Thursday, 23 January, 2020

The Bridge

Proof-of-Stake: Have skin in the game

Abstract

Proof-of-stake is a consensus algorithm first implemented in 2011 that uses staking native tokens as the basis for its incentive scheme and thus differs from proof-of-work. In proof-of-stake, innovation plays a crucial role in building an environmentally-friendly and scalable protocol. In this article, we present an introduction to the concept of staking, and explain its advantages and disadvantages in relation to proof-of-work.

What is staking?

Just as mining[link1] is essential to blockchain ecosystems that use proof-of-work (PoW), staking is essential to ecosystems based on proof-of-stake (PoS). It helps the network to form a consensus[link1] about the validity of transactions. PoS, as a consensus mechanism, has evolved into multiple versions which are explored later in this article. However, the core idea of staking remains the same in all these versions, i.e., having skin in the game. It is achieved by mandating validators to own and maintain a certain amount of the native currency locked in a smart contract.

In a staking ecosystem, unlike mining, validators do not have to use expensive hardware to perform complex calculations to prove the validity of the proposed block. Instead, they must own and maintain a certain number of native tokens in a specified location to qualify as a validator. Furthermore, one validator is selected to propose a new block for validation. If the proposed block is verified as a valid block by the majority, the selected validator is rewarded. We will explore different reward mechanisms in further sections. If the validator proposes an incorrect transaction, their stake is confiscated for misbehaviour. The crux of PoS is that the ownership and collateralisation of the owned native currency are aligned with the incentives of the stakers.

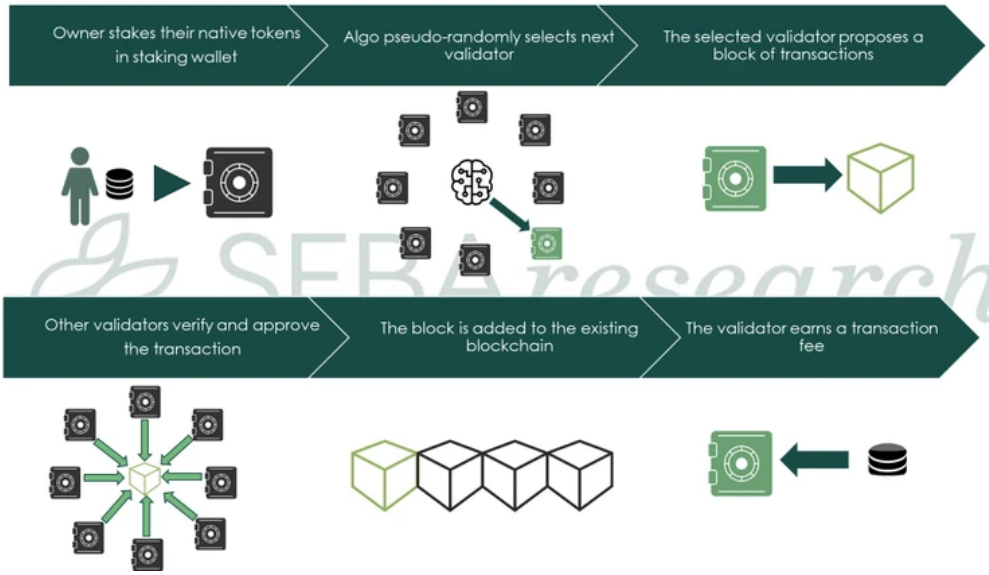
Proof-of-stake as a consensus mechanism can have variations based on the number of tokens to be staked or on the length of time they should be staked for. Similarly, different varieties can be seen around the concept of validator selection, i.e., how a validator is

selected to propose the next block. In the next section, we will look at the staking process, along with its different variants.

Staking process

PoS as a consensus mechanism also faces multiple trade-offs between decentralisation, security and scalability (a.k.a. the blockchain trilemma). These trade-offs can be managed to a certain extent by modifying the process at each step. Therefore, it is crucial to understand that each step can be conducted in multiple ways depending on the network requirements. This results in various forms of staking-based consensus mechanisms. A generic process is shown in Exhibit 1.

