**Difference between Proof of stake and Proof of Work**

**Proof-of-stake (PoS)** is one of the most popular consensus algorithms on blockchain networks. In PoS, the generator of the next block chooses a node with a greater balance – the amount of resources, for example, coins in cryptocurrency. Therefore, the staker with the greatest balance has more chances to generate a new block. For the creation of the block itself, the node does not receive a reward. Remuneration is paid for the transaction.

There are two basic possible node selection options:

* randomly from the “richest” nodes;
* randomly from the oldest nodes.

Instead of solving a cryptographic problem, transactions are validated by “freezing” a certain number of miner coins as collateral. Coins are frozen until an “agreement” on the validity of transactions is reached. After reaching a consensus in the network, transactions are added to the blockchain, and coins are kept frozen for some time in order to protect against attacks on the network. When coins are unfrozen, miners get their coins back plus a small commission for recording transactions on the blockchain. Such an algorithm is designed to discourage attackers from validating fake transactions because of the risk of losing a “collateral”.

**Proof-of-Work (PoW)** was the first successful decentralized blockchain consensus algorithm. PoW is used in Bitcoin, Ethereum (Ethereum plans to switch to Proof-of-Stake), Litecoin, ZCash, Monero, and many other blockchains.

The most famous algorithm works as follows: at the beginning, network users send digital tokens to each other, then all transactions made are collected in blocks and recorded in a distributed open registry – blockchain.

In PoW, all transactions are proven with the help of complicated mathematical calculations, the validity of which can be verified by any user of the network. Miners solve the problem, form a new block, and confirm the transaction. The tasks become more difficult each time, as the number of users grows, and the load on the network becomes greater.

|  |  |
| --- | --- |
| **Proof of Work** | **Proof of Stake** |
| To add each block to the chain, miners must compete to solve a difficult puzzle using their computers processing powers | There is no competition as the block creator is chosen by algorithm based on users’ stake |
| In order to add malicious block, you’d have to have a computer more powerful than 51% of the network | In order to add a malicious block, you’d have to own 51% of all the cryptocurrency on the network |
| The first miner to solve the puzzle is given a reward for their work | There is no reward for making a block, so the block creator takes a transaction fee |

**Read about types in Ethereum & share summary**

Everything stored in an Ethereum block has an address so that the owner can find and access their data in blocks. Data stored in Ethereum blocks can be crypto-assets, such as ether or other tokens, smart contracts, or any other data. The address of the data identifies the owner of that data. And when it comes to crypto-assets, only the owner can access that data. Well, anyone could access encrypted data, but only the owner can decrypt the data and consume the asset.

The person who controls the private key used to encrypt data on the blockchain controls the data. The only way that you can claim any crypto-asset is to prove that you control the private key associated with a crypto-asset’s address.

The only way to protect your crypto-assets is to protect your private keys. You need some mechanism to store your private key so that you can get to it, but no one else can. The primary function of a wallet is as a place to store one or more private keys used to access blockchain data.

The perfect Ethereum wallet makes it really easy for you to get to your keys and impossible for anyone else to access your keys. All wallets balance these two goals and strike some compromise between utility (how easy it is to access your keys) and security (how safe your keys are from attack).

**Types of Ethereum Wallets**

Private keys can be stored in several ways, ranging from very secure to very easy to access. You should consider how important your private keys are and select a wallet type that works for you. The main categories of wallets follow:

**Software wallets** store private keys in data files, where users can easily access them.

**Hardware wallets** store private keys on a physical chip stored inside a device, such as a Ledger Nano S.

**Paper wallets** are pieces of paper with the keys printed on them.

You don’t have to choose just one type of Ethereum wallet. You can use multiple wallets, depending on your needs. Keys for high-value crypto-assets need to be protected more carefully, whereas keys for low-value crypto-assets could be stored online for easier access.

**Software Ethereum wallets**

Software wallets are programs that store private keys and make it easy for users to retrieve and use those keys. After setting up your wallet, you can access your keys by providing a user ID and password or an encrypted file that only you have. Software wallets can be further divided into two main categories: hot wallets and cold wallets.

**Ethereum hot wallet**

A hot wallet is one that stores your keys online. You can easily access your keys, and your Ethereum assets, from anywhere in the world. All you need is an Internet connection and access credentials. Although hot wallets are convenient, that convenience comes at a cost. If someone steals your access credentials, he or she can steal your Ethereum assets.

**Ethereum cold wallet**

A cold wallet is one in which you store your keys offline. You need to provide your keys only when you want to access your Ethereum assets. You can store keys offline in multiple ways, but this approach requires a few extra steps when you want to buy or sell crypto-assets or interact with smart contracts.

**Hardware Ethereum wallets**

A hardware wallet stores private keys on a physical chip. You can connect the device housing the chip to many different types of computers and mobile devices, thus providing multiple ways to access the keys. Most hardware wallets also provide physical buttons to manage access to your keys.

The advantage of a physical wallet is the increased security. You connect your device to a computer only when you want to access your blockchain assets. When the device is not connected, your keys are safe inside the physical device. An attacker would have to physically steal your wallet device and know your access credentials to get to your keys.

The disadvantage of a physical wallet is the loss of convenience and redundancy. You must attach your physical wallet to a computer or device every time you want to access your blockchain assets.

**Paper Ethereum wallets**

The last type of Ethereum wallet can be the most secure. As the name implies, a paper wallet is literally just a piece of paper. After creating an Ethereum account and generating keys, one way of storing those keys is by simply printing them on paper. Most key generation options give you the choice of printing your keys. If you choose that option, you’ll get a hard copy of the private and public keys, along with a QR code of each key.

Whenever you want to access your blockchain assets, such as to buy or sell Ether, you can either type in your private key or scan the QR code. Of course, the software that you’re using to access Ethereum has to support QR scanning.