2021 2nd International Conference for Emerging Technology (INCET)
Belgaum, India. May 21-23, 2021

An Analysis on Blockchain Consensus Protocols for Fault Tolerance

Swathi B H
Department of Computer Science and Engineering
Vidyavardhaka College of Engineering
Mysuru, India
swathibh@vvce.ac.in

Meghana M S
Department of Computer Science and Engineering
Vidyavardhaka College of Engineering
Mysuru, India
meghanams742@gmail.com

Lokamathe P
Department of Computer Science and Engineering
Vidyavardhaka College of Engineering
Mysuru, India
lokamathe26@gmail.com

2021 2nd International Conference for Emerging Technology (INCET) | 978-1-7281-7029-9/20/$31.00 ©2021 IEEE | DOI: 10.1109/INCET51464.2021.9456310

***Abstract*— The revolution with technologies happens very often, here is one such technology called "Blockchain" which will be a game-changer in many functional sectors of the society. Initially, this technology was developed to support cryptocurrencies (such as Bitcoin, Ethereum, and Litecoin etc).Now a days it is gaining the attention of the researchers in almost the entire field. The consensus protocol in the cryptography and peer to peer architecture is one of the essential parts of the blockchain technology. The best consensus protocol in a blockchain system provides the fault tolerance. These censuses in blockchain are broadly classified in to two types. The absolute-finality consensus protocol and probabilistic-finality consensus protocols. In this paper, the different types of censuses protocols are discussed along with their working, strength and weakness. It also gives the overview on the different types of blockchain technology with their advantages and disadvantages. At the last we also presented a comparison of these consensus protocols by considering different qualitative parameters.**

Keywords— Blockchain technology, Consensus Protocol, Fault tolerance

I. INTRODUCTION

Blockchain technology is a system of storing the data in such a way that makes it hard to modify or hack the system. Basically it is a digital ledger of transactions that is replicated and scattered over the network of computer systems on the blockchain. Initially, Satoshi Nakamoto described a new decentralized cryptocurrency in the Bitcoin white paper. Later Bitcoins occupies the blockchain technology and spread over the world [1]. Many cryptocurrencies and blockchain-based ventures start appearing immediately. Hence blockchain becomes one of the emerging technology. Blockchain technology combines many technological inventions like cryptography, peer to peer networking, distributed systems and many more. Along with this blockchain provides high security framework for cryptocurrencies in such a way that anyone can't hack the transactions in the network. For this justification, in different fields, blockchain technology can be widely adopted.

Many applications of Internet of Things, Supply chain management, financial systems and medicals fields are using blockchain. But the use of blockchain in these fields facing many challenges, where designing of the best consensus protocols is one of the major challenge. The consensus of blockchain is that every node uses the identical distributed ledger. As the traditional software architecture maintains a central server, the maintenance of the consensus is very hard. Hence the other nodes should be within the alignment of the centralized server. But in case of distributed network like blockchain every node in the network acts as both server and client. These nodes exchange their information to reach the consensus. The nodes which are malicious or offline will affect the entire consensus method. Hence it is important to design a best consensus fault tolerance protocol to minimize this phenomenon. The system's chosen consensus protocol should also support the different types of blockchain. There are three basic types of blockchain namely, public blockchain, private bolckchain and consortium blockchain. All these are explained in the following section along with their Advantages and disadvantages.

Each of this type of blockchain is adopted in various applications. So the selected consensus protocol should relevant to the application. In this paper, popular consensus protocols of blockchian along with their performance are presented.

For the distributed systems, there seems to be no appropriate consensus protocol, the consensus protocol has to compromise with the availability and consistency. Also it has to address Byzantine Generals Problem. In this paper the most common blockchain consensus protocols that can successfully manage the Byzantine Generals problem are discussed [4].

It is possible for a potential hacker to overtake one block in a chain, but the computation is also compounded as the valid blocks in the emerges, and so overthrowing a long chain takes a large number of computational power. [15] [16].

The paper is structured as follows. In the First section the introduction about the blockchain and consensus protocol is given. The second section describes the different types of blockchains with their pros and cons. The third section illustrates the different types of consensus protocol for blockchain with their working principles. In the final section, the comparison of the different protocols is done by considering various qualitative parameters.

II. CATEGORIES OF BLOCKCHAIN

The three main categories of blockchains are public blockchain, private blockchaion, permissioned blockchain ,consortium blockchains.

