Cryptographic consensus mechanisms[☆]

Shubhani Aggarwal[a], Neeraj Kumar[a], and Pethuru Raj Chelliah[b]
[a]Thapar Institute of Engineering & Technology, Patiala, Punjab, India
[b]Site Reliability Engineering (SRE) Division, Reliance Jio Infocomm. Ltd. (RJIL), Bangalore, Karnataka, India

Contents

Abstract

A consensus mechanism is a fault-tolerant mechanism used in a blockchain to reach an agreement on a single state of the network among distributed nodes. These are protocols that make sure all nodes are synchronized with each other and agree on transactions, which are legitimate and are added to the blockchain. Their function is to ensure the validity and authenticity of the transactions. Common consensus mechanisms that have been described in this chapter such as proof-of-work (PoW), proof-of-stake (PoS), delegated proof-of-stake (DPoS), practical Byzantine fault tolerance (PBFT), proof-of-capacity (PoC), proof-of-activity (PoA), proof-of-publication (PoP), proof-of-retrievability (PoR), proof-of-importance (PoI), proof-of-burn (PoB), proof-of-elapsed time (PoET), and proof-of-ownership (PoO).

[☆] Introduction to blockchain.

Advances in Computers
ISSN 0065-2458
https://doi.org/10.1016/bs.adcom.2020.08.011

Chapter points

- In this chapter, we discuss the different type of consensus mechanisms used in the blockchain network.
- Here, we discuss synchronization and coordination of all the nodes on the blockchain network to reach on one agreement using consensus mechanisms.

Consensus mechanisms are used in blockchain to manage all the nodes that process transactions on the network. It makes sure that all the nodes on the network are synchronized with each other and agree on one consensus in which transaction is legitimate and then added to the blockchain. These mechanisms are a crucial part of the blockchain network. When everyone can take part in the blockchain and submit data to the network, then with the help of the consensus mechanism transactions are continuously checked and verified by all the nodes. Without an agreement, blockchain is at risk of various types of attacks like DoS, DDoS, sybil attack, etc. There are many types of blockchain consensus mechanisms, which are described in Sections 1–12.

1. Proof-of-work

PoW is the most common consensus mechanism used by the most popular cryptocurrency like Litecoin and Bitcoin. The PoW is known as mining and the participated nodes in the process are known as miners. In this, miners solve complex and difficult mathematical problems and puzzles with the help of high computation power and high processing time. The first miner who solves the puzzle to create a block gets a reward with cryptocurrency. A more detailed description of the PoW process is provided in this chapter.

2. Proof-of-stake

PoS is the second most common consensus mechanism alternative to PoW. It uses low-energy, less processing time, low cost, low computational power than PoW. In this consensus mechanism, it uses a randomized method to choose who gets to create a next new block in the chain. Instead of miners, validators are present in PoS. The users can stake their tokens to become a validator which means they lock their money for a certain period of time to create a new block. The user who has the biggest stake has the highest chance to become a validator and a chance to create a new block. This process also depends on that one user how long the coins have been staked. By using this consensus mechanism in the network, we

