solve a math problem for accounting rights and receive virtual currencies as a reward. The algorithm realized the decentralization of blockchain, which can accommodate 50% of malicious nodes, but the energy consumption of PoW is too high, and producing a block in ten minutes also leads to low throughput [14]. Proof of state(PoS) is an improvement of proof of workload. The nodes obtain the equity according to the age of the currency, and the node which has higher equity is more likely to obtain the accounting right [15]. PPCoin, published in 2012, used PoS as the consensus mechanism [16], Ethereum [17] has announced that it will turn to PoS in 2022 [18]. PoS algorithm partially solved the energy consumption problem caused by the PoW algorithm, but it will lead to the nodes with more currency possession frequently obtaining accounting rights, which will lead to more and more currency possession of these nodes.

The practical Byzantine Fault Tolerance(PBFT) consensus algorithm [19] is an improvement of the Byzantine Fault Tolerance(BFT) algorithm. PBFT reduced the problem complexity of BFT from exponential to polynomial level, which enabled it to be applied in reality. PBFT divides nodes into two types by their functions, namely, the primary node and the backup node, and all nodes can be used as customer nodes. The primary node is responsible for forwarding all requests launched by customer nodes to backup nodes. Also, the primary node needs to take the same responsibility as the backup nodes. After receiving the request from customer nodes and the request forwarded by the primary node, backup nodes vote in the preparation and submission stages and return the voting results to the customer node in the reply stage. At the same time, nodes are divided into Byzantine nodes and non-Byzantine nodes by nodes' behavior. Byzantine nodes include fault nodes and malicious nodes. These nodes are called fault nodes that messages cannot send to other nodes during the consensus

process. It can be caused by network, hardware, or various reasons. Non-Byzantine nodes are nodes that can normally participate in the consensus and follow the rules. PBFT solves the energy consumption problem of PoW and also greatly reduces the output time [20]. However, the nodes using PBFT have to broadcast many times in the process, which makes the network bandwidth costly and the scalability limited [21].

At present, most academic studies focus on the improvement of PoX and BFT algorithms [22]. The improvement of the PoX class algorithm mainly focused on the improvement of its energy consumption. The improvement methods include 1) using algorithms to identify nodes and reducing the calculation difficulty of meritorious nodes; 2) changing calculation content and turning meaningless calculations to the work that solves transactions from the chain; 3) changing the proof content, workload, to other resources.

1.2 Contributions

The BW-PBFT, presented here, is a modified PBFT algorithm based on a credit value bidirectionally waning. In this algorithm, a credit value mechanism is introduced to evaluate the node quality. Each node has its own credit value, and the credit value above 50 will gradually decay to 50 with increase of the height of the blockchain, and the credit value below 50 will gradually increase to 50. The algorithm also uses analytic hierarchy process (AHP) [23] to establish a reward and punishment table for node behavior. When nodes actively and correctly participate in the consensus, they will get a credit value reward. On the contrary, when they fail to correctly participate in the consensus, they will be punished by deducting the credit value. The algorithm calculates the comprehensive value based on the voting and credit values. The part with the higher comprehensive value becomes the primary nodes and backup nodes. These nodes form a committee and keep an additional part of the nodes as alternate nodes. The alternate nodes are automatically supplemented as backup nodes when the number of committee nodes is insufficient. If the committee nodes are insufficient and there is no alternate node. The main contributions of this article include four aspects:

1. An algorithm of bidirectionally waning credit is proposed, and the influence on credit will decrease over time which is caused by nodes' behavior, whether good or bad. It makes the credit value assess nodes' quality more accurately and in real-time.
2. Put forward a reward and punishment algorithm (RP). Establish credit value reward and punishment tables based on the AHP. It makes the intensity of reward and punishment more accurate. For nodes that make non-honest behavior several times in a short time, the algorithm will make multiple punishments.
3. The method of selecting committee nodes in DBFT is improved. The committee nodes are selected by comprehending votes and credit value. Through theoretical analysis and simulation experiments on a personal computer, the results show that BW-PBFT can remove malicious nodes from the consensus in time and effectively improve the overall quality of the nodes participating in the consensus.
4. Through theoretical analysis and simulation experiments on a personal computer, the results show that BW-PBFT can remove malicious nodes from the consensus

in time and effectively improve the overall quality of the nodes participating in the consensus.

1.3 Structure of article

The remainder of the article is included as follows. The part 2 introduces current research of other people. In section 3, the article briefly introduces the design purpose and significance of this consensus algorithm. The part 4 describes the consensus algorithm process in detail and theoretically demonstrates the feasibility and safety of the consensus algorithm from several aspects in section 5. The experiment will be mentioned in section 5. The last part(part 6) provides a summary of the work and contributions of this paper.

2 Relate works

At present, most academic studies focus on the improvement of PoX and BFT algorithms [22]. The improvement of the PoX class algorithm mainly focused on the improvement of its energy consumption. The improvement methods include 1) using algorithms to identify nodes and reducing the calculation difficulty of meritorious nodes; 2) changing calculation content and turning meaningless calculations to the work that solves transactions from the chain; 3) changing the proof content, workload, to other resources.

Ai et al.[24] combined BFT-type and PoX-type protocols to generate the Proof-of-Transactions(PoT) consensus, which turns useless calculations into the Internet of Things transactions. Similarly, Song et al.[25] presented Proof-of-Contribution(PoC) protocol, and apply it to intellectual property protection. This protocol uses an algorithm to calculate the contribution of work. The node that has the most contribution point can generate the block. Liu et al. [26] used K-means algorithm to improve DPoS consensus algorithm. It was used to choose good nodes to form a queue. Delegated Byzantine Fault Tolerance(DBFT) consensus protocol came out with the NEO project[27], DBFT elects some nodes to use PBFT making consensus from all nodes. The consensus algorithm partially solves the problem of extendibility in PBFT. The network bandwidth consumption is determined by the number of committee nodes, and the increase in total nodes does not increase the bandwidth consumption. However, DBFT selects a primary node and backup nodes randomly, which cannot guarantee the quality of the selected nodes. It may cause view changes frequently. Since the DBFT birth from the NEO project, most of the improvements to the BFT class consensus algorithms are based on DBFT. These algorithms focus on the selection of nodes participating in the consensus.

