Peer-to-Peer Networking and Applications (2022) 15:1849–1861
https://doi.org/10.1007/s12083-022-01320-9

Research on improvement of DPoS consensus mechanism in collaborative governance of network public opinion

Yuetong Chen[1] · **Fengming Liu**[1]

Received: 5 August 2021 / Accepted: 30 March 2022 / Published online: 2 May 2022

Abstract
With the increasingly complex social situation, the problems of traditional online public opinion governance are increasingly serious. Especially the problem of transmission efficiency, public opinion data management and user information security of Internet users is urgently needed. Here, we design a functional infrastructure framework of the network public opinion collaborative governance model based on the blockchain with strong practicality and comprehensiveness. In order to reach the consensus mechanism requirements under the framework, the algorithm is improved on the basis of the defects of the traditional DPoS consensus algorithm. Considering time dynamic factors in the process of reaching consensus, the paper proposes a reputation-based voting model. Furthermore, the paper purposes a rewards and punishments incentive mechanism, and also designs a new method of counting votes. From the simulation results, it was found that after the improvement of the algorithm, the enthusiasm of node participation was significantly increased, the proportion of error nodes was significantly reduced, and the operating efficiency was significantly improved. It shows that the improved consensus algorithm we propose applies to public opinion governance can not only improve the security of the system with the reduce of false public opinion spreading, but also improve the efficiency of information processing, so it can be well applied to information sharing and public opinion governance scenarios.

Keywords Blockchain · Network public opinion · Delegated Proof of Stake (DPoS) · Reputation · Consensus mechanism

1 Introduction

In the digital era, with the innovation and development of information communication technology, the disposal of public opinion is facing a new situation. Especially during the period of COVID-19 in 2020, a large number of network public opinion information that is difficult to distinguish between authenticity and fake emerges continually. The problems of traditional post-supervision method of the network public opinion governance are more obvious. For example, it is difficult to guarantee the authenticity and security of data transmission. Furthermore, the control of network public opinion is tardy and inefficient through the deployment of the central hub, which makes the network supervision and public opinion governance work overwhelmed. As a matter of fact, the evolution of network public opinion is a complex self-organization and self-adaptation system behavior, which is the result of mutual cooperation, mutual restriction, mutual premise and mutual competition among its internal subsystems [1]. Therefore, the governance of network public opinion needs to realize the collaborative autonomy of multiple subjects from centralization to decentralization. Blockchain technology with decentralized characteristics can realize the cooperative trust and consensus among multiple subjects, which naturally fit with the highly decentralized public opinion field, and is expected to bring a breakthrough innovation to the governance of network public opinion.

Blockchain has technical advantages such as decentralization, openness, anonymity, traceability, and non-tampering of information. At present, it is in full swing in application research in various fields. Similarly, application innovation in the field of network public opinion also has great potential. Existing studies believe that the application of blockchain technology in the field of network public opinion management and public opinion risk perception and

✉ Fengming Liu
liufm@sdnu.edu.cn

Yuetong Chen
983179330@qq.com

[1] Business School, Shandong Normal University, Ji'nan 250358, China

identification can reconstruct the public opinion information ecosystem, eliminate the release of false public opinion information, strengthen the privacy protection of public opinion users, and provide a solid data basis for the identification and perception of public opinion risk [2]. However, at present, domestic and foreign scholars have basically done theoretical research on the governance and control of network public opinion on the blockchain, while few scholars have used blockchain to conduct comprehensive and systematic research on the governance and prevention of network public opinion.

In view of this, considering the characteristics of self-organization and highly decentralization of network public opinion, this paper takes the autonomous and decentralized blockchain as a technical means to achieve intra-chain collaborative autonomy for public opinion. In order to overcome the shortcomings of the existing network public opinion governance, this paper proposes a basic framework of network public opinion collaborative governance model driven by consensus mechanism under the blockchain framework based on the perspective of reputation. By improving the traditional DPoS consensus mechanism (Delegated Proof of Stake), a reputation mechanism based on time dynamics is introduced, and the nodes are self-restrained under the influence of reputation by means of rewards and punishments, so as to realize the collaborative autonomy of multiple subjects under the influence of consensus mechanism.

Thus, the quality of the generated content block and the safety of the system can be guaranteed. This is undoubtedly an innovation of the network public opinion governance mode under the new situation of the complex social public opinion field.

The second section of this paper summarizes the related research on network public opinion governance, the application of blockchain in the field of information dissemination, and the related research on consensus algorithm. In view of the problems existing in the current situation of network public opinion governance, the third section proposes the functional framework of multi-agent collaborative governance mechanism of network public opinion based on blockchain architecture. Section 4 optimizes and improves DPoS from consensus efficiency and system security. Section 5 is the simulation experiment, and analyzes and discusses the experimental results. The sixth part is the conclusion and prospect of this study.

2 Related work

2.1 Network public opinion governance

As a specific form of online information communication, network public opinion refers to information statements that have not been officially confirmed and can cause strong disputes. Most scholars regard network public opinion as the total of different emotions, attitudes and opinions expressed and spread through the network [3]. It is caused by the subject's subjective anxiety, emotional catharsis, psychological imbalance, the loss of individual rationality and the influence of collective emotion, the obstruction of expression mechanism and the aggravation of political distrust [4]. In the complex environment of online public opinion, the governance of network public opinion is faced with the inadaptability of the government structure and the flat Internet structure. The amplification of the negative emotions of netizens in the self-media field also increases the difficulty of governance [5].

The research on response and governance of network public opinion generally continues from the process of passively controlling network public opinion, passively dealing with network public opinion, to actively governing network public opinion [6]. There was a research has put forward many countermeasures for network public opinion management from the aspects of governance concept transformation, infrastructure construction, system reform and system construction, international experience reference and law and regulation construction [7]. Christenal [8] pointed out that netizens would be affected by interactive comments when browsing news, which would cause distraction and inaccurate grasp of the news focus. The government could improve the interface of relevant websites to ensure the audience's attention to news and the independence of news judgment. Arunachalam et al. [9] believe that the government needs to guide the rational participation of netizens, expand the ways for netizens to participate in the discussion and management of national affairs, so as to improve the network management ability of leaders and show the credibility of the government. Cui et al. [10] used life cycle theory to construct a diamond model of the government's ability to respond to public opinion in emergencies, and used case analysis to provide a theoretical reference for the government to improve its ability to respond to network public opinion.

