IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2320-6710


# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

## IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 9, Issue 10, October 2020

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.512

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 9, Issue 10, October 2020||

# Major Consensus Protocols of Blockchain

**Preethy PK[1], Greeshma AK[2]**

Lecturer, Department of Computer Engineering, SCMS College of Polytechnics, Kochi, India[1],

Lecturer, Department of Computer Engineering, SCMS College of Polytechnics, Kochi, India[2]

**ABSTRACT**: Blockchain as a distributed ledger technology has attracted extensive research attention. The main technology of cryptocurrencies is blockchain. The consensus protocol forms the core of the blockchain. They determine how the blockchain works. A good consensus protocol is considered to guarantee the fault tolerance and security of blockchain systems. In addition to cryptography and P2P technology, consensus protocols are also a fundamental component of blockchain technology. Improper tolerance and security of blockchain systems is guaranteed by a good consensus protocol. Byzantine errors have attracted new attention because they also fix blockchain systems. This paper introduces some of the major consensus protocols Proof of Work (PW), Proof of Stake (POS), Practical Byzantine Fault Tolerance (PBFT) and analyses their strengths and weaknesses.

**KEYWORDS**: Blockchain, Consensus Protocol, Byzantine Fault Tolerance.

## I. INTRODUCTION

Trade was a part of our daily activities before the time of industrialization. The famous barter system, which sells or exchanges goods according to needs. But not only trade, it also depends on the trust of the participants. The barter policy proved to be impossible as people did not know whom to trust. Therefore, it has developed a triple-entry bookkeeping system where a trusted third party, equally trusted by two of the participants in the trade, records the details of the transactions along with the participants in the trade. It offers authenticity, rejection and integrity. But greater reliance on third parties did not seem to be the safest way to trade. With the introduction of digital signatures, it will be solved in cryptography. Authenticity and integrity are provided using the elliptic curve digital signature algorithm, thereby providing security. But that did not prevent the system from double-cost attacks. When a party exchanges one of its "shares Y" with party B instead of "share X" there is a double cost. Being a malicious consumer cleverly exchanges the same "share Y" with party C for "share Z". Since Party C is unaware of the transaction between A and B, it agrees to this transaction with A. Now A has X and Z shares. This happened because C did not know about the transactions between A and B.

The solution to this problem is to provide copies of the transaction and distribute it to everyone so that everyone knows who is trading. It maintains the concept of distribution systems, replicas of data distributed through the network, thereby providing integrity. The entities of the system should be available whenever a transaction takes place. Obstacles such as the geographical location of different systems and different time zones also made the proposed idea impossible. It takes into account the idea of peer-to-peer networks. Now all colleagues can get information on all transactions and also verify them. And the number of peers required to verify can be set to zero, where merchants must confirm the transaction (they trust each other) or confirm the transaction, where the minimum n associates must verify the transaction to be verified.

Blackchain[1] first appeared on Nakamoto's Bitcoin White Paper, which explains the new decentralized cryptocurrency. Blackchain simply combines cryptography, distributed system technology, peer-to-peer networking technology and other popular technologies. In addition, Blockchain also provides a secure framework for cryptocurrencies, in which no one can damage the content of the transaction and all nodes participate in the transaction anonymously. For this reason, blockchain technology can be widely used in a variety of fields, e.g., the financial sector, medical systems, the supply chain and the Internet of Things (IoT).

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 9, Issue 10, October 2020||

## II. TYPES OF BLOCKCHAIN

There are basically two types of blockchains[2]; Private and Public Blockchain. There are many variations on the blockchain, such as consortium and hybrid blockchains.

**Public Blockchain** is a licensed, limited, distributed ledger system. Anyone with access to the Internet can sign in to the blockchain platform to become an authorized node and part of the blockchain network.
The node or user that is part of the public blockchain has the authority to access current and past records, verify transactions, or work proof of incoming block and mining. Basic use of public blockchain for mining and exchange of cryptocurrencies. The most common public blockchains are Bitcoin and Litcoin blockchains. Public blockchains are much safer if consumers strictly follow safety rules and practices. However, it is only dangerous if participants do not follow safety protocols wholeheartedly. Example: Bitcoin, Ethereum, Litcoin

**Private blockchain** operator only on closed network. Private blockchains are usually used in an organization where only selected members participate in the blockchain network. Security, powers, permissions, access level control is in the hands of the organization. Therefore, we use private blockchains as public blockchains but can use smaller and more limited networks. Private blockchain networks are used for voting, supply chain management, digital identification, property ownership, etc. Common examples of private blockchains; Multichain and Hyperledger projects (Fabric, South), Carda, etc.