Li et al. [28] proposed an improved PBFT blockchain consensus mechanism based on a reward and punishment strategy(SVBFT). The nodes using SVBFT only send information to the first node, to reduce the complexity of communication from $O(n^2)$ to $O(n)$. Zhang et al. [29]improved the scalability of the PBFT. They first produced a method to judge the low-energy nodes and excluded them from consensus in time. Moreover, they change the number of transactions included in one block to be alterable due to the application scenario and performance of nodes. Zhan et al. [30]used a

random selection algorithm called RS to improve the DBFT. RS chose the nodes participating in consensus from the nodes having won the voting process. It reduced the number of nodes participating in the consensus. Qiao et al. [31]improved Byzantine Fault Tolerance by using a trusted list. It improved the security and the quality of nodes in the blockchain network. Zhang et al. [32]proposed a genetic algorithm and used it in PBFT. It monitored the behavior of the nodes in the committee, and selected nodes multiple times due to the indicators to get the best consensus group. Li et al. [33]proposed Scalable Hierarchical Byzantine Fault Tolerance(SHBFT). It divided nodes into two layers and a primary node and separated client nodes into several groups. Each group only sent requests to their own secondary node and other nodes in the same layer. It obviously reduced the connection pressure above the blockchain network. In a similar way, Qushtom et al. [34] divided the system in to two layers. The higher layer was constituted by virtual nodes which are maps of clusters from lower layer. Li et al. [35] also used stratification, proposed H-PBFT consensus algorithm.

3 Design goals

The traditional PBFT consensus algorithm has a high network complexity. With the increase of consensus nodes, the blockchain network will finally reach a state the network cannot work due to excessive network pressure. The DBFT algorithm and its improved algorithm focusing at the present stage did not combine the performance in the consensus process with the election process, which lead to that the nodes elected are not certainly the nodes having performed well in the consensus process. This article presents the BW-PBFT consensus algorithm and will show the detail in Part 3. The partial objectives of this consensus algorithm are as follows:

1. The consensus algorithm retains the advantages of traditional PBFT, ensures that the containment of Byzantine nodes will not decline, and absorbs the advantages of other studies.
2. With the increase of time, the influence on the credit value caused by the good or bad performances of the withdrawal nodes in the consensus process will gradually weaken. This way can reduce the influence of network factors on the credit value.
3. Nodes having performed poorly will be removed from the consensus and the overall quality of the committee nodes will be continuously optimized.

4 BW-PBFT

BW-PBFT is an improved algorithm based on DBFT. Its core idea is to select some nodes to participate in the consensus according to the credit value and votes. This section details each part of the consensus algorithm.

4.1 System model

As shown in Figure 1, BW-PBFT divides the nodes into four types, namely, the primary node, the alternate nodes, the backup nodes, and the ordinary nodes.

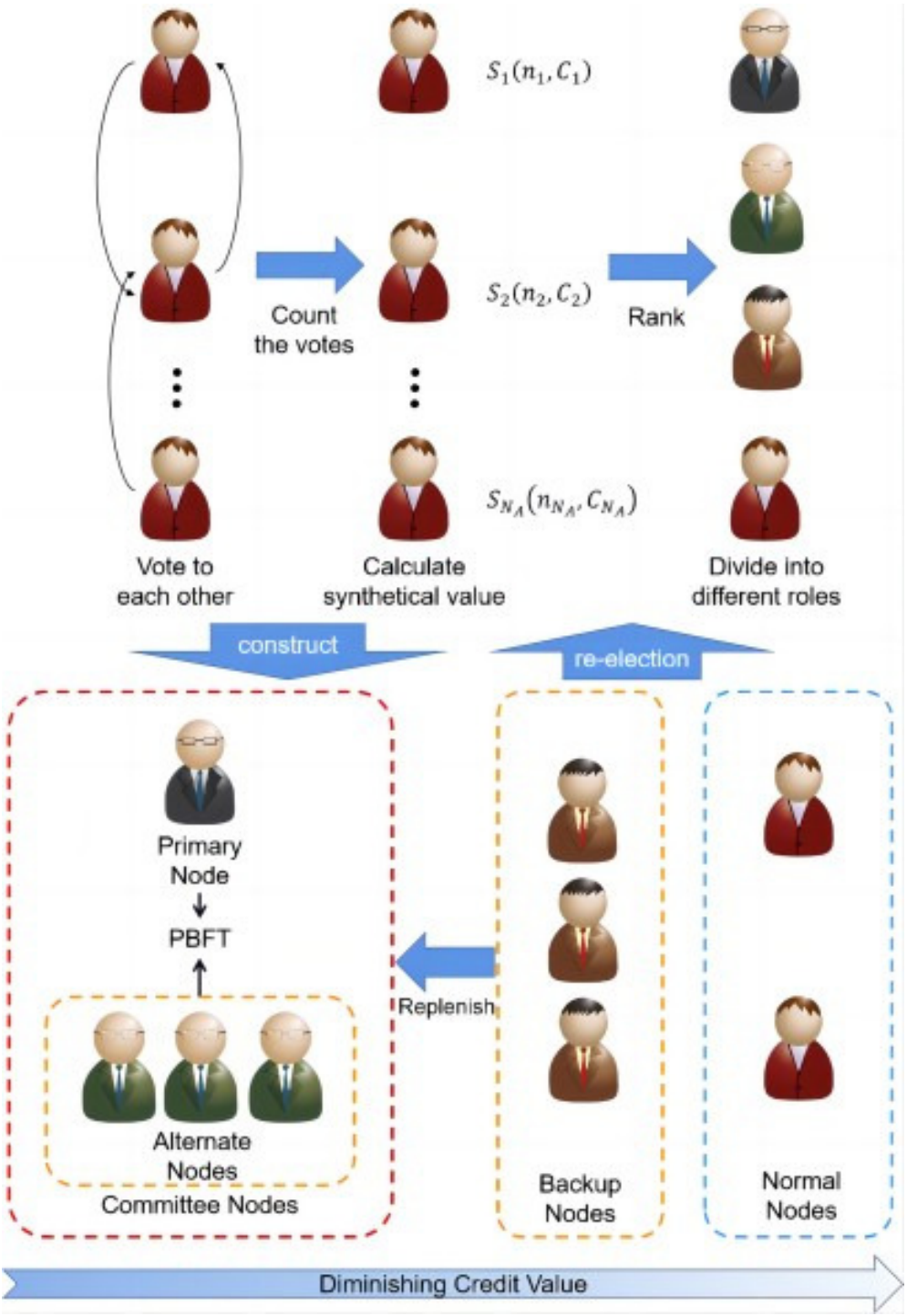

Fig. 1 System model in election stage and consensus stage, and transition between two stage

4.1.1 The primary node

The primary node in BW-PBFT is basically equivalent to the first node in PBFT. Differently, the first node in BW-PBFT is also responsible for launching elections, participating in voting, and collecting nodes' behavior. The primary node belongs to the committee;

4.1.2 Alternate node

Alternate nodes use PBFT for consensus. The alternate nodes are basically equivalent to the backup nodes in PBFT. In addition, the alternate nodes are also responsible for participating in voting and collecting nodes behavior, alternate nodes also belong to the committee;

4.1.3 Backup node

The backup nodes are as same as the ordinary nodes before entering the committee. These nodes do not participate in the consensus. When committee nodes are vacant, the backup nodes shall be supplemented in order;

4.1.4 Normal node

Normal nodes do not participate in the consensus and broadcast their own transaction to all committee nodes.

