Cross Staking

technical description

Table of contents

1. Purpose

This document is a technical description of the Cross Staking technology and is intended to inform potential users about the principles and aspects of its operation.

2. Terms and definitions

Blockchain is a tamper-proof public digital ledger that records transactions in a public or closed peer-to-peer network. Such a registry continuously records the history of transactions with assets between peers in the network in the form of blocks of information. In the next step, the approved blocks of transactions will be written into the chain. Any block of information contains a timestamp, information about the users in the operation, a link to the previous block, etc. The connection between the blocks in the chain is carried out not only by numbering, but also by the following rules: any block contains both its own hash sum and the hash sum of the previous block.

A sidechain is a separate blockchain with two-way connection to the parent blockchain which differs from the main blockchain to which it is linked in its capabilities and functions. The parent blockchain is usually called the “main chain”, additional chains are called side chains.

The consensus algorithm (consensus) is a set of rules by which blocks are generated in the blockchain.

PoW (proof-of-work, means proof of the work done) is a blockchain consensus algorithm that is used to confirm transactions and create new blocks. Miners must solve complex mathematical problems (hash functions) to confirm

transactions. With PoW, miners compete with each other to complete transactions on the network and for rewards.

PoS (proof-of-stake, means proof of stake ownership) is another blockchain consensus algorithm. How PoS works: instead of solving mathematical problems new coins are mined through staking, a mechanism that allows you to add new blocks by proving ownership of the cryptocurrency of this network.

Validators are nodes in the blockchain system that take on the task of keeping the network running. They distribute staking rewards, provide network statistics, and control block integrity.

L1 (level 1, main network) is a block chain based on PoW consensus.

L2 (level 2, solutions) are infrastructure software projects, applications and technologies deployed on top of underlying blockchains. L2 is an additional network (block chain) based on PoS consensus.

Staking is the process of storing or locking cryptocurrencies on a target wallet for a certain period of time in exchange for rewards and getting passive income in cryptocurrencies in order to verify transactions on PoS blockchains. These tools help maintain the security and maintenance of certain blockchains.

3. Introduction

Cross Staking is a second-level protocol technology designed to be introduced into staking platforms for staking cryptocurrencies based on proof-of-work consensus (e.g. Bitcoin, Litecoin, Monero, etc.). The process is carried out by deploying a second level L2 technology (an additional block chain) on top of the main blockchain.

