University of London

MSc Data Science and Artificial Intelligence

DSM070 Blockchain Programming Coursework

Consensus Mechanisms in Bitcoin and Ethereum

Program: 50% - Essay: 50%

Table of Contents

List of Tables

Abbreviations:

PoW Proof of Work

PoS Proof of Stake

PoA Proof of Authority

P2P peer-to-peer

TPS Transactions Per Second

PoET Proof of Elapsed Time

EVM Ethereum Virtual Machine

IoT Internet of Things

ETH Ether

1. Introduction to Consensus Mechanisms:

Historically ledgers have been used to keep track of any kind of transactions, and then those are authenticated by some central authority. However, unlike traditional financial systems, in blockchain, as proposed by Satoshi Nakamoto, there is no central authority to verify and approve transactions. In contrast, there is a global public ledger containing all the details of transactions and each node in the network has a copy of that ledger, which is considered the record of ownership (Lashkari & Musilek, 2021).

However, the challenge is how the bitcoin network achieves global consensus on a single universal truth and reaches the same conclusion while eliminating the need for a central authority (Lashkari & Musilek, 2021).

This is where Bitcoin's decentralized network-wide consensus occurs based on four processes that occur through an asynchronous interaction between all nodes across the blockchain network. The processes cover the following areas:

- Independent verification and mining: this is where any new transactions are verified in terms of, for example, syntax, data structure and size. This will ensure that invalid transactions are rejected, and only verified transactions are broadcasted to the network. This is done by particular nodes in the network called "miners", who, in return for doing the verification they get a reward in the form of new coins for each new block and transaction fee from all the transactions in the particular block
- Aggregation of transactions into new blocks: once a transaction is validated, it will be added to the memory pool and accordingly can be added into a block (aggregated into a candidate block)
- Verification of the new blocks: Once a new block is generated and before it is propagated into the blockchain network, independent validation is performed by each node. The validation ensures that only valid blocks will continue, and miners will accordingly get the rewards. Otherwise, the block will be discarded, and that miner will not be rewarded if any kind of cheating occurred
- Finally, the last process in bitcoin's consensus mechanism is the selection of the chain with the longest blocks: This is based mainly on assembling the block having the most proof-of-work (PoW), which is then connected to the existing blockchain in "the main chain" which is basically a valid chain with the most cumulative PoW. This is how network-wide consensus is achieved between all the nodes in the blockchain while discrepancies get resolved over time as more blocks are added to the chain

(Antonopoulo, 2014)

2. Type of Mechanisms:

Blockchain is widely known to be as a decentralized technology that is secure-by-design. The security promised by blockchain is really unprecedented and very innovative.

In addition to cryptography and P2P (peer-to-peer) technology, distributed consensus protocols play a key role in the underlying blockchain technology, particularly the security and performance aspects. This goes back to the Nakamoto consensus protocol, which is implemented in the bitcoin network based on PoW mechanism. However, it has faced performance problems such as low Transactions Per Second (TPS) and high energy consumption. This has led the blockchain community to explore new mechanisms such as proof of stake (PoS), proof of authority (PoA), and Proof of Elapsed Time (PoET) to address the below limitations and cater for the needs of other applications, which are leveraging blockchain (Xiao et al., 2020; Zhang & Lee, 2020).

2.1 Consensus Mechanisms in Bitcoin:

Bitcoin follows Nakamoto's consensus protocol, whereby transactions are propagated through the P2P network through a mechanism called advertisement-based gossiping. In summary, whenever a new block is received by a node and validated, that node will advertise it within the network. Then other nodes will extend their local blockchains using that new block (Xiao et al., 2020).