A. Public blockchain

In this type of blockchain anyone can join and leave as they wish. . The disadvantages of public blockchain are less security and no privacy for transactions. It requires more computational power. Bitcoin is the best example for this type for blockchain. In bitcoin the miners validates the transaction and receives transaction fees in the form of

bitcoin. Ethereum and Bitcoin are the suitable examples for public blockchain [5].

B. *Private blockchain:*

The private blockchain restrict the access to transactions. It is a permissioned blockchain where only the authorized entity can access the network .This also gives some grants to the participants to access the network. It is a more centralized network, because only a certain number of users can control the network. Hyperledger and Ripple(XRP) are the best example for private Blockchain [3].

C. *Consortium blockchain:*

Consortium blockchain is also called as federated blockchain. Here multiple organization uses the platform. This type of blockchain is similar to private blockchain but they are different. This type of blockchain is suitable where many organizations work on the single industry and when they require more secured transactions.

TABLE I. DIFFERENT TYPES OF BLOCKCHAINS WITH THEIR ADVANTAGES AND DISADVANTAGES

Type of Blockchain	**Advantages**	**Disadvantages**
Private blockchain	• It is Open to all and transparent • Trustable • Secure	• It is slow and faces scalability problems • Lower TPS • High Energy Consumption
Private blockchain	• Higher Transactions per Second (TPS) • More Scalable	• It is a Centralized blockchain • Not secure • Needs Trust-building • Lower Security
Consortium blockchain	• Higher Transactions per Second • Secure	• Partial Immutability • Centralized and prone to attack

III. CONSENSUS PROTOCOLS FOR FAULT TOLERANCE

A. *Proof of Work(PoW)*

In each round of consensus, it chooses a node to generate a new block by computational power competition. Here, the node which is in the competition has to find the solution for cryptographic puzzle. The node which finds the solution first can get the chance to create a new block. Fig.1 shows the block creation flow in PoW. It is very tricky to solve the puzzle. The node needs more computational power to adjust the nonce value to get the exact answer. It is possible for a malicious actor to overthrow single block within a chain, however as the correct blocks within the chain emerges, the load is compounded, so a huge proportion of computational power is needed to overthrow a long chain. It is normally used in Bitcoin and Ethereum[5][6].

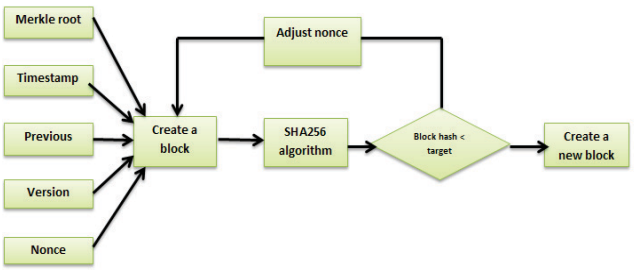

Fig. 1. Proof of Work Flow

B. *Proof of Stake (PoS)*

In Proof of Stake, choosing the rounds for a node to create a new block is completely depends on the held stake. It is not going to consider the computational power. The PoS does not adjust nonce for every time[10]. It uses less computational power to reach the consensus[11]. Many cryptocurrencies like Nxt, PPcoin, ouroboros and so on, use this PoS Consensus protocol[7][8][9]. The working of the PoS is shown in the fig. 2.

C. *Delegated Proof of Stack (DPoS):*

The principle of Delegated Proof of Stack is to allow the node which holds the stake vote to choose block creators. This can avoid the stakeholder to create the nodes by themselves. They can grant the rights of building the blocks to the members whom they assist. This method decreases computing power consumption to 0.The fig. 3 shows the flow of DPoS. If the delegate fails to create the block during turns, they will be removed and stakeholders take the lead to identify the new nodes to replace these delegates. The stakeholder's vote will be used by the outstretch a consensus in a best way. DPoS is less expensive as well as more efficient when compare to PoW and PoS.

