Proof of Burn (PoB)

Return to Consensus Mechanism

The definition is provided by Reiff[1]:

Proof of Burn (PoB) *is one of the several consensus mechanism algorithms implemented by a blockchain network to ensure that all participating nodes come to an agreement about the true and valid state of the blockchain network. POB is often called a POW system without energy waste. It operates on the principle of allowing miners to "burn" virtual currency tokens. They are then granted the right to write blocks in proportion to the coins burnt.*

Iain Stewart, the inventor of the POB algorithm, uses an analogy to describe the algorithm: burnt coins are like mining rigs. In this analogy, a miner burns their coins to buy a virtual mining rig that gives them the power to mine blocks. The more coins burned by the miner, the bigger their virtual mining "rig" will be.

To burn the coins, miners send them to a verifiably un-spendable address. This process does not consume many resources (other than the burned coins) and ensures that the network remains active and agile. Depending upon the implementation, miners are allowed to burn the native currency or the currency of an alternate chain, such as Bitcoin. In exchange, they receive a reward in the native currency token of the blockchain.

You can send out transactions to the network that will burn your own cryptocurrency coins. Other participants can mine/burn on top of your block, and you can also take the transactions of other participants to add them to your block. Essentially, all of this burning activity keeps the network agile, and participants are rewarded for their activities (both burning their own coins and burning other people's coins).

To prevent the possibility of unfair advantages for early adopters, the POB system has implemented a mechanism that promotes the periodic burning of cryptocurrency coins to maintain mining power. The power of burnt coins "decays" or reduces partially each time a new block is mined. This promotes regular activity by the miners, instead of a one-time, early investment. To maintain a competitive edge, miners may also need to periodically invest in better equipment as technology advances.

1)
Nathan Reiff, Investopedia, Cryptocurrency 'Burning': Can It Manage Inflation?, 24 November 2020, Accessed: 18 July 2021, https://www.investopedia.com/tech/cryptocurrency-burning-can-it-manage-inflation/