Research on the Consensus Mechanisms of Blockchain Technology

Ying Zhao[1, a]

[1]Shandong labor vocational and technical college, China

[a]zhaoying@sdlvtc.cn

Keywords: blockchain; consensus mechanism; proof of work; proof of stake; Byzantilne consistency

Abstract: As the underlying technology in Bitcoin, the blockchain technology has gained wide attention. Blockchain is a kind of feasible method to solve the consistency problem of distributed system. Consensus mechanism is the core of the blockchain technology. Delicate consensus mechanism can improve system performance and promote the application of blockchain in many fields. Based on the consensus mechanisms in existing design of blockchain, this paper summarizes the basic consensus mechanisms including proof of work, proof of stake and Byzantine consistency agreement, and evaluates them from various aspects such as security, scalability, performance, etc. The future research on the blockchain consensus mechanism will be based on the different characteristics of the consensus mechanisms, and design should be carried out around the combination of different consensus mechanisms.

1. Introduction

Blockchain technology was originally proposed by Satoshi Nakamoto in article--*Bitcoin: A P2P E-cash Payment System*, bringing new technical ideas to solve the consistency problem of distributed systems. Consensus mechanism is the core of distributed system.

In P2P network, it is called consensus that the nodes that distrust each other finally achieve data consistency through following the preset mechanism. The key to the design of blockchain technology is the design of consensus mechanism, which aims at solving the security, extensibility, performance efficiency and energy cost of blockchain. The typical consensus mechanisms supported by blockchain technology include Proof of work, Proof of stake and Byzantine agreement of consistency, as well as the combination of different mechanisms.

2. Overview of Blockchain Technology

2.1 Basic Concepts

China Blockchain Technology and Application Development White Paper (2016) regarded the blockchain technology as an innovative application model in the Internet era from the application point of view, is a kind of a decentralized, open and transparent database for storing information such as transactions, it can be used in distributed data storage, point-to-point transmission, consensus, encryption algorithm, and other areas of the computer technology. Information such as transactions are stored in blocks which go back and forth to form a chain and store a series of orderly transactions together. Figure 1 takes the bitcoin system as an example to introduce the data structure of the underlying blockchain. Because the upper consensus mechanism is different, the corresponding blockchain data structure is also slightly different.

  DOI: 10.25236/icefbd.18.062

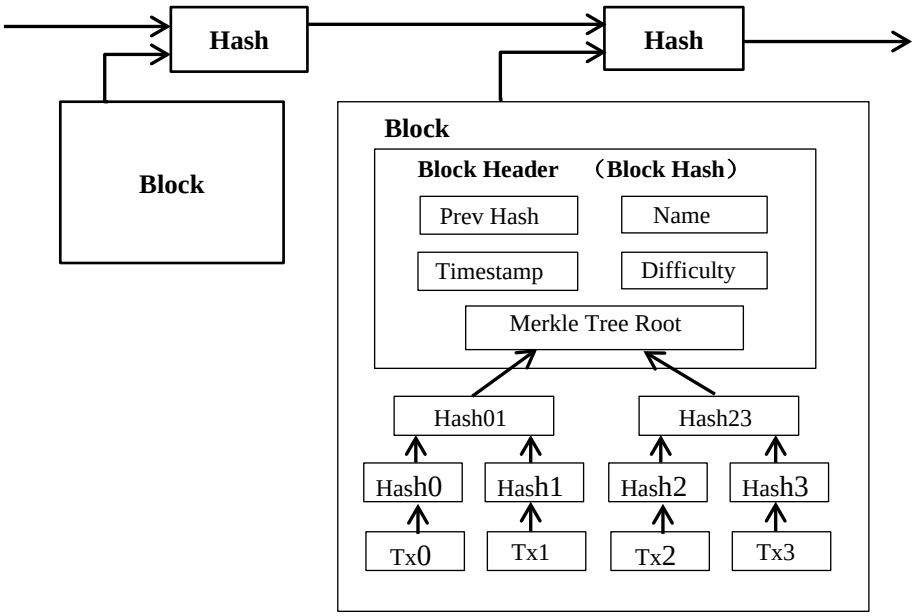

Figure 1. Data structure of blockchain technology in bitcoin system

In the blockchain, except for the continuity between blocks, every change in data is stored on the blockchain by a legitimate digital signature. The blockchain records every change in a piece of data from generation to death, providing traceability. Data traceability also indirectly ensures data transparency.