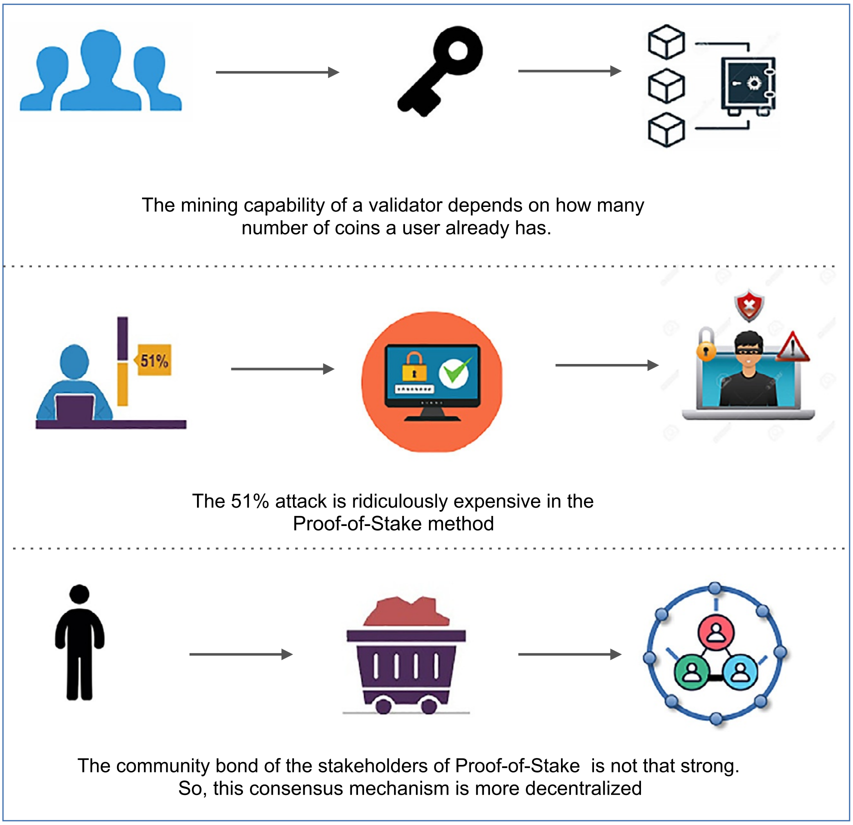

The mining capability of a validator depends on how many number of coins a user already has.
51%
The 51% attack is ridiculously expensive in the Proof-of-Stake method
The community bond of the stakeholders of Proof-of-Stake is not that strong. So, this consensus mechanism is more decentralized

Fig. 1 Proof-of-stake.

can save the energy of other validators because only selected validators can create a block. It is a very useful consensus mechanism because in which when a validator does wrong things during the creation of block then they lose their stakes. Hence, the validator gets rewarded for honestly. The other validators who verify and validate the block take their transaction fees because they get no rewards, unlike PoW. It uses the Ethereum platform. The pictorial representation of the PoS consensus mechanism is as shown in Fig. 1.

The main difference between PoW and PoS is as shown in Fig. 2.

3. Delegated proof-of-stake

Delegated proof of stake (DPoS) is a very fast consensus mechanism and used for the implementation of EOS. Firstly, we understand the word

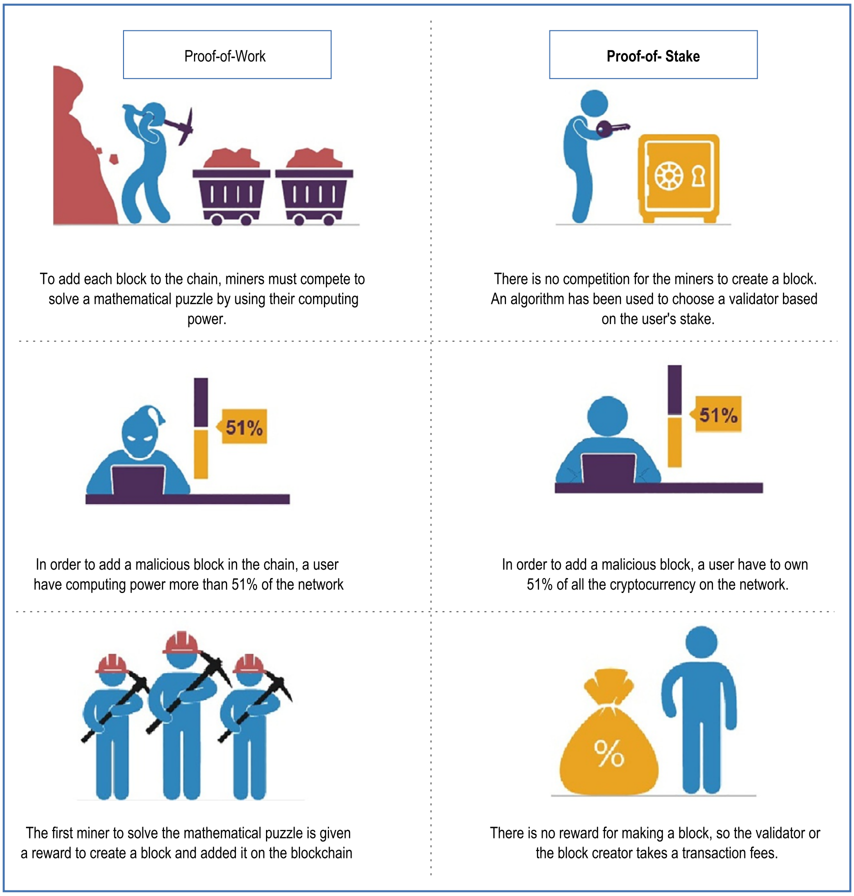
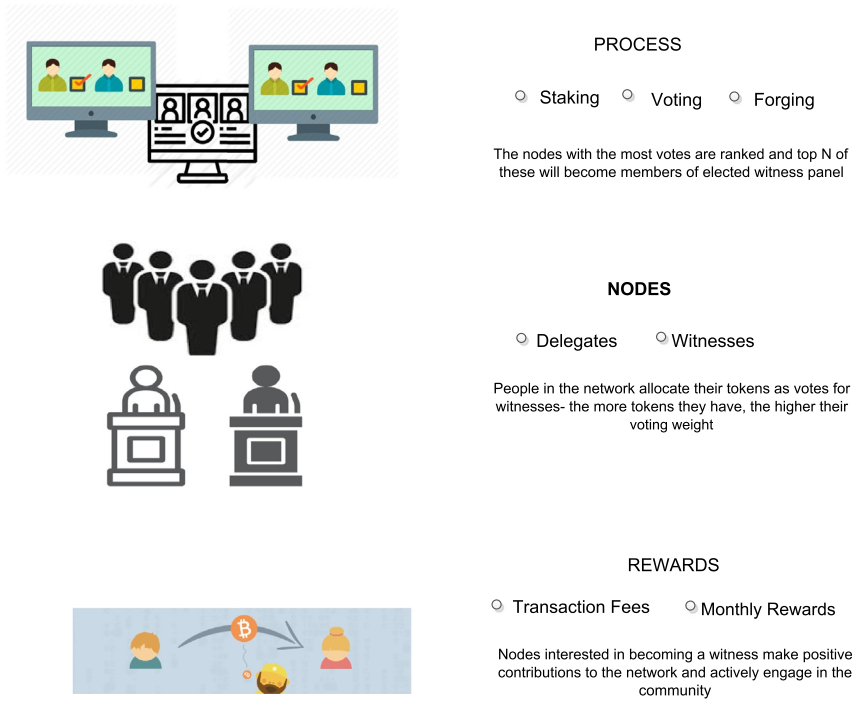

