Overview On Classical Distributed Consensus Mechanism

Chengqi Wu

***Abstract*—Since Bitcoin was proposed, in the era of digital currency rotation, the blockchain technology behind it also has some specific interactive interests derived from interests. , Determined the security, scalability, and degree of integration of a part of the chain technology. For the classic application mechanism, it can guide the design and practice of partial chain applications. This article summarizes the parts. PBFT, Paxos, Hotstuff and SBFT in the synchronization network introduce the important research and conclusions of the algorithm in the traditional partial synchronization network. The basic model in the classic network is proposed.**

***Index Terms*—consensus mechanism, blockchain, Byzantine fault tolerance**

I. Introduction

A. Background

In 2008, Satoshi Nakamoto proposed Bitcoin, and digital currency entered a new field and a new field. The large-scale direction chain technology of digital currency has attracted the attention and needs of a large number of users. Blockchain technology is being distributed. In an unreliable and unreliable environment, all nodes reach a consensus on the technical core of the public ledger through certain specific mechanisms. aspect. The research and design of classic and self-correlated theoretical research and design have very good significance and guiding significance.

B. Overview on consensus

The classic distributed consensus mechanism refers to a group of nodes that implement state machine replication in an authorized network.

The research on the classic distributed consensus mechanism originated from the thought experiment proposed by Akkoyunlu, Ekanadham and Huber in 1975-the two armies problem. This problem proves that it is difficult to exchange information and reach consensus through unreliable communication channels. Lamport, Shortstack, and Pease put forward the thought experiment of ”Byzantine Generals Problem” to study how non-faulty nodes can communicate in peer-to-peer situations when there may be faulty nodes. The Byzantine Generals problem has become the basis of consensus mechanism research. The solution to the ”Byzantine Generals Problem” has been further developed into algorithms and protocols for distributed consensus mechanisms.

C. related works

Lamport proposed the Paxos algorithm to solve the ”Byzantine Generals Problem”. The Paxos algorithm can tolerate the collapse of a certain number of nodes in the network, and in a distributed system, agree on a specific data.

In 1999, Liskov and Castro proposed using the Byzantine fault tolerance protocol as a solution to the Byzantine problem. PBFT allows a certain number of Byzantine nodes to exist in the network. These nodes create false information in the process of reaching a consensus and use various means to prevent other honest nodes from completing the consensus. PBFT achieves the consensus of the final honest node when the number of opponents does not exceed $\frac{1}{3}$ of all nodes.

Abraham, Gueta and Malkhi proposed an improved HotStuff algorithm for the PBFT algorithm. The use of threshold signatures, parallel pipeline processing and linear view conversion techniques to improve PBFT greatly improves the efficiency of distributed consensus algorithms.

Golan-Gueta and others proposed a scalable Byzantine fault-tolerant protocol, which mainly solves the problem of decentralization and expansion of the Byzantine fault-tolerant protocol when it is applied to the blockchain. The scalable Byzantine fault-tolerant protocol uses the leader as the collector of information and signatures, and uses threshold signatures to reduce communication complexity.

References

[1] LIU Y Z, LIU J W, ZHANG Z Y, XU T G, YU H. Overview on Blockchain Consensus Mechanisms. Journal of Cryptologic Research, 2019, 6(4): 395-432.

[2] Fan J, Yi LT, Shu JW. Research on the technologies of Byzantine system. Ruan Jian Xue Bao/Journal of Software, 2013,24(6):13461360 (in Chinese). http://www.jos.org.cn/1000-9825/4395.htm

[3] YUAN Yong, NI Xiao-Chun, ZENG Shuai, WANG Fei-Yue. Blockchain Consensus Algorithms: The State of the Art and Future Trends. ACTA AUTOMATICA SINICA, 2018, 44(11): 2011-2022. doi: 10.16383/j.aas.2018.c180268