What Is Proof Of Work And Proof Of Stake?

ino.com/blog/2021/08/what-is-proof-of-work-and-proof-of-stake

Wayne Burritt August 24, 2021

One of the best features of cryptocurrency is that there is no need for a central authority like a bank to sign off on business transactions. So I can do business with someone without a massive bank or other financial behemoth looking over my shoulder. And so long as the terms of the transactions are fulfilled – whether it's buying something with Bitcoin and executing a contract with Ethereum – the deal is done.

Driving this whole process is a network of computers with multiple copies of all the transactions – including the one I just mentioned. When everyone on the blockchain verifies these transactions, the transaction is added as a new block. The process is complete until the next transaction comes around the corner.

But here's the rub: When I first go into crypto, I knew that people would do all this work on the blockchain because they would get paid in coins that made up the blockchain. But if you have a ton of people all doing the same work, who decides which person gets paid?

Well, there's just two ways of getting paid if you work on a blockchain: Proof of Work and Proof of Stake. And here's the nitty-gritty on both.

Why Do We Need Proof of Work or Proof of Stake?

The answer is pretty straightforward: To manage the issuance of new coins and to make sure people don't cheat.

At its heart, a blockchain works because many people are looking at the same transactions and then signing off on them. This signing-off or verification process is called a blockchain's "consensus mechanism." And it's what keeps track of new coins, makes the blockchain secure, and keeps cheaters at bay.

There are a handful of consensus mechanisms used by blockchain networks. But two of the most common are Proof of Work and Proof of Stake. And once you get your head around them, you'll understand why blockchains are so interesting and potentially profitable.

Proof of Work

Proof of Work (PoW) was first introduced in the 1990s to get rid of email spam. And the driving principle was pretty clever: Make computers expend a small bit of additional computational energy to send an email. But, of course, this marginal increase in energy expenditure would be meaningless for a single, legitimate user. But for a spammer, it would be prohibitive enough to make spamming a big pain.

The same process is at the heart of Bitcoin, where Proof of Work came to life. It is a decentralized consensus mechanism that makes people on the network expend energy – and money – to verify transactions on the network and make it secure. If they can do that, they'll be rewarded with new Bitcoin.

Accomplishing that task isn't easy. If you want to be selected to get the reward – "winning" a block reward -- you have to solve a complex mathematical problem using sophisticated cryptography and high-powered computers. And you must be the first one to do so. If you're second, you went to a lot of effort for nothing.

But before you go out and buy your first mining rig, remember that the difficulty level of these problems is so high that the computational power needed to win is mind-boggling: One estimate says that if Bitcoin mining were a country, it would rank in the top 30 of worldwide energy consumption.

That's more power than the whole of Argentina.

But if you win, you get paid. And right now, a new block reward on Bitcoin pays 6.25 coins. With a recent price of $46,440, that's a whopping $290,250. Not bad for 10 minutes of work. (A new Bitcoin block is added every 10 minutes.)

Proof of Stake

An alternative to a Proof of Work consensus mechanism is Proof of Stake. And as its name implies, you get invited to this party by ponying up – or "staking" -- gobs of the cryptocurrency your blockchain uses.

Here's what I mean...

If you want to be selected to mine some Bitcoin, you need to load up on the computational power and the electrical resources. That proves to the network that you're serious and here to play for real.

It's similar to a Proof of Stake mechanism. But instead of proving your worth with power and energy, you prove it by putting up actual cryptocurrency. That's why instead of being called a miner in a Proof of Stake consensus environment, you're called a "validator."

While the details vary depending on the blockchain network and the cryptocurrency project, you're in the running once you stake your crypto. And the person with the largest stake and the longest tenure in the game has a better chance to win the block reward than another validator.

What's Ahead?

The big energy bill for Proof of Work mechanisms is a huge problem: You can't consume a country-size helping of energy without people taking notice. Plus, Proof of Work consensus mechanisms has more difficulty processing sophisticated transaction environments, like smart contracts and DeFi (Decentralized Finance) transactions.

In other words, Bitcoin is great at being a complicated, massive checkbook that people can use to buy and sell stuff. But it's not designed to handle real estate transactions, complex financial deals, or other innovations developers can come up with.

That's why down the road, Proof of Stake will most likely eventually become the consensus mechanism of choice.

So, stay tuned!

Wayne Burritt
INO.com Contributor

Disclosure: This contributor may own cryptocurrencies mentioned in this article. This article is the opinion of the contributor themselves. The above is a matter of opinion provided for general information purposes only and is not intended as investment advice. This contributor is not receiving compensation (other than from INO.com) for their opinion.