MAERKI BAUMANN & CO. AG

PRIVATBANK

Staking – passive income and a security component all at once

Proof-of-work, proof-of-stake or rather proof-of-history? Consensus mechanisms form the backbone of every blockchain. And, as the name suggests, they are responsible for achieving consensus in decentralised networks. In the world of digital assets, and unlike in the traditional financial industry, investors do not purchase shares in companies, but rather units in a network-based project. They thus benefit from the growth of the network, as the network, and therefore its coin, should increase in value against the backdrop of a rising number of transactions and thus greater demand. What a lot of people don't know, however, is that digital assets can also be productive assets and generate income on the capital provided in the form of "staking rewards" – in a similar fashion to securities lending.

Consensus mechanisms – the backbone of every blockchain

A blockchain represents trust, traceability, transparency and immutability without the involvement of a central supervisory body. Transactions are decentralised and are conducted directly between the individual users on a peer-to-peer (P2P) basis. It has to be possible to validate these transactions in a uniform manner according to the parameters of the code and the community's rules.

So-called consensus mechanisms are used for this purpose in a blockchain. To understand how consensus can be established within a network, we first need a definition. Put simply, the consensus mechanism is a pre-defined rule (consensus protocols or code) that allows the respective users in a decentralised network to coordinate activities and prevent disagreements. Here, it is of the utmost importance that all players within the network agree on a single source of truth. This should also be the case if some of the players are temporarily no longer online, for example owing to a power outage.

But just why is such unanimity an essential requirement in a decentralised system? In a centralised system, there are people or bodies who make decisions and ensure that these decisions are also implemented effectively across the various levels. As no such functions are provided for in a decentralised network, however, there is a need for ways in which such decisions can be taken and implemented accordingly. In a decentralised network, the consensus protocol (the code) therefore supports those tasks for which responsibility is assumed by the respective decision-makers in a centralised network.

There are three important rules that apply to nearly all consensus mechanisms and which ensure that agreement can be reached between the various players:

1. Those participants in the network who add new blocks to the blockchain are known as "validators". These validators have to provide input in order to be able to participate in the generation of new blocks in the first place. This input can take the form of computing power in the case of the "proof-of-work" mechanism or the depositing of coins in the case of the "proof-of-stake" mechanism. This ensures that validators act conscientiously and in compliance with the network rules.
2. In order to keep the validators happy (incentivisation), so to speak, an attractive reward is required in return for the input they provide and the veracity of their actions – in other words, remuneration. In most networks, this remuneration is paid out in the currency of the respective blockchain at a fixed rate. The reward that the validators receive comprises the transaction fees, newly created coins or a combination of the two.
3. The third and final rule is the creation of transparency. If there is a lack of transparency in terms of the validators' actions, it is not possible to detect fraudulent behaviour and punish it.

Proof-of-stake – the consensus mechanism of the future?

Many new types of consensus mechanism have emerged over recent years. For a layperson, it can understandably be difficult to maintain an overview of everything going on. While they in principle all follow the same objective, the approaches they use could hardly be any more different: from proof-of-work and proof-of-stake to proof-of-burn and proof-of authority – there is no right or wrong approach. We explain the two most important approaches below.

Proof-of-Work (PoW)

The proof-of-work consensus mechanism is the forefather of all consensus mechanisms and is the approach that underpins the cryptocurrency Bitcoin (BTC). This approach sees participants in the network compete to add a new block to the blockchain by solving a specific cryptographic puzzle, which essentially involves finding a hash value that meets the specified level of difficulty. The solving of these puzzles is responsible for a new block being added and ensures that the transactions are executed and validated without errors (“mining”). Solving these puzzles requires energy input in the form of the invested computing power. As several participants, also known as “miners”, attempt to mine new blocks simultaneously, the power consumption is extremely high.

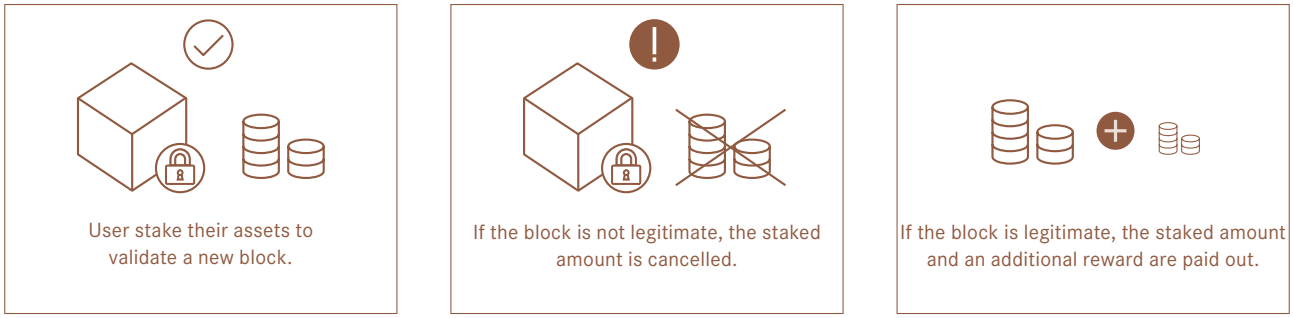
Proof-of-Stake (PoS)

The proof-of-stake consensus mechanism, by contrast, can generally be seen as the more environmentally friendly alternative to the proof-of-work protocol, as the validators of new blocks are predefined. The approach is fundamentally the same: validators have to provide input.