Proof-of-Work
Proof-of- Stake
To add each block to the chain, miners must compete to solve a mathematical puzzle by using their computing power.
There is no competition for the miners to create a block. An algorithm has been used to choose a validator based on the user's stake.
51%
51%
In order to add a malicious block in the chain, a user have computing power more than 51% of the network
In order to add a malicious block, a user have to own 51% of all the cryptocurrency on the network.
%
The first miner to solve the mathematical puzzle is given a reward to create a block and added it on the blockchain
There is no reward for making a block, so the validator or the block creator takes a transaction fees.

Fig. 2 Proof of work vs. proof of stake.

"*delegate*." It means a person or an organization that can produce blocks on the network. It receives the maximum number of votes from all the nodes of the network to create a block and gets rewarded. The delegates get rewarded either from the transaction fees or from a fixed amount of coins that are created during inflation. Secondly, the process of "*DPoS*" consensus mechanism. In this, the nodes of the network can stake their coins to vote for delegates. The weight of the vote depends upon the stakes. For example, If A stakes 5 coins for a delegate and B stake 1 coin then A*'s* vote weight is 5 times more than the B*'s* vote. The pictorial representation of DPoS is as shown in Fig. 3.

The DPoS is much more efficient at processing the transactions in comparison to another consensus such as PoW, PoS and is as shown in Fig. 4.



PROCESS

○ Staking ○ Voting ○ Forging

The nodes with the most votes are ranked and top N of these will become members of elected witness panel

NODES

○ Delegates ○ Witnesses

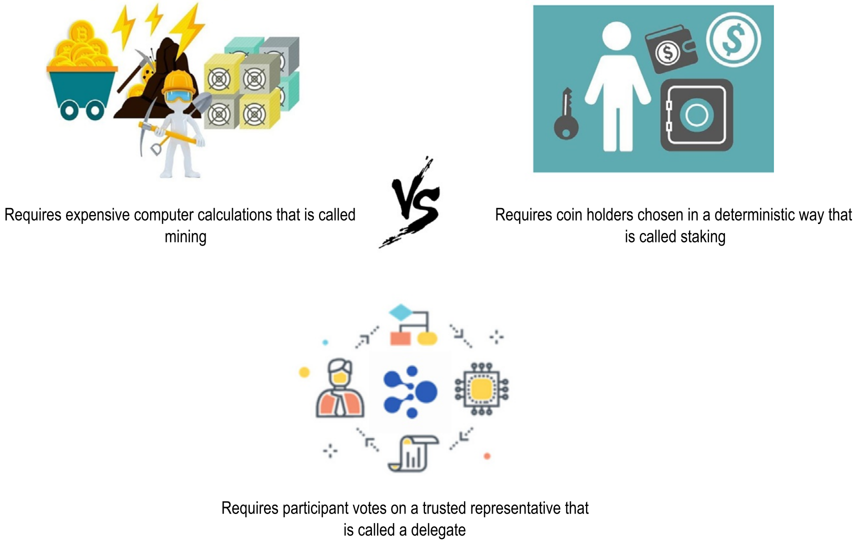
People in the network allocate their tokens as votes for witnesses- the more tokens they have, the higher their voting weight

REWARDS

○ Transaction Fees ○ Monthly Rewards

Nodes interested in becoming a witness make positive contributions to the network and actively engage in the community

Fig. 3 Delegated proof of stake.



