Blockchain Council™

Proof-of-Burn

Understanding Proof-of-Burn (PoB)

There are several versions of PoB, but the Proof-of-Burn concept popularised by Iain Stewart is perhaps the most well-known in the Cryptocurrency ecosystem.

Initially, Proof-of-Burn may appear like a Proof-of-Work system but with reduced energy consumption rates.

The block validation procedure in PoB-based networks does not necessitate the utilization of high-performance computing resources or mining gear (like ASICs).

Instead, cryptocurrencies are burned to "invest" resources in the Blockchain, removing the need for potential miners to commit physical resources.

Miners invest in virtual mining machines, or we can say virtual mining power in PoB consensus.

How PoB Works?

If we talk about Proof-of-Work consensus, they are secure due to the fact that miners need to invest a lot of resources to be profitable finally, which implies that a PoW miner will have all the incentives to act truly and help the network to prevent the initial investments from wastage.

Now, if we talk about Proof-of-Burn, this idea is similar. Instead of investing in electricity or processing capacity, PoB Blockchains are designed to be protected solely by coin burns.

PoB systems will pay block rewards to miners, similar to PoW Blockchains, and the rewards are supposed to cover the initial investment of the burned coins within a specified amount of time.

Here it is important to note that the Proof-of-Burn consensus algorithm can be implemented in a variety of ways. Thus some initiatives achieve consensus by burning Bitcoins, whereas others establish consensus by burning their own native cryptocurrency.

Advantages and Disadvantages of PoB

Advantages

- The most significant advantage of this consensus is that it reduces power consumption; thus, it is considered more sustainable.
- The second benefit is that there is no need for mining hardware.
- The third benefit is that coin burns reduce the circulating supply (or we can say market scarcity).
- The other benefit is that it promotes long-term commitment by the miners.

Disadvantages

- One of the drawbacks associated with PoB is that it is not proven to work on larger scales. There is a lot more testing needed to confirm the efficiency and security of PoB.
- Also, the verification of the work done by miners tends to be delayed, and it is not as fast as in PoW systems.
- The other drawback is that burning coins is not always transparent or verifiable by the average user.

Example of PoB: Slimcoin

Slimcoin, a virtual currency network that uses POB, allows miners to burn coins, which not only provides them the right to fight for the next block but also offers them the opportunity to obtain blocks for at least a year.

Slimcoin's POB implementation is essentially a combination of three algorithms: POW, POS, and the basic POB concept.

POW is used in the process of burning coins; the more coins burned, the more chances there are to mine, ensuring the POS concept and the entire ecosystem is based on the POB principle.

Although the POB consensus exhibits similarities with both PoW and PoS, it follows its own way of reaching consensus and validating blocks.

Proof-of-Weight(PoWeight)

Understanding Proof-of-Weight

Proof-of-Weight (PoWeight) is a consensus algorithm based around the Algorand consensus model.

In other words, we can say that this is a notable upgrade of the PoS system in which the more tokens one owns, the better their chances are to discover more. But this whole idea makes the system somewhat biased.

Well, when it comes to Proof-of-Weight, it tries to solve such a biased nature of the PoS.

In a PoWeight system, instead of using your portion of tokens owned in the network to reflect your chance of “discovering” the next block, some other weighted value is employed.

The Proof-of-Weight Concept

Proof-of-Weight is based on the Algorand consensus model.

Every user on a PoWeight network has a “weight” assigned to them. This weight is determined by the amount of money in the user’s account.

The network will stay secure as long as the total weighted proportion of users is honest – usually two-thirds or more. This approach safeguards against double-spend attacks on the network.

Proof-of-weight techniques, on the other hand, can form a committee made up of random network users to perform each step of the protocol. As a result, the procedure ensures that the majority of committee members are truthful while simultaneously introducing some centralization.

Algorand and Proof-of-stake may seem similar, but actually, they are not. In a PoS environment, the number of tokens held defines the amount of additional rewards users earn. Proof-of-weight, on the other hand, uses an entirely different weighted value.

Advantages and Disadvantages of PoWeight

Advantage:

PoWeight is known for its super scalability and high customization. The fundamental algorithm can be adopted by the developers to allow for the formation of committees.

Disadvantage:

Despite its advantages, it has proven challenging to get consumers enthused about the concept due to a lack of incentivization, as the protocol does not pay users for maintaining a node and validating transactions.