4.2 Hypothesis

The BW-PBFT relies on the following three hypotheses.

1. Initially, the number of Byzantine nodes in the committee nodes is less than f (the total number of committee nodes is $3f + 1$). It is mean that the composition of initial committee nodes complies with the minimum criteria of PBFT operating.
2. The state of the blockchain network and nodes hardware is stable, which means the loss probabilities of nodes will not change in a long time.
3. The number of non-Byzantine nodes in all the nodes is much greater than $2f + 1$.

4.3 Transactions, Rewards and Punishment Records, Blocks

There are three important data structures in BW-PBFT: 1) transactions (hereinafter referred to as Ts); 2) rewards and punishment records (hereinafter referred to as RPr); 3) blocks. These three data structures are shown in Table 1.

The reward and punishment records are organized as the data type of a dictionary. For example, in the reward record 1:2,4:1, it means that the object node will get 2 rewards in level 1 and 1 reward in level 4 in this round of consensus. Ts and RPr are organized in one block as the two Merkle Trees [36](see Figure 2), which are the main content in the block body, and write the root hash into the block.

Table 1 Ts, RPr, and the block structure

Struct	Member	Description
Ts	Hash	Hash of other members.
	From	Hash address of the payer.
	To	Hash address of the payee.
	Message	Any message from the payer.
	Signature	Signature from the payer.
RPr	Hash	Hash of other members.
	Address	Address of the object.
	flag	Mark this record as punishment or reward.
	Record	Records dictionary.
Block	Index	Auto-increment from 1.
	Pre-Hash	Hash of the last block.
	Time	Time of this block be built.
	Hash	Hash of other members.
	Trroot	Hash address of the payer.
	To	Hash address of the payee.
	Message	Any message from the payer.
	Signature	Signature from the payer.

4.4 Flow Path

The consensus process of BW-PBFT is shown in Figure 3, unlike PBFT, the nodes involved in the consensus process should collect the behavior of the nodes and convert them into RPr, and the transformation of rewards and punishment records will be detailed in section 4.5. The settlement of credit values of nodes are made after the block is generated, and the settlement will be detailed in section 4.6 of this chapter. Then set the nodes which credit value below the threshold as ordinary nodes, and supplement committee nodes from backup nodes. If there is no more backup node and the number of committee nodes is still insufficient, a re-election must be initiated by the primary node, and the election process is detailed in section 4.7.

4.5 Reward and punishment table and RPr

Table 2 Judgment matrix

Objective	C_1	C_2	C_3	C_4
C_1	$g_{11} = 1$	g_{12}	g_{13}	g_{14}
C_2	$g_{21} = 1/g_{12}$	$g_{22} = 1$	g_{23}	g_{24}
C_3	$g_{31} = 1/g_{13}$	$g_{32} = 1/g_{23}$	$g_{33} = 1$	g_{34}
C_4	$g_{41} = 1/g_{14}$	$g_{42} = 1/g_{24}$	$g_{43} = 1/g_{34}$	$g_{44} = 1$

The reward and punishment table is divided into reward behavior table and punishment behavior table, which use AHP to establish. In Figure 4, the good behaviors of nodes are associated with the factors in the efficient and normal operation of the blockchain. Bad behaviors should also be established in the same way. Then, the

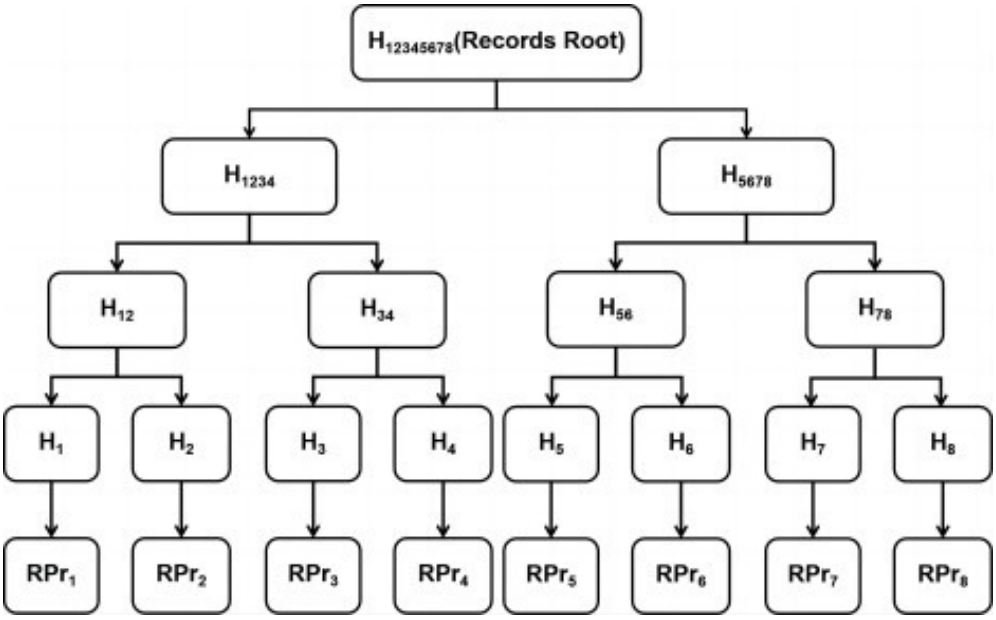

Fig. 2 Recording Merkel tree. The hash value of each RPr and Ts will be used as leaf nodes of the Merkel tree. Each two next leaf nodes will be merged and hashed, and the hash will be used as the last layer node, in this way, it will finally merge into one node, which will be the Merkel root and written in the block. The trading Merkel tree is a similar structure.

judgment matrix (see Table 2) can be constructed. Compare the importance of these criteria relative to objective and test consistency, C_k (k=1,2,3...) in the table represents criteria, g_{ij} (i,j=1,2,3...) represent the degree of the importance of Ci relative to C_j The importance of the degree, g_{ji} is the reciprocal of g_{ij}.

Table 3 Reward Level Table

Level	Behaviors	Level	Behaviors
1	B_3, B_5	3	B_1, B_2
2	B_4, B_7	4	B_6, B_8

Secondly, the judgment matrix is also established for the good and bad behavior about each factor. Subsequently, construct the judgment matrix among behaviors and each criterion in same way. Then, it can obtain the weights of the influence of each good and bad behavior on the objective and the consistency test is conducted. Behaviors can be sorted due to the weights. Finally, the behaviors are divided into different levels according to the equal frequency binning method, so as to establish the reward and punishment table (see Table 3), which is displayed as the reward table in the paper.