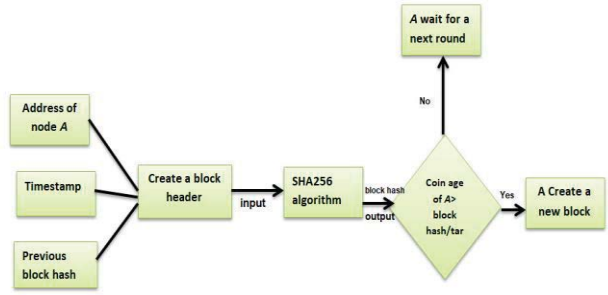

Fig. 2. Proof of Stack

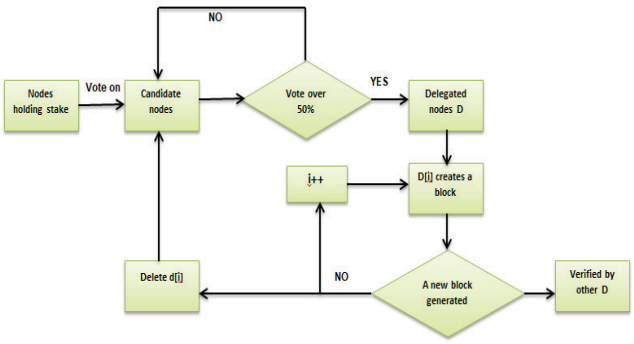

Fig. 3. Delegated Proof of Stack (DPoS)

D. *Practical Byzantine Fault Tolerance (PBFT)*

Practical Byzantine Fault Tolerance is one of the consensus protocols for Fault Tolerance Protocol. It is one of the more practical protocols with minimal algorithm complexity. It has five important phases as follows. Request, pre-pare, prepare, commit and reply [12]. The same process is explain the figure 4. The client forwards the message to the primary node. Then it will forward to the other three nodes. If these three nodes crashed, then the message passes through the said five phases. Then to complete the round the nodes will give reply to the client. PBFT is a consistent protocol and each node maintains same state in each round of consensus. The Stellar protocol is the extension of the PBFT and it uses Federated Byzantine agreement [13].

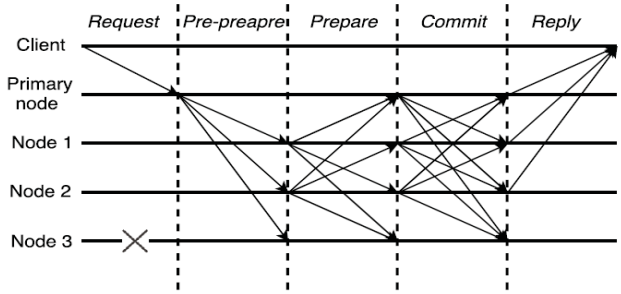

Fig. 4. Practical Byzantine Fault Tolerance [2]

E. *Ripple:*

It is one of the open source protocol for payments. It starts the transactions by clients and broadcasts to all over the network through the nodes. In Ripple the consensus process is carried out by validating the nodes. All the nodes in the Ripple maintains a table of genuine node called as Unique Node List (UNL). These nodes which are in the list can vote the transactions that they support [14]. In Ripple every validating node sends transaction set as a proposal to other validating nodes. Once receiving this proposal, the validating node checks all the transaction in the proposal. If the transaction of the local transaction set is same as the transaction which is in the proposal, then the proposal gets one vote. When to reaches to the 50% of the vote, then it moves to the next round. If it reaches to 80%. Then it will be recorded in the ledger. The process of the ripple is shown in the fig5.

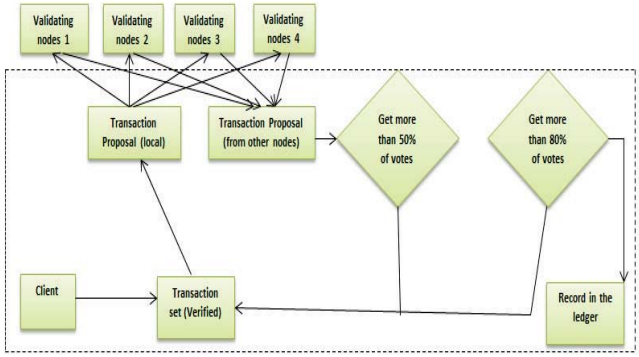

Fig. 5. Ripple

IV. COMPARISON BETWEEN THE CONSENSUS ALGORITHMS

In this section, the differences between the various consensus algorithms are presented. Table 2 shows the differences between the protocols.