Requires expensive computer calculations that is called mining

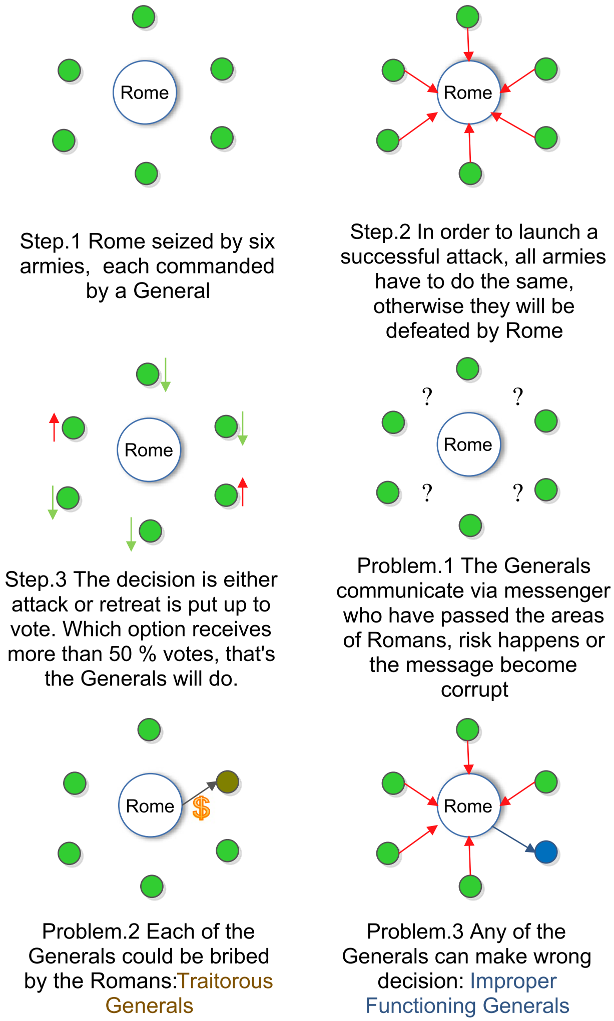
Requires coin holders chosen in a deterministic way that is called staking

Requires participant votes on a trusted representative that is called a delegate

Fig. 4 Proof of work vs proof of stake vs delegated proof of stake.

4. Practical Byzantine fault tolerance

Byzantine fault tolerance (BFT) is the resistance of a fault-tolerant distributed computer system against component failures. This is used by the NEO platform as a consensus mechanism. BFT is an analogy for the problem faced by a distributed computing system. The problems in BFT are described in Fig. 5.



Step.1 Rome seized by six armies, each commanded by a General

Step.2 In order to launch a successful attack, all armies have to do the same, otherwise they will be defeated by Rome

Step.3 The decision is either attack or retreat is put up to vote. Which option receives more than 50 % votes, that's the Generals will do.

Problem.1 The Generals communicate via messenger who have passed the areas of Romans, risk happens or the message become corrupt

Problem.2 Each of the Generals could be bribed by the Romans:Traitorous Generals

Problem.3 Any of the Generals can make wrong decision: Improper Functioning Generals

Fig. 5 Problems in Byzantine fault tolerance.

To solve the problem of a distributed computing system in BFT, practical Byzantine fault tolerance (PBFT) was developed. This consensus mechanism operated on the principle of BFT for verifying and the blocks using an election process comes after the validation process.

- Unlike DPoS, a *speaker* is chosen randomly from all the nodes then the remaining nodes on the network assume the role of delegates is as shown in Fig. 6.
- The*speaker* is responsible to construct a new block from the transaction. It verifies the transaction and also calculates the hash value. The pictorial representation is as shown in Fig. 7.
- Then, the block is sent to the delegates, who will validate the block and their transactions (scripts, data, claims, smart contracts). The pictorial representation is as shown in Fig. 8.
- The delegates validate the block by sharing and comparing their findings and all they reach to the same conclusion (more than 66.66% consensus). The pictorial representation is as shown in Figs. 9 and 10.

5. Proof-of-capacity

Proof of capacity (PoC) is a consensus mechanism used for plotting. In PoW, miners use computational power to choose a correct solution but in PoC, solutions are prestored in the memory hard-disks. The miners used this storage data to draw a plot. So, this process is called plotting. After the storage data has been plotted, miners can take part in the process of block creation. The more capacity, a miner have, the more solutions, a miner can store. So, in this way, the larger storage capacity of the miners has a high probability to create a new block using this mechanism.

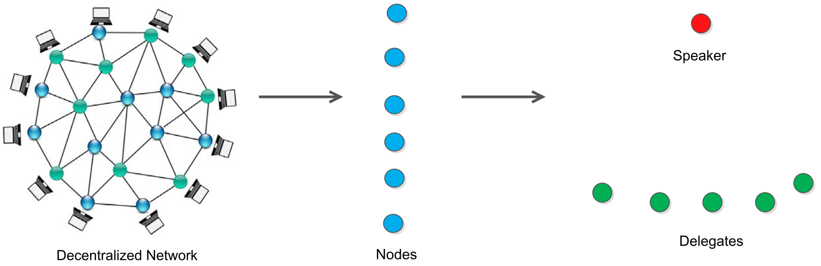


Fig. 6 Practical Byzantine fault tolerance-1.