However, the governance of network public opinion is complex, extensive, profound and long-term. Although the government plays a leading role in the governance of network public opinion, it cannot completely control the behavior of the main body [11, 12]. Therefore, re-examining the positioning and concept of network public opinion governance is a crucial step to realize the innovation of public opinion governance. In the Internet public opinion governance system, the regulators, producers, disseminators, and decomposers of public opinion are not only the maintainers of the harmonious development of the public opinion governance system, but sometimes also consciously or unconsciously become the disruptors of the harmonious development of the public opinion governance ecosystem [13]. Public opinion governance is a competition and coordination relationship

that is both opposed and unified between multiple subjects. Network public opinion governance is based on the theory of system evolution of multi-subject consultation and co-governance, multiple subjects in the network public opinion governance system in the different division of labor, their rights and responsibilities are naturally different [14]. The governance of network public opinion is a self-organizing system supported by three-dimensional disposal strategy and rule of law. The positioning and implementation path of network governance should be based on government regulatory departments and supplemented by industries and non-governmental organizations. It should comply with public opinions, reflect the aspirations of the public and meet the needs of citizens [15].

Thus it can be seen that the governance of network public opinion is not only the responsibility sharing of the government, network regulatory authorities and other organizations, but also requires the cooperation of multiple social subjects, and relies on the internal subjects of the public opinion system to fulfill their responsibilities and form an orderly self-organizing system in a coordinated manner in accordance with the tacit rules [11]. Therefore, the network public opinion governance system clearly maintains the essence of public interests, needs to uphold the concept of transparency and legality, and relies on the spirit of consensus, behavior self-discipline, and the system, norms and consultation applicable to the whole people to achieve democratic autonomy.

2.2 Blockchain and its applications in network governance

The blockchain was first proposed by Satoshi Nakamoto, the originator of Bitcoin. Its key and advantage lies in the decentralized design based on encryption algorithms, timestamps, tree structures, consensus and reward mechanisms, so as to realize the point-to-point transaction based on decentralized credit [16]. The core technology of blockchain includes distributed architecture, consensus mechanism, encryption algorithm, smart contract, etc. As an independent technical solution, its application has extended from a single digital currency to various fields of economy and society, and has significant application advantages.

There is no central server in the blockchain technology architecture, and all blockchain computing devices are peer nodes that do not need to establish a trust relationship. All information interaction data in a certain period of time is encrypted and stored in a data block, and a hash is generated for linking to the next block and used for verification. A reliable database is established by collective verification and maintenance. The underlying data of the blockchain is stored in the form of blocks, and the computing power of "miners" is recorded in accordance with the workload proof mechanism. The data of each block is based on the timestamp and hash link to form a blockchain. Each node saves a blockchain ledger, uses the P2P protocol for communication, and verifies the data based on the consensus mechanism [17]. In order to ensure the security of the data, generally the plaintext data will not be directly stored in the block, but the SHA256 hash function or other encryption algorithm is used to calculate the original transaction record, and then save it in the block. In order to ensure the security of the data, generally the plaintext data will not be directly stored in the block, but the SHA256 hash function or other encryption algorithm is used to calculate the original transaction record, and then stored in the block [18]. The consensus mechanism is the core of solving the trust problem, which can ensure the consistency and security of the data in each block [19]. Peer-to-peer(P2P) network is guaranteed by the consensus mechanism, establishes mutual trust between nodes, transmits information by broadcasting, and uses an incentive mechanism to ensure computing power to promote the continuous operation of the network. Smart contract gives the blockchain flexible programmable features and provides a convenient interface for the upper-level applications of the blockchain scene, which makes it possible for industry applications such as product traceability, public opinion traceability, and financial credit [20].

At present, there are few researches combining blockchain with network public opinion at home and abroad, and even fewer researches on network public opinion governance based on blockchain technology. Nevertheless, scholars at home and abroad generally believe that the application of blockchain technology in the field of information management and network public opinion management can be expected to eliminate the spread of false information, improve the efficiency of network public opinion management, strengthen information security and privacy protection, and thus reconstruct the network information ecological environment. Deloitte pointed out in its Blockchain Frontier Research Report that the combination of Blockchain and media has a variety of possible changes, and the report affirmed the positive application of Blockchain technology in the field of information dissemination [21]. Arquam et al. [22] builds a safe and credible network information dissemination framework based on blockchain technology. By combining information blocks to create a chain, each node in the network transmits information to its peer nodes based on its reliability, and the credibility of the node will be based on Individual information changes. Zhao et al. [2] took the public opinion information on the Steemit platform as an example, adopted the social network analysis method, carried out a study on the characteristics and rules of the communication of public opinion on blockchain, and drew a research conclusion that the network public opinion communication ecology is more harmonious under the

blockchain environment. Bin et al. [23] based on the relevant research of Zhao, based on the infectious disease theory and game theory, constructed the SEIR model of network public opinion dissemination under the blockchain environment, and analyzed and explained that the incentive mechanism, benefit and risk mechanism in the blockchain public opinion network have an impact on the public opinion information dissemination. Huang and Zhao [24] study the governance optimization of network public opinion based on blockchain theory, and pointed out that blockchain technology can be applied in the traceability of online public opinion sources, public opinion fuse mechanism, and emotional early warning mechanism construction. Considering the openness and lack of supervision of social network media, malicious users often take this opportunity to spread fake news, Saad et al. [25] proposed a new blockchain system to combat the spread of fake news in social network. Wang et al. [26] established a network rumor screening model based on blockchain. Hu et al. [27] built an emergency information system based on the comprehensive technology and core characteristics of blockchain in the context of COVID-19. Lee et al. [28] designed a service reputation management system in point-to-point network based on block chain. Vivekanandan et al. [29] uses blockchain architecture to design identity information protection mechanisms for mobile users in distributed cloud environments.

To sum up, there are only a few systematic studies on the application of blockchain in the field of public opinion governance, and some scholars have applied it to the study of information dissemination. There are two main forms. One is to develop a social media platform based on blockchain in the field of media. Although this platform has been successfully put into use, it is not accepted by the public and is not a mainstream network information medium. Therefore, it is still unable to control and govern public opinion in a timely manner when the situation is grim. The other is a combination of public opinion in a blockchain environment propagation law, validation blockchain can play an inhibitory effect on public opinion spread, although such studies proved that blockchain research in the field of public opinion to control superiority, provides the reference to the research of back, but it is only a model research, did not give a system function framework based on blockchain architecture.

2.3 Consensus mechanism of blockchain

At present, the four mainstream consensus mechanisms of blockchain are PoW, PoS, DPoS and PBFT respectively. Their implementation ideas and focuses are different, but in fact, they all aim at reaching a consensus on the allocation of accounting rights.

