Proof of Activity (PoA)

Return to Consensus Mechanism

Seth[1] provides the following definition:

Proof of Activity (PoA) *is a blockchain consensus algorithm used in cryptocurrencies and similar systems. It is used to ensure that all transactions occurring on the blockchain are genuine, as well as to ensure that all miners arrive at a consensus. PoA is a combination of two other blockchain consensus algorithms: proof-of-work (PoW) and proof-of-stake (PoS).*

Bitcoin, the most popular cryptocurrency, uses the PoW consensus algorithm. A special feature of this algorithm is that it increases the difficulty level of the mining as time passes by. This method also prevents the bitcoin network from being hacked. However, because the difficulty of mining increases more and more computing power must be used. As a result of there being more energy consumption, there are more costs involved (including the costs of wear and tear on the hardware).

With a PoW system, a miner can mine or validate transactions based on the amount of effective work they have already contributed to the blockchain. As energy and hardware costs spiraled upwards, as a result of increased mining difficulty in PoW networks, the PoS system emerged as an alternative.

With a PoS system, a miner's ability to mine or authenticate transactions depends on how many cryptocurrency coins they hold. Although the PoS system achieves a reduction in electricity bills, an unintended side effect of it is that it can promote coin hoarding (rather than spending).

Both PoW and PoS systems are intended to prevent the likelihood of a 51% attack—a situation where a group of participants gains control of more than half the network's mining computing power. The danger of a 51% attack is that that group can then have full control of the network, including the power to halt new transactions from getting confirmed, stop payments between various blockchain users, and even reverse the transactions completed in the past during their control of the network, allowing them to double-spend the cryptocurrency coins.

PoA also prevents the chance of a 51% attack, like in POW and POS, because it is impossible to predict who the signing peer would be in the future, and coin-saving competition among signers does not allow the computing power to be accumulated within a group.

1)

Shobhit Seth, Investopedia, Proof of Activity, 1 April 2021, Accessed: 18 July 2021, https://www.investopedia.com/terms/p/proof-activity-cryptocurrency.asp