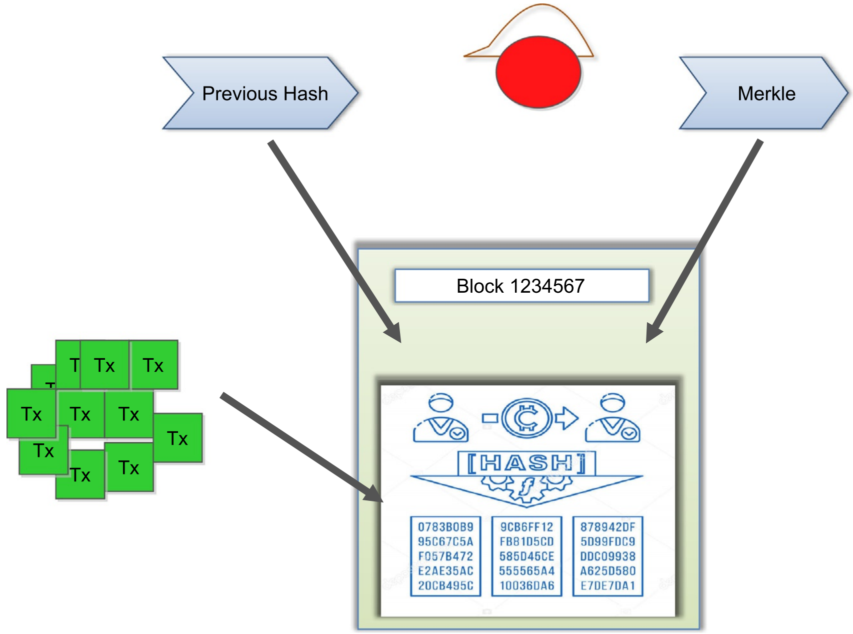


Fig. 7 Practical Byzantine fault tolerance-2.

6. Proof-of-elapsed time

Proof-of-elapsed time (PoET) is a consensus mechanism that chose miners in a random and fair manner. It also decides that who gets to produce a new block by choosing a miner. This consensus mechanism is based on the time that the miners have waited for the creation of the block. The process assigns a random and fair wait time to all the nodes on the network. The node on the network whose wait time finishes first gets to produce a new block. This mechanism works well for verification if a system has no multiple nodes and an assigned wait time is actually a random value.

7. Proof-of-activity

Proof-of-activity (PoA) consensus mechanism is much more work like PoW with reduced complexity in which the solution takes more time from a fraction of seconds to several minutes. It is a hybrid approach that combines PoW and PoS. Like PoW, miners solved the cryptographic puzzles and then, shifts to the PoS. The difference is that in which blocks contain templates instead of transactions that include header information and address

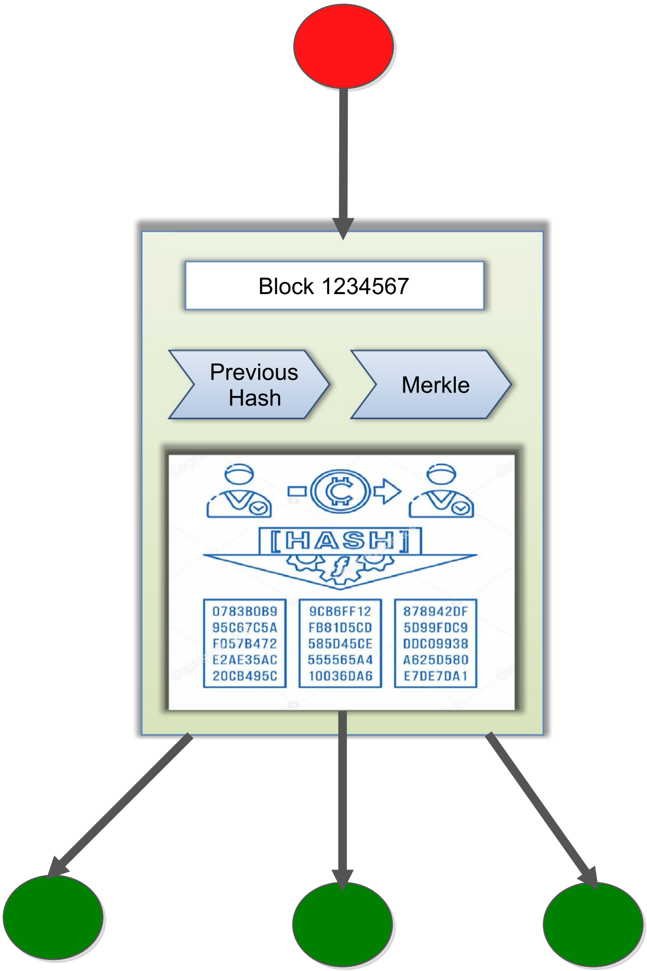
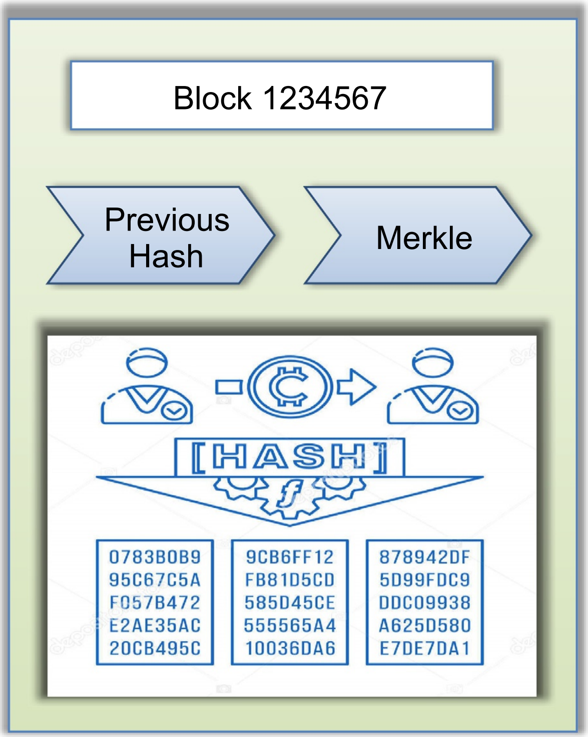


