

Protocol Embedded Staking – A new way of stabilizing crypto tokens

Staking and Proof of Stake (PoS)

The main idea behind the Proof-Of-Stake concept is that participants can lock coins (their “stake”) and the protocol randomly assigns the right to one of them to validate the next block at particular intervals. Typically, the probability of being chosen is proportional to the amount of coins – the more coins locked up, the higher the chances.

This way, what determines which participants create a block isn’t based on their ability to solve hash challenges as it is with Proof of Work. Instead, it’s determined by how many staking coins they are holding.

Staking cryptocurrency means that you are taking responsibility to transactions and to support the network by using your cryptocurrency holdings as a guarantee. In order to do this you have to lock a certain amount of tokens, in order to confirm this guarantee. In exchange for locking tokens and strengthening the network this way, users can receive a reward or interest in the form of extra tokens. Thus with staking you can generate a passive income by holding and locking coins.

Often in colloquial language the term staking is taken as a synonym for this general aspect of having the opportunity to earn extra tokens just by holding coins, without attaching importance to the technical details described above.

Market effects of Staking within Proof of Stake

Typically there are certain requirements on amount and locking duration within Proof-Of-Stake networks. Only certain minimum amounts of tokens can be staked for at least a minimum amount of time. Although this is very reasonable

from a security perspective, these conditions lead to market effects which aren't always welcome by token holders: At the end of locking periods users feel an incentive to claim the rewards they had been waiting for while their tokens had been locked away and thus had not been usable by them. The end of a staking period leads to a higher probability of tokens being sold on the market, which in turns can lead to some selling pressure and dropping market prices.

Moreover users cannot “work” with the tokens they hold during the locking period. Therefore classical staking is in competition to generating profit by using DeFi products like lending, participating in liquidity pools or similar.

Protocol Embedded Staking (PES)

Protocol embedded staking was invented in reaction to the undesirable market effects described above. Although the mechanism of protocol embedded staking is not suitable for the basic infrastructure currencies (like ETH or Cardano) themselves, it can be an interesting alternative for tokens setup on top of these currencies, for instance for ERC20-tokens within the Ethereum blockchain.

Protocol Embedded Staking (PES) is anchored in the base code of the currency's smart contract and does not require any explicit control or triggering by the user. All wallets holding tokens automatically and permanently take part in the staking process. Obviously, the term "staking" is used in colloquial manner here, since no tokens have to be locked. Nevertheless, the main idea of strengthening the stability of the currency is well fulfilled since creating an incentive to hold on to the tokens acquired leads to less price volatility.

Algorithms for protocol embedded staking work by inflating the total token supply in a strategically planned manner according to a mathematical logic implemented into the smart contract. Account balances are defined by their individual fragment of the total supply thus guaranteeing a non-dilutive allocation of tokens. This way the relative staking profit is and remains equal for all accounts independent of size and user related parameters like staking duration, choice of staking pool etc.

The mathematical basis for this kind of staking should follow some specific characteristics:

- Transparent supply calculation predictable for token holders
- Stability of the calculation towards user behavior and network effects
- Effectiveness of the calculation regarding computing power and thus gas costs

Moreover it has to be granted by the code of the smart contract that no manipulations of staking mathematics or total supply can be performed.

Advantages for Currency Holders

The technical attributes described above facilitate some special advantages holders of crypto currencies constructed in this way can expect:

1. **Multi-Beneficiary**

Since Protocol Embedded Staking allows complete availability of token usage in DeFi products, staking rewards will always be paid additionally to fees users may earn by using DeFi products. This way users can accumulate several income streams and multiply their benefits.

2. **Convenient**

Staking being embedded within standard ERC20 functions leads to a complete automation of the staking process with no need for user decisions or interactions to receive rewards.

3. **Flexible**

Tokens implementing PES stay compatible with the protocols of the base currency they are built on. For example, coins set up as ERC20 tokens can be used within all DeFi products created for this protocol, like pooling, lending, yield farming, mining and so on.

