# CRYPTOCURRENCIES: IS PROOF OF STAKE OVERTAKING PROOF OF WORK?

**As the blockchain and crypto community prepares for the upcoming bitcoin 'halving' milestone, a fundamental shift in consensus mechanisms may be on the cards, with new blockchain networks steering away from Proof of Work (PoW) to Proof of Stake (PoS).**

Unlike Proof of Work, the bitcoin miner's original consensus mechanism, Proof of Stake does not require costly hardware or exorbitant electricity bills to collaborate on the network. Nor does the investment needed to facilitate mining devalue over time, meaning PoS is overall more scalable and sustainable.

The next bitcoin halving is expected to take place in May 2020. Occurring on average every four years, these milestone events see the reward for mining new blocks halved, meaning miners receive 50 percent fewer bitcoins (BTC) for verifying transactions on a blockchain. Over the past eleven years, the bitcoin reward has shrunk from 50 to 12.5 BTC per block; and following this year's event we will see still fewer bitcoins flowing into the market, as the reward is halved again to 6.25 BTC per block.

Bitcoin halving brings to the fore the underlying weaknesses of the Proof of Work consensus mechanism. With under 3 million bitcoins still to be mined (out of the absolute total of 21 million that can be mined), there had been an expectation that crypto prices were set to reach another new high with this latest halving event. (In 2019 the value of bitcoin rose by 87 percent, and by early March 2020 it had increased by a further 33 percent. Analysts were predicting that the price of BTC could go as high as $20K and, as bitcoin is used as reference for other cryptocurrencies. However, the proliferation of Covid-19 has rapidly impacted cyptocurrencies, with a 30 percent price drop already witnessed as this article went to press.)

There is, however, another side effect to bitcoin halving which does not receive as much attention as such price volatility. As the reward for miners diminishes, the incentive to mine BTC also decreases. So one might justifiably ask whether miners will be able to cover their costs after the reward is halved again in May.

It is quite possible that smaller mining companies will find it much harder to survive, leaving only large corporations specialized in mining. Alternatively, miners will need to move toward using more efficient energy sources. This would lower costs and make it easier to stay afloat (for companies that are not already mining with renewable energy).

One could argue that bitcoin halving is leading to the erosion or even destruction of bitcoin developer Satoshi Nakamoto's original core principle of a decentralized means of value transfer. Today, 81 percent of all bitcoins are mined in China - and almost 50 percent by just three companies. So the concept of decentralization is already questionable. Once the halving takes place and smaller mining companies find it difficult to recover, China and its larger mining companies will dominate the market to an even greater degree, gaining new influence and power in the process.

The solution to these challenges lies in the evolution of consensus mechanisms. While Proof of Work has been bitcoin miners' algorithm of choice, other mechanisms - notably Proof of Stake and the more advanced Delegated Proof of Stake (DPoS) - offer viable alternatives.

With Proof of Stake, the right to create the next block is allocated to participants by the network itself, based on a combination of random criteria, such as age, wealth or weight of assets staked by a participant. If a participant cheats, they lose their stake.

In addition to using significantly less computing and electrical power than PoW, Proof of Stake mechanisms are faster, less risky and maintain decentralization.

Whether PoS will eventually take over PoW remains to be seen. The impact of this could be huge. Bitcoin has paved the way for digital currencies, but we all know that it's an unfinished product. One of its major limitations is its consensus mechanism – Proof of Work. As blockchain specialists move to adapt new technologies, they will move away from PoW. The financial services industry is also more likely to avoid transacting on blockchains with Proof of Work mechanisms, opting instead for smart contracts on (distributed) Proof of Stake mechanisms. This would effectively mean that both on technical and transactional levels, bitcoin and PoW are likely to be left behind and another cryptocurrency could rise to enjoy the status as reference for digital money.


## AUTHORS:

**Cedric Loyens,** Consultant

**Steven Deleu,** Associate

## CONTACT:

**Jeroen Dossche,** Partner

**M** +32 478 22 11 80

**E** Jeroen.Dossche@capco.com


**WWW.CAPCO.COM**

CAPCO