PoW (Proof of Work) [16] was first successfully applied in Bitcoin, which gained the block accounting right through the hash operation of each node. Due to the large amount of computing power and other resources consumption, this method makes the process of data agreement very slow, resulting in significant efficiency problems. In PoS(Proof of Stake) [30], the difficulty for nodes to obtain block accounting rights is inversely proportional to the tokens held by the nodes. Tokens are the rights and interests held by the nodes in the system. Nodes that hold many tokens for a long time are striving for blocks. The easier it is to win when accounting rights, although the efficiency of block verification is improved to a certain extent, it still does not get rid of the nature of system mining. DPoS(Delegated Proof of Stake) [31] was first adopted by Bitstock (BTS), which is similar to a joint-stock company. The company generates returns for shareholders without mining, and votes according to the amount of currency held by each node, namely the equity. The one with the highest number of votes becomes the authorized witness node, which is the decision maker in the process of reaching the consensus, and then they take turns to produce and verify the block. Although efficient proof can be achieved, there are many difficulties in dealing with malicious nodes in the system. PBFT(Practical Byzantine Fault Tolerance) [32] has a strict and reliable algorithm proof, which makes the consensus participating nodes dynamic and votes according to the proportion of holding interests. It has high system throughput and availability, but it is not suitable for the blockchain network with too many nodes, and malicious nodes will cause the system to fork.

Through the comparative analysis of several mainstream consensus mechanisms, considering a series of problems caused by information asymmetry and disposal lag in the current situation of network public opinion governance, the DPoS consensus mechanism, which greatly improves system throughput at the cost of de-centrality, is relatively faster to verify and more widely applicable scenarios. Although DPoS is the fastest, most efficient, most decentralized and most scalable consensus model, the introduction of DPoS is very important for many applications that require high scalability, there are still many shortcomings in the current general DPoS algorithm. For example, in the process of voting by voter nodes, it is inevitable that there will be low enthusiasm. It may also happen that the processing of the abnormal behavior of the proxy node (abnormal voting behavior or invalid block) is not timely, which affects the security of the system data; there may also be a phenomenon that the voting cycle is too long, which will make it difficult to remove the wrong node in time, cause the stability of the system to be affected. Some scholars solve the problems of traditional algorithms by introducing additional mechanisms in the DPoS consensus mechanism. For example, Tan and Yang [33] introduced voting incentive mechanism to enhance community activity. Liu and Xu [34] optimized the dispersion degree of representative nodes in

the DPoS algorithm based on adjacency voting and average ambiguity of fuzzy values. Zhang and Ren [35] proposed the mechanism of node classification and then pairing to improve the enthusiasm of node participation in DPoS. Some scholars also introduce and improve DPoS consensus algorithm to solve problems in application for different scenarios. For example, Liu et al. [36] applied it to the donation scenario and solved the node concentration problem to a certain extent by introducing k-means clustering algorithm to optimize the selection method of proxy nodes. Wen et al. [37] quantified the difference of job completion and voting ranking before and after the change of node ranking by introducing DPoS consensus mechanism, and proposed an analysis strategy of node combination effectiveness.

This paper aims to build a collaborative governance mechanism of network public opinion based on blockchain. Aiming at the problems that have not been improved in the above-mentioned DPoS consensus mechanism, this paper improves the algorithm based on the DPoS consensus mechanism to further enhance the verification performance and block generation rate to ensure the security of blocks.

3 Functional architecture design

An ideal network public opinion governance system needs to be gradually implemented under the impetus of the competition and coordination of multiple public opinion subjects. In this process, it is necessary to avoid malicious spreading, selfishness and other irrational behaviors of the subject, and resist lies, rumors and falsehoods from the source. News also needs to give play to the supervision and incentive role of the mechanism, and stimulate the main body to actively participate in the coordinated operation of the system.

The decentralized nature of blockchain can decentralize the right of public opinion control, so that each member has equal rights and interests. Distributed architecture can guarantee data security and information sharing efficiency. Consensus mechanism can ensure the efficient opinion reached under the multi-party cooperation environment. Contract activities executed by smart contracts can automatically solve the problem of distrust between different subjects, point-to-point information sharing and transparent and open features promote the truth to be publicized, and can establish fair and transparent information exchange channels. Thus it can be seen, the blockchain with many technical advantages naturally fits with the highly decentralized network public opinion field, and can realize the autonomous mechanism of transforming from decentralization to coordination and from de-trust to intelligent trust in a complex network environment. This is in line with the innovation needs of the network environment governance model in the complex society of the current information age, so as to realize the collaborative governance mechanism of network public opinion under community co-management.

In this paper, the research on the collaborative governance mechanism of network public opinion under the blockchain framework aims to solve the main problems of improving the efficiency of consensus, reducing system overhead and ensuring the effectiveness of consensus, and applying it to the network public opinion control system in a better way. Blockchain-based network public opinion collaborative governance architecture is mainly divided into six layers, from bottom to top, the data layer, network layer, consensus layer, incentive layer, contract layer and application layer.

The data layer is the decentralized database of the system, which stores the data information generated by the behavior of the system nodes, including block data, chain structure, data signature, hash function, Merkle tree and encryption algorithm. The system security is realized based on the immutable property and the time stamp and password mechanism in this layer. The network layer is responsible for information communication, including P2P networking mechanism, data transmission and verification mechanism. The incentive layer includes the issuing mechanism and distribution mechanism of economic incentives, and encourages nodes to participate in the security verification work through incentive measures such as reward, punishment and additional income. The contract layer encapsulates the script code, algorithms and smart contracts of the blockchain system, and the contract activities executed by smart contracts can automatically solve the problem of distrust between different parties. The application layer mainly includes the front-end user interface and the system function module, which is respectively responsible for the visual UI interface and the functions of different systems.

In view of the disadvantages of the existing network public opinion information sharing, this paper uses the principle of blockchain technology to improve the design, and proposes the network public opinion governance and control model framework based on the optimized DPoS consensus algorithm. The network public opinion governance system based on blockchain trust designed here uses a consensus mechanism based on reputation voting to generate blocks and complete verification. The mechanism is mainly realized by the consensus layer. When the speech information is created and the content is changed, the storage of the data layer changes, so the network layer needs to transfer and share the data information through the P2P broadcast mechanism. At this time, the consensus layer needs to play a role to maintain the consistency of the data, and the rules formulated by the consensus algorithm need to be confirmed by the whole network. The system will deal with all the acquired information transparently, so as to realize the trusted sharing within the whole system. Inspiring the enthusiasm of nodes

to participate in the maintenance of the system is completed by the incentive layer, where the system designs the incentive layer based on the reward and punishment incentive mechanism to regulate node behavior and guide the direction of speech. When users create high-quality content, they will receive token rewards. If the node is found to have participated in the dissemination of false news after traceability verification, it will be punished by devaluation, and the trust degree will be permanently recorded. If it is the initiator of public opinion, it will lose the right to participate in the communication and cooperation in the system. The smart contract layer implements corresponding algorithm mechanism deployment for application scenarios. Through the system design, algorithms such as semantic analysis and emotion recognition are embedded in smart contracts to rectify speech in a timely manner to achieve user autonomy. When a node has abnormal behavior, or when the information transmitted is found to have the appearance of public opinion after identification, it can be traced back to the source. Even if the information generated by the release or dissemination of a node has been deleted long ago, the behavior record cannot be destroyed or denied.