Exhibit 1: How staking works in the proof-of-stake consensus mechanism



Source: SEBA Research

1. Becoming a validator

It is necessary to own a certain number of native tokens locked up at a designated deposit address to become a validator in a staking-based protocol. There are two common types of PoS consensuses based on the number of validators allowed:

- **Proof-of-stake** – In this basic version of PoS there is no limit to the number of validators that can join the network, provided that they stake the required number of tokens. It allows for a more decentralised network with a minimum barrier to entry for validators.
- **Delegated proof-of-stake (DPoS)** – In this modified version, the network delegates the responsibility of validation to a limited number of entities only. In a DPoS network, other token holders usually have some voting rights for selecting these validators. It is quite similar to modern-day democracy. However, this creates a less decentralised ecosystem.

2. Selecting validators

Once tokens have been staked, a selection algorithm chooses a validator, based on a predetermined algorithm, to propose a new block of transactions. There are multiple variations on these selection processes; some of these are mentioned below:

- **Staking size** – In this approach, the network selects a validator based on the number of tokens staked. The higher the number of tokens, the greater the possibility of being selected. It is an undesirable approach if used in its pure form. This is because it leads to skewed token distribution within the network, as affluent stakers have a higher probability of receiving block rewards.
- **Staking age** – According to this selection process, the network chooses the validator based on how long the tokens have been staked for. Validators who have staked their tokens for a more extended period will have a higher chance of being selected. Once

the validator has been selected for proposing a new block, the age of the token they had staked is readjusted to zero.

- **Randomisation** – In this approach, validators are selected using a formula that looks for the lowest hash value[1] in addition to the staking size. As the stakes are known publicly, it is possible to predict with reasonable accuracy who will be selected to propose the next block.

Selecting a validator is one of the most crucial aspects of a PoS algorithm. Therefore, it is essential to align the selection process with network incentives. As a result, different blockchains employ different methods, which may correspond to one of the above techniques or represent a combination of several of techniques suitable for the desired purpose. Most of these methods are pseudo-random by nature.

3. Adding a new block

Once the validator has been selected, two further variations can direct how the consensus mechanism adds the new block to the blockchain.

Chain-based proof-of-stake – the validator is selected according to a pre-defined frequency (e.g. every 60 seconds) and assigned the right to create a single block.

Byzantine-fault-tolerant[link1] **proof-of-stake** – a validator is assigned the right to propose the next block. Once the selected validator has proposed a new block of transactions, other validators vote on the validity of the proposed block.

The second approach is mostly used in the PoS consensus.

4. Receiving block rewards

Once the block has been added to the blockchain, the selected validator receives their block reward. These block rewards can be transaction fees, new tokens or both. However, rewarding stakers with new coins results in an initial distribution problem.

To understand the initial distribution problem, imagine that a validator acquired 10% of their tokens when the system was launched by paying USD 1,000. Once the network has gained popularity, the old validator would be in an advantageous position compared to a new validator who invests USD 1,000 to gain only 0.01% of the network tokens. To overcome this, PoS networks tend to either pre-mine all their tokens or use a PoS and PoW hybrid consensus where PoW is used for creating new tokens and PoS is used for validating transactions.

Advantages and disadvantages of PoS

Advantages

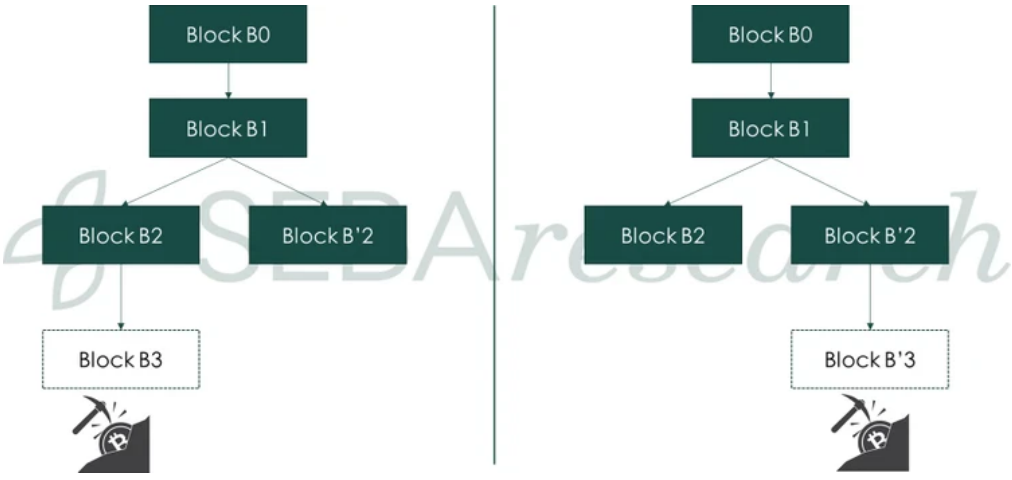
- *Energy-efficient* – One of the most significant benefits of PoS over PoW is its energy efficiency. A proof-of-stake consensus is designed in a manner which does not require any significant hardware or electricity investments. Consequently, the energy efficiency of PoS drastically increases in relation to PoW, making it environmentally friendly.
- *Scalability* – Higher transaction throughput affects the scalability of a network. In a PoS/DPoS network, the transaction throughput is generally observed to be much higher on average than in a PoW network. This is achieved by reducing the block time, as the network quickly reaches a consensus by limiting the number of validators on the network.