After a round of consensus, the behaviors information should be converted to the corresponding reward and punishment records. For example, after one round of

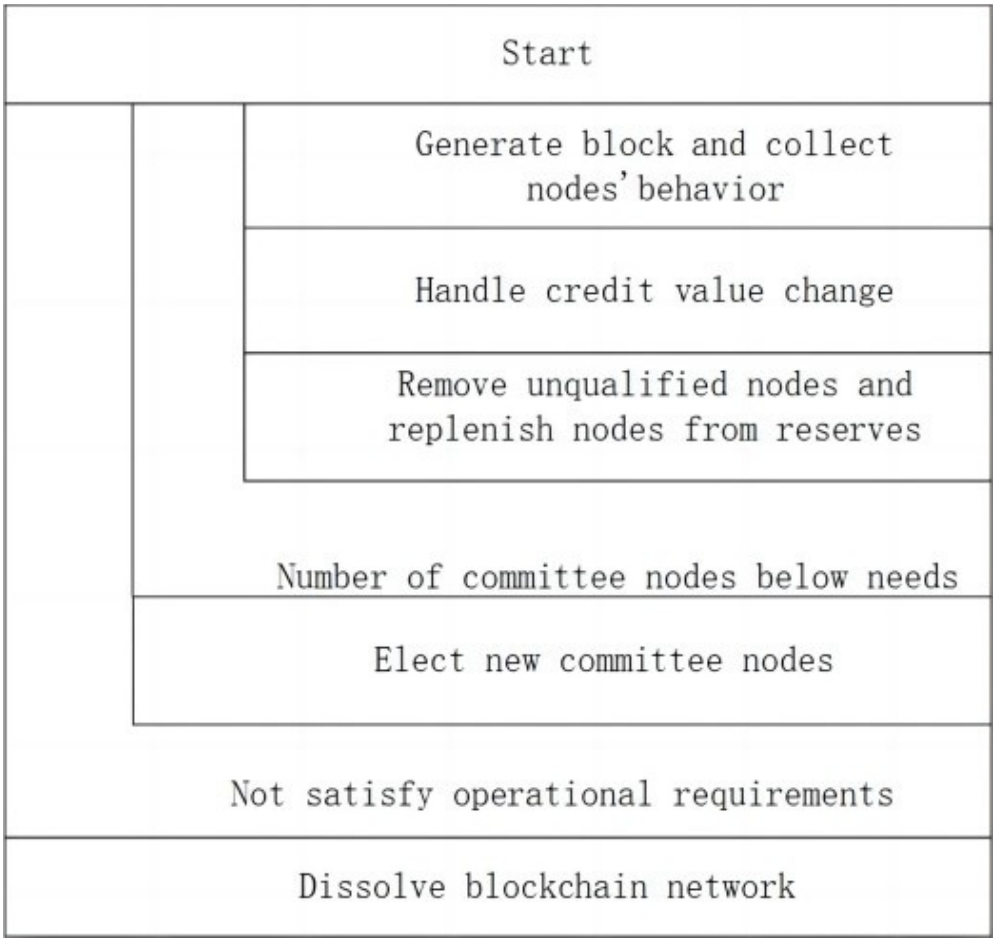

Fig. 3 BW-PBFT consensus process. Nodes are divided into three groups due to credit value.

consensus, node i has two behaviors B_3, one behavior B_7, one behavior B_4. The reward dictionary in the reward and punishment records is {1:2,2:2}.

4.6 Credit Value Settlement

Credit value settlement includes two parts, credit waning and credit rewards and punishments. First, the waning value is calculated, and the specific Algorithm 1, k is a parameter no greater than 49. As the k larger, as the waning of credit value slower. The reward value is calculated by the following equation 1:

$$AwardValue_t^i = \sum_{(a:b)\in Dict}^{A_t^i} Award_a \times b. \tag{1}$$

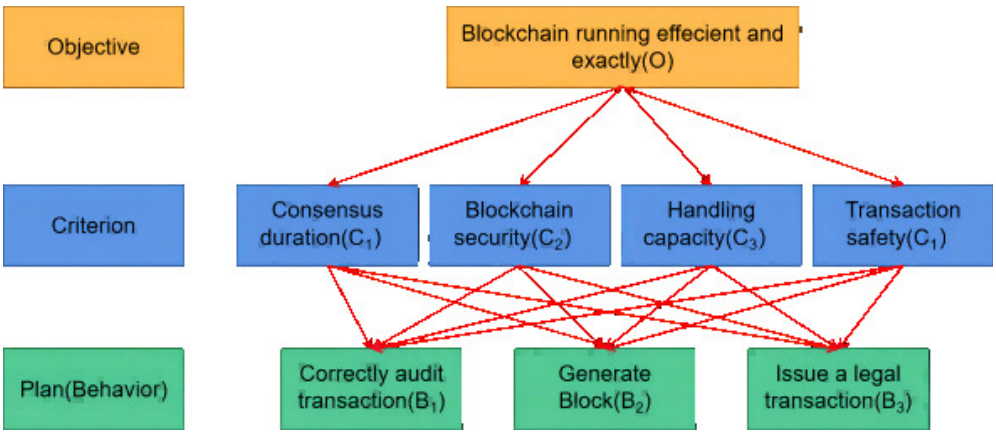

Fig. 4 Hierarchical chart. The Objective layer is the object that blockchain runs efficiently and exactly. The criterion layer is the factors affecting the operation of the blockchain. Some examples of factors are listed in the figure. The scheme layer is the behavior of nodes in this model.

Algorithm 1 Credit Bidirectionally Wane

Input: $OldCredit$
Output: $WaneValue$

if $OldCredit < k$ **then**
  return Round down$((49-k)/k^2 * OldCredit^2 + 1)$
else
  if $OldCredit < 100 - k$ **then**
    return Round down$(50 - OldCredit)$
  else
    return Round down$((k-49)/k^2 * (OldCredit - 100)^2 - 1)$
  end if
end if

$Dict$ is a reward dictionary,a represents the level of behavior, and b represents count of behavior in level a. $Award_a$ is the reward value of the level of integrity behavior. A_t^i is the RPr dictionary of node i between blocks $t-1$ and t. $AwardValue_t^i$ is the award value of node i after the generation of block t.

The calculation method of punishment value is similar to the reward at the beginning, which is obtaining the initial punishment value according to the recording dictionary. Differently, each node independently has a punishment coefficient M_i and the deadline of penalty D_i, the initial value must be multiplied by the coefficient to obtain the final punishment value. The specific algorithm(see algorithm 2) is used to calculate punishment value.

