A Comparative Study of Blockchain Consensus Algorithms

A Comparative Study of Blockchain Consensus Algorithms

Qianwen WANG[a], Jiehua Huang, Shen WANG, Yibo CHEN, Pan ZHANG, Li HE

Aisino Corporation, No. 18, Xingshikou Road, Haidian District, Beijing

[a]8618811792502, wangqianwen@aisino.com

ABSTRACT. A blockchain is a decentralized distributed public database. It does not have a central authority to maintain this public database by running a cryptographic protocol with distributed nodes. Bitcoin is currently the hottest item in the blockchain, and the Bitcoin node can verify the transaction content and package it into the block. The blockchain guarantees the consistency of the books through the underlying consensus agreement. These consensus algorithms are different because the algorithm security assumptions are different from the actual requirements. This paper sorts and compares various blockchain consensus algorithms, sorts out the development based on blockchain consensus, and points out the advantages and disadvantages of various algorithms, and proposes the development direction of blockchain consensus algorithm.

CCS Concepts

•Anonymity and privacy issues and measures to enhance them→Consensus protocols for blockchains

1. INTRODUCTION

The consensus mechanism is the core cornerstone of the blockchain and an important guarantee for the security of the blockchain system. The blockchain is a decentralized system, and the consensus mechanism mathematically allows thousands of nodes scattered around the globe to agree on the creation of blocks. The consensus mechanism also includes an incentive mechanism to promote the effective operation of the blockchain system, which is the basis for building trust in the blockchain. In short, the blockchain consensus mechanism is an algorithm for reaching a distributed consensus on blockchain transactions. Due to the high network delay in the peer-to-peer network, the order of transactions observed by each node may not be exactly the same. Therefore, the blockchain system needs to design a mechanism to agree on the order of transactions that occur within a similar period of time. This algorithm for agreeing on the order of transactions within a time window is called a "consensus mechanism." Blockchain is a kind of distributed system. For centralizing different levels of blockchain, we need different strategies to implement fault-tolerant consensus algorithms to ensure the security of the books.

Commonly used consensus mechanisms for blockchain public links include POW, POS, DPOS, PBFT, and a consensus mechanism with a variety of mechanisms.

2. POW: Proof of Work

The proof of workload is the proof of work (POW) involved in the article "Bitcoin: A peer-to-peer electronic cash system". The pow consensus mechanism is to solve the trust between nodes on the basis of decentralization. The problem is that the blockchain can reach a balance between many nodes. The blockchain solves the problem of transmitting trusted information and value transfer on untrusted channels, and the consensus mechanism solves how the blockchain is in a distributed scenario. The issue of consistency has laid the foundation for the security of the Bitcoin system.

Bitcoin uses the POW mechanism in the block generation process. A matching Block Hash consists of N leading zeros, and the number of zeros depends on the difficulty value of the network. To get a reasonable Block Hash requires a lot of trial calculations, the calculation time depends on the machine's hash speed. When a node provides a reasonable Block Hash value, it indicates that the node does undergo a lot of trial calculations. Of course, the absolute value of the number of calculations cannot be obtained, because finding a reasonable hash is a probability event. When a node has a computing power of n% of the entire network, the node has a probability of n/100 to find the Block Hash.

There are incentives in the system to encourage users to benefit from maintaining the blockchain system. The user participating in the consensus process collects the newly generated transaction record construction block and attempts to modify the value of Nonce in the block until the hash value of the block is smaller than the hash value of the specific difficulty, and the block can be broadcasted externally. The block is verified and approved by other users. After successfully adding to the main chain, the user can get the corresponding reward.

Here we represent a block as a packet containing triples B = <h', txs, nonce>, where h' is the hash of the previous block and txs is the transaction record contained in the block. Nonce is a 32-bit integer. In order to reach a consensus, the system equalizes the node construction block to solve a difficult problem and sets a difficulty value D. D defines how many leading zeros are needed for the current block hash value. The more the leading 0 number, the more difficult it is. Since nonce changing any bit will completely change the hash H(B) of the entire block, there is no way to predict which form of nonce can meet the requirements. Therefore, in order to meet the block requirements, the node needs to use its computing resources to try a large number of possible nonce values such that $H(B) < D$.

The process of embedding the consensus algorithm into the digital currency system is as follows:

1) The new transaction is broadcast to the entire network of miners.

2) Each miner collects transaction records and constructs a new Merkle tree.

3) The miner uses computing resources to find a nonce that meets the current difficulty value.

4) The miner finds a feasible nonce solution and broadcasts the block to the entire network.

