Research and analysis on consensus mechanism of blockchain

Dewen Wang, Lixin Wang [a]

School of North China Electric Power University, Baoding 071003, China.

[a]15076508926@163.com

Abstract

With the successful application of Bitcoin, the blockchain as its underlying support technology has attracted the attention of the academia and become the darling of the new generation of computer technology. The consensus mechanism is an important core technology of the blockchain. It brings new technical ideas to solve the consistency problem of distributed systems, and aims to achieve data consistency by following the preset rules. This paper introduces the basic principles of various mainstream consensus mechanisms based on Proof of Work， Proof of Stake and Practical Byzantine Fault Tolerance mechanism, and analyzes the advantages and disadvantages of various consensus mechanisms, followed by performance efficiency, decentralization, and fault-tolerant performance. The characteristics of various consensus mechanisms are compared and analyzed in several aspects such as resource consumption and whether tokens are needed, and the consensus performance of different consensus mechanisms is summarized and analyzed.

Keywords

Blockchain, Consensus mechanism, Proof of Work, Byzantine fault-tolerant mechanism.

1. Introduction

Blockchain technology originated in the article "Bitcoin: A Peer-to-Peer E-Cash System" published by Nakamoto[1]. Nakamoto Satoshi proposed the idea of digital cryptocurrency and realized decentralized electronics in P2P networks. Cash payment system. In the Bitcoin system, all nodes in the whole network are mined by contributing computational power, and the nodes that successfully mine can obtain bitcoin rewards and have the right of billing.

The successful application of Bitcoin has attracted wide attention from all walks of life around the world， As its underlying supporting technology, it is favored by people in the academia. Blockchain technology is composed of data layer, network layer, consensus layer, incentive layer, contract layer and application layer and it can be used as the underlying framework in finance, economy, technology and even politics. Blockchain can provide technical support and bring profound changes to various fields in decentralization, encryption protocols, smart contracts, etc.[2] It is worth mentioning that the consensus mechanism is an important technology to realize decentralization of the whole network, and brings new technical ideas to solve the problem of consistency of distributed systems. However, according to the "FLP Impossible Principle", there is no deterministic consensus algorithm that can solve the consistency problem in a minimized asynchronous model system with reliable network but allowing node failure[3]. Therefore, for different application scenarios, a consensus mechanism for different performances needs to be designed to achieve consistency of the distributed system. At present, the typical consensus mechanisms supported by blockchain technology Proof of Work， Proof of Stake and Practical Byzantine Fault Tolerance, and also the combination of different mechanisms.

2. Consensus mechanism

2.1 Proof of Work

The Bitcoin system uses a proof of work mechanism to achieve an effective consensus across nodes. In the Bitcoin system, new transactions are generated all the time. These transactions are stored in the mining pool. Each node stores the transactions in a block cycle in the block according to the Merkle tree rules. The obtained Merkle root and target hash, timestamp and other data are stored in the block header.The node (miner) participating in the competition billing right needs to calculate the random number smaller than the target hash by hash calculation. This process is called mining. The miner who successfully searches for the random number will have the right to link the block to the main chain. And broadcast the block to the entire network. Therefore, the working mechanism of the Bitcoin system is that all nodes in the world with free computing can freely enter and exit the system, voluntarily mine to obtain bitcoin rewards and even billing rights, thus achieving complete decentralization.

The proof of work mechanism requires the miner to perform a certain amount of calculations, which means that the miner must consume a certain amount of computing resources (time, computing power) to get an easily verifiable result. The purpose is to let the miners consume a certain amount of computing power and waste certain economic resources, thus avoiding service abuse and attack [4]. All miners may successfully search for random numbers at the same time and obtain billing rights, which can lead to block fork problems, which reduces the efficiency of the system. The research in literature [5] shows that under the premise of ensuring the same security, in order to solve the block bifurcation problem in the Bitcoin system, a link of 6 consecutive blocks is specified to determine a valid block, but this results in a block confirmation delay time of 1h (bit). The block interval of the currency system is 10min).The Ghost protocol used in the Ethereum system to solve the block bifurcation problem requires about 37 blocks. Confirmation time (the interval of the Ethereum system is about 25s) [6]. In addition, Litecoin and Dogecoin have added the scrypt encryption algorithm based on the proof of work, in order to reduce the difficulty of mining miners to shorten the block interval. In the case of comparable security performance, Litecoin requires 28 block confirmation times (block interval 2.5min), and Dogecoin requires 47 block confirmation time (block interval 1min).

2.2 Proof of Stake

The proof of Stake mechanism determines the billing rights based on the size of the currency. The currency age is the product of a certain number of coins and the length of time of their last transaction, and each transaction will consume a certain amount of currency. It is easier for a coin-aged person to solve the problem of random numbers than a coin-aged node to obtain the accounting right. The dot-coin is a Digital cryptocurrency based on the stake proof mechanism [7].Compared with the proof of work mechanism, the proof of stake mechanism does not solve the problem of the fork chain fork, but it greatly reduces the waste of resources and shortens the time for each node to reach an effective consensus. However, since all miners are not competing for a bookkeeping right at a starting point, they lose their fairness to a certain extent, and the nodes with large ages spend less computing power to obtain the bookkeeping rights. Therefore, the stake proof mechanism cannot effectively avoid Network attacks.