TABLE II. COMPARISONS BETWEEN VARIOUS CONSENSUS PROTOCOLS

Consensus Protocol	Protocol type	Application	Scalability	Energy utilization
PoW	Probabilistic-finality	Public	More	High
Pos	Probabilistic-finality	Public	More	Low
DPos	Probabilistic-finality	Public	More	Low
PBFT	Absolute-finality	Permissioned	Less	Negligible
Ripple	Absolute-finality	Permissioned	More	Negligible

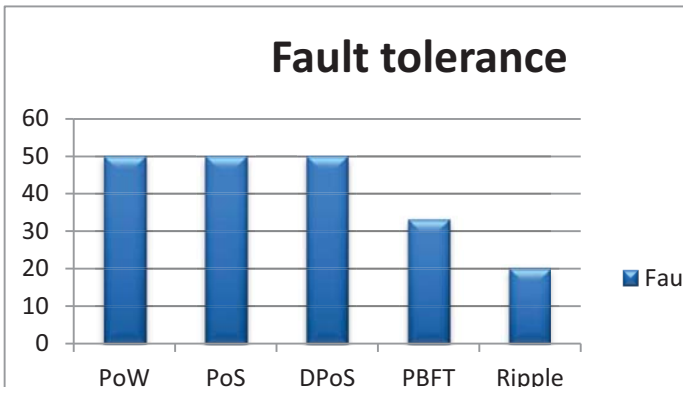

Fig. 6. Fault tolerance among the various consensus protocols.

Pow, PoS and DPoS protocols belongs to probabilistic-finality protocols. These protocols allow only the 50% of stakeholders to hold the stake. But PBFS and Ripple provides the fault tolerance up to 33% and 22% respectively. The fault tolerance of these protocols is illustrated in the fig 6.

V. CONCLUSION

The stability of the blockchain system is given by consensus protocol. Through this consensus protocol a node can approve on certain value or through some transactions. In this paper, the different types of blockchain are introduced along with their advantages and disadvantages. Then the most popular blockchain consensus protocols are introduced along with their applications scenario. The working procedure of the consensus protocols are also summarized with their strengths, weakness and comparisons. It is observed that, only the designing part of a consensus protocol with fault tolerance is not sufficient. But usage of the protocol also plays a major role.

REFERENCES

[1] S. Nakamoto, et al., Bitcoin: A peer-to-peer electronic cash system.

[2] Shijie Zhang, Jong-Hyouk Lee,vAnalysis of the main consensus protocols of blockchain, ICT Express, Volume 6, Issue 2, 2020, Pages 93-97, ISSN 2405-9595, DOI: 10.1016/j.icte.2019.08.001 (2019)

[3] V. Buterin, On public and private blockchains, https://blog.ethereum.org/2015/08/07/on-public-and-private blockchains/, 2015.

[4] S. Gilbert, N. Lynch, Brewer's conjecture and the feasibility of consistent, available, partition-tolerant web services, ACM SIGACT News 33 (2) (2002) 51–59.

[5] L. Lamport, R. Shostak, M. Pease, The byzantine generals problem, ACM Trans. Program. Lang. Syst. (TOPLAS) 4 (3) (1982) 382–401.

[6] G. Wood, et al., Ethereum: A secure decentralised generalised transaction ledger, Ethereum Proj. Yellow Pap. 151 (2014) 1–32.

[7] S. King, S. Nadal, Ppcoin: Peer-to-peer crypto-currency with proof-of-stake, self-published paper, August 19.

[8] N.community,Whitepaper:Nxt,http://nxtwiki.org/wiki/Whitepaper:Nxt.

[9] A. Kiayias, A. Russell, B. David, R. Oliynykov, Ouroboros: A provably secure proof-of-stake blockchain protocol, in: Annual International Cryptology Conference, Springer, 2017, pp. 357–388.

[10] D. Larimer, Delegated proof-of-stake (dpos), Bitshare whitepaper.

[11]]EO IO, EOS.IO Technical White Paper v2, https://github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md, 2018.

[12] M. Castro, B. Liskov, et al., Practical byzantine fault tolerance, in: OSDI, Vol. 99, 1999, pp. 173–186.

[13] D. Mazieres, The Stellar Consensus Protocol: A Federated Model for Internet-Level Consensus, Stellar Development Foundation, Citeseer, 2015.

[14] D. Schwartz, N. Youngs, A. Britto, et al., The ripple protocol consensus algorithm, Ripple Labs Inc White Paper 5.

[15] J. Poon, T. Dryja, The bitcoin lightning network: Scalable off-chain instant payments, 2016.

[16] J. Poon, V. Buterin, Plasma: Scalable autonomous smart contracts,White paper, 1–47, 2017.