Bitcoin Suisse | Decrypt

October 1, 2019 | Season 1 Episode 11

Staking on Chains

Proof-of-stake consensus continues to attract considerable interest due to its potential advantages over proof-of-work. What are the pros and cons? How can investors benefit? And what are the technological and operational challenges related to staking cryptocurrencies?

Written by Dr. Raffael Huber from Bitcoin Suisse Research
and Demelza Kelso Hays and Mark J. Valek from incrementum

Ethereum, the second largest cryptocurrency by market capitalization, will soon move towards its version 2.0. With the switch also comes a gradual transition from its current proof-of-work consensus algorithm to *proof-of-stake* (PoS). In proof-of-stake chains, the network is secured by *staking*, i.e. committing a certain amount of cryptocurrency to be locked up, on the validity of the chain – as opposed to proof-of-work, where a computational puzzle is solved to validate blocks. A variation is delegated proof-of-stake (dPoS, e.g. in EOS), where coin holders can vote for their preferred block validators.

Depending on the individual blockchain, the terminology for stakers varies: They are called validators (in Cosmos and Ethereum 2.0), bakers (in Tezos), or block producers (in EOS), among others. Rewards for staking are paid out through issuing the native currency and collecting transaction fees, same as in proof-of-work chains. In the end, this issuance is the price that the protocol is willing to pay for network security, as we mentioned in Episode 3 of Bitcoin Suisse Decrypt.

A key challenge for proof-of-stake chains is the "nothing-at-stake" problem. Early implementations of proof-of-stake, such as Peercoin,[1] failed to sufficiently account for this issue. In proof-of-work, miners are economically incentivized to mine on the chain which they believe will remain valid also in the future. Mining on a block which will later become stale (i.e. is no more part of the longest chain) leads to a decrease in overall expected mining revenue, since the miner's hash rate was split up across the different forks. On the other hand, in proof-of-stake, validators could theoretically put up their stake for multiple forks at no cost, since their stake is present in each fork. This ensures that they have validated on the surviving chain and hence, this defeats the purpose of putting up a stake to a specific chain.

In Tezos, Cosmos and in Ethereum 2.0 (once live), the nothing-at-stake problem is addressed with a penalty for malicious or faulty behavior (*slashing*). Bakers or validators lose part of their stake in such cases – an overview of cases where this has occurred in Tezos is publicly available.[2] As such, stakers must ensure that their nodes are secure, correctly set up and properly maintained.

> *"It's as though your ASIC farm burned down if you participated in a 51 % attack"*
> *– Vlad Zamfir*

[1] https://www.peercoin.net/whitepapers/peercoin-paper.pdf

[2] https://tzscan.io/double-baking

As a protocol in general, proof-of-stake has a much shorter history than proof-of-work. Its viability, both from a technical and economical point of view, still needs to be proven over the next years. However, it also has several advantages over proof-of-work. One advantage would be significantly lower electricity consumption. Bitcoin has recently been in the news for its potential environmental impact,[3] as its annualized electricity consumption has overtaken that of Switzerland.[4] The need to invest large amounts of computational power to secure the blockchain falls away in proof-of-stake.

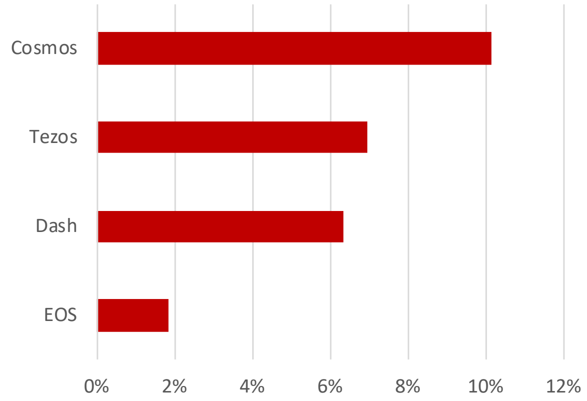
On top of that, the degree of blockchain decentralization might benefit from proof-of-stake. As mentioned in Episode 3, cheap electricity sources are a centralizing force for cryptocurrency mining. Large mining businesses for proof-of-work coins also profit from economies of scale. These are much less pronounced in proof-of-stake, since the initial investment for staking largely comes from buying the cryptocurrency rather than buying mining equipment.