5) Other miners verify the block.

6) If the transaction record in this block is valid, the block hash meets the difficulty value requirement, and the block is the longest block among all the forks, then other honest nodes will construct the next block after this block. Piece.

Advantage:

1. High degree of decentralization: the algorithm is simple and easy to implement, the nodes can enter freely, and the degree of decentralization is high.

2. high security: damage to the system requires a huge investment, security is extremely high.

3. Machine trust: The choice of block producers is solved by the node solving hash function. The final process of generating and verifying the proposal to the consensus is a purely mathematical problem. The nodes can reach consensus without exchanging additional information. The whole process No human involvement is required.

Disadvantages:

1. Long confirmation time: In order to ensure the degree of decentralization, the confirmation time of the block is difficult to shorten.

2. poor expansion: no finality, the need for checkpoint mechanism to make up for the finality, but the possibility of reaching consensus with the increase in the number of confirmations has also increased exponentially.

3, waste of resources: the difficulty of mining, coupled with the upgrade of hardware, resulting in double waste of hardware + resources.

3. POS: Proof of Stake

Due to the special data structure of the blockchain, the consensus process of the blockchain can be seen as a leader election mechanism that randomly selects the leader (booking miner) through a fixed mechanism, and the person releases a new block, avoiding a single The user or group controls the ledger for a long time. However, with the development of the blockchain, we can see that the workload proof mechanism has various problems. First, the bitcoin network consumes a lot of power. Some mines are even built next to hydropower stations to save resources. In many scenarios, blockchains are not required for value anchoring. Second, the security of such a mechanism is not as high as imagined, such as a selfish mining strategy, which can successfully control the blockchain without the need of 51% of the entire network.

In the process of the equity certification mechanism, the consensus algorithm selects the next person to be listed based on the proportion of shares held by each person in the consensus process. This idea also comes from the economic society. The more shares a person owns, the higher the dividends and dividends he receives. If the blockchain can be maintained in this form, no additional resource consumption is required. It can make blockchain assets have natural inflation. This sounds ideal and has attributes similar to physical currency.

Peercoin and Blackcoin, using the POS consensus protocol, use currency age as a variable to influence the hashing difficulty of mining. In the process of consensus, the node needs to submit a transaction record to prove the ownership of the blockchain assets. At the same time, the more blockchain assets that are owned, the longer the holding time, the easier the mining will be. The equity proof algorithm hopes that users can make a transfer to themselves to prove a certain number of blockchain assets. These assets can affect the difficulty of mining the miners in the blockchain. The more assets there are, the more organic accounting Calculate the nonce that meets the criteria. So the hashing problem we have to solve becomes:

Proofhash < coins· age ·target

You can understand POS in this way, similar to the property stored in the bank, this model will assign you the corresponding interest according to the amount and time of the digital currency you hold. Simply put, it is a system that gives you interest based on the amount and time of money you hold. In the AAA mode of equity proof, there is a noun called the currency age. Each coin produces 1 currency per day, for example, you hold 100 coins, for a total of 30 days, then, at this time your currency is 3000, this time, if you find a POS block, your currency will be cleared to 0. Every time you are emptied by 365, you will get interest of 0.05 coins from the block (assuming interest is 5% of the annual interest rate), then in this case, interest = 3000 * 5% / 365 = 0.41 The currency, this is very interesting, and there is interest on the currency.

Advantage:

1. Save resources: mining does not waste electricity, and the currency is in a interest-bearing mode.

2. The block confirmation time is fast: the pos consensus improves the block confirmation efficiency, because node mining does not require physical calculations and only requires equity proof, which greatly reduces the time for consensus confirmation.

Disadvantages:

1. Poor security: The implementation rules are complex, there are many intermediate steps, and many human factors are involved, which is easy to generate security holes.

2. pointcheck: As with the POW consensus mechanism, there is no finality, and a checkpoint mechanism is needed to make up for the finality.

3. Matthew effect: The total amount of equity under the POS consensus mechanism is multiplied by the number of coins held by the time of holding the currency. It is bound to form a winner-take-all situation.

4. the accounting node incentive problem: mining in pos is not wasting power costs, although pos mining has a certain incentive, but the incentive for miners is very limited compared to pow.

5. Nothing-at-Stake attack: Because mining does not cost, so the fork attack success rate is very high, it is easy to be split attack. And even without a 51% interest, you can successfully launch a fork attack.

4. DPOS: Delegated proof of stake

DPos similar to the board vote, allows the holder to cast a certain number of nodes and proxy them for verification and accounting.