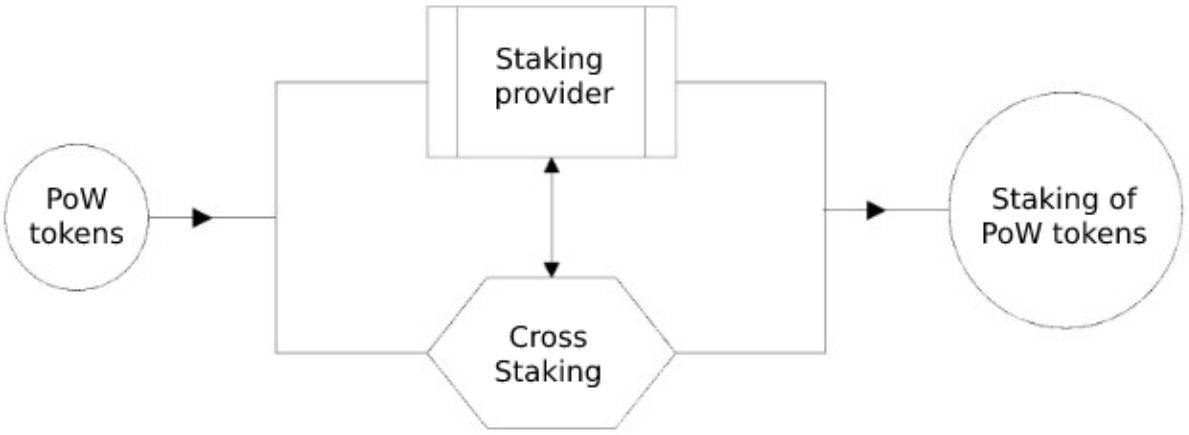
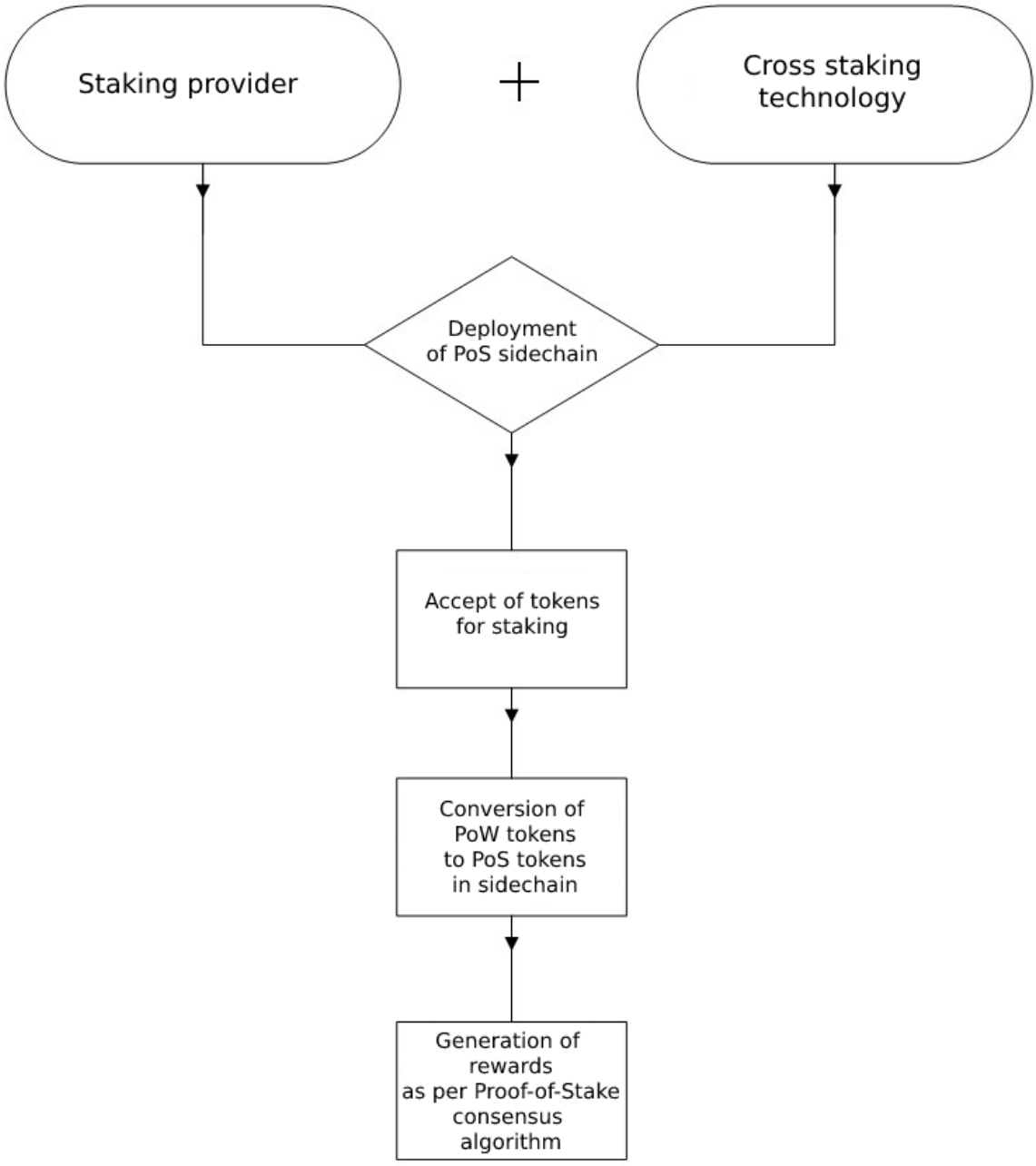