Finally, the new credit value is calculated according to the waning value, reward value, and punishment value. The calculation equation 2 is as follows:

Algorithm 2 Calculate Punishment Value

Input: node id i
Output: $PunishValue$

Sum original value based on i.
$PunishValue \Leftarrow$ Origin Value
Get Blockchain Height.
if $i.PunishDeadline < Height$ **then**
    $i.PunishMultiple \Leftarrow 1$
else
    $i.PunishMultiple \Leftarrow Smalleronein(5, i.PunishMultiple + 1)$
end if
$i.PunishDeadline \Leftarrow (Height + 20)$
return $PunishValue$

$$C_{t+1}^{i} = Min(Max(C_{t}^{i} + WaneValue_{t}^{i} + AwardValue_{t}^{i} - PunishValue_{t}^{i}, 0), 100) \quad (2)$$

4.7 Election

When the number of committee nodes does not meet the operational requirements, an election need relaunched. In the election phase, all the nodes on the chain can vote for a node, which can be either itself or any one node on the chain. Then, according to the comprehensive value obtained by the votes and the corresponding credit values. The equation 3 for the comprehensive value is:

$$S_i = n_i/N_A * 100 * \alpha + C_i * (1 - \alpha) \quad (3)$$

In this formula, S_i is the comprehensive value of node i, n_i is the number of votes obtained of node i in the commission stage, N_A is the number of all nodes, C_i is the credit value of node i, α is a number greater than 0 and less than 1. When α approaches 1, the entrance of the committee is more dependent on voting, conversely, it is more dependent on the credit value. Subsequently, according to the comprehensive value, nodes are arranged from large to small. The previous N_c nodes are selected to form the committee, and the first node is the primary node. When the number of nodes is sufficient, keep nodes between $N_c + 1$ and $3/2 * N_c$ to be retained as alternate nodes. N_c is the number of nodes required by the committee. Set the credit value of the N_c+1 node, C_{N_c+1}, to be threshold.

5 Protocol analysis

This chapter will analyze the algorithm from the theoretical aspects. The analysis is based on feasibility, consistency, blockchain activity, communication complexity, time of block generation, extendibility, and comparison with other consensus protocols. The number of committee nodes is $3f + 1$. Nodes are considered to be composed of these parts, reliable nodes R, disconnected nodes D and evil nodes E, among which

bad nodes and lost nodes are collectively referred to as Byzantine nodes. The reliable nodes are the nodes that participate in the consensus agreement and rarely fail. The lost node is a node that does not communicate with other nodes. The evil behavior of malicious nodes will be judged as the higher level behavior in the punishment table. When the malicious behavior is detected, the punishment will make the credit of evil node under the threshold, and it will be directly removed from the committee.

5.1 Feasibility

Feasibility refers to the ability that the blockchain using BW-PBFT for consensus operates normally and correctly and records on-chain transactions exactly. The consensus protocol initially meets the necessary and sufficient conditions for PBFT operation, that is, the number of Byzantine nodes is less than or equal to f, and the reliable nodes are more than or equal to $2f + 1$. The reliable nodes are considered to be the nodes with few network and hardware failures. When the consensus protocol is running, reliable nodes will correctly participate in the consensus and contribute to the blockchain network, and the nodes can get the credit value reward. Even if the network or software failure occasionally, the credit value will increase again after continuing to participate in the consensus correctly, so the reliable nodes will not be removed from the committee. Therefore, the reliable nodes are always more than $2f + 1$.

5.2 Consistency

Consistency requires all nodes to achieve the same result after one round of consensus is completed, that is, no fork in blockchain. The necessary and sufficient condition of consistency is as same as feasibility, that the number of Byzantine nodes is less than or equal to f. Therefore, the BW-PBFT meets the consistency.

5.3 Blockchain activity

Blockchain activity is expressed as the proportion of reliable nodes and evil nodes in the committee. The evolution of the activity is shown in Table 4. As the consensus progresses, the proportion of reliable nodes gradually increases, and blockchain activity will also rise in fluctuation.

5.4 Communication Complexity

If the committee nodes are n, the committee uses PBFT for consensus. All the preparation and submission stages in the consensus need to broadcast all nodes within the committee, so the communication complexity is $O(n^2)$.

5.5 Block Generation Time

The generation interval of a block of blockchain can be basically equivalent to the time of one consensus round. In the case of the consensus method of PBFT, the consensus time is affected by the activity of the blockchain. The higher the blockchain activity, the shorter the consensus time and the block generation cost. The initial block-out

Table 4 Activity Evolution

Index	T_0[1]	T_1[2]	T_2[3]	$\lim_{n\to\infty} T_n$[4]
Number of evil nodes	E_0	$E_1(E_1 \geq E_0)$	$E_2(E_2 \leq E_0 \leq E_1)$	$\lim_{n\to\infty} E_n = 0$
Number of disconnected nodes	D_0	$D_1(D_1 \leq D_0)$	D_2	$\lim_{n\to\infty} D_n = 0$
Number of reliable nodes	R_0	$R_1(R_1 \geq R_0)$	$R_2(R_2 \geq R_1 \geq R_0)$	$\lim_{n\to\infty} R_n = N_c$
Activity	$L_0 = (E_0 + R_0)/N_c$	$L_1 \geq L_0)$	L_2	$\lim_{n\to\infty} L_n = 1$

[1]Origin state.

[2]After the first time the credit values of the disconnected nodes are below the threshold, the original disconnected nodes are removed from the committee. Alternate nodes do supplement.

[3]After the evil nodes first do evil, the malicious nodes are removed from the committee.

[4]The number of dependent nodes increases with the number of consensus rounds and approaches to the number of committee nodes.

time is equivalent to the PBFT block-out time T_0. As the consensus proceeds, the blockchain activity increases, and the block-out time will be lower than the PBFT block-out time.

5.6 Extendibility

Nodes can join the blockchain at any time according to the requirements of the blockchain, and the initialized credit value of the new node is 50. A new node can get information on blocks by broadcast requests in the blockchain network. Adding nodes will not affect the communication complexity of the committee, so the scalability is good.

5.7 Comparison with Other Consensus Agreements

As shown in Table 5, BW-PBFT is compared with PBFT, DBFT, and PoW in terms of environment, communication complexity, first node selection, power cost, blockchain activity, block generation time, and fault tolerance.

6 Experiment

In this section, simulation experiments will be used to separately verify the feasibility of the bidirectionally waning credit mechanism, and the characteristics of the BW-PBFT algorithm, which are feasibility, high efficiency, and self-optimization. The experiment was simulated on a personal computer in Python language. The experimental configuration is 1) CPU: Intel (R) Core (TM) i7-6700HQ CPU @ 2.60GHz; 2) RAM: 16GB; 3) OS: Windows 10.

Table 5 Consensus Agreement Comparison

Items	BW-PBFT	PBFT	DBFT	PoW
Environment	Consortium	Consortium	Consortium	Public
Communication Complexity	$O(n^2)$	$O(m^2)$	$O(n^2)$	-
First Node Selection	The first node in rank thatcombined credit and vote.	Random select or by election.	Select by vote	The first node that solve the puzzle.
Power Cost	Low	Low	Low	High
Blockchain Activity	$> L_0$	L_0	L_0	-
Time Cost for Block Construction	$< T_0$	T_0	T_0	10min
Fault-Tolerant	$3f + 1 < n$	$3f + 1 < m$	$3f + 1 < n$	$< 50\%m$

n is the nodes amount in committee, m is the amount of all nodes.

