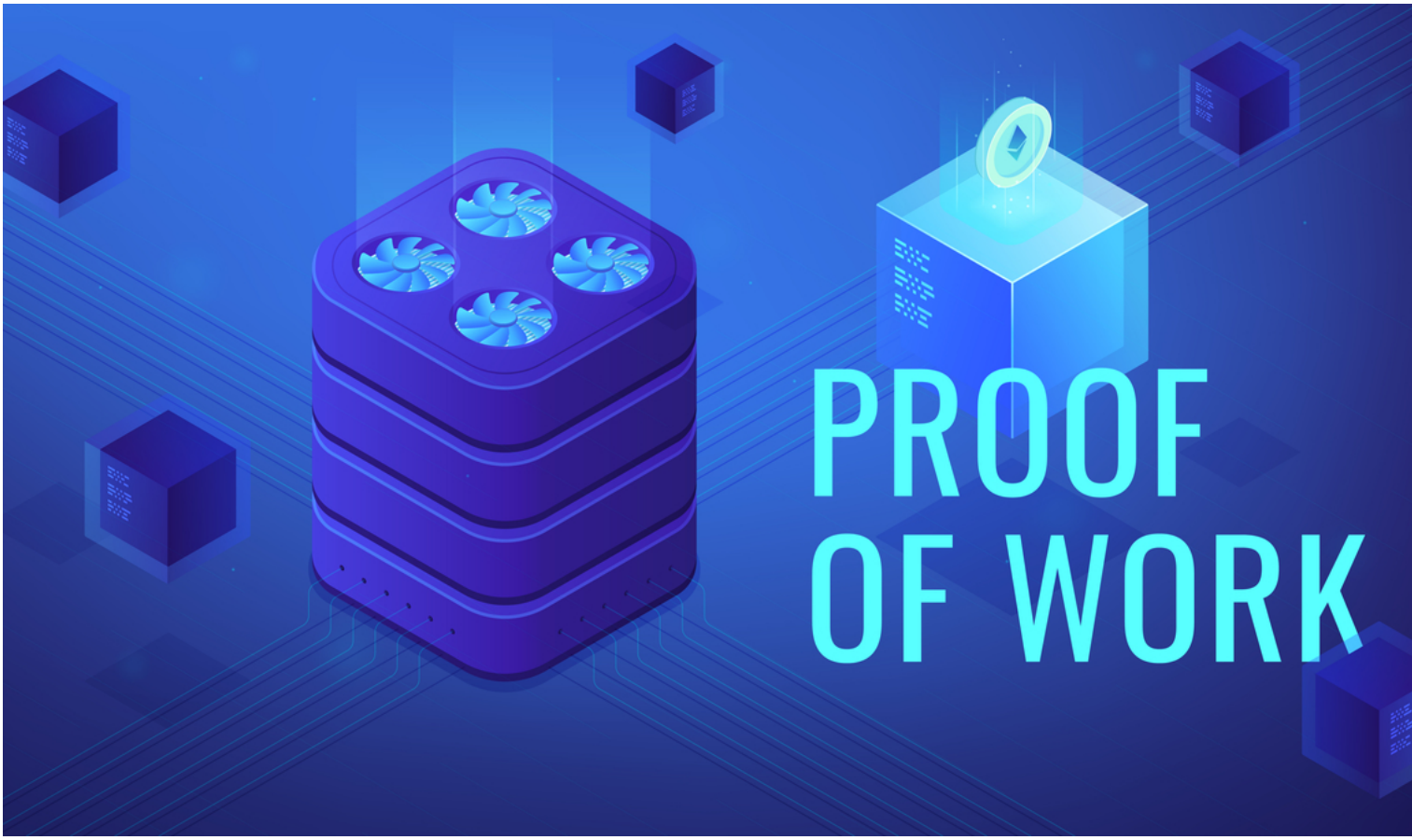
Blockchain : Proof-of-Work (PoW)

BEGINNER BLOCKCHAIN

This article was published as a part of the Data Science Blogathon.

Introduction

Proof-of-Work (PoW) in the blockchain is a consensus mechanism that allows miners to add a new block to the network based on calculations made to find the perfect hash. Network participants verify the transactions added by the new block.
For a decentralized network like Blockchain, keeping all network participants in sync is essential. However, it seems far-fetched for everyone to agree on one thing. Blockchain uses a consensus mechanism to create governance among all network participants. In this article, we will go through one of the most popular and basic consensus protocols i.e., Proof-of-Work (PoW) in the blockchain.

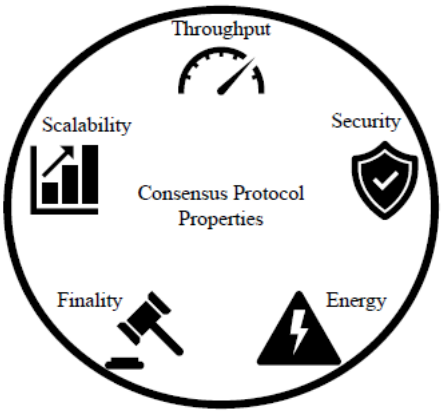


source: https://www.btcc.com/en-US/tags/proof-of-work-blockchain

What is a consensus mechanism?

