A Review of Consensus Algorithms in Blockchain

Lusheng Ji

Abstract— **Consensus algorithm is the key to achieve the final consistency of blockchain system. The consensus algorithm of blockchain also provides a solution to the consensus problem in distributed system.After explaining the development history of consensus algorithm, this paper analyzes the current mainstream block chain consensus algorithm model as well as its advantages and disadvantages.And the development of block chain consensus algorithm in the future is prospected.**

Index Terms—**Blockchain,consensus algorithms,distributed systems, consistency.**

I. INTRODUCTION

Consensus is the process of achieving consistency in distributed system. When multiple nodes cooperate, how to ensure the synchronization of all nodes is the key.Distributed systems follow the principle of CAP[1], which means that only two conditions can be met in CAP.The design of distributed systems also leaves out only one feature, for example, Zookeeper guarantees A CP and Eureka guarantees an AP.As you can see, usability cannot be abandoned.All the nodes of the block chain are peer nodes, and the latest records are transmitted by the way of p2p network through broadcasting. There is no central node, and all the staff are encouraged to participate in verification, transmission and other work through the incentive mechanism, thus ensuring the fairness of the system.

II. RADITIONAL CONSENSUS ALGORITHM

The consensus algorithm revolves around solving the Problem of Byzantine generals, two armies fighting each other, and how generals can communicate the right commands in the presence of spies.In a distributed system, the node may go down, and the node in the down state will no longer be reliable, but the system must be able to operate normally.Early consensus algorithms were Paxos, followed by many variants of consensus algorithms based on Paxos.

A. *BPFT Byzantine fault tolerant algorithm*

BPFT[3] selects the leader node in all nodes mainly based on message passing, and other nodes follow the status of the leader node.When other nodes find the leader node unreliable, a new leader node is elected.BPFT can tolerate one third of node failures.

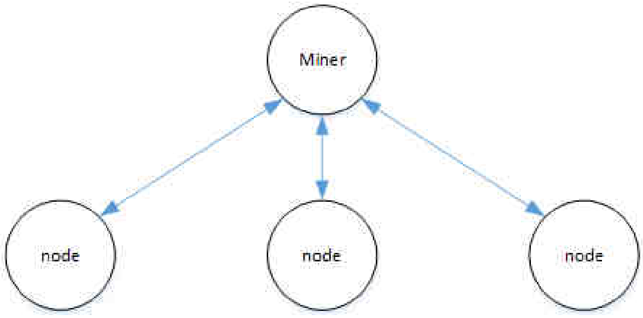
Manuscript received September 06, 2020

Lusheng Ji, School of Computer Science and Technology, Tiangong University, TianJin, 300387

III. CONSENSUS ALGORITHMS IN BLOCKCHAIN

A. PoW

PoW proved to be a perfect solution to the Byzantine general problem.Blockchain system is a scheme to motivate all staff to contribute to the consistency of the system.The main idea is to create a mathematical puzzle that all the miners have to work out, and to reward the miners who work out the answer first. The scheme allows fair competition without a central node, ensuring randomness in the system's next state deciders.Elliptic curve algorithm is a one-way function, irreversible push, can only enumerate all possible answers into, the stronger the processor performance the faster the calculation.In this power with that in mind, to assure the currency of the block rate, its difficult to limit for every 10 minutes out of a piece, if the current processor is too high will shorten the time, so the system will check the average block time, will improve the mathematical difficulty, if less than 10 minutes in order to ensure the stability of the system.The scheme wastes a lot of power and, over time, the system is in the hands of the more computational miners.



B. PoS

PoS is the proof of equity, mainly to solve the problem of power resource waste in PoW.The state of the system is verified by the nodes holding a certain amount of COINS. The more COINS there are, the greater the weight will be, so as to determine the state of the system.But this scheme may also result in partial centralization.

C. PoB

PoB combustion proof is an alternative to the recognized consensus algorithm for equity proof. The main idea of PoB is that the participants of the system need to prove their contribution to the system, and only a part of the nodes that want to participate in verification need to participate in verification.All it takes is to destroy a certain amount of cryptocurrency to prove the investment in the blockchain system to gain the right to mine and verify transactions.

D.The super node

Some blockchains also adopt super nodes as the consensus scheme of the system. This chain is partially decentralized. The status and data authentication of the system are determined by some nodes and the rights are in the hands of some people, thus avoiding complete decentralization to a certain extent.

IV. Knot and prospect

UBitcoin [4] is a blockchain 1.0, but Bitcoin only serves as a trading platform, from which ideas have been borrowed to produce various schemes for blockchain 2.0, such as Ethereum [5] and super ledger [6].The private chain and the public chain correspond to different application scenarios.The consensus algorithm of block chain controls the fairness and consistency of the system, which will be the research hotspot in the future. After a period of time, it will compete for a stable and reasonable scheme.

References

[1] Gilbert S, Lynch N. Brewer' s conjecture and the feasibility of consistent, available, partition-tolerant web services. Acm Sigact News, 2002, 33(2): 51−59.

[2] Lamport L, Shostak R, Pease M. The byzantine generals problem. ACM Transactions on Programming Languages and Systems, 1982, 4(3): 382−401.

[3] Castro M, Liskov B. Practical Byzantine fault tolerance. In: Proceedings of the 3rd Symposium on Operating Systems Design and Implementation. New Orleans, USA: OSDI, 1999. 173−186 .

[4] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system[R]. Manubot, 2019.

[5] Wood G. Ethereum: A secure decentralised generalised transaction ledger[J]. Ethereum project yellow paper, 2014, 151(2014): 1-32

[6] Cachin C. Architecture of the hyperledger blockchain fabric[C]//Workshop on distributed cryptocurrencies and consensus ledgers. 2016,