In order to solve the problem of the fork of the block chain, the mechanism for authorizing the shareholding equity is proposed on the basis of the equity certificate. The specific operation process is similar to the election of the board of directors [8]. All nodes vote to elect the node they trust to become the authorized node, and the node with the top 100 nodes will become the authorized node, and the authorized node will generate the block in turn within a certain period of time. Since the authorized stock equity proof mechanism has only one node at each time with the billing right, the problem of branching of the block chain is effectively avoided, and the consensus mechanism does not need to spend the power to compete for the billing right, so It has lower consumption than the stake proof mechanism.

There are still many changes on the basis of the proof of stake, such as the proof of importance [9], the proof of leasehold rights [10], the proof of activity [11], etc. These consensus mechanisms have more or less solved the existence of the proof of stake problem.

2.3 The practical Byzantine fault-tolerant mechanism

The practical Byzantine fault-tolerant algorithm is a state machine-based replica replication algorithm for distributed asynchronous environments. The state machine performs replica replication at different nodes of the distributed system. A copy of each state machine preserves both the state of the service and the operation of the service. All replicas can be classified into a primary node and a backup node, and also contain a client identity in one view. The client is the sender of the request. The master node is responsible for receiving the client's send request and broadcasting the request to all backup nodes. The backup node receives the information from the master node, verifies its authenticity, performs the corresponding operation after verification, and returns the result to the client.

The practical Byzantine fault-tolerant algorithm is divided into five phases: Request, Pre-prepare, Prepare, Commit, and Reply. The consensus process is shown in Fig.1.

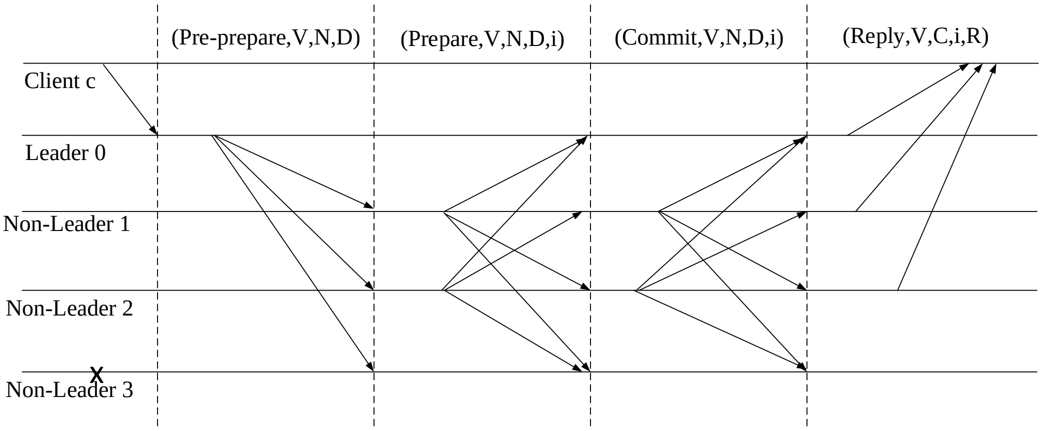

Fig. 1 Practical Byzantine Fault Tolerant Algorithm Consensus Process

Client C is the sending requester, Leader0, Non-Leader 1, 2, and 3 are the server, and Non-Leader 3 is the server of the downtime. The specific steps are:The first step is the request phase. A master node (Leader) is elected from the entire network node, where is 0, the new block is generated by the master node, and the requesting end C sends a request to the master node.In the second step, in the pre-preparation phase, each node broadcasts the transaction sent by the client to the entire network, and the master node 0 collects the multiple transactions that need to be placed in the new block from the network, and then deposits the list into the list. The list is broadcast to the entire network and spread to 123.In the third step, the preparation phase, after each node receives the transaction list, it executes these transactions according to the sorting simulation. After all the transactions are executed, the hash summary of the new block is calculated based on the transaction result, and broadcast to the entire network, 1→023, 2→013, 3 because the downtime cannot be broadcast.In the fourth step, in the commit phase, if a node receives 2f (f is a tolerable Byzantine node number) and the other nodes send the digests equal to themselves, a Commit message is broadcast to the entire network.In the fifth step, in the reply phase, if a node receives 2f+1 Commit messages, it can submit new blocks and their transactions to the local blockchain and state database.

In the case of going to the center, the Byzantine fault tolerance mechanism can achieve effective consensus among nodes in the blockchain network without any computational power, and avoid waste of resources. In addition, at a certain time, only one master node can propose a new block, and other nodes verify the block, which not only avoids block fork, but also greatly shortens transaction confirmation and block confirmation time, and improves system efficiency. .