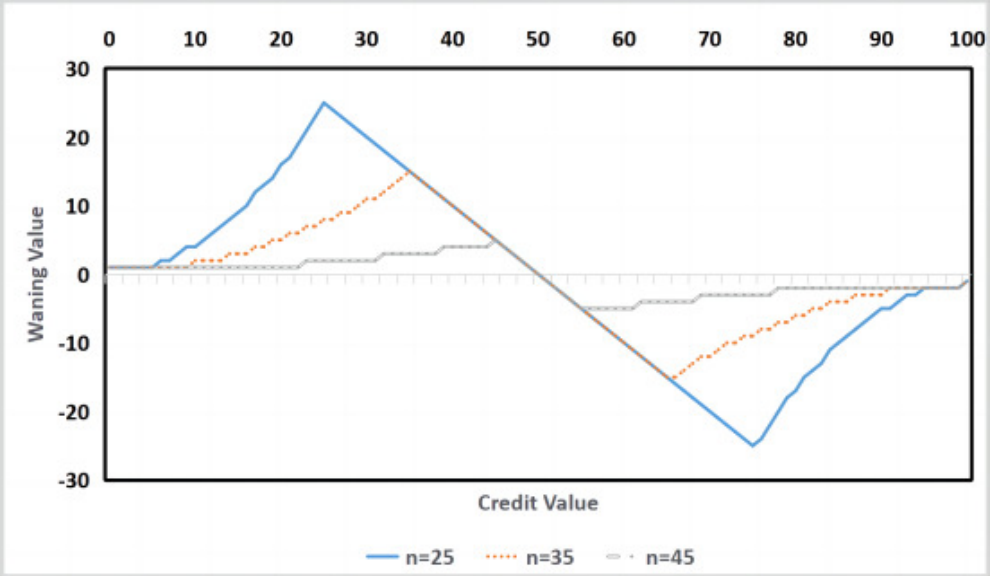

Fig. 5 Waning values of nodes at each credit value

6.1 Validation of the Bidirectional Attenuation Mechanism

To verify the credit value decay mechanism, do the following experiments, make k to be 25,35 and 45, and get the waning value at each credit value between 0 and 100 (see Figure 5); make k to be 25,35 and 45, and test how many blocks need to make the credit value to decrease from 100 to 50 and increase from 0 to 50. The experimental

results show that the node credit value will gradually decay to 50 with the increase of the blockchain height, and the credit value will be slow to 50 when the credit value of the node is away from 50, and be fast in contrary.

6.2 Verify Feasibility, High Efficiency, and Self-optimization

Table 6 Experimental Parameters

Experimental label	Number of committee nodes	Number of backup nodes	Total number of nodes	k
1	20	10	100	35
2	20	10	100	45
3	30	15	100	35
4	30	15	100	45
5	50	25	1000	35
6	50	25	1000	45
7	80	40	1000	35
8	80	40	1000	45

In this section, eight experiments were performed according to the parameters of Table 6. Assuming that there are evil nodes in all the nodes, the evil nodes will have an evil behavior every 10 rounds. In addition, the stability levels of the nodes are different. In each round of consensus, different nodes have different loss rates, and the non-evil nodes with a loss rate lower than 5% are called stable nodes. A total of 200 rounds of consensus were performed for each experiment. After each consensus, counted the current status of the committee network and the number of malicious nodes. The committee network status representation method is the proportion of stable nodes in the committee nodes. In the experiment, the case of that Byzantine nodes are more than f, it can get feasible.

The results of experiences were plotted as graphs. As shown in Figure 6, eight results show that with the increase of the block chain height, committee network condition can be improved, in the smaller committees can faster get promotion. In experiments 1-4, the stable nodes in the committee has occupied hundred percent in the committee. In blockchain with larger scale, the committee is larger, network stability can quickly get more than 30% of the ascension.

According to Figure 7, in each experiment, when evil nodes do illegal things at the first time, the committee can find the evil nodes in time and exclude them out of the committee, and it is difficult for the evil nodes to re-enter the committee.

7 Summary and The Future Work

Blockchain has a fairly broad application prospect because it is programmable, timing, and tamper-proofing. One of the problems that blockchain can not be widely used is that its consensus mechanism is not suitable. The PoX type consensus mechanisms are