To sum up, this article designs a framework for collaborative governance of network public opinion based on the blockchain infrastructure, and each part of the framework cooperates with each other to realize timely containment of false information and malicious behaviors, and then realize collaborative governance of network public opinion. The functional framework of each layer of blockchain architecture is designed, as shown in Fig. 1.

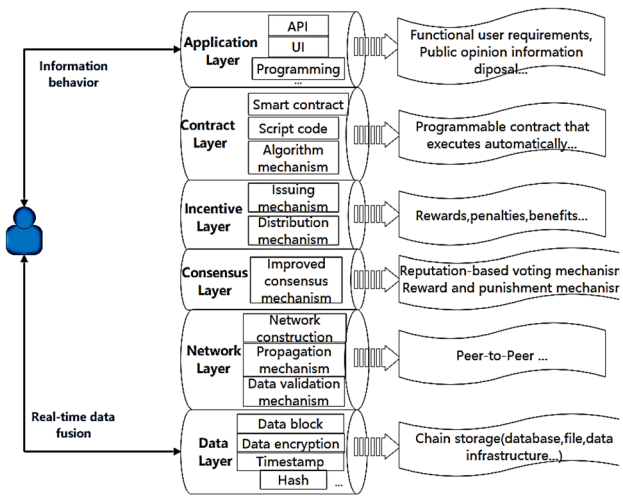


Fig. 1 Functional architecture design

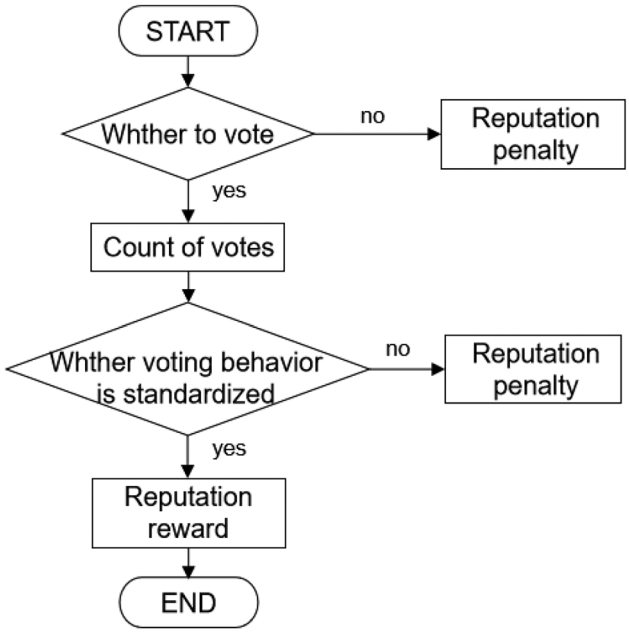


Fig. 2 The consensus mechanism process

4 DPoS consensus mechanism improvement scheme

In a complex multi-party cooperation environment, when a strong common cognition is quickly generated between subjects, that is, consensus is reached, it means that the trust crisis of false public opinion information collapses. This is the role of consensus mechanism in the cooperative and co-governance model of public opinion. The collaborative operation function of the collaborative governance mechanism of network public opinion proposed in Sect. 3 is realized by the consensus layer, and DPoS consensus mechanism with high efficiency and low consumption is selected as the core of realization. The DPoS consensus mechanism takes the elected witness nodes as the representatives of the entire alliance, and a consensus is reached between them. In fact, each block generation authority is only in the hands of a few witness nodes. As a result, DPoS consensus often has the problem that nodes are not motivated to vote, and often ignores the opposition to suspicious nodes. Therefore, it is usually difficult to avoid the selfish behavior of nodes for free and malicious behaviors such as bribery and collusion attacks in the system. If this behavior exists for a long time in the application scenario of information transmission and sharing, it will cause unpredictable security threats to the system and network environment. To solve these problems, this paper introduces a reputation voting mechanism and a reward and punishment incentive mechanism that considers time dynamics to improve the DPoS consensus algorithm. The

operating principle of this mechanism can be represented by the flowchart shown in Fig. 2.

4.1 Reputation voting mechanism based on rewards and punishments

4.1.1 Reputation voting model

The reputation value is the reputation parameter assigned by the system when a node joins the network. Considering the application environment for network information interaction, the state of a node can be regarded as a mark of a certain moment or time period of the node. Denote the reputation value of node i in the blockchain network at time t as $C_i(t)$. The system uses a [0,1] multi-value scoring system, and each time a node correctly exercises its rights, it will get 0.01 reward points. According to the behavior of nodes in the blockchain network, the reputation value is quantitatively evaluated by algorithm calculation, and the node is divided into different levels of reputation types including excellent nodes, normal nodes, selfish nodes and malicious nodes.

1. **Excellent nodes**. In the process of communication and interaction with other nodes, the excellent node can maintain the honest and reliable node behavior, and the number of effective block generation exceeds the threshold value set by the system. This type of node can ensure the correctness of data transmission in the system, maintain the reliability of the information transmission link, and have a high reputation value. The reputation value interval is divided into [0.9,1];
2. **Normal nodes**. The system defaults the state of the newly added node to the normal type, the behavior reputation value is initialized to 0.5, and the node reputation value interval in the normal behavior state is [0.5, 0.9). Nodes in normal state do not have malicious behaviors that cause bad effects on other nodes in the process of information exchange. The behavior activity of normal nodes is lower than that of excellent nodes. Normal nodes can enhance their enthusiasm under the action of incentive mechanism to obtain higher reputation;
3. **Selfish nodes**. In the actual network, some nodes have selfishness to some extent and selectively broadcast blocks for the purpose of obtaining benefits. There are selfish behaviors such as "free riding" and trying to get extra rewards. Such nodes with a series of abnormal behaviors are divided into selfish nodes. The reputation value of the node in this state is [0.25, 0.5). Although this type of node does not pose a security threat to the system, it has certain hidden dangers. To ensure the reliability of the communication chain, when the honest nodes and normal nodes in the network communication link are sufficient, try not to choose selfish nodes as communication nodes. It can be arranged at the position of the communication leaf node;
4. **Malicious nodes.** Since users in the blockchain network create new identities and generate new nodes without cost, in reality, some nodes will perform malicious behaviors to seek benefits after learning the identity information of other nodes, such as disguising false information and forwarding, generating invalid blocks, or even malicious attacks. The reputation value of the node in this state is [0, 0.25). Once a node is found to have a clear bad behavior, it is immediately classified as a malicious node.