The blockchain in the **consortium** is a semi-decentralized type where more than one organization operates the blockchain network. This is in contrast to a private blockchain, which is run by a single entity. More than one company acts as a node in the consortium blockchain and can exchange information or do mining. Consortium blockchains are commonly used by banks and government agencies. Common examples of consortium blockchain; Energy Web Foundation, R3, etc.

**A hybrid blockchain** is a combination of public and private blockchains. It uses the features of two types of blockchains, a private licensed-based system and a public-licensed-less system. In a hybrid network, users can control who can access the data stored in the blockchain. A section of selected data or records from the blockchain is allowed to go public to keep the rest of the private network system confidential. Blockchain's hybrid system is simple, allowing users to easily join a private blockchain with multiple public blockchains**.**

## III. PROPERTIES OF BLOCKCHAIN

The characteristics of blockchain are discussed below.
**Distributed consensus on chain status**: One of the key features of any blockchain is the ability to achieve distributed consensus on chain status without relying on a trusted third party. It opens the door to opportunities for miners in public blockchain systems or by authorized entities in private blockchain systems to build and use a system that verifies states and interactions.

**Immutability and Irreversibility of chain state:**Achieving a distributed consensus with the participation of a large number of nodes, the chain state becomes practically unchanged and irreversible after some time. This also applies to smart contracts and therefore enables the deployment and implementation of unchanging computer programs.

**Data (transaction) persistence**: Data in a blockchain is stored in a distributed fashion, ensuring data persistence as long as there are participating nodes in the P2P network.

**Data provenance:**The data storage process in any blockchain is facilitated by a process called transaction. Each transaction is required to be digitally signed using public key cryptography, which verifies the authenticity of the data source. Combining this with the unchanging and irreversible potential of blockchain provides a powerful denial tool for any data in blockchain.

**Distributed data control:** A blockchain ensures that data stored in the chain or retrieved from the chain can be carried out in a distributed manner that exhibits no single point of failure.

**Accountability and transparency:** Since the state of the chain, along with every single interaction among participating entities, can be verified by any authorised entity, a blockchain promotes accountability and transparency.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 9, Issue 10, October 2020||

## IV. MAJOR CONSENSUS PROTOCOLS

Literally consensus mean is agreement. Consensus algorithms[3] are those algorithms that help a distributed or decentralized network to unanimously take a decision whenever necessary. Its features include assuring decentralized governance, quorum structure, authentication, integrity, non- repudiation, byzantine fault tolerance and performance. The public blockchain, bitcoin uses the concept of proof of work (PoW). There are other forms of consensus protocols such as Proof of Stake (PoS), Practical Byzantine Fault Tolerance (pBFT).

**Proof of Work (PoW):**Satoshi Nakamoto introduced the PoW consensus model to the Bitcoin network as the backbone of the system. The Pow protocol requires adopting different conventions, such as the number of certifiers (called "miners") in the bitcoin case in monetary creation, for each "block" size that bothers the transactions waiting for certification, and the amount of the reward adjustment limit. In the PW protocol, it is a combination of cryptography and computational power that creates consensus and ensures the authenticity of the data entered into the blockchain. To prove that a block is valid and that work has been done, nodes in the network (known as miners) use their computational power to verify transactions (i.e. verify that the sender has sufficient funds and not double the cost) and most importantly one in a race to solve the cryptographic issues imposed by the protocol. This process is called mining [9]. Minors are encouraged to join the race twice: the first minor to find a solution will be rewarded with a protocol-defined ount and will be charged all transaction fees related to the transactions included in his / her block. When a minor finds a solution, he / she creates Block X by adding the hash, timestamp and transactions of the previous block. The miner transmits the newly created block X to the network and the other miners verify the transactions and then verify the block. Block is considered legal while other miners continue to work to extend the chain from Block X. When a chain splits, the longer chain should be chosen because the miners have done more work. Miners can work on multiple chains if they wish but their computing power is at risk of splitting.