Fig.1 Cross Staking Technology

Briefly, the principle of operation of Cross Staking is as follows: a staking provider deploys a sidechain based on an improved proof-of-stake (PoS) consensus, connects it with a two-way connection to the parent proof-of-work (PoW) consensus blockchain, and staking takes place using this connection. Fig. 2 shows how Cross Staking works.

Further, in the following chapters the technical part of Cross Staking technology will be described in detail.



Pic.2 How Cross Staking works

4. Statement of the problem

Three main criteria are used to evaluate the performance of the blockchain, namely:

— decentralization;

— scalability;

— security.

For the optimal and fast operation of the blockchain a compromise must be found between scalability, security and decentralization. This problem is known as the Scalability Trilemma. It lies in the difficulty of creating a fast, decentralized and secure network at the same time. Therefore, developers often have to choose and optimize a maximum of two out of three components.

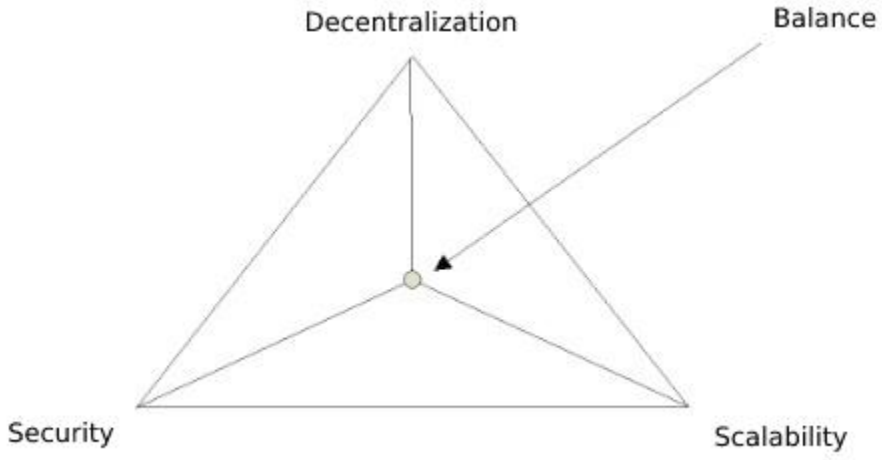


Fig. 3 Scalability Trilemma

Scalability in a broad sense means the ability of a system to expand with an increasing load. Blockchain scalability is the expansion of the system to serve a large number of transactions.

Blockchains based on “Proof of Work” consensus have a small network bandwidth. For example, the bandwidth of the Bitcoin network is 5-7 TPS (transactions per second), Ethereum is about 15 TPS.

These factors lead to the fact that processing transactions in PoW networks require a large amount of computing power, and a considerable amount of energy is also spent. In addition, with the increase in the number of users in the network, the complexity of calculating new blocks increases which further exacerbates the problem.

To solve the scalability trilemma, the off-chain concept was created (a chain that is located outside the main blockchain). Off-chain scaling is defined as an approach that allows transactions to take place without loading the main chain. Off-chain protocols process all transactions and they are not visible on the main chain. There are currently two such solutions: sidechains and state channels.

So, the solution to the scalability problem can be achieved on the off-chain, while security and decentralization must be maximized on the underlying blockchain. One of the off-chain options is the sidechain.

5. Solutions of the second level technology in the problem of scaling.

Solutions of the second level L2 technology are infrastructure solutions in the form of applications and various software built on top of basic blockchains. They can process large volumes of transactions and thus reduce the load on the main network. Now there are several options for second level solutions: sidechains, state channels as well as optimistic and ZK rollups. Level 2 solutions are designed to overcome the limitations of scalability, isolation and lack of flexibility for developers.