After adding a reputation mechanism to the DPoS consensus, each node has a reputation status flag. The reputation status of excellent nodes is GREAT, the status type of Normal nodes is Normal, the status type of Selfish nodes is Selfish, and the status type of malicious nodes is Bad. Different behaviors of nodes have different effects on the reputation of nodes, and nodes can improve their reputation in the system by modifying their own behaviors. The system judges the behavior of nodes according to certain conditions. After the comprehensive reputation assessment of nodes by consensus in each round, the reputation status is dynamically updated, and the types will be transformed accordingly. The threshold value of effective block generation times of GREAT node is set as N_G, that is, the node can only become GREAT if the effective block generation times of GREAT node are at least N_G within the specified time of the system. The threshold of invalid block generation times for BAD state nodes is N_B, and the threshold for the cumulative number of malicious voting behaviors is V_B, that is, when the cumulative number of invalid blocks generated by the node reaches N_B times, or when the cumulative number of malicious voting behaviors reaches V_B, it is reduced to the BAD type.

The conditions for satisfying the state transition include:

(a) The cumulative number of valid blocks generated within the specified time of the system exceeds the threshold N_G, no invalid blocks are generated, and there is no malicious voting (i.e., voting against GREAT type nodes and NORMAL type nodes, or voting for BAD type nodes).
(b) The number of valid blocks generated within the time specified by the system but does not reach the threshold N_G, no invalid blocks are generated, and there is no malicious voting behavior.
(c) The number of valid blocks generated within a certain period of time but does not reach N_G, and no malicious voting behavior is found.
(d) Invalid blocks are generated but the number of times does not exceed the threshold N_B, or there

is an improper voting behavior but the threshold V_B is not reached.

(e) Within the specified time, the block no longer generates invalid blocks, and no malicious voting behavior is found.

(f) The number of invalid blocks generated exceeds the threshold N_B, or the number of malicious voting activities exceeds the threshold V_B.

The reputation status transition of the witness node is shown in Fig. 3.

In each round of voting and election, the nodes marked with the GREAT status are given priority as the candidate set. If the number of candidates for the GREAT status node is insufficient, the NORMAL node will be considered next. Nodes in the Great state indicate that valid blocks can be generated during multiple consensus processes. For the sake of system security, these nodes will be given priority when voting. Therefore, nodes with higher reputation values tend to have more advantages in each round of election, and it is more likely to be selected as witness nodes again. Each node with interests has the right to vote independently. The elected witness nodes take turns to participate in the generation and verification of blocks in a given order, while the other nodes are only responsible for monitoring and forwarding.

The traditional DPoS consensus algorithm usually only considers the election of witnesses by voting in support. This article also introduces the form of voting against it. The introduction of negative votes can prevent nodes with low reputation from doing evil. During the voting process, if voters find that there are abnormal nodes (i.e., nodes in the Selfish and Bad states) in the set of candidate witness nodes, they can vote against them. If the number of votes reaches the threshold set by the system, they will be removed from the set of witness nodes, and the nodes that have not been removed will replace this node according to the total number of votes.

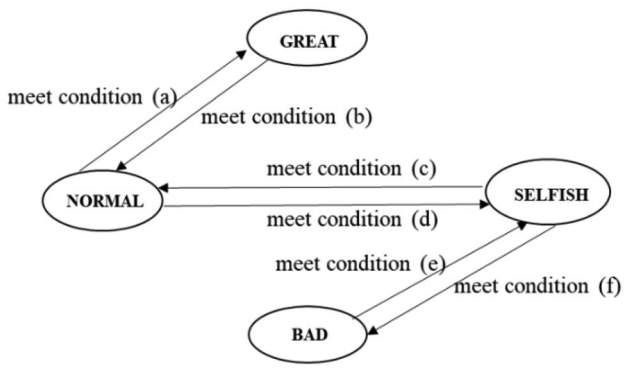


Fig. 3 Node reputation status transition diagram

4.1.2 Reputation voting mechanism based on rewards and punishments

The traditional DPoS consensus mechanism has the disadvantage of not actively voting by nodes. This paper introduces a reputation reward and punishment mechanism to encourage nodes to encourage voting nodes to actively participate in system elections to ensure consensus efficiency and achieve reputation autonomy. If the witness generates a valid block, then the rewards will be distributed to his voting nodes, including reputation value rewards and token rewards (this article mainly considers reputation rewards); if the witness node is detected malicious behavior, the reputation penalties will be assigned to its supporters. In order to avoid some nodes from delaying voting when there is no time limit, this paper considers the reputation reward and reputation penalty under the time factor to realize the reputation incentives for the nodes to improve the election efficiency. $C_i(t)$ represents the original reputation value of node i at time t, and $C_i^{'}(t)$ represents the reputation value after the reward and punishment mechanism. Timespan represents the time interval between the completion of voting by node i and the voting initiated by the system, and T is the time interval for completing voting specified by the system, which is a time constant. If the node completes voting within T, that is, when timespan < T, the reputation value of the node does not change. If the voting is overdue, the reputation value will be depleted. E represents the rate of reputation loss, which is a constant. The value of E can be adjusted according to the requirements of the specific application scenarios of the system. $R_i(E)$ represents the reputation rewards and punishments in the node voting process. The formula for calculating the reputation value of node i after reputation punishment is as follows:

$$C_i^{'}(t) = C_i(t) - \lfloor \frac{timespan}{T} \rfloor * E + R_i(E) \tag{1}$$

$$timespan = \begin{cases} \lceil T_i - T_s \rceil, & T_s \le T_i \\ \lceil T_i + 24 - T_s \rceil, & T_s > T_i \end{cases} \tag{2}$$

If the SELFISH or BAD type node that the voting node voted fails to become a witness, the voting node will be rewarded with reputation. Within the specified time period of T, a node can only exercise the right to vote against it once. If a node votes against NORMAL and GREAT nodes, or votes for SELFISH and BAD nodes, it is considered as malicious voting, the system will penalize the reputation. The formula for credit rewards and punishments is as follow:

$$R_i(E) = \begin{cases} E, \text{ Reasonable voting behavior} \\ -E, \text{ No vote or malicious vote} \end{cases} \tag{3}$$

Considering that the node's support votes, negative votes, and reputation values all have different effects on the final number of votes, a new calculation method for voting results is proposed here for the improved DPoS consensus mechanism in this paper. The formula for calculating the final number of votes for a node is as follows:

$$\text{VoteResult} = \alpha * \text{SupportVotes} - \beta * \text{AgainstVotes} + \gamma * C_i(\text{t}) \quad (4)$$

Three parameters are introduced in the improvement plan of the counting method: among them α and β are the parameters generated according to the node reputation status, which are the coefficient of support and the negative coefficient and $\alpha + \beta = 1$; γ is the reputation value coefficient, which is set according to the system service. The specific value can be set by representatives according to business characteristics and decided by voter nodes. This paper sets different values for the corresponding α and β in the four reputation states of the node: when a node is in the NORMAL state, the values of α and β are both set to 0.5, which is also the initial parameter when a new node just joins the system Value; when the node is in GREAT, $0.75 < \alpha < 1$, $0 < \beta < 0.25$; when the node is in SELFISH, $0.25 < \alpha < 0.5$, $0.5 < \beta < 0.75$; when the node is in the BAD state, $0 < \alpha < 0.25$, $0.75 < \beta < 1$. According to (4), it can be seen that for nodes in the same state, their reputation values are almost the same, and the node with more votes is more likely to become a witness node. For two nodes in different states, a node with a higher reputation value corresponds to a larger β value, which means that a node with a low reputation value needs more support votes to become a witness node. Therefore, this new calculation method of voting results ensures the fairness of the election results, thereby improving the security of the system.