Fig. 8 Practical Byzantine fault tolerance-3.

of mining reward. In this, the blocks are verified by limiting the minimum possible time for the creation of a block that allows the maximum number of blocks added to the chain. Hence, preventing the network from spam transactions, i.e., emergence of floods.

8. Proof-of-publication

Proof-of-publication (PoP) is used in Bitcoin to check whether some particular information has been published at a certain time and date. This consensus mechanism entails the encoding of the secure hash of a certain plain text inside the bitcoin blockchain.



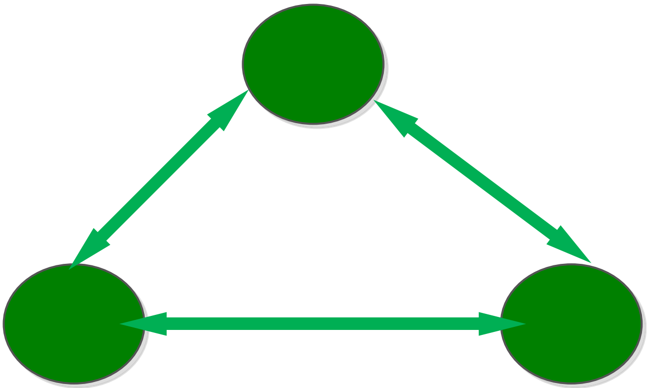


Fig. 9 Practical Byzantine fault tolerance-4.

9. Proof-of-retrievability

Proof-of-retrievability (PoR) is a consensus protocol wherein a server proves that a target file is fully downloaded and retrieved by a client from the server. The main advantage of PoR over other consensus mechanisms is

