A Deep Analysis of Staking

Original:
https://www.btcc.com/en-US/academy/research-analysis/a-deep-analysis-of-staking

Suggestion: It's important to understand the basics of proof-of-stake (PoS) before getting into staking — and staking is becoming increasingly important for many new protocols.

Digital assets differ in many ways from the traditional fiat currencies (like dollars) most people are used to. One of the most important characteristics that sets digital assets apart is that they are not printed by or held by any central bank — digital assets exist in decentralized systems totally alien to those of traditional banks.

The decentralized nature of digital assets means that the technology underpinning most of them — blockchain — is the key to their decentralization. Digital assets are usually (not all of them time, but most of the time!) created through a process called mining, where computers solve complex equations that support the creation of new blocks.

The two most popular types of mining are called proof-of-work (PoW) and proof-of-stake. In this article, we are going to dive into the technical workings of specifically PoS and staking in general.

Ordinarily, staking involves locking one's asset on cryptocurrency wallets to participate in the transaction validation processes and ultimately earn newly minted coins as rewards. This framework is particular to blockchains that use the PoS consensus mechanisms as opposed to the PoS systems also commonly used by blockchains. In light of this, it is imperative to have a basic knowledge of PoS to understand the intricacies of staking.

What Exactly Is PoS?

PoS validators are picked randomly or nominated through prespecified conditions to ascertain the validity of the transactions executed on the blockchain and create new blocks. It's important to note that one of the conditions commonly used to handpick validators is based on the number of digital assets that each address vying for the position has staked on the blockchain. Typically, a strong validator network is determined by the number, digital asset volume and size of the validators, many of which are validators as a business.

Some PoS blockchains pick validators based on the quantity and quality of the validator's staked digital assets. In this case, the higher the number of staked coins, the higher the chances of becoming a legitimate validator. Conversely, some blockchains fix a specific amount as the staking requirement and then randomly pick validators from the list of addresses that meet these criteria.

The PoS consensus model does not require that validators own specialized hashing equipment or solve complex problems. Instead, all they need to do is to hold a sufficient amount of digital assets and put those assets up for consideration to create new blocks.

The PoS framework is less cumbersome and expensive than the proof-of-work alternative. Likewise, if executed properly, it is possible to maintain a decent degree of decentralization. Although a vast majority of PoS-based blockchains opt for a single currency-based staking system, some establish a double token ecosystem where a digital asset is locked, and an entirely different cryptocurrency is distributed as the staking reward.

Note that staking is vital to the security of PoS blockchains. Therefore, these blockchains come with fail-safes and stake-slashing settings to ensure that validators have the interest of the network at heart. In other words, the stake (the locked asset) is at risk once the network suspects that a validator allowed double-spending.

Staking on Cosmos-Based Blockchains

Now that you have grasped the concept of staking in its simplest form, it is easier to understand some of the iterations of this concept on specialized blockchain infrastructures. In this guide, we will focus on staking on Cosmos-based blockchains.

Cosmos is a crypto network designed to facilitate scalable and interoperable transactions and processes. Unlike a majority of application-based blockchain systems, Cosmos provides all the tools

necessary for developers to create their blockchains in tandem with Cosmos' core model and interact with other blockchains with similar infrastructures.

Therefore, the Cosmos ecosystem is a network of interoperable blockchains built with the Cosmos SDK. At the center of this network is the PoS-based Cosmos Hub, which acts as the bridge between chains and permits interoperability by tracking and logging the present state of each.

Some of the blockchains utilizing the customizable Cosmos SDK framework are Kava, Binance Chain, Terra and Irisnet. Since they all have a similar working principle as the Cosmos blockchain, these blockchains rely on the proof-of-stake or permissioned proof-of-authority mechanisms to validate transactions.

In other words, in a majority of these chains, participants have to stake the network's native token to qualify as validators. While this is a given, few alterations set this type of staking apart from our generic definition at the beginning of this guide.

When it comes to Cosmos-based staking, token holders can either delegate their staking power to validators or become one themselves. The blockchain picks validators assigned with the tasks of signing new blocks from the first 100 with the highest number of staked coins.

This is why delegation is a crucial option for low stakers — it lets more network participants partake in staking. Besides, delegators can easily switch their allegiances and force validators to remain competitive and maintain network-centric ideals.

The delegation system is non-custodial, which eliminates some risks. However, all delegated tokens will suffer the same consequences if the validator goes offline or attacks the network. One of the advantages of using the Cosmos SDK is that it allows each chain to set unique parameters for its staking operations.

So Why Choose the Cosmos SDK?

Cosmos prides itself as an enabler of application-specific blockchains. In simpler terms, developers or startups can create their blockchains and finetune them to establish improved scalability and interoperability. Like the emergence of Chrome and Firefox at the expense of Internet Explorer, Cosmos-based chains like Kava have more efficient base codes to deliver improved security and simplicity. In contrast, Ethereum still uses a flawed virtual machine system and runs a redundant model for its consensus processes.

With a security-primed infrastructure, applications launched on the Kava blockchain like Harvest are unsusceptible to bugs predominantly associated with DeFi protocols as a result of errors on smart contracts coding. Moreover, network congestions, which often causes high gas fees on Ethereum, are avoidable.

In cases where gas fees rise astronomically to let's say $100, a yield farmer would shell out $3,000 to pay as transaction fees to diversify into 30 yield farming pools. As a result, it is often difficult for small players to participate in the DeFi market. In response, Kava is designed specifically to meet the challenges of Ethereum and is optimized for scalable, secure, and cheap blockchain facilities.