Simply put, consensus means reaching a decision that all network participants agree on. For example, a group of friends agrees to play soccer without conflict. Reaching a decision to play football together is a

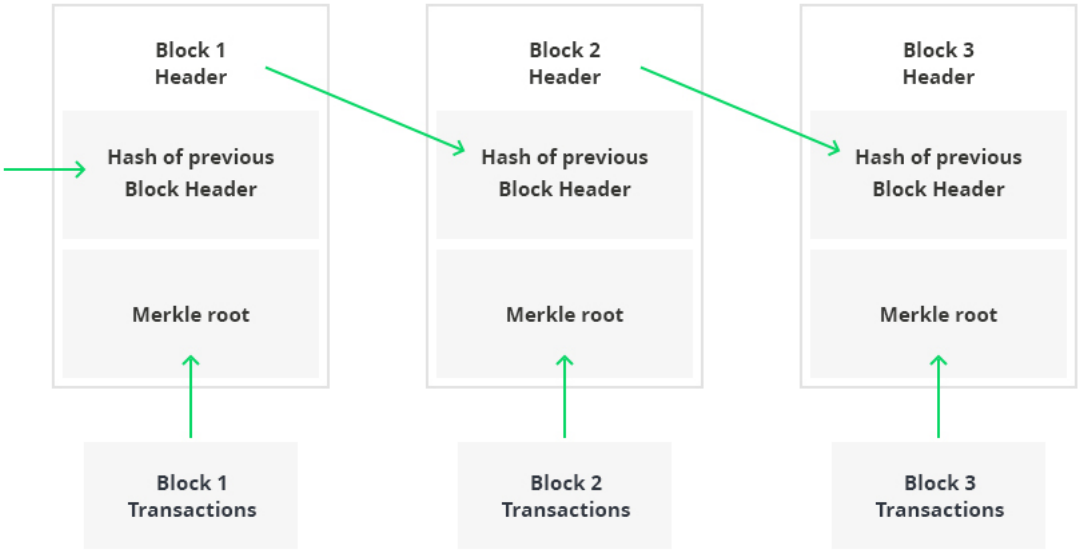
state of consensus or mutual agreement here.
“The main purpose is giving a group of different kinds of nodes. However, the update will take place according to several established rules among a group of participants in a secure manner.”
In the case of Blockchain, at least 51% of nodes or network participants agree on the upcoming change. If this happens, the network is updated with the new change. Otherwise, he rejects the change by mutual agreement.



source: https://bootcamp.uxdesign.cc/blockchain-consensus-mechanisms-692497f0d5f9

What is Proof-of-Work (PoW)?

The Proof-of-Work (PoW) consensus mechanism is the oldest yet most popular. The idea emerged in 1993 when Moni Naor and Cynthia Dowrk published a paper exploring the potential of algorithms to prevent fraud. Later, Satoshi Nakamoto created the algorithm (the anonymous figure behind the discovery of Bitcoin) in his white paper “Bitcoin: a peer-to-peer E-Cash system” in 2008.
PoW plays a significant role in the development of Blockchain technology. The goal is to create an authentication system that is hard to crack.
The decentralized network works on the principle of distrust but cooperation. Blockchain (decentralized network) is a chain of linearly connected blocks containing information secured by cryptography. Here, each block contains the hash of its previous block to stay connected.
Additionally, each block contains several other information such as timestamp, block height, transaction records, Merkle Root Hash, block hash, previous block hash, difficulty level, and many more in the block header. The second part contains a set of financial transactions, the hash of which is eventually converted to a Merkle root. So Blockchain is defined as the chain of blocks of transactions.



source: https://jovian.ai/paulbindass/chapter-2-blockchain-basics

Block Mining

Adding a new block to the chain is considered a new update to the current system. It, therefore, requires permission from network participants. In order to decide whether to add a new block or not, Proof-of-Work (PoW), a consensus mechanism, is used. Only verified transactions are added to the network.
In contrast, not all blocks are valid. Most proposed block networks are considered invalid. The Blockchain protocol defines the validity of a block. The blockchain network has an arbitrary “Difficulty” setting managed by the protocol that changes how hard it is to mine a block. Mining here means adding a new block.
Miners design new blocks in the chain. They are externals who want to add their block to the network. The work required to develop a valid block is where the value comes from. Miners receive rewards in proportion to their share of the computing power they spend mining a new block. The miner proves the work done by mining a valid block.
The difficulty level can vary in blockchains such as the Bitcoin network or Ethereum to ensure that blocks are created at regular intervals.

How does the PoW algorithm work?

The Proof-of-Work (PoW) consensus algorithm works by requiring each miner to overcome a difficulty level to prove the validity of a block. A block is marked as “valid” only if the hash value of the entire block is lower than the difficulty hash.

