Proof of Work (PoW)

Return to Consensus Mechanism

The definition is provided by Frankenfiels[1]:

Proof of Work (PoW) *describes a system that requires a not-insignificant but feasible amount of effort in order to deter frivolous or malicious uses of computing power, such as sending spam emails or launching denial of service attacks. The concept was subsequently adapted to securing digital money by Hal Finney in 2004 through the idea of "reusable proof of work" using the SHA-256 hashing algorithm.*

Following its introduction in 2009, Bitcoin became the first widely adopted application of Finney's PoW idea (Finney was also the recipient of the first bitcoin transaction). Proof of work forms the basis of many other cryptocurrencies as well, allowing for secure, decentralized consensus.

This explanation will focus on proof of work as it functions in the bitcoin network. Bitcoin is a digital currency that is underpinned by a kind of distributed ledger known as a "blockchain." This ledger contains a record of all bitcoin transactions, arranged in sequential "blocks," so that no user is allowed to spend any of their holdings twice. In order to prevent tampering, the ledger is public, or "distributed"; an altered version would quickly be rejected by other users.

The way that users detect tampering in practice is through hashes, long strings of numbers that serve as proof of work. Put a given set of data through a hash function (bitcoin uses SHA-256), and it will only ever generate one hash. Due to the "avalanche effect," however, even a tiny change to any portion of the original data will result in a totally unrecognizable hash. Whatever the size of the original data set, the hash generated by a given function will be the same length. The hash is a one-way function: it cannot be used to obtain the original data, only to check that the data that generated the hash matches the original data.

Generating just any hash for a set of bitcoin transactions would be trivial for a modern computer, so in order to turn the process into "work," the bitcoin network sets a certain level of "difficulty." This setting is adjusted so that a new block is "mined" – added to the blockchain by generating a valid hash – approximately every 10 minutes. Setting difficulty is accomplished by establishing a "target" for the hash: the lower the target, the smaller the set of valid hashes, and the harder it is to generate one. In practice, this means a hash that starts with a very long string of zeros.

1)
Jake Frankenfield, Investopedia, Proof of Work (PoW), 19 March 2021, Accessed: 18 July 2021, https://www.investopedia.com/terms/p/proof-work.asp