4.2 Improved algorithm design

4.2.1 Reward and punishment incentive mechanism

Taking into account the time dynamics of reputation, a time loss coefficient is introduced in the node's reward and punishment incentive mechanism. According to (1), the reputation penalty of voting nodes will occur in the case of overtime voting and malicious voting. The algorithm as shown in *Algorithm 1 NodeIncentive()* is described as follows:

Algorithm 1 NodeIncentive()

Input：*T, E* // Enter the set voting time limit and reputation loss factor

Output：$C_i(t)$ // The reputation value of node i at time t

1. T_s←*starttime*，T_i←*votetime* // The time the system initiates voting and the time when node i completes the voting
2. if $T_s <= T_i$ then *timespan* = $\lceil T_i - T_s \rceil$
3. else *timespan* = $\lceil T_i + 24 - T_s \rceil$
4. if *(SupportVote is to Great or Normal Node) and (AgainstVote is to Bad or Abnormal Node)*
5. then $R_i(E) = E$
6. else $R_i(E) = -E$
7. $C_i(t) = C_i(t) - \lfloor \frac{timespan}{T} \rfloor$ *E + $R_i(E)$
8. return $C_i(t)$

4.2.2 Voting method based on reputation factor

Voting result statistics is a key step of fairness rationalization in reputation voting mechanism. In this paper, a new voting method is designed for the improved DPoS mechanism, and the reputation factor is introduced into the voting method, so that the voting result is determined by the number of votes and the reputation value based on time decay, so as to improve the scientific rationality of the election result and ensure the security of the system. The algorithm as shown in *Algorithm 2 VoteResult()* is described as follows:

Algorithm 2 VoteResult()

Input：*SupportVotes, AgainstVotes,* $C_i(t)$ //Support votes, negative votes and reputation value

Output：*VoteResult* // Final voting result

1. *support*←*SupportVotes, against*←*AgainstVotes*
2. result←VoteResult
3. if $C_i(t)$ <=1 and $C_i(t)$ >=0.9 then
4. α ← 0.875
5. β ← 0.125
6. else if $C_i(t)$<0.9 and $C_i(t)$>=0.5 then
7. α ← 0.625
8. β ← 0.375
9. else if $C_i(t)$<0.5 and $C_i(t)$>=0.25 then
10. α ← 0.375
11. β ← 0.625
12. else if $C_i(t)$<0.5 and $C_i(t)$>=0 then
13. α ← 0.125
14. β ← 0.875
15. result = α* support – β* against + γ* $C_i(t)$
16. return *result*

5 Experiment and discussion

In order to make the consensus mechanism to ensure the security and credibility of the system in the information sharing scenario, this paper conducts simulation experiments to verify whether the improved DPoS consensus mechanism will attract more nodes to vote, and whether it can reduce error nodes more efficiently and effectively. The basic environment for the simulation of this experiment selects Intel i5-1035G1 CPU 1.19 GHz processor, system memory 16 GB, 64-bit win10 system. The experiment simulation cycle is 50 times, and each cycle includes voting for agent nodes and calculating reputation value and votes. In the process of experiment, 301 independent nodes are simulated based with Python programming. And the number of consensus nodes is set as 100 in the experiment.

5.1 Comparison of the network throughput

In the blockchain system, the network throughput (i.e., Transactions Per Second, TPS) is an important indicator to measure the performance of the system. It represents the number of transactions confirmed and written into the chain in a unit time. In general, transactions are considered to be confirmed when they are packaged into blocks during the operation of consensus mechanism. The calculation method of blockchain system throughput is as (5):

$$TPS = \frac{Transactions_{\Delta t}}{\Delta t} \tag{5}$$

Among them, Δt is the length of recording time, and $Transactions_{\Delta t}$ represents the number of transactions confirmed by the system in this time period.

The higher the system throughput TPS is, the higher the data processing efficiency is under the consensus mechanism. In order to verify the performance of the system throughput, the test was repeated several times under different block generation times. We compare the original algorithm, research [33] algorithm, and changes in system throughput of this algorithm, as shown in Fig. 4.

Because the TPS of the system is related to the state of the system CPU, the initial state and the range of change of TPS are different when the three algorithms just start running. According to the TPS broken line change chart, when the block generation time is short in the initial stage of system operation, the performance of the improved algorithm does not change much. The main reason is that the amount of data transmission is small at this time, and some blocks cannot be complete the consensus within a short period of time, resulting in low system throughput. As the running time goes on, the time of block generation gradually increases, and the system throughput performance is gradually stable. It can be found that our improved consensus algorithm runtime system server unit time has been significantly higher than two other algorithms. The main reason is that the improved consensus mechanism accelerates the processing speed of the error node, improves the system data processing speed, and significantly improves system throughput.

5.2 Comparison of node participation enthusiasm

The proportion of the number of nodes participating in the system is taken as the active degree of nodes participating in voting. The experiment set the initial proportion of nodes participating in voting to 50%. After 50 rounds of voting, the number of nodes participating in the voting changes as shown in Fig. 5.

According to the analysis of the fold line, it can be seen that when voting in accordance with the original DPoS consensus mechanism, the proportion of participants is between 40%–50%. After the introduction of the reward and punishment, the algorithm is improved, with the increase of the