2.2 Application Scenarios

At present, there are many projects combining blockchain technology and financial industry, especially since the second generation of smart contract on blockchain technology was proposed, the advantages of blockchain technology in solving financial payment, settlement and liquidation business across institutions and industries have become increasingly prominent. In addition, blockchain technology has great potential value in financial services, supply chain services, public services, public philanthropy and the Internet of things. Table 1 shows the application scenarios of blockchain technology in some industries.

Table 1 Application Scenarios of blockchain technology

Industry	Application Examples
Financial services	Financial Transaction Payments (Inter-agency, Cross-border Payments), Settlement, Liquidation, Insurance. Securities, Crowdfunding
Supply Chain Service	Supply chain Finance, Supply chain trace
Public Service	Intellectual property rights protection, copyright protection, sharing economy, file management, identity certification, digital medical records
Public Charity	Public donation platform, donation tracking and management
IoT (Internet of things)	Tracing, tracking, counterfeiting and certification of goods

3. Consensus Mechanism

3.1 Concepts

As a data structure that stores in chronological order, blockchain can support different consensus

mechanisms. Consensus mechanism is an important component of blockchain technology. The goal of it is to enable all honest nodes to keep a consistent blockchain view while satisfying two properties:

1) Consistency.

All honesty nodes save blockchain with exactly the same prefix.

2) Validity.

The information published by one honest node will eventually be recorded by all other honest nodes in their own blockchain.

3.2 Workload Certificate

The consistency of blockchain can be achieved by using the workload proof mechanism. When the blockchain is very long, except for the last few blocks, the rest have been confirmed by the whole network and the consistency has been achieved. The node can freely join the blockchain and the addition or withdrawal of the node will not affect the consistency and security of the blockchain. The probability of each node to complete the work that is determined by its computational resources, the attacker cannot increase the probability of completing the proof by creating multiple public key addresses, this can effectively fend off Sybil attacks. At the same time, with the majority of computing resources owned by the honest party, it can effectively resist secondary payments and guarantee the security of the system.

3.3 Equity Certificate

Interest mechanism to a certain extent, solve the workload prove that the problem of large energy consumption of the mechanism, shortened the time of block and set the time, improve the efficiency of the system, but there are no perfect blockchain based on interest in practical application. The equity certificate shows that each round produces multiple verified representatives, that is, multiple blocks. In the case of poor synchronization of the network, the system is easy to generate bifurcation and affect the consistency. If the malicious node becomes the representative, the network partition will be formed by controlling network communication. Sending different undetermined blocks to different network partitions will result in network bifurcation, which can be used for secondary payment attacks, seriously affecting system security. A malicious adversary can also bribe an honest representative to undermine consistency. The key of equity certification lies in how to choose the right equity and construct the corresponding verification algorithm to ensure the consistency and fairness of the system. Improper rights and interests will affect the fairness of the system. PPCoin, for example, USES the currency of age as a factor, rights and interests of in the if part of the node in the system remain used to pay for part of the small and the currency of age is big enough, the node is more likely to be selected as the representative, affect system fairness.

3.4 Byzantine Agreement of Consistency

The Byzantine conformance protocol was originally used for small-scale server replication problems, and later expanded to dozens of servers. The Byzantine agreement protocol mainly studies how to achieve the agreement of all the correct nodes to a certain input value in a distributed system with wrong nodes.

In the case of decentralization, the Byzantine consistency protocol can be used to achieve the consistency of blockchain, eliminate the redundant computation and avoid resource waste. In addition, at some point, there is only one master node can put forward the new blocks, the other nodes on the block, avoid points again, shortening the time of the transaction confirmation and block, improve the efficiency of the system.

3.5 Combination of Consensus Mechanism

To the existing blockchain work certificates, certificate of rights and interests and Byzantine agreement mechanism such as consensus from consistency, security, scalability, performance, efficiency, resource consumption, etc, this paper compares and analyzes their application in blockchain on the advantages and disadvantages are shown in table 2.