This consensus protocol follows the below rules:

- PoW: in order to generate a new block, a hash function has to be resolved against a target value
- Gossiping Rule: Any generated or received transaction must be immediately propagated and broadcasted to the network nodes
- Validation Rule: before the block or transaction is broadcasted, there is a validation on the block header against double-spending or PoW tampering
- Longest-Chain Rule: this is fundamentally the network-wide consensus and must be accepted by all nodes in the network, and any further mining will aim to extend that chain
- Block Rewards and Transaction Fees: once Miners generate a new block, they can claim a Coinbase as a reward. Moreover, a specific transaction fee is collected from all transactions received by the miner. This amount is fixed and halves every four years - Expected to be exhausted entirely by 2140

(Xiao et al., 2020)

2.1.1 Proof of Work:

Bitcoin relays on PoW as a consensus algorithm. PoW was introduced in 1992 and utilized later in 2002 to combat spam emails by making it time-consuming for someone to send multiple emails. This was achieved by requiring a function to be calculated before sending the email, and the obtained value will be added to the email header. Later, the recipient can verify the email (Ismail & Materwala, 2019).

Satoshi Nakamoto proposed to use the PoW algorithm in 2008 as part of the bitcoin blockchain network. In his proposal, the mining nodes will compete in generating new blocks with valid

transactions. Each miner will hash the block data using a counter value, known as nonce. The hashing will generate an output that will be less than a particular threshold, and this is intended to increase the mining complexity (Ismail & Materwala, 2019).

The block hash is calculated by miners using the SHA-256 hash function of the following (Merkle root, transaction timestamp, previous block hash, block version, and nonce). Then, the hash value is added along with the nonce to the block header, and finally, the block will be broadcasted to the blockchain network by the miner. Meanwhile, other miners will evaluate whether the proposed is valid and stop the mining. In case the block turns out to be valid, the miner will receive a transaction fee and mining reward for the efforts and electricity used, the ledger will be updated accordingly, and miners will focus on mining the next block.

The PoW algorithm difficulty level determines primarily the time required to generate a new block, and the difficulty and target value in the network have been usually adjusted after every 2016 block so that one block is generated every 10 minutes constantly (Ismail & Materwala, 2019).

Below Equations (1) and (2) provide the calculation of difficulty and target value.

(1) $D_{new} = D_{current} \times \frac{20160}{T_{2016}}$

(2) $Target_{new} = Target_{current} \times \frac{T_{2016}}{20160}$

Where D_{new} and $D_{current}$ are the new and current difficulty levels, respectively, and $Target_{new}$ and $Target_{current}$ are the new and current target.

However, there are gaps between PoW consensus algorithm and the application needs in terms of, for example, cost-effectiveness and energy efficiency. Networks implementing PoW have a throughput of only 60 transactions per second. Moreover, miners usually gather in what is known as mining pools where each miner uses its computing power and accordingly, the reward will be divided among them. The issue is that if that mining pool owns above 50% of the computing power, it will pose a risk that miners could prevent validation of transactions. This is also known as the problem of 51% attack. Another challenge with PoW is that for a particular minor to have a chance of mining a block, that chance is correlated to the computational resources owned by the miner. The environmental impact is influenced by high amount of energy consumption from mining, contributing to the increasing global warming phenomena (Ismail & Materwala, 2019).

2.2 Consensus Mechanisms in Ethereum:

Ethereum was initially proposed in 2013 by Vitalik Buterin in his white paper as a decentralized platform based on blockchain technology and went live in July 2015. Although Ethereum is considered, like Bitcoin, as a cryptocurrency, its architecture of Ethereum also allows it to enable other applications running on peer-to-peer networks, such as smart contracts (Chowdhury, 2019).

Ethereum widens the possibilities from blockchain one step by allowing users to run programs using Ethereum Virtual Machine (EVM). This is suited mainly for applications that require direct peer-to-peer interaction within a network such as Internet of Things (IoT) or voting. Ether (ETH) is the native token in Ethereum and is distributed for users when running transactions or smart contracts on Ethereum (Chowdhury, 2019).