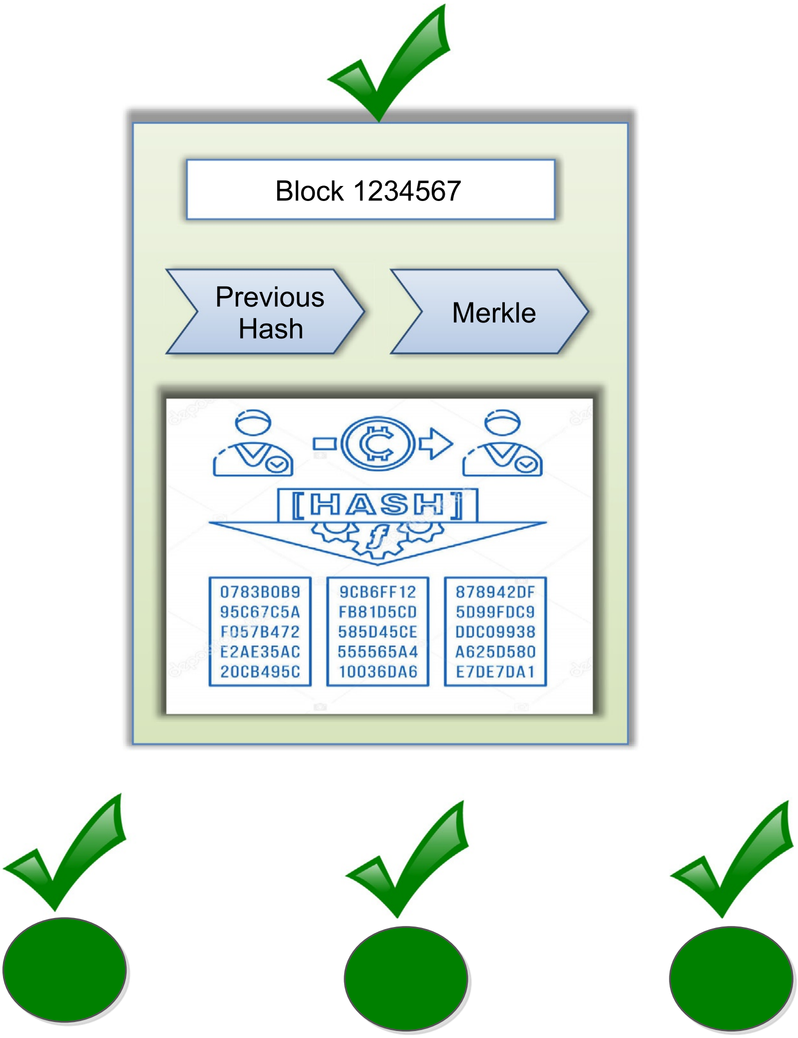


Fig. 10 Practical Byzantine fault tolerance-5.

efficiency. It is mainly deployed in an environment, where files are allocated across several systems in a redundant form.

10. Proof-of-importance

Proof-of-importance (PoI) is a consensus algorithm, introduced during the new economy movement (NEM), is used to check the entity responsible to verify the blockchain transactions.

11. Proof-of-ownership

Proof-of-ownership (PoO) is used to track the owners of some specific information at a certain time. This consensus mechanism can be used by entities, such as business organizations, to certify the integrity, date of publication, and ownership of their creations or contracts. It is implemented in CodeChain. As shown in Fig. 11, the buyer (prover) and the seller (verifier) can check the ownership of a asset. This allows safe P2P transactions. The buyer can check whether seller actually owns the pass before making the decision to buy. On the other hand, the receiver is guaranteed with an instant payment (due to the benefits of blockchain) as long as the seller is the actual owner.

12. Proof-of-burn

An alternative consensus protocol for PoS and PoW. In proof-of-burn (PoB) mechanism, the miners prove that they burn one cryptocurrency to create another currency, i.e., they are sent to a bitcoin address which is unsupendable. The significance of PoB depends on the burning tokens in an unrecoverable manner. As comparative to PoW and PoS, it is easily verifiable but hard to undo.

The difference among all consensus mechanisms are described in Table 1.

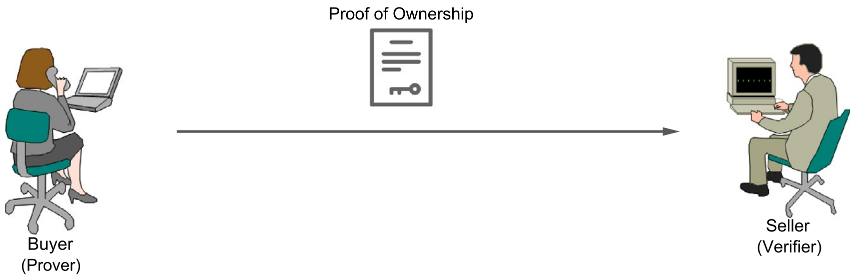


Fig. 11 Proof of ownership.

Table 1 Consensus mechanisms used in blockchain.

Consensus mechanism	Node identity	Language used	Execution environment	Energy efficient	Resource consumption	Cost	Through-put	Limitations
PoW	Public	Golang, C++, Solidity, Lisp Like Language (LLL)	Native, ethereum virtual machine (EVM)	No (high power)	High CPU	High	Low	Less secure, high power consumption
PoS	Public	Michelson	Native	Yes	Fast	Medium	Low	Consensus control to highest paid stakeholders
DPoS	Public	—	Native	Yes	Fast (faster than PoS)	Low	High	Limited token holders
BFT	Private	Any language	—	Yes	High CPU	Low	High	Semitrusted, complex with more nodes, less scalable
PBFT	Private	Golang, Java	Docker tool	Yes	High bandwidth	Low	High	Communication overhead is high for large nodes
PoC	Public	—	—	Yes	High memory	High	High	Chances of malicious vulnerable to mining tasks
PoET	Public	Python	Native	Yes	High	Low	Medium	Works only on dedicated hardware security