Table 2 Comparison of Consensus Mechanism on Blockchain

Consensus Mechanism	Consistency	Safety (Fault Tolerance)	Expansibility	Performance Efficiency	Resource Consumption
proof of work	Split Ends	<50%	Poor	High	High
proof of stake	Split Ends	<50%	Good	latency Low	Low
Byzantine Agreement of Consistency	No Split Ends	<33%	Poor	latency Low latency	Low

In view of the advantages and disadvantages of each consensus mechanism, we can try to combine different consensus mechanisms to form a new obstacle of consensus mechanism.

1) Combination of Workload Certification and Equity Certification

When the proof of work mechanism is adopted, the nodes can obtain higher relative benefits through the selfish mining strategy, which affects the fairness and security of the system.2-hop blockchain tries to combine workload certification and equity certification, and use equity certification mechanism to reduce system resource consumption and improve fairness and security. The system takes wheel as the unit, each round contains the workload proof stage and the equity proof stage. In the proof of work stage, the node tries to complete the workload certification and proposes a new block. Then, the equity certification stage is entered, and the new block is verified and confirmed by the node that has completed the equity certification. Through the alternation of workload proof and equity proof, the security of the system can be guaranteed even if there is a node with a large amount of computing resources. At the same time, the influence of nodes with dominant computing resources on blockchain in the initial state is weakened, and the security and fairness of the system are further improved.

2) Byzantine Consistency and Proof of Interest

Algorand system, for example, consider the Byzantine agreement, poor scalability problems Algorand system combining proof mechanism and Byzantine agreement, to participate in the Byzantine agreement through interest in limiting the number of nodes, in order to improve the scalability of the system. First, the node verifies whether it is selected as the representative through the equity certification mechanism, and the verified node can propose the undetermined block. Then, a new round of equity certification is carried out to select new representatives to verify the validity of the pending blocks. After a limited rotation, the question of representation was agreed upon on the highest priority blocks through the Byzantine agreement. Through interest elected representatives, effectively solved the Byzantine agreement of scalability and efficiency, at the same time use the Byzantine agreement to avoid the interest bifurcation weakness, improve the consistency and security.

4. Conclusion

As a crucial component of blockchain technology, consensus mechanism has attracted much attention from academia and the business community. Good consensus mechanism is beneficial to the spread of blockchain technology in theory and practice. However, the existing consensus mechanism for blockchain technology is not perfect.For the analysis of consensus mechanism in blockchain technology, it can be considered from the aspects of consistency, security, extensibility, performance efficiency and resource consumption. Improvement and combination of basic consensus mechanisms such as workload certification, equity certification and Byzantine agreement is the research focus of future consensus mechanism.

References

[1] EYAL I, GENCER A E, SIRER E G, et al. Bitcoin-NG:A Scalable Blockchain Protocol [C]//USENIX. The 13th Usenix Conference on Networked Systems Design and Implementation, March 16-18, 2016.Santa Clara, CA, Berkeley: USENIX Association, 2016:45-59.

[2] KARAME G O, ANDROULAKIE, CAPKUNS Double-spending Fast Payments in Bitcoin [C]//ACM ACM Conference on Computer and Communications Securicy, October 16-18, 2012. Raleigh, North Carolina, USA. New York: ACM, 2012:906-917

[3] Hyperledger. Hyperledger Whitepaper [EB/OL]. https://www.//hyperledger.org/, 2017-6-21.

[4] World Economic Forum The Future of Financial Infrastructure: An Ambitious Look at How Blockchain Can Reshape Financial Services [EB/OL]. https://www.weforum.org/reports/the-future-of-financial-infrastructure-an-ambitious-look-at-how-blockchain-can-reshape-financial services, 2016-8-12.

[5] ETHEREUM WiKi. White Paper[EB/OL]. https://github.com/ethereum/wiki/wiki/White-Paper, 2015-6-18.

[6] GARAY J, KIAYIAS A, LEONARDOS N. The Bitcoin Backbone Protocol: Analysis and Applications[A]//Advances in Cryptology-EUROCRYPT 2015 [M]. Heidelberg: Springer Berlin Heidelberg,2015:281-310.

[7] EYAL I, SIRER E G. Majority Is Not Enough: Bitcoin Mining Is Vulnerable[J]. Computer Science, 2013,8437:436-454.

[8] HEILMAN E, KENDLER A, ZOHAR A, et al. Eclipse Attacks on Bitcoin's Peer-to-Peer Network [C]//UsENIX. The 24th USENIX Conference on Security Symposium, August 12-14,2015. Washington, D C.Berkeley: USENIX Association,2015:129-144.