MINING CITY

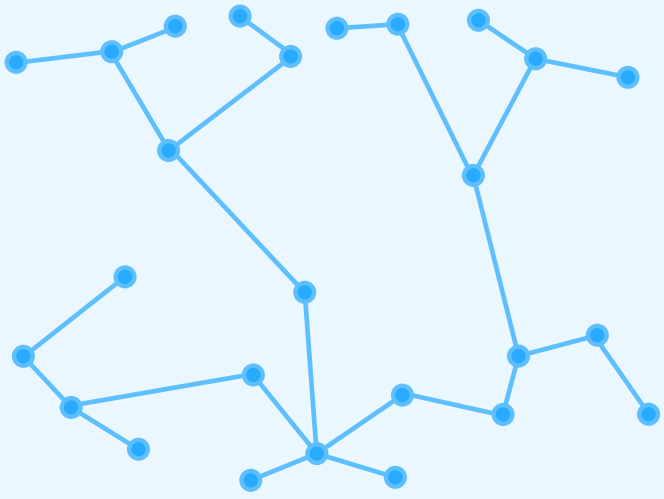
What is Proof of Work (PoW)?

There are two major systems of mining for crypto. Proof of Work (PoW) and Proof of Stake (PoS). This article will focus on PoW, essentially a way for powerful computers to compete against each other to be able to solve difficult problems and earn a crypto reward. This is the underlying system behind Bitcoin, Ethereum, and Bitcoin Vault mining.

Proof-of-Work, as the name suggests, is a system that proves that certain work was done. In general, the concept of Proof of Work predates crypto by well over a decade. It was developed in 1993 by Cynthia Dwork and Moni Naor to prevent abuse such as spam on a network by requiring some work from the service user, usually meaning processing time by a computer.

In terms of cryptocurrency, **Proof of Work refers to the process of mining where miners – very powerful computers connected to the network – compete to solve complicated mathematical problems**. As a reward for their efforts, they receive newly created coins.

In the crypto industry, PoW was first used in Bitcoin mining. And as a result of the growing amount of computing power connected to the network, these mathematical problems have become more and more complex. People who own the mining facilities need to invest in the latest equipment to be ahead of the competition in terms of computing power – known as hash rate – per unit of electricity.



MINING CITY

How does it work?

Let's understand how PoW works through the concepts of blockchain and mining. Blockchain is a distributed ledger, which is database containing a record of all the transactions on the network. These transactions are grouped in the form of data blocks in chronological order.

Miners compete to be first to solve the complex mathematical problem and confirm the new block. This mathematical problem is based on a cryptographic hashing algorithm. Once a miner successfully solves and finds the hash of the block, the new block is broadcast to the blockchain network. All the remaining nodes in the network, verify the solution and confirm it. Once the required consensus or number of confirmations is reached, the block is added to the blockchain.

By finding the hash, the miner proves that enough computational effort has been done to validate the transactions, therefore this mechanism is called Proof of Work.

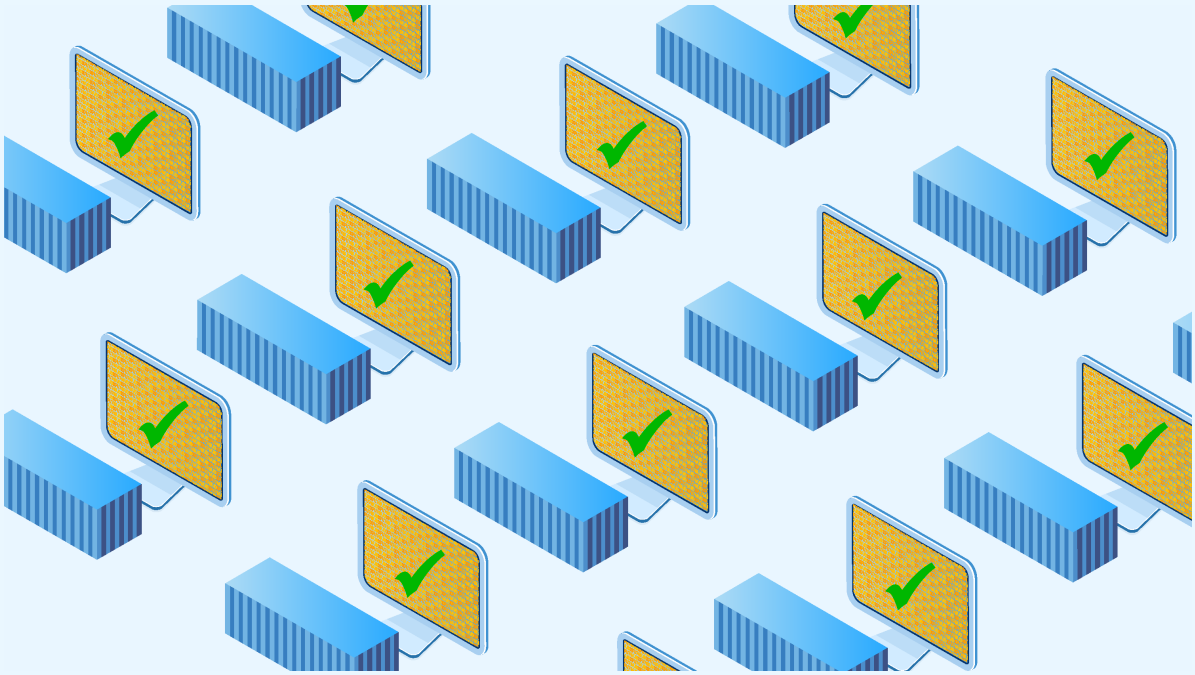
It is important to note:

- This cryptographic solution is significantly difficult to find but can be easily verified once confirmed.
- PoW protects the blockchain because it would require an impossibly large amount of computational effort to change any value. This is because in order to falsify transactions, miners would have to find solutions to the blocks all over again.

Bitcoin and Bitcoin Vault use SHA-256 function as their PoW consensus algorithm. However, there are many other PoW based cryptographic hashing algorithms including Scrypt, Blake-256, CryptoNight, and Quark.

MINING CITY

A lot of the criticism against the negative environment effects of crypto mining is targeted towards PoW. In order to keep up with the hash rate demands of crypto, miners consume enormous amounts of electricity. Bitcoin mining alone uses up more electricity than a small country. This has been the focus of protests by environmentalists who criticize the need of cryptocurrencies to generate so much pollution.



Why is PoW useful?

PoW based mining is very secure and difficult for any attacks to the blockchain, it is highly energy intensive derived from lot of computational effort. And this computational effort does not have any utility other than mining and securing blockchain. Although, currently most popular cryptocurrencies are based on PoW mechanism, other consensus mechanisms exist whose working process and implementation is quite different.

MINING CITY

Proof of Stake (PoS) is one such popular consensus mechanism where a miner is chosen to verify the transactions on the blockchain based on the number of coins staked rather than the hashpower of mining equipment.