The computational power that a miner possesses plays a deterministic role in the PoW protocol as the bigger the capacity to generate guesses, the higher the probability to find a solution. To do the mining process, computers run at maximum capacity, therefore consuming a considerable amount of electricity which makes by nature the PoW a resource-intensive consensus protocol; time and energy serve as proofs that work has been done.It is the probability that the PoW system can be attacked if a miner alone or a collusion of miners who possess more than half of the network total mining power.
This is also known as the 51% attack. In practice, attackers would create their own secret chain andbroadcast it to the network once it gets longer than the honest chain.

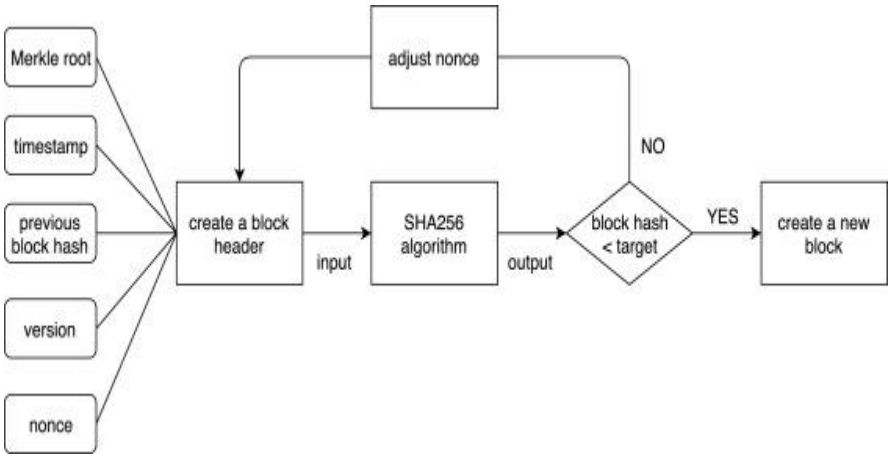


Fig 1: Flow of PoW.

**Proof of Stake (POS):** Proof of Stake (POS) is a consensus algorithm intended to achieve consensus on cryptocurrency blockchain network distribution. In pos-based cryptocurrencies, the creator of the next block is chosen by random selection and various combinations of age or wealth. In contrast, the algorithm of PW-based cryptocurrencies such as Bitcoin uses mining; That is, the solution of computationally intensive puzzles to verify transactions and create new blocks.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 9, Issue 10, October 2020||

Everyone at PoW may be a minor, but not everyone at PoS can join the network. POS requires currency ownership or a deposit on the network to participate in the minting process, i.e. to verify transactions and create blocks. No computational power is required to solve cryptographic puzzles in the PW scheme. There are no prizes in the form of money creation: certifiers collect fees from customers and pay as consumer intermediaries. Since certifiers only accept transaction fees, certifiers can avoid the scenario of creating empty blocks by encouraging them to include the maximum number of transactions to maximize their profits. The problem of early affordable coin distribution arises because new coins are not created in the purest form of posture and the money supply must be issued from the beginning.

One of the problems with POS is that it costs the validator nothing to vote for more than one block. This problem can be solved by allowing validators to vote only once and by imposing heavy fines on those who vote on more than one chain.

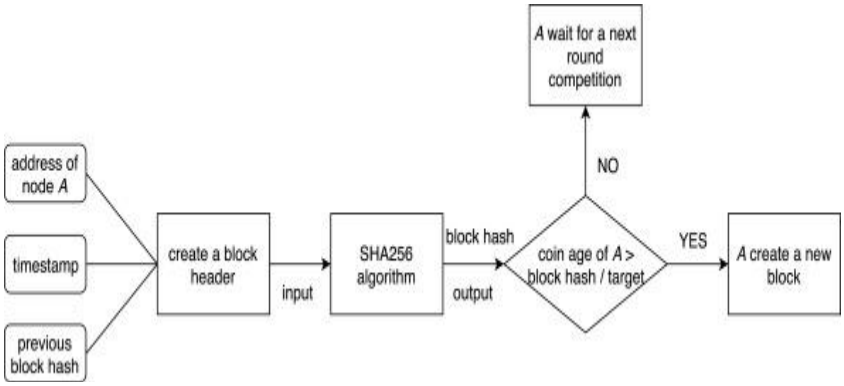


Fig2: Flow of PoS.