Disadvantages

- *Speed at the cost of security and decentralisation* – As we mentioned earlier, all blockchains operate within the trilemma. PoS results in increased throughput at the cost of either decentralisation and/or security. The reasons for this are beyond the scope of this document.
- *Nothing at stake* – The nothing at stake problem is one of the most critical issues that exists in the PoS ecosystem. It occurs when the PoS blockchain splits into two different chains (deliberate or accidental). In this case, the PoS validators are incentivised to stake coins on both chains.

In a PoW consensus, the probability that a miner will mine the next block depends on the amount of mining power. If the miner intends to mine on both chains, they will have to split their mining power between two chains. Splitting the mining power will reduce the miner's likelihood of mining the next block by 50% (assuming the mining power is equally distributed between both chains), whilst the electricity cost remains the same. This incentivises the miners to stay on one of the chains and not to mine both chains (Exhibit 2).

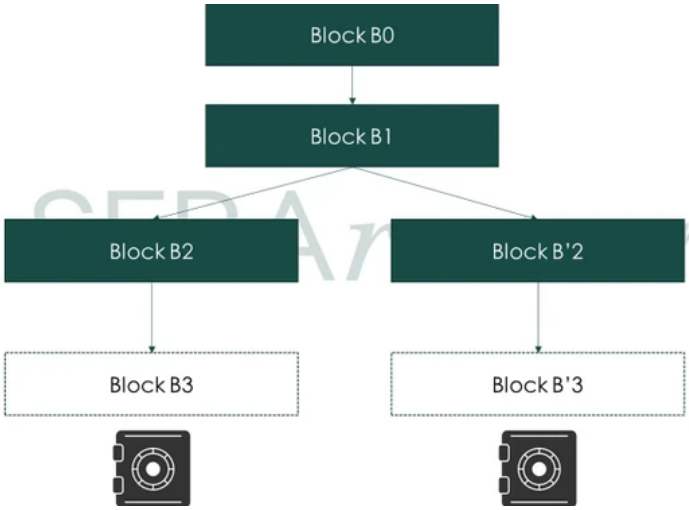
Exhibit 2: Miner incentive in a PoW-based blockchain split



Source: SEBA Research

However, in a PoS-based ecosystem, there is no significant external cost associated with staking for the validators. Also, as both Block B2 and Block B'2 have the same previous block (Block B1), the account balances for all the validators are the same. Hence, the probability that a validator will mine the next block on both chains remains the same. This is because their staked coin balances are duplicated on both chains. This incentivises the validators to stake their tokens on both chains to optimise their profitability. This can also lead to many network problems like double-spending (Exhibit 3).

Exhibit 3: Validator incentive in a PoS-based blockchain split



Source: SEBA Research

Conclusion

Staking is an exciting approach towards creating a secure and cost-efficient consensus mechanism. Currently, some of the top tokens by market capitalisation such as EOS, Tron and NEO rely on PoS as their consensus mechanism. Furthermore, Ethereum's plan to migrate from PoW to PoS is a sign of the increasing popularity of proof-of-stake within the blockchain ecosystem.

However, it is not a foolproof method and comes with trade-offs in terms of security and decentralisation in its current form. Existing implementations of PoS are a long way behind prominent PoW networks in terms of network security and decentralisation. Blockchain companies and communities are actively working on developing new mechanisms within the staking ecosystem to minimise these trade-offs. Going forward, we might see a matured version of the PoS mechanism that could help build a more efficient network.