It should be noted that there are two important parameters that classify L2 solutions:

— cryptographic verification;

— data availability (DA) off-chain or on-chain.

The two types of cryptographic verification are reality verification and fraud verification.

On-chain data availability means that all state and transaction data is processed and verified in the L2 network, while off-chain means that all data and state data is processed outside L2.

Rollups are solutions in the Ethereum network that execute part of the transactions outside the main network in sidechains but at the same time send the data of these transactions to the main network after the calculations are completed. They execute transactions on a separate chain, but the result of the transactions is recorded on the main blockchain.

Depending on the type of cryptographic verification used in the project, there are optimistic and ZK rollups.

Optimistic Rollups work using fraud proof, and operate on the basis of an EVM-compatible virtual machine OVM (Optimistic Virtual Machine). The basic idea of fraud proofs is to send a minimum of data to the first layer and make an optimistic assumption that the data is correct. Data senders must provide collateral which will be forfeited if the blockchain detects fraud. The main problem with optimistic rollups is the long withdrawal period.

ZK rollups unite hundreds of off-chain transactions and generate a zero-knowledge cryptographic proof known as SNARK which allows one user to prove that they have certain information without revealing that information. This provides a high level of privacy on public blockchains and other networks. ZK-rollups provide a fairly fast withdrawal of funds compared to optimistic rollups, but this

solution is more complex in its technical implementation because it uses compatibility with the EVM (Ethereum virtual machine). ZK-rollups are more demanding on computing resources.

The state channel is a solution that allows users to open their own channel off the blockchain where they can make an infinite number of private transactions. Only the first and last transactions are recorded in the blockchain. The first transaction opens the channel, users must lock funds in a multi-signature smart contract. The second transaction closes the connection. When all transactions between the users are completed, the last transaction is sent to the network and the funds are unlocked. All transactions in the channels are visible only to the users themselves. Only the initial and final state is recorded on the main blockchain.

Sidechains (sidechains, side chains) are separate independent chains of blocks that operate in parallel with the main “parent” blockchain network. Sidechains are a technology that allows tokens, as well as other digital assets of one blockchain, to be securely used in another blockchain and then returned to the original blockchain.

Cross Staking uses a modified sidechain based on PoS consensus in its technology. Such a sidechain solves problems and tasks that classic PoW blockchains can not solve, specifically, the problem of scalability. Modified with PoS technology, the sidechain processes a much larger number of transactions in a shorter time period because this technology allows you not to block data and not waste time on unlocking. These factors make Cross Staking an ideal solution to the scalability problem. From a technical point of view, a sidechain created using the upgraded PoS consensus algorithm does not form blocks as such. The term "block" in improved consensus refers to a sequence of records that are voted on by validators and produce a confirmation. In the current implementation the block confirmation speed is 2.5-3.5 times faster than in the main network.

6. Detailed description of technology

Cross Staking technology allows PoW tokens of the main blockchain to be used securely in the deployed PoS blockchain, then these tokens are returned to the main blockchain. In order for tokens to move from the main PoS blockchain to the L2 sidechain they are frozen in the main (parent) chain and activated in the secondary chain.

A cross-staking sidechain is a separate second-level block chain based on improved PoS consensus which is attached to the parent chain using a two-way pegging.

Cross Staking will be applied by those validators that have the best infrastructure to run the required nodes and guarantee close to 100% uptime. Large staking providers are ideal for this role. They take on all the main tasks to maintain the health and safety of the blockchain network, and will also be able to provide it with large resources. The more resources the provider has, the more secure the network is.

