

Staking Explained



What is Proof of Stake (POS) vs. Proof of Work (POW)?

The first Cryptocurrencies, notably Bitcoin, use Proof of Work (POW) as method to define who (which “miner”) can add the next block. That is, potential miners need to solve additional mathematical problems which are unrelated to the task of processing transactions. This is called “difficulty”. The aim is to make the threshold for mining high enough so that not too many blocks are mined. Increasing difficulty of expensive coins leads to extreme waste of resources, most notably electricity. Proof of Stake tries to avoid this waste. Instead of solving mathematical puzzles, potential miners (here called stakers) need to leave a certain amount of coins “unspent” in their wallet. The coins are put “at stake” while they are staking.

What is Staking?

Leaving your wallet online, to support the network, and leaving some of your coins unmoved on the same address for some time, and thus earning rewards.

Is your wallet is fully synced but “Not staking because you don’t have mature coins”?

For staking Electra, coins need to rest (not be moved) for a minimum of 24 hours. So, if all your coins are just new in the wallet, or if you have recently rearranged all the coins in your wallet, or the one and only block has just staked, there are no coins “mature”, so you are not actually staking. Wait 24 hours, and the indicator should turn green.

How long does it take until I get reward?

This depends on how many coins you stake, and on how many other coins are staked by other stakers. You get a reward every time you find a block.

How much is the reward?

The reward is 50 % annually. There is no fixed reward per block, rewards are proportional.

How are rewards calculated?

Every time a new block is found, your wallet selects an input (a pile of coins that have been added to the wallet at the same time / together) and calculates the full reward for this block. That is $(\text{number of coins} \times \text{time [CoinDays]} / 730)$ (730 is 2×365 , thus 50 %). The input is then reset (marked as spent) and together with the reward saved as a new input with now zero CoinDays.

What does “Your Weight” mean?

This is the total of CoinDays staking (All mature coins in your wallet – from one or more addresses – multiplied with their respective age) (This number + the number of coins in your wallet / 730 gives the pending reward).

What does “Network Weight” mean?

This is the accumulated weight of all the wallets on the network that are actually online (staking coins x age).

What does “expected time” mean? How is it calculated, and is it reliable?

It's a raw guess on how much time might be needed until your wallet will stake next. The formula is basically $(\text{network weight} / \text{your weight} = \text{number of blocks until your weight would be sufficient} / \text{by number of expected blocks per day})$. It's not reliable. If you just started staking, the expected time will be too high. Even if you are staking for quite some time, change in the network weight (wallets that have been offline coming online again – or vice versa) will influence expected time. If you have only relatively few coins in your wallet, it might effectively take significantly longer than shown, as much larger wallets will push ahead with their many coins. If you have few very large blocks, it should take significantly shorter amount of time.

Will I get the full reward even if I only get a block after quite some time?

Yes, reward is always calculated for the full CoinDays of the input that gets reward. You might however miss out on compound interest. (Staking reward for coins staked earlier).

Do I need to have my computer running and online 24/7?

NO. While a high number of online full nodes (staking wallets) is essential for the smooth operation of the network, occasional downtimes do not affect your expected reward. You can only get reward whenever you find a block. For the calculation of the reward, only the time the coins have not been moved from their address on the blockchain is relevant, and not the uptime of your wallet.

Should I split my coins in many small inputs for better staking results, or rather combine them into blocks as large as possible?

Mostly “the larger the better” is a good rule of thumb, because many small inputs increase the time for everyone to get their due reward. Usually only ONE input is reset / rewarded at each block, and the number of blocks per day is given. If you have few very large inputs you will likely get a reward early, but each time you get reward for an input of less than 11 days of age, the wallet will create TWO outputs of equal size at the output, thus creating smaller and smaller inputs, and slowing the network down.

So how to get the best performance for the network (optimal staking)?

If your wallet contains too many small inputs, you can recombine them manually (resend them to your own wallet address). Very small inputs that are in the same wallets with much larger ones will likely never get rewards because they are squeezed by their larger brethren. To avoid losing CoinDays (and thus potential reward) you should combine only inputs that have recently staked, and thus not yet accumulated a lot of potential reward. Taking a wallet with a small number of very large inputs offline for a few days will accelerate staking for everyone – it reduces network weight and makes it easier for others to stake. Once you bring your wallet online again, you will have a large weight and stake sooner – especially if you leave it offline for enough time to avoid auto-splitting.