Seeking Alpha

Cryptocurrency

Not Every 'Crypto' Is Decentralized: Proof-Of-Work Vs. Proof-Of-Stake

Mar. 24, 2022 11:12 AM ET | BITQ, ETH-USD, BTC-USD... | 13 Comments | 7 Likes

American Institute of Economic Research
1.25K Followers

Summary

Cryptocurrencies operate differently than the money that we are used to.

A “consensus mechanism” is the process of validating transactions across many nodes of the network.

Current cryptocurrency adoption rates outpace early adoption rates of the internet.
By David Waugh

Cryptocurrencies operate differently than the money that we are used to. Because they are solely electronic, there is no physical currency to trade. Instead, each network creates a record or “blockchain” of every transaction that takes place on the network.

There are currently two main types of mechanisms used to verify transactions on the network: Proof-of-Work (PoW) and Proof-of-Stake (PoS). While the industry was founded on PoW, many networks are moving to PoS. The MIT Technology Review dubbed PoS as one of the top ten breakthrough technologies of 2022 while the European Union almost banned PoW.

Consensus Mechanisms

A “consensus mechanism” is the process of validating transactions across many nodes of the network. Consensus mechanisms are necessary for cryptocurrency networks to maintain the accuracy and validity of their blockchains, or ledgers. Since no central authority controls the ledger, a consensus of the majority of the network verifies each transaction to make sure it does not contain incorrect or fraudulent transactions.
With a centralized payment network such as PayPal or Venmo, verification is easy. A single authority controls the ledger and acts as a trusted party to verify or clear the transactions. An individual cannot “double-spend” on these networks.

On a cryptocurrency network, however, because of the ease with which a digital currency can be reproduced without a central authority verifying transactions, an individual could attempt to sneak duplicate transactions into the blockchain before the next block is added.

**Proof-of-Work**

PoW was implemented in 2009 by Satoshi Nakamoto as the consensus mechanism for Bitcoin, the original cryptocurrency network. The Bitcoin network continues to operate using PoW.

So how does Proof-of-Work work? When someone wants to transfer funds from one Bitcoin address to another, he announces the transaction to the network by signing it with his private key and sending it to the recipient address via its public key. The transaction is bundled with other recent transactions into a block that is added roughly every ten minutes to the Bitcoin blockchain.

The blocks are created through “mining.” For each block, Bitcoin miners (computers) compete to solve a cryptographic puzzle, using processing power, which requires a significant amount of electricity. Once the first miner solves the problem, a block of verified transactions is added to the chain, and they become part of the permanent record. In exchange for their work, the miner receives a reward in Bitcoin.

Mining is “the work” in the term “Proof-of-Work.” Miners use their computing power, or “work” to “prove” the network. Because the network creates a permanent record of verified transactions, PoW eliminates the need for a central authority.

**Proof-of-Stake**

Proof-of-Stake emerged in 2013 as an alternative to PoW. It is used by networks such as Cardano and Solana. The Ethereum network plans to switch from PoW to PoS in the future, and its creator, Vitalik Buterin, is a major proponent of PoS as a consensus mechanism.
Whereas PoW relies on the work put in by miners to create the longest blockchain, PoS involves network participants “staking,” or locking up their crypto assets, in exchange for becoming validators of the blockchain. Validators are randomly selected by the network to verify the blockchain. PoS validators are similar to PoW miners, but instead of work, their “stake” allows them to validate the network. As Campbell Harvey states in *DeFi and the Future of Finance*,

Validators make themselves available by staking their cryptocurrency and then they are randomly selected to propose a block. The proposed block needs to be attested by a majority of the other validators. Validators profit by both proposing a block as well as attesting to the validity of others’ proposed blocks.

PoS uses a process of “slashing” that can be used to penalize bad actors. If a validator proposes or validates bad blocks, or is inactive on the network and doesn’t sign transactions, they can have their stake “slashed.” Slashing helps the PoS network discourage downtime and double signing, both of which are harmful to the network.

**Tradeoffs Between PoW and PoS**

PoS networks don’t require anywhere near the same amount of energy as a PoW network because they don’t involve thousands of specialized computers churning away simultaneously, consuming significant electricity, “working” to solve a cryptographic puzzle. The significantly lower amount of energy required by PoS to achieve consensus is viewed by many as a positive feature of the protocol. Further, because PoS networks do not require many computers “working” to achieve consensus, they potentially exhibit increased throughput, or the ability to process transactions faster.

That said, there are significant drawbacks to PoS. Cryptocurrencies are, on the whole, presented to the public as “decentralized,” but networks using PoS consensus mechanisms are drawn into a process that moves away from any meaningful decentralization. As Lyn Alden elaborates,
With a proof-of-stake system, the more coins you have, the more voting power you have, and those with the coins are also the ones earning the new coins from staking. Since they don’t need to expend resources to stake, they can simply increase their overall staking amount as they earn ongoing coins from staking rewards, and exponentially grow their influence on the network over time, forever. Network dominance tends to lead to more network dominance, in other words.

The governance of PoS networks, therefore, becomes more like that of a centralized corporation than a decentralized cryptocurrency. And with respect to monetary networks, a corporate board of unelected officials is arguably similar to the fiat system we already have.

Further, PoS networks face technical challenges that PoW networks do not. PoS algorithms involve hundreds of thousands of lines of code while the PoW algorithm can be created with a few hundred lines of code.

As a more concrete example, the Solana network routinely suffers from partial outages, recently for a full 48 hours, due to “excessive duplicate transactions.” This problem arises because one essentially needs a data center to run a Solana validator, which gives the network higher throughput but sacrifices decentralization and security. While networks prioritizing throughput is not inherent to PoS, PoS networks use high throughput as a way to distinguish themselves from their competitors (Solana vs. Cardano). This leads PoS networks to value throughput over decentralization and security.

**The Future of Consensus Mechanisms**

Current cryptocurrency adoption rates outpace early adoption rates of the internet. “Crypto” is here to stay; it will be intricately linked to the future of money and financial markets.

PoW uses more energy than PoS, but it’s battle-tested, decentralized, and secure. Policymakers seeking to ban PoW, or thinking it can be easily replaced by PoS would do well to keep the inherent and important tradeoffs between the two consensus mechanisms in mind.
Levels of decentralization and trust vary across cryptocurrency networks, and different networks serve different purposes for consumers. The choice of consensus mechanism between PoW and PoS is a key determinant of the decentralization, efficiency, and security of the cryptocurrency network.

Original Post

**Capitalize on supply constraints with top oil and gas stocks**

As sentiment around peace talks fluctuates, volatility in the markets continues. Oil prices have now rallied after dipping below $100/barrel on Tuesday.

Meanwhile, the energy sector is up almost 40% YTD - and one expert believes the best opportunity still lies ahead.

Analyst Michael Boyd believes that one specific subset of undervalued energy stocks could see gains of 50% or more. His personal portfolio is outpacing the S&P 500 by more than 65% since 2016, and is **already ahead by nearly 20% YTD**.

You can see which stocks Michael is buying right now, and why, by joining his 5-star rated investing community, Energy Investing Authority. Join now to **get a 20% discount**.

**Editor's Note:** The summary bullets for this article were chosen by Seeking Alpha editors.