> *“The staking yield should be thought of more as the penalty rate for non-stakers than as the reward rate for stakers.”*
> *– Ben Davenport*

There’s No Such Thing as a Free Lunch

To the traditional finance investor, staking yields may look like interest earned on a bank account; however, there is one key difference: Investors that stake coins are actually being paid for offering a service to the network. There are several cryptocurrencies that offer staking rewards to investors that are willing to participate in securing the network. A few examples of the cryptocurrencies with the most assets staked include EOS, Tezos, Cosmos, Algorand, and Dash. Currently, Cosmos has one of the highest annualized staking returns at 10.13 % (Illustration 1).

Illustration 1: Cosmos currently offers the highest staking yield (10.13 %) of large cap coins, followed by Tezos (6.94 %) and Dash (6.34 %).



Source: stakingrewards.com, Incrementum AG.

Although staking offers attractive annual yields, there are risks. The risks can be divided into operational, currency, and counterparty. On the operational side, if a validator or baker exhibits abnormal behavior (either intentional or non-intentional), the validator is punished. The punishment amount depends on the protocol and on the severity of the abnormal behavior. For example, if the node gets disconnected from the network and does not participate in consensus, the validator will lose a percentage of their staked coins (liveness fault punishment). If the node votes multiple times with contradicting ballots, they are also punished (governance fault punishment).

The second type of risk, currency risk, deals with the volatility of the coin’s price in USD. Since the coins are staked, the investor has long exposure. This risk exists for all cryptocurrencies, regardless of whether the protocol employs proof-of-stake or proof-of-work.

The final type of risk, counterparty risk, occurs when the investor stakes their coins. The most common way to stake coins is by sending the coins to a pool of coins from various investors held in a hot wallet on an exchange. If an investor decides to hire a third-party company to stake their cryptoassets, the investor also introduces counterparty risk. Delegating control to a validator is akin to trusting a bank with your assets; however, the companies offering custody of staked coins are often not insured, and they are sometimes not even incorporated. In fact, there are already reports of validators not paying out staking rewards to investors, and investors have little recourse. Therefore, choosing a competent validator is key.

To address counterparty risk, some cryptocurrencies allow investors to stake coins from cold storage wallets

[3] https://www.bbc.com/news/technology-48853230
[4] https://cbeci.org/comparisons/

on hardware. However, accepting staking rewards requires a transaction, and this transaction can reveal information to hackers. Advanced validator services work with virtual private networks to obfuscate transactions.

Final word: Proof-of-stake is an alternative to the proof-of-work and longest chain consensus mechanism employed by Bitcoin. Staking returns are a type of seigniorage that accrues to stakers via inflation in the coin supply. However, staking is not without risk. Investors should do due diligence on third-party companies offering staking services and consult a tax advisor regarding possible tax implications of staking reward payouts.

Bitcoin
Suisse

Bitcoin Suisse AG
CH-6300 Zug
bitcoinsuisse.com

in collaboration with

incrementum

Disclaimer:

The information provided in this document pertaining to Bitcoin Suisse AG and its Group Companies (together “Bitcoin Suisse”), is for general informational purposes only and should not be considered exhaustive and does not imply any elements of a contractual relationship nor any offering. This document does not take into account nor does it provide any tax, legal or investment advice or opinion regarding the specific investment objectives or financial situation of any person. While the information is believed to be accurate and reliable, Bitcoin Suisse and its agents, advisors, directors, officers, employees and shareholders make no representation or warranties, expressed or implied, as to the accuracy of such information and Bitcoin Suisse expressly disclaims any and all liability that may be based on such information or errors or omissions thereof. Bitcoin Suisse reserves the right to amend or replace the information contained herein, in part or entirely, at any time, and undertakes no obligation to provide the recipient with access to the amended information or to notify the recipient hereof. The information provided is not intended for use by or distribution to any individual or legal entity in any jurisdiction or country where such distribution, publication or use would be contrary to the law or regulatory provisions or in which Bitcoin Suisse does not hold the necessary registration or license. Bitcoin Suisse 2019.