The DPOS consensus was first proposed by the BitShares community. The main difference between it and the POS consensus is that the node elects several agents, which are verified and billed by the agent. DPOS can greatly improve the efficiency of elections compared to POS, and performance is improved at the expense of some decentralization features. Bitshares allows three types of people to vote in the consensus process: witnesses, delegates, and workers. Witnesses get paid by dealing with transactions and maintaining blockchains. The representative will not be paid but he can initiate a request to update Bitshare. Workers can propose what they want to do, and if the project is voted for, they can get paid.

DPOS's consensus process is divided into two processes: the witness's election process and the witness's block. The witness is only responsible for witnessing the transaction, verifying the signature and time stamp of the transaction, and not participating in the transaction. Each account on the network can vote for its own witness. The more blockchain assets you have, the more votes you have.

1) Witness Election The permanent node with the right to vote accepts the vote and eventually the top N witnesses are selected. N votes will receive more than 50% of the votes. The list of witnesses is rotated at regular intervals (one day).

2) Witnesses out of the block Witnesses are paid for each block they produce, and their salary levels are determined by the votes they receive. If the witness does not have a production block, they have no income and may be voted to lose the identity of the witness.

The DPOS consensus mechanism does not require mining, nor does it require full node verification, but is verified by a limited number of witness nodes, so it is simple and efficient. Due to the limited number of verification nodes, the DPOS consensus has been generally questioned too centrally, and there is also a huge man-made operational space in the election process of the proxy accounting nodes. Because of the loop out of the block, the identity of the blocker has long been known, and it is more likely to cause collusion attacks. Compared to the first two consensus algorithms, the DPOS algorithm is more centralized.

Advantage:

1. Simple and efficient: Significantly reduce the number of participating verification and accounting nodes to achieve a second-level consensus verification.

2. Save resources: only need the primary node to verify the network

3. High scalability: second-level verification, fast block-out, strong capacity of the main network.

4. Disadvantages: The entire consensus mechanism relies on tokens, and many commercial applications do not require tokens.

Disadvantages:

1. Centralization: reducing the number of verification nodes, not the universal verification node, deviating from the basic spirit of everyone in the blockchain world, excessive centralization.

2. Bribery makes the main network fail: the well-known EOS bribery issue, the main network vote can not be completed, plus the super-node bribery to make the eos governance confusing.

5. PBFT: Practical Byzantine Fault Tolerance

PBFT is a state machine replica replication algorithm, in which the service is modeled as a state machine, and the state machine performs replica replication at different nodes of the distributed system. A copy of each state machine saves the state of the service and also implements the operation of the service. A collection consisting of all copies is represented by an uppercase letter R, and each copy is represented by an integer from 0 to |R|-1. For convenience of description, assume |R|=3f+1, where f is the maximum number of replicas that are likely to fail. Although there may be more than 3f+1 copies, the extra copy does not improve reliability in addition to performance.

The whole algorithm operates according to the following process. There are 3f + 1 nodes in a distributed system, which can tolerate f Byzantine error nodes.

1) The client requests the calling service from the primary node.

2) The master node multicasts the request to the secondary node.

3) The secondary node executes the request and sends a reply to the client.

4) The client receives f + 1 replies with the same answer, and the client gets the requested data.

Since the Byzantine fault-tolerant algorithm needs to know the number of nodes in advance, the nodes can establish connections with each other, and the nodes cannot be dynamically managed, which cannot meet the requirements of the public chain. However, in certain circumstances, the blockchain consensus can be achieved using the PBFT algorithm, such as the China Central Bank's electronic billing system, Hyperledger Fabric, whose number of nodes is determined.

Advantage:

1.the main network is stable without fork

Disadvantages:

1. Low scope of application: only for alliance chain and private chain

2. the system, poor scalability.

3. the system node is fixed: can not cope with the open environment of the public chain, only applies to the alliance chain or private

4. Low fault tolerance: The PBFT algorithm requires the total number of nodes n>=3f+1 (where f represents the number of evil nodes). The number of failed nodes of the system shall not exceed 1/3 of the nodes of the whole network, and the fault tolerance rate is relatively low.

6. Advantages and disadvantages of the four major consensus

We compare the consensus algorithms of the blockchain common chain and the license chain, and compare the advantages and disadvantages of each algorithm from resource consumption, centralization degree, throughput, and transaction confirmation time.