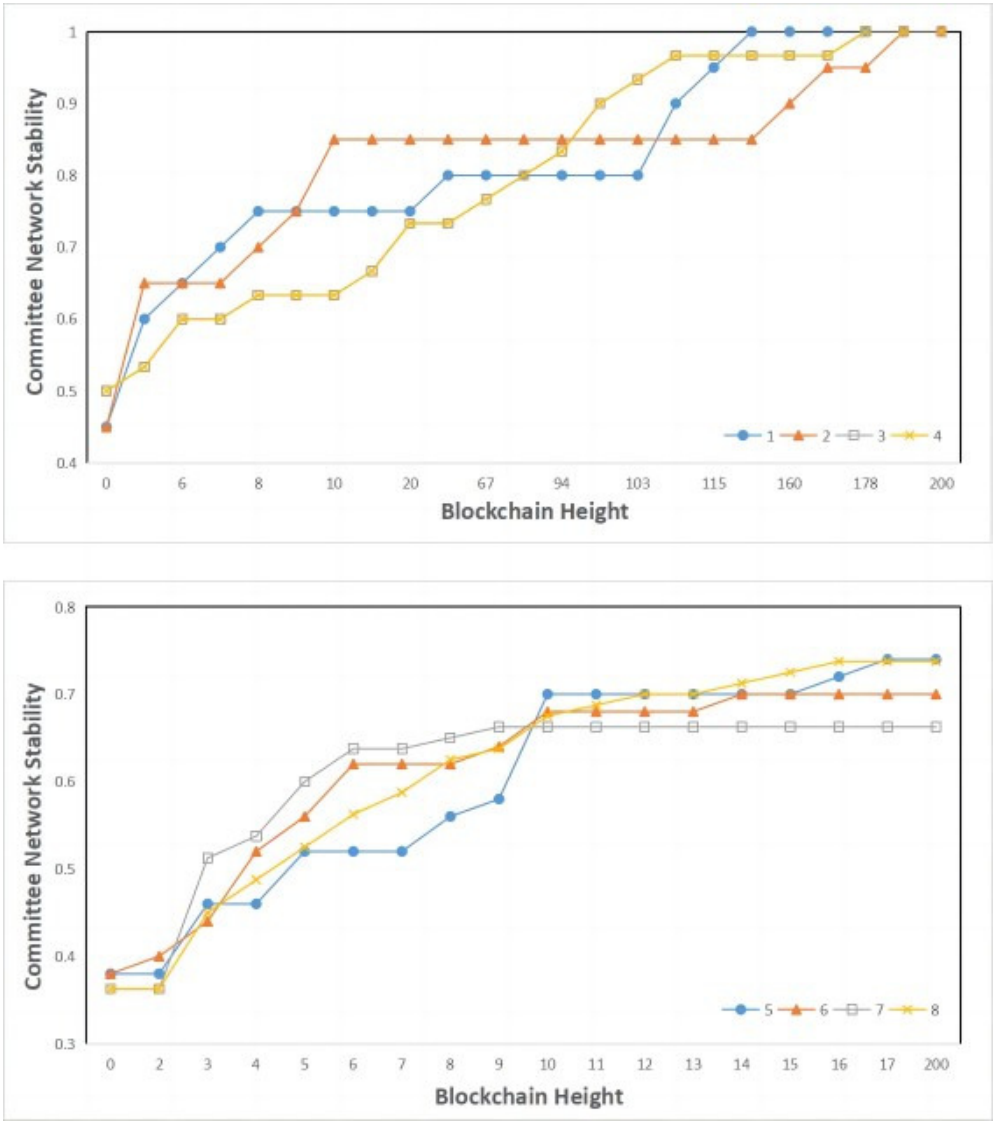

Fig. 6 The changes of stability of the blockchain network with the increase of blockchain height

prone to waste resource and have a long transaction delays. The consensus mechanisms of BFT type also have some problems, such as large network load pressure and poor scalability.

The BW-PBFT algorithm proposed in this paper is an improved algorithm based on PBFT, which is used to solve the problems in the PBFT algorithm, such as poor extendibility, uneven quality of consensus nodes, and poor blockchain activity. The core idea of the algorithm is to use a credit value to represent the quality of the node,

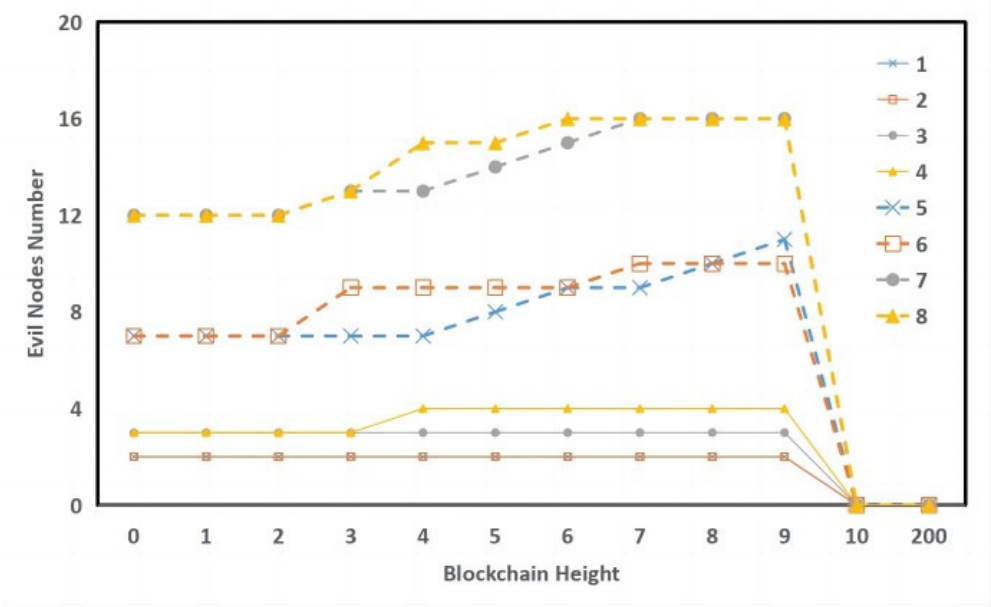

Fig. 7 The changes of evil nodes number with the increase of blockchain height

and transform the performance of the node during the consensus through the algorithm into a credit value reward or punishment, but also use the credit bidirectionally waning algorithm to weaken the influence of the nodes' past behavior on the current state. Within this algorithm, the credit value of nodes will tend to 50 with the increase of blockchain height. In the election stage of the committee, the voting and credit value are combined, and the node with a high comprehensive ranking is selected as the primary node and the backup node. It can be seen in the analysis in part 5, BW-PBFT is superior to other consensus mechanisms in aspects of energy consumption, blockchain activity, and block generation time. The experiments in part 6 also demonstrate the feasibility and characteristics of self-optimization of the algorithm.

Future work will focus on solving the problem that the primary node is vulnerable to be attacked for the primary node is in an open situation.

Acknowledgments. I would like to give thanks to three people: Professor Zhen-Fei Wang, for guiding me into the gate of blockchain; Ph. D. Li-Ying Zhang, for guiding me on the article writing; Yong-Wang Ren, for answering me the questions in the blockchain.

Declarations

- Funding
  National Natural Science Foundation of China, 62276238
- Competing interests

l declare that the authors have no competing interests as defined by Springer, or other interests that might be perceived to influence the results and/ordiscussion reported in this paper.

- Ethics approval
  Not
- Consent to participate
  Not
- Consent for publication
  Yes
- Availability of data and materials
  Not
- Code availability
  Not
- Authors' contributions
  Zhen-Fei Wang give guidance in blockchain to researchers. Shi-Qi Liu performed the data analyses and wrote the manuscript. Pu Wang helped with article review. Li-Ying Zhang helped with article writing.
- Authors' information
  Affiliations
  School of computer and artificial intelligence, Zhengzhou University, No.100, Kexuedadao, Zhengzhou, Henan, China
  Zhen-Fei Wang, Shi-Qi Liu, Pu Wang & Li-Ying Zhang
  Corresponding author
  Li-Ying Zhang

References

[1] Nakamoto, S.: Bitcoin: A peer-to-peer electronic cash system. Decentralized business review, 21260 (2008)

[2] Lu, Y.: The blockchain: State-of-the-art and research challenges. Journal of Industrial Information Integration **15**, 80–90 (2019)

[3] Shen, H., Chen, Q., Huang, H.: Review on research of semantic blockchain. Application Research of Computers **38**, 1937–1942 (2021)

[4] Kushwaha, S.S., Joshi, S., Singh, D., Kaur, M., Lee, H.-N.: Ethereum smart contract analysis tools: A systematic review. IEEE ACCESS **10**, 57037–57062 (2022) https://doi.org/10.1109/ACCESS.2022.3169902

[5] Ou, W., Huang, S., Zheng, J., Zhang, Q., Zeng, G., Han, W.: An overview on cross-chain: Mechanism, platforms, challenges and advances. COMPUTER NETWORKS **218** (2022) https://doi.org/10.1016/j.comnet.2022.109378

[6] Zeng, S., Huo, R., Huang, T., Liu, J., Wang, S., Feng, W.: Survey of blockchain:principle,progress and application. Application Research of Computers

41 (2020)

