Advances in Computer Science Research, volume 86
International Symposium on Communication Engineering & Computer Science (CECS 2018)

Interpretation of Consensus Mechanism in Block Chain and Its Future Development Trend

Sirui Yang [a]
Yali Middle School, ChangSha 410007, China
[a]1292451442@qq.com

Abstract. At present, block chain has become a data thinking mode. In view of the decentralization characteristic of block chain, the consensus mechanism emerges, which to guarantee the generation of valuable data and information in a friendly, democratic and open form. Firstly, the position and role of consensus mechanism in the block chain are defined; secondly, the evaluation criteria and specification of consensus mechanism are grasped; thirdly, the algorithms of consensus mechanism are analyzed and compared; finally, the future development trend of consensus mechanism is predicted. Through the analysis of the above consensus mechanism, consensus mechanism plays a very important role in the process of the continuous change and innovation of block chain technology; at the same time, it also enhances its robustness, universal applicability and artificial intelligence.

Keywords: Block chain; consensus mechanism; evaluation criteria; consensus mechanism algorithm.

1. Interpretation of the Background of Consensus Mechanism

Currently, the "consensus mechanism" is mainly emerging in the application process of block chain [1]. In order to fully understand the consensus mechanism, block chain is first objectively recognized [2]. The essence of block chain is data, and its operation behavior is characterized by "distributed and decentralized". The premise of its operation behavior is consensus. Its behavior motivation is that the data on the chain generates value and exchanges according to market value. Its behavior risk management relies on encryption to realize information tampering prevention.

Generally speaking, to achieve a certain purpose in the form of block chains, it is necessary to reach a consensus in the process of its implementation before carrying out specific work, and then on the basis of consensus iteration and statistical data to form an application-oriented consensus mechanism [3,4]. On the one hand, the consensus mechanism has been constantly improved, on the other hand, the consensus mechanism guarantees the healthy development of the connotation and extension of block chain.

2. Evaluation Criteria and Specification of Consensus Mechanism

The purpose of the consensus mechanism is to serve block chain. In order to maintain the smooth development of its own work, the consensus mechanism should first formulate standards, and then formulate the consensus behavior specification based on the standards.

2.1 Evaluation Criteria of Consensus Mechanism

Different consensus mechanisms are adopted on block chain, which will have different impacts on the overall performance of the system while satisfying the consistency and effectiveness [5,6]. Considering the characteristics of each consensus mechanism, the evaluation criteria of the consensus mechanism are discussed from the following four dimensions, shown in Fig.1.

Copyright © 2018, the Authors. Published by Atlantis Press.
This is an open access article under the CC BY-NC license (http://creativecommons.org/licenses/by-nc/4.0/).

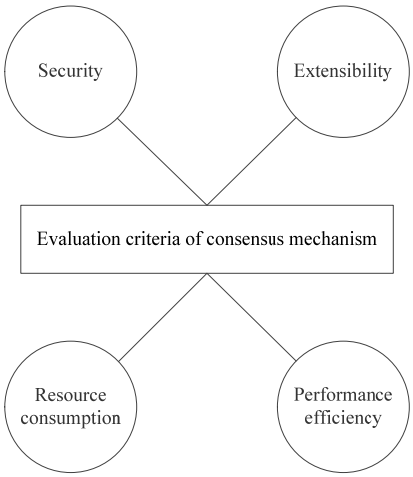

Fig.1 Evaluation criteria of consensus mechanism

2.1.1 Security

The security question is whether it can prevent secondary payment, self-propelled mining and other attacks, and whether it has good fault tolerance. In the process of realizing consistency in block chain system driven by financial transactions, the most important security problem is how to prevent and detect the secondary payment behavior. By adopting appropriate strategies to publish its own generated blocks and to obtain higher relative benefits, selfish mining is a theoretical attack method that threatens the security and fairness of the Bitcoin system. In addition, the Eclipse attack controls the network communication of the target object, forming a network partition and blocking the spread of the transaction. Sybil attack affects system security by producing a large number of meaningless nodes.

2.1.2 Extensibility

The extensibility issue is whether to support network node expansion. Extensibility is one of the key factors to be considered in block chain design. According to different objects, extensibility can be divided into two parts: the increase of the number of system members and the increase of the number of transactions to be confirmed. When the number of system members and transactions to be confirmed increases, the system load and network traffic changes. So, Extensibility should be considered.

2.1.3 Performance Efficiency

Performance efficiency problem is the time delay problem from the transaction consensus being recorded in block chain to the final confirmation. Unlike traditional third-party supported trading platforms, block chain technology is agreed through a consensus mechanism, so its performance efficiency issues have always been the focus of research.