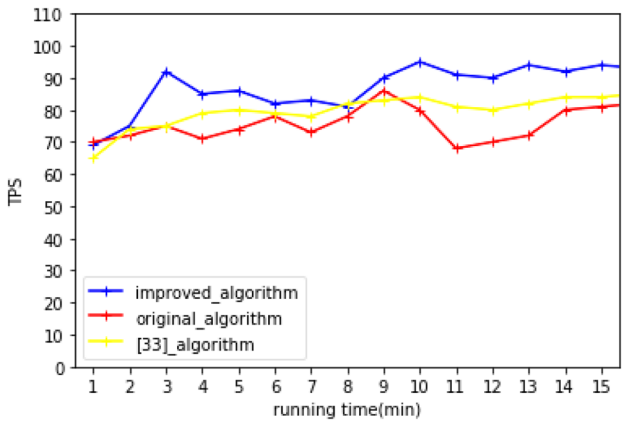


Fig. 4 Throughput variation

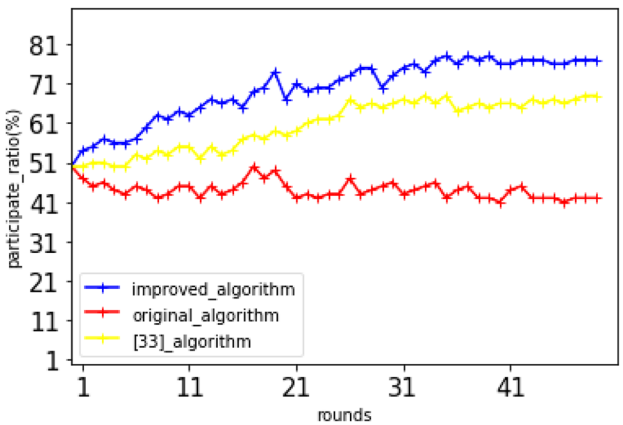


Fig. 5 Variation of the proportion of participants

number of voting wheels, the number of nodes involved in voting is increasing, and it is finally maintained between 70%–80%. It can also be seen from the picture that this result is also improved than the performance of the study [33] with the result of mainly from 60%–70%. Therefore, this paper improves the improvement of the DPoS algorithm to improve the enthusiasm of the node involved in the system, thereby increasing the efficiency of the consensus, that is, the efficiency of generating blockage information is greatly improved. Studies have shown that this consensus mechanism can be applied to public opinion in public opinion governance.

5.3 Comparison of the proportion of error nodes

After the witness node is selected in the first round of voting, if a wrong block is generated during the process of generating a block or a valid block is not generated within the specified time, it is considered an error node (including selfish nodes and malicious nodes). Under the action of the reward and punishment incentive mechanism, they are punished by reputation. According to the voting results, new verification nodes are generated, and the proportion of error nodes in the three DPoS consensus mechanisms are compared and analyzed. After 50 rounds of voting, the proportion of error nodes changes as shown in Fig. 6.

According to the comparison diagram analysis of the line, our improved DPoS consensus mechanism tends to stabilize in the seventh round, while the other two algorithms have a large fluctuation in the experiment. The results show that we have improved the stability of the system after the improvement of the algorithm. This experiment is set to compare the comparative analysis under conditions having a high fault tolerant rate, so the number of fault nodes of the subsequent cycle fluctuate between 0 to 2. If the mechanism can eliminate all fault nodes more quickly in an environment with a lower fault tolerant rate. The experimental results show that the improved DPoS mechanism with the reward and punishment Mechanism can eliminate the wrong node more quickly. When the error node reaches 50%, it can also significantly reduce the probability of the error node into witnesses. A large number of reduced error nodes ensure the maintenance of system trust in system trust, thereby increasing the security of the entire system. Therefore, this paper improves the existence of the DPoS algorithm to reduce the existence of the error node, improve the security and stability of the system, indicating that this consensus mechanism can resist malicious public opinion information in public opinion governance scenarios.

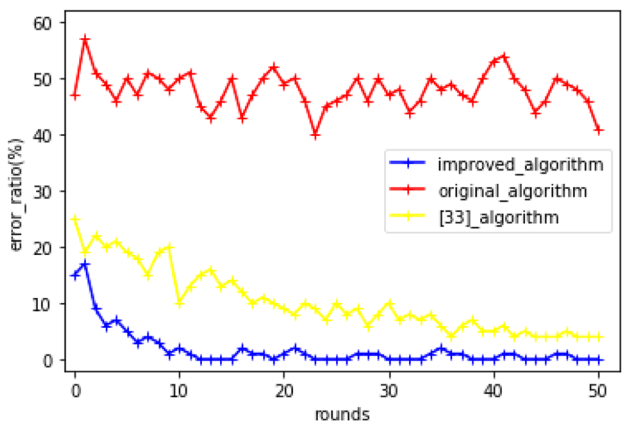


Fig. 6 Variation of the proportion of error nodes

6 Conclusion and prospect

As an emerging information technology in recent years, blockchain can achieve collaborative trust and consensus among multiple subjects, naturally fits with the highly decentralized public opinion field, and is expected to bring technological breakthrough innovations to the governance of network public opinion.

In order to solve the shortcomings of network public opinion governance under the new social situation, this paper proposes a functional framework of network public opinion collaborative autonomy mechanism based on blockchain, so that users in the system have equal rights and realize collaborative autonomy, and spontaneously carry out various node behaviors to obtain rights and interests. Based on the system's requirements for timeliness and safety of information sharing under the situation of public opinion governance, the consensus algorithm is improved. This paper introduces a reputation model to ensure the maximum trust and reliability of information interaction in the system. Aiming at the disadvantages of the original DPoS consensus mechanism, such as laziness in nodal voting and failure to remove the wrong nodes in time, the reputation voting mechanism and the reward and punishment incentive mechanism are designed.

The simulation results show that, after the improvement of DPoS consensus mechanism, not only the enthusiasm of nodes to participate in voting is significantly improved, the proportion of wrong nodes in the system is significantly reduced, but also the system throughput is improved. It shows that this mechanism can make the system to efficiently produce reliable and efficient blocks, avoid malicious nodes become witnesses, which not only guarantee the system safety and stable operation, and can improve the trust between nodes in the process of information transmission problems, and solve the traditional problem such as slow network public opinion rigid governance mode. The introduction of the reputation mechanism can make the consensus

mechanism suitable for public opinion governance scenario, which can not only stimulate the participation of voters, but also make the information behavior of the witness nodes more honest, so that participants can face up to their own behavioral norms in the process of information transmission, and further solve the problem of lack of trust in information behavior.

Nevertheless, the optimization of public opinion governance through the consensus mechanism only starts from the perspective of the participants, but cannot change the ontology of public opinion. Therefore, in addition to improving the consensus algorithm, it is also necessary to combine blockchain with big data and artificial intelligence to trace, identify and warn the public opinion information ontology. Our future research focuses on embedding relevant algorithms into the automatic execution of smart contracts, continuing to improve the collaborative governance mechanism of network public opinion, so as to curb the spread of false public opinion from the source. From the perspective of technical performance, the communication delay of blockchain is a major bottleneck, which is also a problem to be considered in our next research.

Acknowledgements This research was supported in part by the National Social Science Foundation of China (No. 21BGL001), the National Natural Science Foundation of China(71701115), Shandong Natural Science Foundation (ZR2020MG003), Special Project for Internet Development of Social Science Planning Special Program of Shandong Province (17CHLJ23).

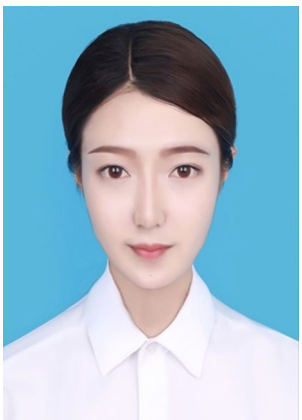
Declarations

Competing interest The author(s) declare no competing financial interests.