[7] Ali, O., Ally, M., Clutterbuck, Dwivedi, Y.: The state of play of blockchain technology in the financial services sector: A systematic literature review. INTERNATIONAL JOURNAL OF INFORMATION MANAGEMENT **54** (2020) https://doi.org/10.1016/j.ijinfomgt.2020.102199

[8] Kuo, T.-T., Rojas, H.Z., Ohno-Machado, L.: Comparison of blockchain platforms: a systematic review and healthcare examples. JOURNAL OF THE AMERICAN MEDICAL INFORMATICS ASSOCIATION **26**(5), 462–478 (2019) https://doi.org/10.1093/jamia/ocy185

[9] Salah, K., Rehman, M.H.U., Nizamuddin, N., Al-Fuqaha, A.: Blockchain for ai: Review and open research challenges. IEEE ACCESS **7**, 10127–10149 (2019) https://doi.org/10.1109/ACCESS.2018.2890507

[10] Taylor, P.J., Dargahi, T., Dehghantanha, A., Parizi, R.M., Choo, K.-K.R.: A systematic literature review of blockchain cyber security. DIGITAL COMMUNICATIONS AND NETWORKS **6**(2), 147–156 (2020) https://doi.org/10.1016/j.dcan.2019.01.005

[11] Makhdoom, I., Abolhasan, M., Abbas, H., Ni, W.: Blockchain's adoption in iot: The challenges, and a way forward. JOURNAL OF NETWORK AND COMPUTER APPLICATIONS **125**, 251–279 (2019) https://doi.org/10.1016/j.jnca.2018.10.019

[12] Tan, M.-s., Jie, Y., Lin, D., Li, X.-j., Xia, S.: Review of consensus mechanism of blockchain. Computer Engineering **46**(12), 1–11 (2020)

[13] Cao, X., Zhang, J., Wu, X., Liu, B.: A survey on security in consensus and smart contracts. PEER-TO-PEER NETWORKING AND APPLICATIONS **15**(2), 1008–1028 (2022) https://doi.org/10.1007/s12083-021-01268-2

[14] Andoni, M., Robu, V., Flynn, D., Abram, S., Geach, D., Jenkins, D., McCallum, P., Peacock, A.: Blockchain technology in the energy sector: A systematic review of challenges and opportunities. Renewable and sustainable energy reviews **100**, 143–174 (2019)

[15] Saleh, F.: Blockchain without waste: Proof-of-stake. The Review of financial studies **34**(3), 1156–1190 (2021)

[16] King, S., Nadal, S.: Ppcoin: Peer-to-peer crypto-currency with proof-of-stake. self-published paper, August **19**(1) (2012)

[17] Buterin, V.: A next-generation smart contract and decentralized application platform. white paper **3**(37), 2–1 (2014)

[18] Ethereum: Ethereum Whitepaper. https://ethereum.org/en/whitepaper/. Accessed 19 April 2023 (2022)

[19] Castro, M., Liskov, B., *et al.*: Practical byzantine fault tolerance. In: OsDI, vol. 99, pp. 173–186 (1999)

[20] Feng, L., Ding, Y., Liu, K., Ma, K., Chang, J.: Research advance on bft consensus algorithms. PEER-TO-PEER NETWORKING AND APPLICATIONS **49**(4), 329–339 (2022)

[21] Wang, Z.-F., Ren, Y.-W., Cao, Z.-Y., Zhang, L.-Y.: Lrbft: Improvement of practical byzantine fault tolerance consensus protocol for blockchains based on lagrange interpolation. PEER-TO-PEER NETWORKING AND APPLICATIONS https://doi.org/10.1007/s12083-022-01431-3

[22] Wang, W., Hoang, D.T., Hu, P., Xiong, Z., Niyato, D., Wang, P., Wen, Y., Kim, D.I.: A survey on consensus mechanisms and mining strategy management in blockchain networks. Ieee Access **7**, 22328–22370 (2019)

[23] Vaidya, O.S., Kumar, S.: Analytic hierarchy process: An overview of applications. European Journal of operational research **169**(1), 1–29 (2006)

[24] Ai, Z., Cui, W.: A proof-of-transactions blockchain consensus protocol for large-scale iot. IEEE Internet of Things Journal **9**(11), 7931–7943 (2021)

[25] Song, H., Zhu, N., Xue, R., He, J., Zhang, K., Wang, J.: Proof-of-contribution consensus mechanism for blockchain and its application in intellectual property protection. Information processing & management **58**(3), 102507 (2021)

[26] Liu, W., Li, Y., Wang, X., Peng, Y., She, W., Tian, Z.: A donation tracing blockchain model using improved dpos consensus algorithm. PEER-TO-PEER NETWORKING AND APPLICATIONS **14**(5, SI), 2789–2800 (2021) https://doi.org/10.1007/s12083-021-01102-9

[27] Neo: Neo White Paper. https://docs.neo.org/v2/docs/en-us/basic/whitepaper.html. Accessed 19 April 2023 (2020)

[28] Li, C., Zhang, J., Yang, X., Youlong, L.: Lightweight blockchain consensus mechanism and storage optimization for resource-constrained iot devices. Information Processing & Management **58**(4), 102602 (2021)

[29] Zhang, B., Kong, L., Li, Q., Min, X., Liu, Y., Che, Z.: Eb-bft: An elastic batched bft consensus protocol in blockchain. Future Generation Computer Systems **139**, 267–279 (2023)

[30] Zhan, Y., Wang, B., Lu, R., Yu, Y.: Drbft: Delegated randomization byzantine fault tolerance consensus protocol for blockchains. Information Sciences **559**, 8–21

(2021)

[31] Qiao, K., Tang, H., You, W., Wang, L.: Improved byzantine fault tolerance algorithm based on trusted lists. Computer Applications and Software **39**(2), 274–280 (2022)

[32] Zhang, J., Yang, Y., Zhao, D., Wang, Y.: A node selection algorithm with a genetic method based on pbft in consortium blockchains. Complex & Intelligent Systems, 1–21 (2022)

[33] Li, Y., Qiao, L., Lv, Z.: An optimized byzantine fault tolerance algorithm for consortium blockchain. Peer-to-Peer Networking and Applications **14**, 2826–2839 (2021)

[34] Qushtom, H., Misic, J., Misic, V.B., Chang, X.: A high performance two-layer consensus architecture for blockchain-based iot systems. PEER-TO-PEER NETWORKING AND APPLICATIONS **15**(5), 2444–2456 (2022) https://doi.org/10.1007/s12083-022-01363-y

[35] Li, J., Li, X., Zhao, H., Yu, B., Zhou, T., Cheng, H., Sheng, N.: Mandala: A scalable blockchain model with mesh-and-spoke network and h-pbft consensus algorithm. PEER-TO-PEER NETWORKING AND APPLICATIONS https://doi.org/10.1007/s12083-022-01373-w

[36] Becker, G.: Merkle signature schemes, merkle trees and their cryptanalysis. Ruhr-University Bochum, Tech. Rep **12**, 19 (2008)