**PBFT (Practical Byzantine Fault Tolerance (PBFT)):** Practical Byzantine Fault Tolerance is a consensus algorithm introduced by Barbara Liskov and Miguel Castro in the late 90s. PBFT is designed to work on asynchronous systems. It is optimized for low overhead time. Its main goal is to solve many of the problems associated with the already available Byzantine fault tolerance solutions**.**

**Byzantine Fault Tolerance (BFT)** is a characteristic of a distributed network to reach consensus even when certain nodes in the network fail to respond or respond to misinformation. The goal of the BFT mechanism is to protect against system failures through the use of collective decision-making, which minimizes the impact of faulty nodes. Taken from the BFT Byzantine Generals issue.

**Byzantine Generals' Problem**

**Byzantine Generals' Problem[4]**was explained aptly in a paper by LESLIE LAMPORT, ROBERT SHOSTAK, and MARSHALL PEASE at Microsoft Research in 1982:

*Imagine that several divisions of the Byzantine army are camped outside an enemy city, each division commanded by its own general. The generals can communicate with one another only by messenger. After observing the enemy, they must decide upon a common plan of action. However, some of the generals may be traitors, trying to prevent the loyal generals from reaching an agreement. The generals must decide on when to attack the city, but they need a strong majority of their army to attack at the same time. The generals must have an algorithm to guarantee that (a) all loyal generals decide upon the same plan of action, and (b) a small number of traitors cannot cause the loyal generals to adopt a bad plan. The loyal generals will all do what the algorithm says they should, but the traitors may do anything they wish. The algorithm must guarantee condition (a) regardless of what the traitors do. The loyal generals should not only reach agreement, but should agree upon a reasonable plan.*

**Working of pBFT**: pBFT tries to provide a practical Byzantine state machine replication that can work even when malicious nodes are operating in the system.
pBFT contains five phases: **request, pre-prepare, prepare, commit and reply.**

The primary node forwards the message sent by the client to the other three nodes. In the case that node 3 is crashed, one message goes through five phases to reach a consensus among these nodes. Finally, these nodes reply to the client

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 9, Issue 10, October 2020||

to complete a round of consensus. PBFT guarantees nodes maintain a common state and take a consistent action in each round of consensus. PBFT achieves the goal of strong consistency, thus it is an absolute-finality consensus protocol takes a combined consensus protocol. EOS leverages PBFT to simultaneously work with the block validation and creation in DPoS, greatly reducing the time required for a round of consensus. A new protocol called Stellar is an improvement of PBFT. Stellar adopts FBA (Federated Byzantine Agreement) protocol, in which nodes can choose the federation they trust to conduct the consensus process

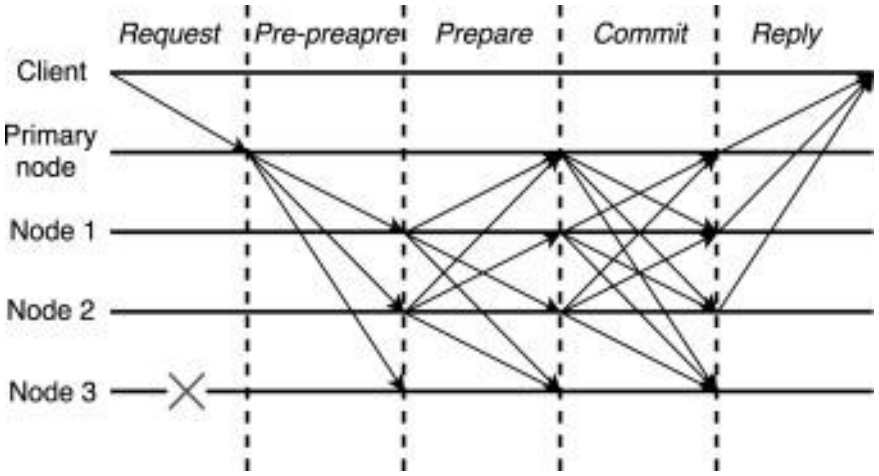


Fig3:Process of pBFT

## V. ANALYSIS AND COMPARISON OF MAJOR CONSENSUS PROTOCOLS

We analyse the major consensus[6] protocols in terms of fault tolerance, limitation, scalability and application conditions.

**Tolerance**

PoW, PoS are probability-final protocols, and attackers must accumulate large amounts of computational power or coins (stakes) to create a long private chain to replace a valid chain. In Bitcoin, for example, 50% of computational power is sufficient to create a long private chain of attackers to successfully complete a double-cost attack. Therefore, if the fraction of the attacker's computational power is greater than or equal to 50%, the blockchain network is undermined. Like PW, POS can only allow the presence of shareholders with less than 50% stake. In PBFT, if the network has a total of 3 f + 1 nodes, the number of normal nodes must exceed 2f + 1, i.e. the number of malicious or crashed nodes must be less than f. Therefore, the fault tolerance of PBFT is 1/3.