4. **Fair**

Protocol embedded staking evenly adjusts all balances relatively to the fragment of the total supply of coins an address holds. No other preference whatsoever is given to any specific holder. All wallets are

treated in the same way, independent of transaction volume or other parameters (Non-dilutive distribution of staking rewards).

5. **Transparent**

Since the staking algorithm is the only way of inflating the supply, there is absolute transparency concerning the total and circulating supply of tokens. This accounts true only if no extra minting or burning methods are implemented, of course. Many crypto currencies with big market caps do not have clear transparency of circulating supplies making it more difficult to assess their actual market values.

6. **Stable**

As described above staking tokens based on PES does not create any incentives for cyclical dumps at the end of locking periods. This potentially leads to less price volatility and stabilizes the token value.

Examples for Protocol Embedded Staking

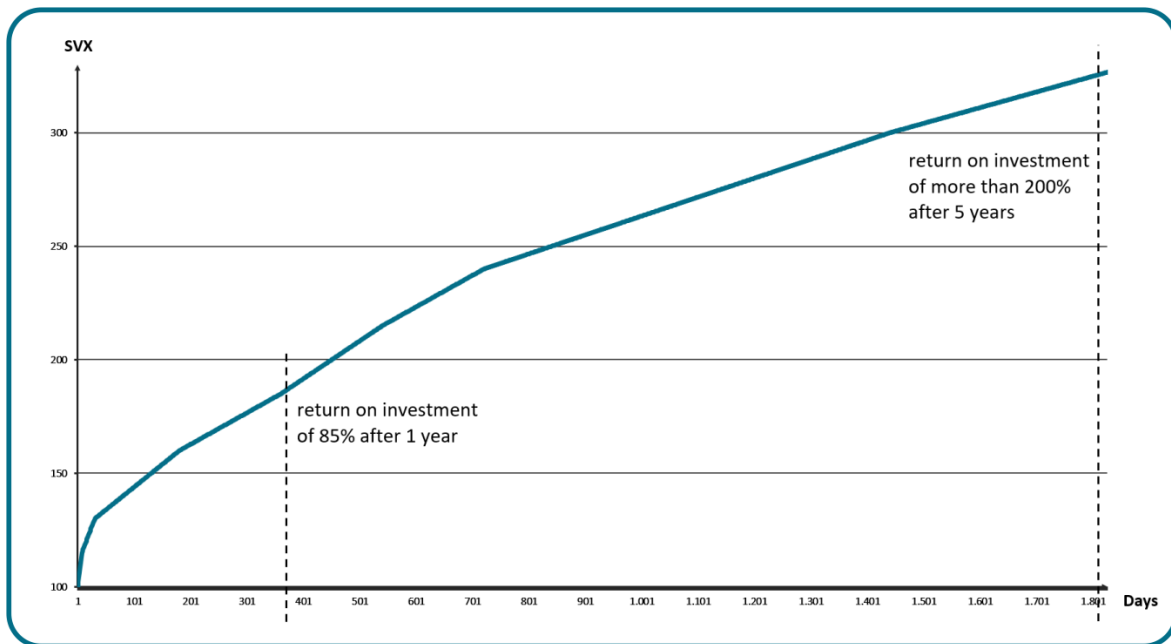
For the time being Savix (SVX) is the only cryptocurrency token implementing protocol based staking.

The Savix supply development curve is gradually defined by a sequence of straights which determines the interest rate at a specific point in time. Start and end points (corner points) of these straights define the global shape of the supply curve. Each straight is defined by the equation

$$F(x) = (X_t - X_1) * [(Y_1 - Y_1) / (X_2 - X_1)]$$

This easy to calculate mathematical logic keeps transaction costs low.

The following diagram shows the temporal development of an investment of 100 SVX after activating the staking mechanism.



The mathematical function and thus the exact numbers are flexible of course. But the graph illustrates well, that the exact return for any time in the future can be calculated beforehand, making the staking process as a whole completely transparent.

Details on the mathematics used in the example above can be found in the whitepaper of the project linked from the website savix.org.

Stay up-to-date

- Follow me on Twitter: https://twitter.com/savix_org
- Contact me on Telegram: @Anatol93