Table 1.Advantages and disadvantages of each algorithm

Consensus protocols	**Advantage**	**Disadvantages**
Pow	1.Safe and stable, high degree of freedom of nodes 2.High degree of decentralization, open node system	1.Weak scalability and low performance 2.Causing hardware equipment waste
Pos	1.Less energy 2.High degree of decentralization, open node system	1.Complex implementation process 2.Security breach
Dpos	1.Less energy 2.High performance 3.Finality	1. Weak degree of decentralization, closed node system
Pbft	1.Higher performance 2.Finality 3.High security	1.Weak degree of decentralization, closed node system 2.Low fault tolerance

7. Hybrid consensus, regression of the pow consensus

The following table summarizes the current consensus mechanisms for the application of various public chain projects:

Public chain project	Consensus mechanism
Bytom	Pow: Artificial Intelligence ASIC Chip-Friendly POW Consensus Mechanism
Aeternity	Pow+Pos: The Pow mechanism generates blocks, and major decisions are made by the Pos mechanism, giving the token holders the rights.
Aelf	Pow+Pos: The main chain adopts the Pos consensus mechanism, and the side chain adopts the Pow consensus mechanism. Pos management costs are high, so it is suitable for the main chain, and the side chain uses Pos to operate safely and autonomously.
Zilliqa	Pow+Pbft: The security of the Pow consensus mechanism is used to verify the nodes, and the verified nodes are handed over to the Pbft consensus mechanism for decision making.

Although many public chains have their own unique design philosophy, for security reasons, they still cannot protect the POW consensus mechanism. For open and autonomous public-chain environments, the POW consensus mechanism has better applicability; while the POS consensus process has high management costs, the POS consensus mechanism can only be used in major decision-making processes such as algorithm changes and fork selection. Its use value, but this is already a relatively central decision-making mechanism.

8. Conclusion

In this paper, the popular consensus algorithm of blockchain is summarized. By describing its different requirements and conditions, the internal implementation, advantages and disadvantages of the four consensus algorithms of POW, POS, DPOS and BPFT are expounded.

At present, the POW-POS hybrid consensus mechanism is the hotspot of research. It is also a new direction to use smart contracts to build more transparent consensus rules. The application of the consensus algorithm to practice is also a test of the algorithm. The new attack method can make us understand the inadequacies of the existing consensus algorithm. In addition, for consensus algorithms on the license chain, pluggable switchables are a trend. For different business scenarios, throughput requirements, and security assumptions, we can use different underlying consensus mechanisms to better serve top-level applications.

ACKNOWLEDGMENTS

This research was financially supported by National Key R&D Program of China (Grant No. 2017YFB0802701).

REFERENCES

[1] Lamport L, Shostak R E, Pease M C. The Byzantine Generals Problem[J]. ACM Transactions on Programming Languages and Systems, 1982, 4(3): 382-401.

[2] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, and E. W. Felten. Sok: Research perspectives and challenges for bitcoin and cryptocurrencies. In Proc. IEEE Symposium on Security and Privacy, May 2015.

[3] Gencer A E, Basu S, Eyal I, et al. Decentralization in Bitcoin and Ethereum Networks[C]//International Conference on Financial Cryptography and Data Security, 2018.

[4] Castro M, Liskov B. Practical byzantine fault tolerance and proactive recovery[J]. ACM Transactions on Computer Systems, 2002, 20(4): 398-461.

[5] Fischer M J, Lynch N A, Paterson M S. Impossibility of distributed consensus with one faulty process[J]. Journal of the ACM, 1985, 32 (2):374-382.

[6] Lamport L. Proving the Correctness of Multiprocess Programs [J]. IEEE Transactions on Software Engineering, 1977, SE-3(2):125-143.

[7] Eyal I, Sirer E G. Majority Is Not Enough: Bitcoin Mining Is Vulnerable [DB]. eprint arXiv:1311. 0243, 2013.

[8] Yeow K, Gani A, Ahmad R W, et al. Decentralized Consensus for Edge-Centric Internet of Things: A Review, Taxonomy, and Research Issues[J]. IEEE Access, 2018, 6 (99):1513-1524.

[9] Lamport L. Proving the Correctness of Multiprocess Programs [J]. IEEE Transactions on Software Engineering, 1977, SE-3(2):125-143.

[10] BELLARE M, KEELVEEDHSI, RISTENPART T. Messagelocked encryption and secure Deduplication [C]. Proceedings of Annual International Conference on the Theory and Application of Cryptographic Techniques, Springer, 2013: 296-312.

[11] AUJLA G S, CHAUDHARY R, KUMAR N, et al. SecSVA: Secure Storage, Verification, and Auditing of Big Data in the Cloud Environment [J]. IEEE Communications Magazine, 2018, 56(1): 78-85.