**Limit**

There is no doubt that PW consumes the most computing power among these consensus protocols, and the bitcoin's transaction output per second (TPS) is only 3–7, which greatly limits PW's application potential in actual payments. PBFT requires each node to communicate with other nodes in order to exchange messages at each round of consensus, so the PBFT network has high-performance requirements. Also, the identity of each node participating in the consensus is known, so there is no guarantee of anonymity.

**Scalability**

PoW, PoS all have good scalability. For example, Bitcoin adopts the Lightning Network to provide off-chain payment to improve scalability. Ethereum proposed Sharding technology and Plasma for Layer 1 and Layer 2 scaling solutions, respectively. The scalability of PBFT is limited because PBFT is compatible with a high-performance network with a small number of nodes.

**Scenes**

Current blockchain systems can be classified into three types. In a public blockchain, everyone can participate in the consensus process and the distributed ledger is visible to the public. Can be applied to PoW, PoS, Public Blockchain. Private blockchain and consortium blockchain belong to the licensed blockchain so only licensed nodes can participate in the consensus process. The identity of each node is known to the public in PBFT; Therefore, they are all suitable for

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 9, Issue 10, October 2020||

private blockchain or consortium blockchain. Although private blockchain and consortium blockchain are not as decentralized as public blockchain, due to the strong consensus and high efficiency of consensus, they are more suitable for certain commercial and medical scenarios.

Table 1
Main consensus protocols comparison.

| Property | PoW | PoS | pBFT |
|---|---|---|---|
| Type | Probabilistic-finality | Probabilistic-finality | Absolute-finality |
| Fault tolerance | 50% | 50% | 33% |
| Power consumption | Large | Less | Negligible |
| Scalability | Good | Good | Bad |

## VI. CONCLUSION

Blackchain technology is expected to revolutionize the finance and banking sectors worldwide. Most banks have already started building their own blockchain application or are looking for ways to launch one. The consensus protocol guarantees the stable operation of blockchain systems. Nodes agree on a specific value or transaction through a consensus protocol. In this paper, we have introduced some well-known blockchain consensus protocols and explored their strengths, weaknesses, and application scenarios.

A PW algorithm for solving a cryptographic puzzle is based on computational complexities or memory size / performance. Blockchain systems that use such a mechanism have specialized nodes called minor nodes that are responsible for solving the puzzle and creating a new and valid block and expanding the chain by adding this block to the existing chain. The probability of solving this problem depends on the network parameter, which is called the difficulty, which is adjusted automatically after some time. As more miners are involved in the network, the network parameters are adjusted to require more computing power to mine the new block. As related systems become more popular, it will attract more miners, which will increase the security of the system. However, increased computing power consumes more energy. Apart from this, PW systems generally have low output and do not scale properly.
To alleviate PW's major problems, Proof of Stack (POS) has been proposed. In POS, the nodes that are willing to participate in the process of creating the block are called miners, and they must hold and lock a certain amount of the corresponding crypto-currency called the share. Such a stake is used to ensure that the miners lose their stake when dealing maliciously so as to act as necessary.

PBFT is designed to work asynchronously (depending on when the response to a request is received). It is optimized for low overhead time. Its purpose is to address a number of issues related to the Byzantine Fault Tolerance Solutions already available.

## REFERENCES

[1] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” https://bitcoin.org/bitcoin.pdf.
[2] C. Cachin, “Architecture of the Hyperledger Blockchain Fabric,” https: //www.zurich.ibm.com/dccl/papers/cachin dccl.pdf.
[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]“Bitcoin energy consumption index,” Digiconomist. [Online]. Available: https://digiconomist.net/bitcoin-energy-consumption.
[6]Andreas M.Antonopoulos, Mastering bitcoins,2014.
[7] David Mazieres,, The Stellar Consensus Protocol:AFederated Model for Internet-level Consensus ,February 25,2016.
[8]. David Schwartz, Noah Youngs, Arthur Britto, TheRipple Protocol Consensus Algorithm, 2014.
[9]. Jae Kwon, Tendermint: Consensus without Mining,2014.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.512

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर
NISCAIR

# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

## IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details