2.1.4 Resource Consumption

In the process of reaching consensus, resource consumption refers to the amount of computing resources, including CPU, memory and so on. Consensus mechanisms on block chain reach consensus through computing resources or network communication resources. Taking the Bitcoin system as an example, the consensus based on the workload proof mechanism needs to consume a large amount of computing resources for mining to provide a certificate of trust to complete the consensus.

2.2 Specification of Consensus Mechanism

The specification of the consensus mechanism is a process of continuous clarification and improvement through a number of rules of the consensus mechanism. In view of the application background of consensus mechanism in different application scenarios, the specification of consensus

mechanism includes four parts: the purpose of consensus, the protocol of consensus, the behavior of consensus, and the object of consensus.

At the same time, the specification of consensus mechanism is subject to the basic decision parameters of consensus mechanism in Fig.2. The basic determination parameters of the specific consensus mechanism are described below.

a. Decentralized governance: A single central authority cannot provide the irreversibility of transactions;

b. Node structure: nodes can exchange information through established ways, which can be divided into stages or levels.

c. Authentication: this process verifies the identity of the participant;

d. Integrity: the integrity of the transaction is verified, such as by means of an encryption algorithm;

e. Non-repudiation: Verification assumes that the sender did send the message;

f. Privacy: It's ensured that information is accessible only to established recipients;

g. Fault tolerance: Even if some nodes or servers fail or run slower, the network can run efficiently and quickly;

h. Performance: it includes throughput, real-time, scalability and latency.

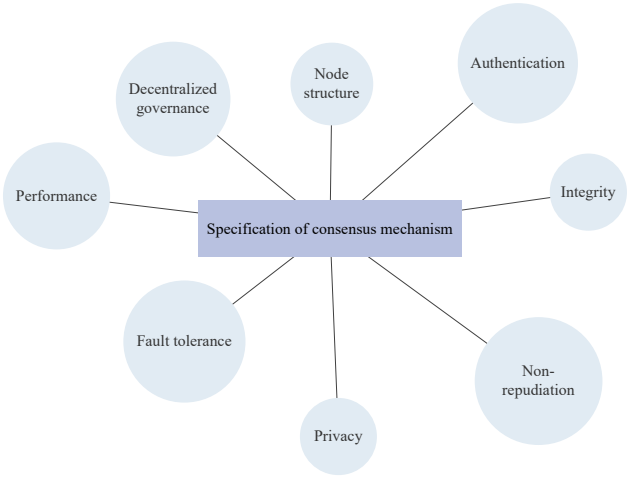

Fig .2 Restrictive factors of consensus mechanism specification

3. Introduction and Comparison of Consensus Mechanism Algorithms

The consensus mechanism algorithm is a way to achieve consensus mechanisms. According to different application backgrounds of block chain, it can be roughly divided into Proof of work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS), Verification Pool (VP), practical Byzantine fault tolerance (PBFT) and authorized Byzantine fault tolerance (ABFT) [7,8].

3.1 Consensus Mechanism Algorithm

3.1.1 PoW

The PoW mechanism is a consensus mechanism for the Bitcoin system [9]. By designing and introducing computational competition among distributed network nodes, data consistency and consensus are guaranteed. All participating network nodes traverse to find a random number to ensure that the double SHA256 result of the current block head is less than or equal to a certain value. Once a node finds a random number that meets the requirements, the node obtains the billing rights of the current block and a certain amount of bitcoin as a reward.

The PoW consensus mechanism links the issuance, trading, and recording of Bitcoin, and also ensures the randomness of billing rights and the security and decentralization of the Bitcoin system.

3.1.2 PoS

PoS essentially uses the proof of stake instead of the proof of work [10]. The billing right is obtained by the node with the highest stake, not the node with the highest computing power. The ownership of a specific amount of currency by a representative node is called the age of currency or the number of days of currency. The currency age is equal to the number of currencies multiplied by the length of the last transaction.

Systems using the PoS consensus mechanism have a limited age at a particular time, and long-term holders have a longer currency age, so the age of the currency can be considered as an stake in the system. The difficulty of the consensus process is inversely proportional to the age of the currency, so that the block with the highest cumulative consumption of the currency will be linked to the main chain. By relying only on the age and rights of the internal currency, the problem of PoW consuming computational power is solved.

3.1.3 DPoS

On the basis of PoS, DPoS specializes the role of biller. The bookkeeper is first elected on the basis of an equity vote and then rotated among the biller. All holders vote for a certain number of nodes. The selected nodes proxy them for verification and accounting, and the biller must guarantee 90% online. Each node in the consensus mechanism is able to autonomously determine the authorization nodes it trusts, and new blocks are generated by these nodes in turn.