Unlike in the case of proof-of-work, however, it is coins that are provided as input rather than computing power. While the network participants make their coins available to the respective validators during this process, they remain in their ownership (“staking”). Depending on the type of staking, these coins are then blocked for a certain amount of time. Proof-of-stake therefore works on the premise that those players in the network who own many coins have a marked interest in keeping the network stable and safeguarding the value of their coins.

When a network's users make their coins available, they receive rewards in return – much like income from securities lending. The networks differ in terms of the amount of income paid out, the duration of their blocking periods for the borrowed coins, their payment cycle and the type of income they provide.

And this is how the proof-of-stake mechanism works:



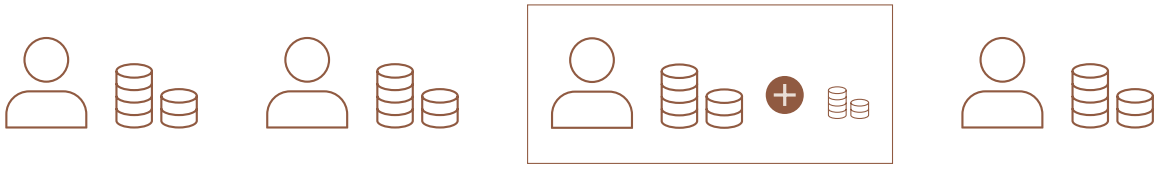
User stake their assets to validate a new block.

If the block is not legitimate, the staked amount is cancelled.

If the block is legitimate, the staked amount and an additional reward are paid out.

The network participant who is allowed to validate the next block is determined by means of weighted random selection. A new validator is drawn for each new block. However, due to the weighted random selection, those who own a large number of coins and actively make them available for the generation of new blocks have a greater chance of being drawn for the next block. In principle, it is the same as a lottery: the more tickets you buy, the greater the chance you have statistically of winning.

Determination through weighted random selection.



Highest chances

The more coins that are actively made available for the generation of new blocks, the greater the chances of being drawn as a staker for the next block.

The advantages of proof-of-stake speak for themselves: the proof-of-stake protocol is up to 10,000 times more environmentally friendly and consumes almost no electricity compared to its proof-of-work counterpart. Increased security may represent a further advantage in the future: due to the transparent structure of the blockchain, the algorithm punishes fraudsters and ensures that they lose their input in the form of coins ("slashing"). The players involved are thus not only incentivised to make their coins available, but rather also to act in the interests of the network.

Finally, the increased level of scalability can be mentioned: most proof-of-stake blockchains are architecturally designed for a higher speed and number of transactions and are thus able to process a higher number of transactions per second.

Digital assets – everything from a single source

Back in 2018, Maerki Baumann became one of the first Swiss private banks to develop a dedicated crypto strategy. The strategy was implemented gradually from 2019, with the private bank's offering initially comprising corporate accounts in fiat currency for companies wishing to make use of blockchain technology or crypto applications. Trading and custody services for common cryptocurrencies followed in mid-2020, before digital assets were incorporated in investment advisory and asset management services and a first discretionary asset management solution with cryptocurrencies was launched in the first half of 2021. These steps have been taken on the basis of our belief that digital assets can represent an interesting way to optimise the return and diversification potential of a traditional portfolio.

Ask us about it!

Parallels to traditional financial market transactions

Where profits can be made, there are also risks. Among others, investors are confronted with market risk. Both the coins deposited and those paid out are subject to market price volatility. There is also the risk of a validator failure, which can lead to a total loss of assets in the case of fraudulent intentions. The same applies here too, however, namely that the more reputable the validator, the lower the risk.

At first glance, there are parallels to the traditional equity market and the returns paid out from securities lending. However, staking rewards represent more than just simple income: by actively participating in the network, you contribute to its security and, in doing so, earn money in the form of coins at predefined intervals. The concept of staking rewards can thus be understood as a kind of lending return on stocks.

Conclusion

Proof-of-stake is now the most widely used consensus mechanism for crypto protocols. The disadvantages of the proof-of-work approach are largely eliminated and, at the same time, it allows many participants to take part in the validation of transactions without investing in infrastructure and computing power. The resulting staking income provides a regular income stream from holding cryptocurrencies, which otherwise, with the exception of any capital gains, do not generate any earnings. Provided you are familiar with the various risks involved, participating in staking can therefore generate a welcome source of side income.

Information and knowledge transfer

As part of our investment advisory and asset management services for digital assets, our proven experts with longstanding experience are also personally available to answer any questions you may have about the topics of blockchain and the world of digital assets. They will provide you with an in-depth and easy-to-understand insight into this new, up-and-coming asset class, meaning you are able to make your investment decisions with greater peace of mind.

When can we talk to you?

Milko Hensel
Head Digital Partnerships
Member of Senior Management
Maerki Baumann & Co. AG

This publication is expressly not intended for individuals resident in Germany.

Editorial deadline: September 2024

Maerki Baumann & Co. AG
Dreikönigstrasse 6, CH-8002 Zürich
T +41 44 286 25 25, info@maerki-baumann.ch
www.maerki-baumann.ch