The Byzantine fault tolerance mechanism still has problems with regard to security and scalability. The security of the Byzantine fault-tolerant mechanism depends on the number of failed nodes, and the number of failed nodes does not exceed 1/3 of the nodes of the whole network. In the block chain system, a malicious node can generate multiple nodes by implementing a Sybil attack, and the proportion of nodes it controls exceeds 1/3 of the nodes of the whole network, thereby destroying the consistency and security of the system. The efficiency of the Byzantine fault-tolerant mechanism depends on the number of nodes in the block chain network. This mechanism does not apply to block chain systems with too many nodes, and the scalability is poor.

3. Analysis and comparison of consensus mechanism

The existing proof of work consensus mechanism, the proof of stake consensus mechanism and the practical Byzantine fault tolerance consensus mechanism are compared and analyzed in terms of performance efficiency, decentralization degree, maximum allowable number of evil nodes, application scenarios, resource consumption, etc. The characteristics in the block chain network are shown in Table 1.

Table 1 Consensus algorithm comparison

Consensus algorithm	PoW	PoS	DpoS	PBFT
Performance efficiency	low	Medium high	high	high
Degree of decentralization	completely	completely	completely	Semicenter
Fault tolerance	50%	50%	50%	33%
Application scenario	Public chain	Public chain	Public chain	Private chain /Alliance chain
LF	High	Medium	Low	Low
With or without fork	with	with	without	without

According to the characteristics of different consensus mechanisms, different consensus mechanisms can be considered to form a new consensus mechanism. For example, the 2-hop blockchain attempts to combine the proof of work with the proof of equity, using the equity proof mechanism to reduce system resource consumption and improve fairness and security [12]. The Algorand system combines the equity certification mechanism with the Byzantine coherence protocol to limit the number of nodes participating in the Byzantine coherence protocol through equity proofs to improve system scalability [13].

4. Conclusion

On the basis of ensuring security and consistency, the research on consensus mechanism has been centered on how to balance the performance efficiency, scalability and resource consumption of the system. Due to the different characteristics of different consensus mechanisms, how to combine the various consensus mechanisms and design the optimal consensus mechanism for comprehensive evaluation is the mainstream direction of future research. For the existing blockchain consensus mechanism, combined with the improvement of the encryption algorithm and the underlying storage technology, the consensus mechanism can exert the maximum effect, such as zero knowledge proof [14], ring signature, lightning network. With the global attention to the blockchain, more and more people are investing in research and development, and in the future there will be more work-efficient and well-designed consensus mechanisms designed.

References

[1] Satoshi Nakamoto S．Bitcoin：a peer-to-peer electronic cash system [J]．Consulted，2009．

[2] YUAN Yong ,WANG FeiYue .Blockchain: The State of the Art and Future Trends[J].ACTA AUTOMATICA SINICA ,2016,42(4):481-494.

[3] Fischer， Lynch， Patterson.Impossibility of Distributed Consensus with One Faulty Process[C]//Proc of ACM SIGACT-SIGMOD Symp on Principles of Database Systems.New York：ACM，1983:1.

[4] Dwork Cynthia,Naor Moni.”Pricing via Processing,Or,Combatting Junk Mail,Advances in Cryptology”.CRYPTO’92:Lecture Notes in Computer Science No.740(Springer):139-147.

[5] Gervais, G. O. Karame, K. Wüst, et al. “On the security and performance of proof of work blockchains,” in Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. ACM, March 2016.

[6] Gramoli, V., From blockchain consensus back to Byzantine consensus. Future Generation Computer Systems, 2017.

[7] Larimer D. Transactions as proof-of-stake [Online],available: http://7fvhfe. com1.z0. glb.clouddn.com/@/wp-content/uploads/2014/01/TransactionsAsProofOfStake10.pdf, 2013.

[8] Larimer D. Delegated proof-of-stake white paper [Online],available: http://www. bts.hk/ dpos-baipishu.html, 2014

[9] Beikbwerdi A.NEM (cryptocurrency) [EB/OL].(2018-03-23) https://en.wikipedia.org/ wiki /NEM_ ((cryptocurrency).

[10] Alexander I. Waves platform[EB/OL].(2018-03-19)

[11] Bentov I,Lee C,Mizrahi A, et al. Proof of activity:Extending Bitcoin’s proof of work via proof of stake[J].ACM SIGMETRICS Performance Evaluation Review,2014,42(3):34-37.

[12] DUONG T, FAN Lei, ZHOU Hongsheng. 2-hop Block chain:Combining Proof-of-Work and Proof-of-Stake Securely [EB/OL].http://eprint.iacr.Org/2016/716. pdf, 2017-4-15.

[13] CHEN Jing, MICALI S. Algorand[EB/OL]. https://arxiv.org/abs/1607.01341, 2016-7-5.

[14] Waclaw B,SteFan D,Daniel M.Efficient zero-knowledge contingent payments in cryptocurrencies without scripts [C]// Proc of European Symp on Research in Computer Security. Berlin:Springer,2016:261-280.