3.1.4 VP

The VP is built on traditional distributed consistency technology and is complemented by a data validation mechanism.

3.1.5 PBFT

This is a consistency algorithm based on message passing. The algorithm reaches agreement through three stages, which may be repeated because of failure. In the case of $N \geq 3F + 1$, consistency is possible, where N is the total number of computers and F is the total number of computers in question. After the information is exchanged between computers, each computer lists all the information obtained, with most of the results as a solution. As long as 2/3 of the nodes in the system are properly working, consistency can be guaranteed.

3.1.6 ABFT

On the basis of using Byzantine fault tolerance algorithm, the request response model of C/S architecture is improved to a peer node model suitable for P2P network by ABFT. The static consensus participation node is improved to dynamically enter and exit consensus participation node; a voting mechanism based on the proportion of holding interest is designed for the generation of consensus participation nodes, and consensus participation nodes are determined through voting. The introduction of digital certificates in the block chain solves the problem of authenticating the real identity of billing nodes in voting.

3.2 Comparison of Advantages and Disadvantages of Consensus Mechanism Algorithm

In order to better satisfy the use of block chain for specific scenarios, the advantages and disadvantages of the above consensus mechanism algorithms are summarized and compared, as shown in table 1.

Table 1. Comparison of advantages and disadvantages of consensus mechanism algorithm

No.	Name	Advantage	Disadvantage
	Pow	Completely decentralized, nodes freely in and out	Waste of energy, the confirmation time of the block is difficult to shorten
	PoS	To some extent, shortened the time for consensus to reach; no longer need to consume a lot of energy	Participants who have rights and interests may not want to participate in accounting or mining.
	DPoS	A substantial reduction in the number of participating verification and accounting nodes can reach the second level consensus verification.	The whole consensus mechanism still depends on tokens. Many commercial applications do not need tokens.
	VP	No tokens are required to work, and seconds consensus verification is implemented on the basis of mature distributed consistency algorithms	The degree of de centralization is not as good as bitcoin; it is more suitable for multi-party business models.
	PBFT	People who vote can be tolerated as traitors or non-responders	Fault-tolerant nodes have limitations
	ABFT	A professional biller; Tolerating any type of error; biller is done by multiple people working together. Each block has finality and does not branch; The reliability of the algorithm has strict digital proof.	When one-third or more billers stop working, the system will be unable to provide services; When a third or more of the biller s are combined for evil and all the other billers are split into two network islands, a malicious biller can branch the system, but leave cryptographic evidence.

4. The Future Development Trend of Consensus Mechanism

In order to play the role of consensus mechanism more energy-efficiently, the development trend of future consensus mechanism will focus on the optimization of security, extensibility, performance efficiency and resource consumption.

The future form of consensus mechanism should be a middleware that can switch application scenarios at will. The specific manifestations are as follows: the algorithm of the consensus mechanism is constantly improved, the behavior of the consensus mechanism is increasingly endowed with artificial intelligence attributes, and the protocol of the consensus mechanism will be universal by means of repeated verification of big data.

References

[1]. Zhang Y, Xiao-Hui L I. The research and implementation of an improved blockchain's consensus mechanism [J]. Electronic Design Engineering, 2018.

[2]. Shen X, Pei Q Q, Liu X F. Survey of block chain [J]. Chinese Journal of Network & Information Security, 2016.

[3]. Mattila J. The Blockchain Phenomenon – The Disruptive Potential of Distributed Consensus Architectures [J]. Etla Working Papers, 2016.

[4]. Zheng Z, Xie S, Dai H, et al. An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends[C]// IEEE International Congress on Big Data. IEEE, 2017.

[5]. Younes A, Hilden P, Coiffier B, et al. International Working Group consensus response evaluation criteria in lymphoma (RECIL 2017) [J]. Annals of Oncology, 2017, 28(7):1436.

[6]. Harris-Huemmert S. Establishing evaluation criteria: reaching consensus on the notion of quality in German Educational Science [M]// Evaluating Evaluators. VS Verlag für Sozialwissenschaften, 2011:191-211.

[7]. Weng S, Yue D, Huang C. Distributed Economic Dispatch Based on Consensus Algorithm Under Event-Triggered Mechanism[M]// Intelligent Computing, Networked Control, and Their Engineering Applications. 2017.

[8]. Yoo S E, Lee B J, Kim K T, et al. Block chain-based consensus algorithm[C]// Korean Society of Computer Information Conference. 2018.

[9]. Wang S, Qin B, Chen J, et al. Blockchain Estimation Model Based on PoW Mechanism [J]. Journal of Cyber Security, 2018.

[10]. Li W, Andreina S, Bohli J M, et al. Securing Proof-of-Stake Blockchain Protocols [J]. 2017.