Currently, PoW and PoS are the consensus mechanisms used in Ethereum. Like Bitcoin, PoW was the protocol used as an incentive-driven security standard. However, there has been lately a shift towards Ethereum 2.0, which is an evolution of the Ethereum blockchain technology, depends on PoS as the consensus mechanism to verify through staking the wealth rather than mining using high power computing, which would require massive amounts of electricity to complete the verification of transactions (Thanujan et al., 2020).

2.2.1 Proof of Stake:

As of Q2 2022, Ethereum started to run two blockchains based on PoW and another chain to test PoS. The plan is that later in 2022, a merge will combine legacy Ethereum (ETH1) and the new Beacon Chain (ETH2) into a single blockchain based on PoS only. PoS protocol is seen as an alternative to PoW whereby instead of mining, the users are considered as validators. They will be required to lock up an amount of tokens, a minimum of 32 ETH, in order to participate in the verification process rather than mining. The higher the amount, the better chance for that user to create the next block. This selection process is expected to consume much less energy and is more environmentally-friendly through the use of sharding (Duggan Wayne & Powell Farran, 2022).

3. Compare and Contrast Different Mechanisms:

In blockchain, there is such thing as a perfect consensus protocol and it will largely depend on the type of application. In reality, a protocol has to strike a trade-off between factors such as consistency, security and energy consumption. Below is a comparison between two of the main consensus protocols (PoW vs PoS) in terms of type, fault tolerance and scalability.

Table 1: Comparison between PoS and PoW

Property	PoW	PoS
Type	Probabilistic finality	Probabilistic finality
Fault tolerance	50%	50%
Energy consumption	Large	Minor
Scalability	Good	Good
Transaction per second	3-7	12-15 expected to reach 100,000
Applications	Public blockchain	Public blockchain

In conclusion, PoS shows more benefits than drawbacks as compared to PoW. PoS enhances the security, scalability and sustainability of the blockchain future. PoS also addresses the environmental concerns since it consumes significantly less electricity and, on the other hand, ensures more throughput while validating transactions (Zhang & Lee, 2020).

4. References:

Antonopoulo, A. M. (2014). Mastering Bitcoin. *Sermaye Piyasası Kurulu Araştırma Dairesi*, *9*(1), 75–82. http://dergipark.gov.tr/doi/10.29048/makufebed.365066%0Ahttp://www.spk.gov.tr/SiteApps/Yayin/YayinGoster/1130

Chowdhury, N. (2019). Inside Blockchain, Bitcoin, and Cryptocurrencies. In *Inside Blockchain, Bitcoin, and Cryptocurrencies*. Auerbach Publications. https://doi.org/10.1201/9780429325533

Duggan Wayne, & Powell Farran. (2022). *What Is Ethereum 2.0? Understanding The Merge*. Forbes Advisor. https://www.forbes.com/advisor/investing/cryptocurrency/ethereum-2/

Ismail, L., & Materwala, H. (2019). A Review of Blockchain Architecture and Consensus Protocols: Use Cases, Challenges, and Solutions. *Symmetry 2019, Vol. 11, Page 1198*, *11*(10), 1198. https://doi.org/10.3390/SYM11101198

Lashkari, B., & Musilek, P. (2021). A Comprehensive Review of Blockchain Consensus Mechanisms. *IEEE Access*, *9*, 43620–43652. https://doi.org/10.1109/ACCESS.2021.3065880

Thanujan, T., Rajapakse, R. A. C. P., & Wickramaarachchi, D. (2020). *A Review of Blockchain Consensus Mechanisms: State of the Art and Performance Measures*.

Xiao, Y., Zhang, N., Lou, W., & Hou, Y. T. (2020). A Survey of Distributed Consensus Protocols for Blockchain Networks. *IEEE Communications Surveys and Tutorials*, *22*(2), 1432–1465. https://doi.org/10.1109/COMST.2020.2969706

Zhang, S., & Lee, J. H. (2020). Analysis of the main consensus protocols of blockchain. *ICT Express*, *6*(2), 93–97. https://doi.org/10.1016/J.ICTE.2019.08.001

5. Word Count:

Total number of words: 1755 **words**