[1] In order to win the right to forge (generate) a block, all active accounts compete by attempting to generate a hash value that is lower than a given base target value. This base target value varies from block to block and is derived from the previous blocks base target value multiplied by the amount of time that was required to generate that block. (https://web.archive.org/web/20150203012031/http://wiki.nxtcrypto.org/wiki/Whitepaper:Nxt#Base_Target_Value)

Authors

Yves Longchamp
Head of Research
SEBA Bank AG

Ujjwal Mehra
Research Analyst
B&B Analytics Private Limited

Saurabh Deshpande
Research Analyst
B&B Analytics Private Limited

research@seba.swiss

Disclaimer

strategy. This document is for distribution only under such circumstances as may be permitted by applicable law. It is not directed to, or intended for distribution to or use by, any person or entity who is a citizen or resident of or located in any locality, state, country or other jurisdiction where such distribution, publication, availability or use would be contrary to law or regulation or would subject SEBA to any registration or licensing requirement within such jurisdiction.

No representation or warranty, either express or implied, is provided in relation to the accuracy, completeness or reliability of the information contained in this document, except with respect to information concerning SEBA. The information is not intended to be a complete statement or summary of the financial investments, markets or developments referred to in the document. SEBA does not undertake to update or keep current the information. Any statements contained in this document attributed to a third party represent SEBA's interpretation of the data, information and/or opinions provided by that third party either publicly or through a subscription service, and such use and interpretation have not been reviewed by the third party.

Any prices stated in this document are for information purposes only and do not represent valuations for individual investments. There is no representation that any transaction can or could have been effected at those prices, and any prices do not necessarily reflect SEBA's internal books and records or theoretical model-based valuations and may be based on certain assumptions. Different assumptions by SEBA or any other source may yield substantially different results.

Nothing in this document constitutes a representation that any investment strategy or investment is suitable or appropriate to an investor's individual circumstances or otherwise constitutes a personal recommendation. Investments involve risks, and investors should exercise prudence and their own judgment in making their investment decisions. Financial investments described in the document may not be eligible for sale in all jurisdictions or to certain categories of investors. Certain services and products are subject to legal restrictions and cannot be offered on an unrestricted basis to certain investors. Recipients are therefore asked to consult the restrictions relating to investments, products or services for further information. Furthermore, recipients may consult their legal/tax advisors should they require any clarifications. SEBA and any of its directors or employees may be entitled at any time to hold long or short positions in investments, carry out transactions involving relevant investments in the capacity of principal or agent, or provide any other services or have officers, who serve as directors, either to/for the issuer, the investment itself or to/for any company commercially or financially affiliated to such investment.

At any time, investment decisions (including whether to buy, sell or hold investments) made by SEBA and its employees may differ from or be contrary to the opinions expressed in SEBA research publications.

Some investments may not be readily realizable since the market is illiquid and therefore valuing the investment and identifying the risk to which you are exposed may be difficult to quantify. Investing in digital assets including cryptocurrencies as well as in futures and options is not suitable for every investor as there is a substantial risk of loss, and losses in excess of an initial investment may under certain circumstances occur. The value of any investment or income may go down as well as up, and investors may not get back the full amount invested. Past performance of an investment is no guarantee for its future performance. Additional information will be made available upon request. Some investments may be subject to sudden and large falls in value and on realization you may receive back less than you invested or may be required to pay more. Changes in foreign exchange rates may have an adverse effect on the price, value or income of an investment. Tax treatment depends on the individual circumstances and may be subject to change in the future.

SEBA does not provide legal or tax advice and makes no representations as to the tax treatment of assets or the investment returns thereon both in general or with reference to specific investor's circumstances and needs. We are of necessity unable to take into account the particular investment objectives, financial situation and needs of individual investors and we would recommend that you take financial and/or tax advice as to the implications (including tax) prior to investing. Neither SEBA nor any of its directors, employees or agents accepts any liability for any loss (including investment loss) or damage arising out of the use of all or any of the Information provided in the document.

This document may not be reproduced or copies circulated without prior authority of SEBA. Unless otherwise agreed in writing SEBA expressly prohibits the distribution and transfer of this document to third parties for any reason. SEBA accepts no liability whatsoever for any claims or lawsuits from any third parties arising from the use or distribution of this document.

Research will initiate, update and cease coverage solely at the discretion of SEBA. The information contained in this document is based on numerous assumptions. Different assumptions could result in materially different results. SEBA may use research input provided by analysts employed by its affiliate B&B Analytics Private Limited, Mumbai. The analyst(s) responsible for the preparation of this document may interact with trading desk personnel, sales personnel and other parties for the purpose of gathering, applying and interpreting market information The compensation of the analyst who prepared this document is determined exclusively by SEBA.

