BLOCKCHAIN

EXPLAINER

Proof of Work

A Proof of Work (PoW) protocol is simply a consensus mechanism to ensure that the information on each newly-generated block was difficult, costly, and time-consuming to be made by competing miners participating in the network. PoW is the consensus mechanism used in the Bitcoin blockchain.

How it Works

Proof of Work (PoW) enables distributed trustless consensus by making it extremely difficult to alter any aspect of the blockchain, since doing so would require re-mining all blocks from the altered block going forward, in addition to computing the current block faster than the rest of the network

- **Puzzles –** PoWs often amount to solving puzzles that require computational effort, which is commonly referred to as mining
- **Incentive –** miners receive fees paid by users sending transactions to include in blocks to be mined
- **Target Value –** the difficulty set by the network in establishing a target value for the hash of the block; the smaller the target, the harder it is to generate
- **Verification –** PoWs can be easily verified in much less time than it takes to create them

PoW vs. Proof of Stake

Proof of Work

+ Distributed trustless consensus makes attacks extremely difficult

- Demanding computational power requires limit scalability

Proof of Stake

+ Participants are accountable and build trustworthy reputation which incentivizes good behavior

- Difficult to succeed in a public blockchain as reputation is necessary for validation
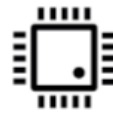
Related Explainers

Consensus Mechanisms | **Link**

Hashing | **Link**

What it Costs

It requires computational power

Hardware   Energy   Time

In Action

Bitcoin's Proof of Work Process

Begin Here → Proposed New Block

Header of the most recent block → Combine and Hash ← Nonce (an incremental number) ← Increment and try again

Combine and Hash → Hash Number

Hash Number → Is Hash < Target Value?

Is Hash < Target Value? — NO →

Is Hash < Target Value? — YES ↓

Proof of Work is Solved! → Mining Reward!