Continued

Table 1 Consensus mechanisms used in blockchain.—cont'd

Consensus mechanism	Node identity	Language used	Execution environment	Energy efficient	Resource consumption	Cost	Through-put	Limitations
PoA	Public	Solidity, Java, Python	EVM, Docker	No (but better than PoW)	High	High	High	Scalability and security is less
PoP	Private	Golang, C++, Solidity, Serpent, LLL	Native, EVM	Yes	Low	Low	High	Only used to check file publications
PoR	Public	Golang, C++, Solidity, Serpent, LLL	Native, EVM	Yes	Low	Low	Medium	Limited nodes usage
PoI	Public, Private	Java	—	Yes	Medium	Medium	Medium	Risk of nothing-at-stake issue
PoO	Public, Private	Any	C#	Yes	Medium	High	Medium	Expensive consensus
PoB	Public	Golang, C++, Solidity, Serpent, LLL	Native, EVM	No	Medium	Medium	Medium	costly for individual node, waste unnecessary resources

Shubhani Aggarwal is pursuing PhD from Thapar Institute of Engineering & Technology (Deemed to be University), Patiala, Punjab, India. She received the BTech degree in Computer Science and Engineering from Punjabi University, Patiala, Punjab, India, in 2015, and the ME degree in Computer Science from Panjab University, Chandigarh, India, in 2017. She has many research interests in the area of Blockchain, cryptography, Internet of Drones, and information security.

Neeraj Kumar received his PhD in CSE from Shri Mata Vaishno Devi University, Katra (Jammu and Kashmir), India in 2009, and was a postdoctoral research fellow in Coventry University, Coventry, UK. He is working as a Professor in the Department of Computer Science and Engineering, Thapar Institute of Engineering & Technology (Deemed to be University), Patiala (Punjab), India. He has published more than 400 technical research papers in top-cited journals such as IEEE TKDE, IEEE TIE, IEEE TDSC, IEEE TITS, IEEE TCE, IEEE TII, IEEE TVT, IEEE ITS, IEEE SG, IEEE Netw., IEEE Comm., IEEE WC, IEEE IoTJ, IEEE SJ, Computer Networks, Information sciences, FGCS, JNCA, JPDC, and ComCom. He has guided many research scholars leading to PhD and ME/MTech. His research is supported by funding from UGC, DST, CSIR, and TCS. His research areas are Network Management, IoT, Big Data Analytics, Deep Learning, and Cybersecurity. He is serving as editor of the following journals of repute: ACM Computing Survey, ACM·IEEE Transactions on Sustainable Computing, IEEE·IEEE Systems Journal, IEEE·IEEE Network Magazine, IEE·IEEE Communication Magazine, IEE·Journal of Networks and Computer Applications, Elsevier Computer Communication, Elsevier

International Journal of Communication Systems, Wiley. Also, he has been a guest editor of various international journals of repute such as IEEE Access, IEEE ITS, Elsevier CEE, IEEE Communication Magazine, IEEE Network Magazine, Computer Networks, Elsevier, Future Generation Computer Systems, Elsevier, Journal of Medical Systems, Springer, Computer and Electrical Engineering, Elsevier, Mobile Information Systems, International Journal of Ad Hoc and Ubiquitous Computing, Telecommunication Systems, Springer, and Journal of Supercomputing, Springer. He has also edited/authored 10 books with international/national publishers like IET, Springer, Elsevier, CRC: Security and Privacy of Electronic Healthcare Records: Concepts, Paradigms and Solutions (ISBN-13: 978-1-78561-898-7), Machine Learning for Cognitive IoT, CRC Press, Blockchain, Big Data and IoT, Blockchain Technologies Across Industrial Vertical, Elsevier, Multimedia Big Data Computing for IoT Applications: Concepts, Paradigms and Solutions (ISBN: 978-981-13-8759-3), Proceedings of First International Conference on Computing, Communications, and Cyber-Security (IC4S 2019) (ISBN 978-981-15-3369-3). One of the edited text-book entitled, "Multimedia Big Data Computing for IoT Applications: Concepts, Paradigms, and Solutions" published in Springer in 2019 is having 3.5 million downloads till June 6, 2020. It attracts attention of the researchers across the globe (https://www.springer.com/in/book/9789811387586). He has been a workshop chair at IEEE Globecom 2018 and IEEE ICC 2019 and TPC Chair and member for various international conferences such as IEEE MASS 2020 and IEEE MSN 2020. He is a senior member of the IEEE. He has more than 12,321 citations to his credit with current h-index of 60 (September 2020). He has won the best papers award from IEEE Systems Journal and ICC 2018, Kansas City in 2018. He has been listed in the highly cited researcher of 2019 list of Web of Science (WoS). In India, he is listed in top 10 position among highly cited researchers list. He is an adjunct professor at Asia University, Taiwan, King Abdul Aziz University, Jeddah, Saudi Arabia, and Charles Darwin University, Australia.

Pethuru Raj Chelliah works for RJIL, Bangalore. He worked for IBM Cloud, Wipro consulting services (WCS), and Corporate Research (CR) of Robert Bosch. His focus areas include containerization, Edge Computing, the Internet of Things (IoT), AI, and Blockchain Technology.