Block Hash < Hash Difficulty

The block contains important transaction information that cannot be changed. So miners change the nonce to get the hash below the difficulty threshold. A nonce is a part of a block that can be changed to limit the difficulty level.
Let’s take an example to understand the working PoW and how it works.

Harry is a Bitcoin miner who wishes to add his block of Bitcoin (digital currency) transactions to the network. However, for his block to be valid. First, he must change the block until the hash of his block falls

below the difficulty threshold.
let's say:
Harry block Hash: 817de9e0c
Hash difficulty: 001000000
Nonce: 8263

Harry will change the nonce until he gets the first 3 digits as zeros.
After continuously changing the nonce for hours, he finally got the hash.
Harry block Hash: 000383ec5
Hash difficulty: 001000000
Nonce: 6778
The difficulty threshold has now been reached. **Block Hash < Hash Difficulty.**

Therefore, Harry's block will be marked as valid and added to the blockchain. For mining a block in the Bitcoin blockchain, Harry gets a few Bitcoins as a block reward for spending the computing power to find a valid hash.
This process is completely based on chance. So the miner's job is to change the nonce value until the total hash of the block is lower than the difficulty hash. There are other responsibilities of miners, but that is a topic for another article.

Advantages of Proof-of-Work

Below are the advantages of the Proof-of-Work (PoW) mechanism:

- A hard-to-find solution. Still, easy verification.
- As an initial consensus mechanism, PoW does not need initial stakes of coins before mining. One can start with 0 coins and it will only be positive.
- Ease of implementation compared to other blockchain consensus mechanisms.
- It is fault tolerant. It means that the failure of one component will not shut down the entire blockchain network.

- Give miners the opportunity to earn by adding a block.
- PoW is the oldest, most trusted, and most popular consensus protocol.

Limitations of Proof-of-Work

Below are the disadvantages of the Proof-of-Work (PoW) mechanism:

- A lot of energy is wasted because only one miner can finally add their block.
- It requires a lot of computing power and, therefore, massive consumption of resources and energy.
- 51% risk of network attack. A controlling person can get 51% to control the network.
- Spread environmental hazards with attachment machines.
- Pow is a time and energy wipe-out process.
- It required a lot of hardware costs.
- Risk of Denial of Service Attacks by Intruders.

Which cryptocurrencies use PoW?

Below are the Major cryptocurrencies that currently use Proof-of-Work (Pow):

1. **bitcoin**
2. **Ethereum**
3. **Dogecoin**
4. **Litecoin**
5. **Monero**
6. **Bitcoin Cash**
7. **DigiByte**
8. **Bitcoin gold**
9. **Ethereum Classic**
10. **Zcash**

Outside of PoW:

This doesn't seem like a fair deal to miners who don't have the heavy machinery to run such massive calculations. Complying with a Proof-of-Work (PoW) mechanism involves considerable cost and effort. It also requires gas as a transaction fee. Therefore, much research is going on to replace this consensus mechanism. Some alternative algorithms include Proof-of-Stake (PoS), Proof-of-History (PoH), Proof-of-Authority (PoA), Proof-of-Capacity (PoC), Proof-of-Elapsed-Time (PoET), and many others.

Proof of Work vs. Proof of Stake

Proof of work and proof of stake are two discrete consensus mechanisms for cryptocurrency, but there are important differences between them.
Both methods confirm incoming transactions and add them to the blockchain. With Proof of Stake, network participants are known to as “validators” other than miners. One important difference is that instead of solving math problems, validators lock up a set amount of cryptocurrency – their stake – in a smart contract on the blockchain.
In interchange for “staking” cryptocurrency, they get a chance to prove new transactions and earn a reward. However, if they incorrectly verify wrong or fraudulent data, they may lose some or all of their deposit as a penalty.
Proof of stake makes it easy to involve more people in blockchain systems as validators. There is no need to buy expensive computing systems and consume huge amounts of electricity to bet cryptocurrencies. All you need are coins.

Conclusion

Proof of work is the most desired of the two main consensus mechanisms for verifying transactions on blockchains. While not without limitations, miners using proof of work help ensure that only legitimate transactions are recorded on the blockchain. The above article goes through the basics of consensus mechanisms and Proof-of-Work (PoW). It also covered how PoW works, its benefits, and its limitations.

Key takeaways:

- Proof of work (PoW) is a decentralized consensus mechanism that stands in need of network members to put attempts into solving an arbitrary mathematical puzzle to prevent anyone from gaming the system.
- Proof of work is largely used in cryptocurrency mining to clarify transactions and mine new tokens.
- With proof of work, Bitcoin and other cryptocurrency transactions can be processed peer-to-peer securely without needing a trusted third party.
- Proof of work at scale requires a huge amount of energy, which only increases as more miners join the network.
- Proof of Stake (POS) was one of several new consensus mechanisms created as an alternative to proof of work.

The media shown in this article is not owned by Analytics Vidhya and is used at the Author’s discretion.

Article Url - https://www.analyticsvidhya.com/blog/2022/09/blockchain-proof-of-work-pow/



ANURAG SINGH CHOUDHARY