Austria: SEBA is not licensed to conduct banking and financial activities in Austria nor is SEBA supervised by the Austrian Financial Market Authority (Finanzmarktaufsicht), to which this document has not been submitted for approval. France: SEBA is not licensed to conduct banking and financial activities in France nor is SEBA supervised by French banking and financial authorities. Italy: SEBA is not licensed to conduct banking and financial activities in Italy nor is SEBA supervised by the Bank of Italy (Banca d'Italia) and the Italian Financial Markets Supervisory Authority (CONSOB - Commissione Nazionale per le Società e la Borsa), to which this document has not been submitted for approval. Germany: SEBA is not licensed to conduct banking and financial activities in Germany nor is SEBA supervised by the German Federal Financial Services Supervisory Authority (Bundesanstalt für Finanzdienstleistungsaufsicht), to which this document has not been submitted for approval. Hong-Kong: SEBA is not licensed to conduct banking and financial activities in Hong-Kong nor is SEBA

supervised by banking and financial authorities in Hong-Kong, to which this document has not been submitted for approval. This document is not directed to, or intended for distribution to or use by, any person or entity who is a citizen or resident of or located in Hong-Kong where such distribution, publication, availability or use would be contrary to law or regulation or would subject SEBA to any registration or licensing requirement within such jurisdiction. This document is under no circumstances directed to, or intended for distribution, publication to or use by, persons who are not "professional investors" within the meaning of the Securities and Futures Ordinance (Chapter 571 of the Laws of Hong Kong) and any rules made thereunder (the "SFO"). Netherlands: This publication has been produced by SEBA, which is not authorised to provide regulated services in the Netherlands. Portugal: SEBA is not licensed to conduct banking and financial activities in Portugal nor is SEBA supervised by the Portuguese regulators Bank of Portugal "Banco de Portugal" and Portuguese Securities Exchange Commission "Comissao do Mercado de Valores Mobiliarios". Singapore: SEBA is not licensed to conduct banking and financial activities in SIngapore nor is SEBA supervised by banking and financial authorities in Singapore, to which this document has not been submitted for approval. This document was provided to you as a result of a request received by SEBA from you and/or persons entitled to make the request on your behalf. Should you have received the document erroneously, SEBA asks that you kindly destroy/delete it and inform SEBA immediately. This document is not directed to, or intended for distribution to or use by, any person or entity who is a citizen or resident of or located in Singapore where such distribution, publication, availability or use would be contrary to law or regulation or would subject SEBA to any registration or licensing requirement within such jurisdiction. This document is under no circumstances directed to, or intended for distribution, publication to or use by, persons who are not accredited investors, expert investors or institutional investors as defined in section 4A of the Securities and Futures Act (Cap. 289 of Singapore) ("SFA"). UK: This document has been prepared by SEBA Bank AG ("SEBA") in Switzerland. SEBA is a Swiss bank and securities dealer with its head office and legal domicile in Switzerland. It is authorized and regulated by the Swiss Financial Market Supervisory Authority (FINMA). This document is for your information only and is not intended as an offer, or a solicitation of an offer, to buy or sell any investment or other specific product.

SEBA is not an authorised person for purposes of the Financial Services and Markets Act (FSMA), and accordingly, any information if deemed a financial promotion is provided only to persons in the UK reasonably believed to be of a kind to whom promotions may be communicated by an unauthorised person pursuant to an exemption under the FSMA (Financial Promotion) Order 2005 (the "FPO"). Such persons include: (a) persons having professional experience in matters relating to investments ("Investment Professionals") and (b) high net worth bodies corporate, partnerships, unincorporated associations, trusts, etc. falling within Article 49 of the FPO ("High Net Worth Businesses"). High Net Worth Businesses include: (i) a corporation which has called-up share capital or net assets of at least £5 million or is a member of a group in which includes a company with called-up share capital or net assets of at least £5 million (but where the corporation has more than 20 shareholders or it is a subsidiary of a company with more than 20 shareholders, the £5 million share capital / net assets requirement is reduced to £500,000); (ii) a partnership or unincorporated association with net assets of at least £5 million and (iii) a trustee of a trust which has had gross assets (i.e. total assets held before deduction of any liabilities) of at least £10 million at any time within the year preceding the promotion. Any financial promotion information is available only to such persons, and persons of any other description in the UK may not rely on the information in it. Most of the protections provided by the UK regulatory system, and compensation under the UK Financial Services Compensation Scheme, will not be available.