SNS COLLEGE OF ENGINEERING

Kurumbapalayam (Po), Coimbatore – 641 107

An Autonomous Institution

Accredited by NBA – AICTE and Accredited by NAAC – UGC with 'A' Grade
Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

COURSE NAME: 19CS622-Blockchain Technology

III YEAR /VI SEMESTER

Unit 1- INTRODUCTION TO BLOCKCHAIN

Topic 5 : Blockchain –consensus algorithms

Block chain Consensus algorithms

Block chain Consensus algorithms

1.   **Proof of Work (PoW)**

- Developed by [Satoshi Nakamoto](#),

- Proof of Work is the oldest consensus mechanism, named as mining where the participating nodes are called miners.

- In this mechanism, the miners have to solve complex mathematical puzzles using comprehensive computation power.

- is used by multiple cryptocurrencies like Bitcoin, Litecoin, ZCash, Primecoin, Monero, and Vertcoin to name a few.

Block chain Consensus algorithms

2. Proof of Stake (PoS)

- In this blockchain method, the block producers are not miners, but they act like validators.

- They get the opportunity to create a block over everyone which saves energy and reduces the time.

- The two popular variations of Proof of Stake (PoS) are DPoS and LPoS.

Delegated Proof of Stake (DPoS)

- Here the participants stake their coin and vote for a certain number of delegates such that the more they invest, the more weightage they receive.

- The delegates also get rewarded in the form of transaction fees or a certain amount of coins.

Leased Proof of Stake (LPoS)

- LPoS is an enhanced version of PoS consensus mechanism that operates on the Waves platform.

- Here each node with some amount of cryptocurrency is entitled to add the next blockchain, users can lease their balance to full nodes in this consensus algorithm blockchain.

Block chain Consensus algorithms

3. Proof of Authority

- Proof of Authority is a modified version of Proof of Stake in which the identities of validators in the network are at stake.

- In this, to verify the validator's identity, the identity is the resemblance between validators' personal identification and their official documentation.

- These validators put their reputation on the network.

- In Proof of Authority, the nodes (that become validators) are the only ones allowed to produce new blocks.

Block chain Consensus algorithms

4. Byzantine Fault Tolerance (BFT)

- Byzantine Fault Tolerance(BFT) is the feature of a distributed network to reach consensus(agreement on the same value) even when some of the nodes in the network fail to respond or respond with incorrect information.

- **The two variations of the BFT consensus model are PBFT and DBFT.**

4. Byzantine Fault Tolerance (BFT)

Practical Byzantine Fault Tolerance (PBFT)

- PBFT is a lightweight blockchain algorithm that solves the Byzantine General's problems by letting users confirm the messages that have been delivered to them by performing a computation to evaluate the decision about the message's validity.

- The party then announces its decision to other nodes who ultimately process a decision over it.

- This way, the final decision relies upon the decisions retrieved from the other nodes.

- Stellar, Ripple, and Hyperledger Fabric are some use cases of this blockchain consensus mechanism.

Block chain Consensus algorithms

4. Byzantine Fault Tolerance (BFT)

Delegated Byzantine Fault Tolerance (DBFT)

- the NEO token holders get the opportunity to vote for the delegates.

- The speaker creates a new block from the transaction that is waiting to be validated.

- Also, he sends a proposal to the voted delegates who have the responsibility to supervise all the transactions and record them on the network.

- These delegates have the freedom to share and analyze the proposals to check the accuracy of data and honesty of the speaker.

- If, then, 2/3rd of the delegates validates it, the block is added to the blockchain.

- This type of Blockchain consensus protocol is also called 'Ethereum of China' and can be a helpful resource in building a 'smart economy' by digitising assets and offering smart contracts on the blockchain.

Block chain Consensus algorithms

5. Direct Acyclic Graph (DAG)

- In this type of Blockchain consensus protocol, every node itself prepares to become the 'miners'.

- Now, when miners are eradicated and transactions are validated by users itself, the associated fee reduces to zero.

- It becomes easier to validate transactions between any two closest nodes, which makes the whole process lightweight, faster, and secure.

- The two best examples of DAG algorithms are IOTA and Hedera Hashgraph.

6. Proof of Capacity (PoC)

- In the Proof of Capacity (PoC) mechanism, solutions for every complex mathematical puzzle are accumulated in digital storages like Hard disks.

- Users can use these hard disks to produce blocks, in a way that those who are fastest in evaluating the solutions get better chances for creating blocks.

- The process it follows is called Plotting.

- The two cryptocurrencies that rely on PoC blockchain consensus protocol are Burstcoin and SpaceMint.

References

TEXT BOOKS

1. Mastering Bitcoin: Unlocking Digital Cryptocurrencies, by Andreas M Antonopoulos 2018

2. Imran Bashir, "Mastering Blockchain: Distributed Ledger Technology, Decentralization and Smart Contracts Explained", Second Edition, Packt Publishing, 2018.

3. https://101blockchains.com/blockchain-vs-database-the-difference/

REFERENCES

1. William Mougayar, "Business Blockchain Promise, Practice and Application of the Next Internet Technology, John Wiley & Sons 2016.

2. Josh Thompson, 'Blockchain: The Blockchain for Beginnings, Guild to Blockchain Technology and Blockchain Programming', Create Space Independent Publishing Platform, 2017.

3. Arvind Narayanan, "Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction", Princeton University Press, July 19, 2016.

4. Henning Diedrich, Ethereum: Block chains, Digital Assets, Smart Contracts, Decentralized Autonomous Organizations-2016

Thank You