References

1. Hou BZ (2019) Research on Self-organization Evolution of Internet Public Opinion from the Perspective of Synergetics. Technol Int Eng 5(04):53–61
2. Zhao D, Wang XW, Han JP, Yang WC (2018) Research on the Propagation Characteristics and Rules of Network Public Opinion Information in Blockchain Environment. J Intelligence 37(09):127-133+105
3. Liu Yi (2007) On the concept, characteristics, expression and dissemination of network public opinion. Theory Horizon 01(1):11–11
4. Zhang YL (2012) Causes and Control Strategies to the Network Public Opinion of Emergencies: Psychological Analysis of Their Subjects. J Intelligence 31(04):54–57
5. Shang HL (2016) The Dilemma of Government Governance of Internet Public Opinions and Its Resolution. Administrative forum 23(02):59–62
6. Yu YY, Wu Q, Yu Y (2020) Exploration of Multiple Source of Network Public Opinion Data Based on Blockchain Incentive Mechanism. Cult Commun 9(02):63–67
7. Liu W (2016) On the Thoughts and Countermeasures of Network Public Opinion Governance in the Transitional Period. Theory and Reform 03:93–101
8. Christen CT, Huberty KE (2007) Media Reach, Media Influence?. The effects of Local, National, and Internet News on Public Opinion Inferences. J Mass Commun Q 84(2):315–334
9. Arunachalam R, Sarkar S (2013) The New Eye of Government: Citizen Sentiment Analysis in Social Media. Sixth International Joint Conference on Natural Language Processing 23
10. Cui P, Zhang W, He Y (2018) Dynamic Evolution Research on the Government's Response Capability to the Public Opinions in the Context of Public Emergencies. J Modern Inf 38(02):75-83+95
11. Wang LF, Han JL (2018) Constructing Network Integrated Governance System: An Effective Way to Deal with Network Public Opinion Governance Risk. Theory Monthly 8:182–188
12. Sun RY (2020) Research on the Self-organizing Evolution Mechanism of Coordinative Punishment Governance of Network Public Opinion. J Modern Inf 40(05):122-129+168
13. Zhu YH (2008) Review of the evolvement of information system & its development trend. Inf Studies Theory Appl 04:631–636
14. Dong QL (2014) Multi-player cooperationism and cyber security governance. World Econ Politics (11):52–72,56–157
15. Ma FC, Li XY (2014) Study on the Structure and Evolution of China's Internet Content Regulation Actors. Journal of the China Society for Scientific and Technical Information 33(5):452–464
16. Natamoto S (2008) Bitcoin: a Peer-to-Peer Electronic Cash System, [2018–6–11]. https://bitcoin.org/bitcoin.pdf
17. Dori A, Steger M, Kanhere SS et al (2017) Blockchain: A distributed solution to automotive security and privacy. IEEE Commun Mag 55(12):119–125
18. Lee B, Lee JH (2017) Blockchain-based secure firmware update for embedded devices in an Internet of things environment. J Supercomput 73(3):1–16
19. Peck ME (2017) Blockchain world-Do you need a blockchain? This chart will tell you if the technology can solve your problem. IEEE Spectr 54(10):38–60
20. Eyal I (2017) Blockchain technology: Transforming libertarian cryptocurrency dreams to finance and banking realities. Computer 50(9):38–49
21. Deloitte (2018) Blockchain: A Media Game Changer. IBM Watson Advertising (6)
22. Arquam M, Singh A, Sharma R (2018) A blockchain based secure and trusted framework for information propagation on online social networks. Comput Sci 62(4):1157–1164
23. Bin S, Sun GX, Zhou S (2019) Public opinion propagation model in social network based on blockchain. J Appl Sci 37(2):191–202
24. Huang XH, Zhao B (2019) Research on optimization of network public opinion based on blockchain technology. Sci Technol China's Mass Media 1:48–51
25. Saad M, Ahmad A, Mohaisen A (2019) Fighting Fake News Propagation with Blockchains. 2019 IEEE Conference on Communications and Network Security (CNS), IEEE
26. Wang XW, Zhang L, Huang B, Wei YN (2021) Study on Detection Model and Simulation of Internet Rumor Based on Blockchain. J Intelligence 40(02):194–203
27. Hu J, Zhu P, Qi Y (2022)Construction of emergency intelligence system for major public health events based on blockchain. Inf Theory Pract: 1–13. http://kns.cnki.net/kcms/detail/11.1762.G3.20211122.1450.006.html
28. Lee YJ, Lee KM, Lee SH (2020) Blockchain-based reputation management for custom manufacturing service in the peer-to-peer networking environment. Peer-to-Peer Netw Appl 13(2):671–683
29. Vivekanandan M, Sastry VN (2021) Blockchain based privacy preserving user authentication protocol for distributed mobile cloud environment. Peer-to-Peer Netw Appl 14(3):1572–1595

30. Larimer D (2013) Transactions as Proof-of-Stake. http://7fvhfe.coml.z0.glb.clouddn.com/@/wpcontent/uploads/2014/01/TransactionsAsProofOfStake10.pdf
31. Larimer D (2014) Delegated Proof-of-Stake Whitepaper. http://www.bts.hk/dpos-baipishu.com
32. Gan J, Li Q, Chen ZH, Zhang Z (2019) improvement of blockchain practical Byzantine fault tolerance consensus algorithm. J Comput Appl 39(07):2148–2155
33. Tan SP, Yang C (2019) Research and Improvement of Blockchain's DPoS Consensus Mechanism. Modern Comput (Professional Edition) 6:4
34. Liu Y, Xu G (2021) Fixed degree of decentralization DPoS consensus mechanism in blockchain based on adjacency vote and the average fuzziness of vague value. Comput Netw 199:108432
35. Zhang YP, Ren XL (2021) DPoS consensus mechanism based on pairing system. Comput Appl Res 38(10):2909–2914
36. Liu W, Li Y, Wang X et al (2021) A donation tracing blockchain model using improved DPoS consensus algorithm. Peer-to-Peer Netw Appl 1–12
37. Wen XL, Li CL, Zhang XY, Liu SS, Zhu M (2022) Visual Analysis Method for Community Evolution Based on DPOS Consensus Mechanism. Com Sci 49(01):328–335



Yuetong Chen is a graduate student whose main research area is information management and application of blockchain technology. Mailing address: No. 88 Wenhua East road Jinan Shandong Province China.

Fengming Liu is the professor serves for the School of Management Science and Engineering, Shandong Normal University, and is the doctoral supervisor and Assistant Dean. My research focuses on Social Network and Game Theory, Information Security and Public Opinion to Control, Quantum Information and Quantum Optimizing. Mailing address: No.88 Wenhua East road Jinan Shandong Province China.