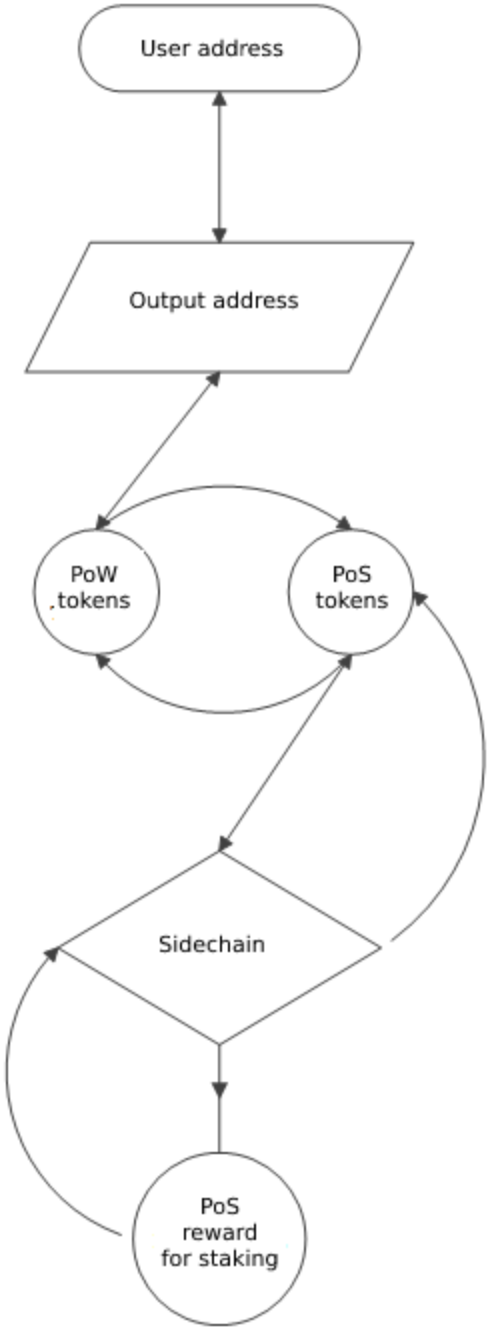


Fig.4 Cross Staking: movement of assets

Assets movement in Cross Staking

Let us consider in detail how assets move when using the Cross Staking technology (see Fig. 4 and 5).

1) The main blockchain tokens are sent to an exit address in the PoW network where they will be frozen, which is designed to prevent their use elsewhere. This means that the sent coins will not be able to be used.
2) After the transaction is verified by the security system of the main PoW network, the PoS sidechain receives information that the necessary tokens are blocked, are at the output address.
3) Further, an equivalent number of coins is created in the PoS sidechain, based on the transmitted information from the main network. Here it becomes possible to use them for staking according to the proof-of-stake algorithm. At the same time, transactions performed on the secondary blockchain are not recorded in the main blockchain, so the cost of fees can be much less or zero.

Cross Staking Security Mechanisms

The main chain (L1) is responsible for security and decentralization and acts as the data availability layer for the secondary chain. If the main network goes down L2 will go down as well. However, if L2 fails all funds will be safe and protected by L1. The main chain is also responsible for the availability of data, and the sidechain built on top of it is responsible for accruing rewards to users. Cross Staking serves to combine the protection of the main and secondary layers, thus ensuring the safety of both layers. The main proof-of-work chain takes advantage of the security provided by the hashing power of the proof-of-stake chain. This opportunity appears through a group of notary nodes that add information from the first block chain to the second. Therefore, in order to break the first chain, it is necessary to break the second one as well.

In addition, the deployable PoS sidechain, like other PoS blockchains, has its own security system. The staking mechanism incentivizes the initiator to create only verified blocks. If the network detects a fraudulent transaction, the initiator will lose part of their stake in staking and the right to create blocks in the future. Thus, if the share in staking is greater than the reward an unscrupulous validator will lose more coins than he gains. In order to control the network and confirm fraudulent transactions the node must own a larger stake in the network, which is known as a "51% attack". Accordingly, the larger the network, the more secure it is. The scale of the network is precisely provided by a large staking provider.

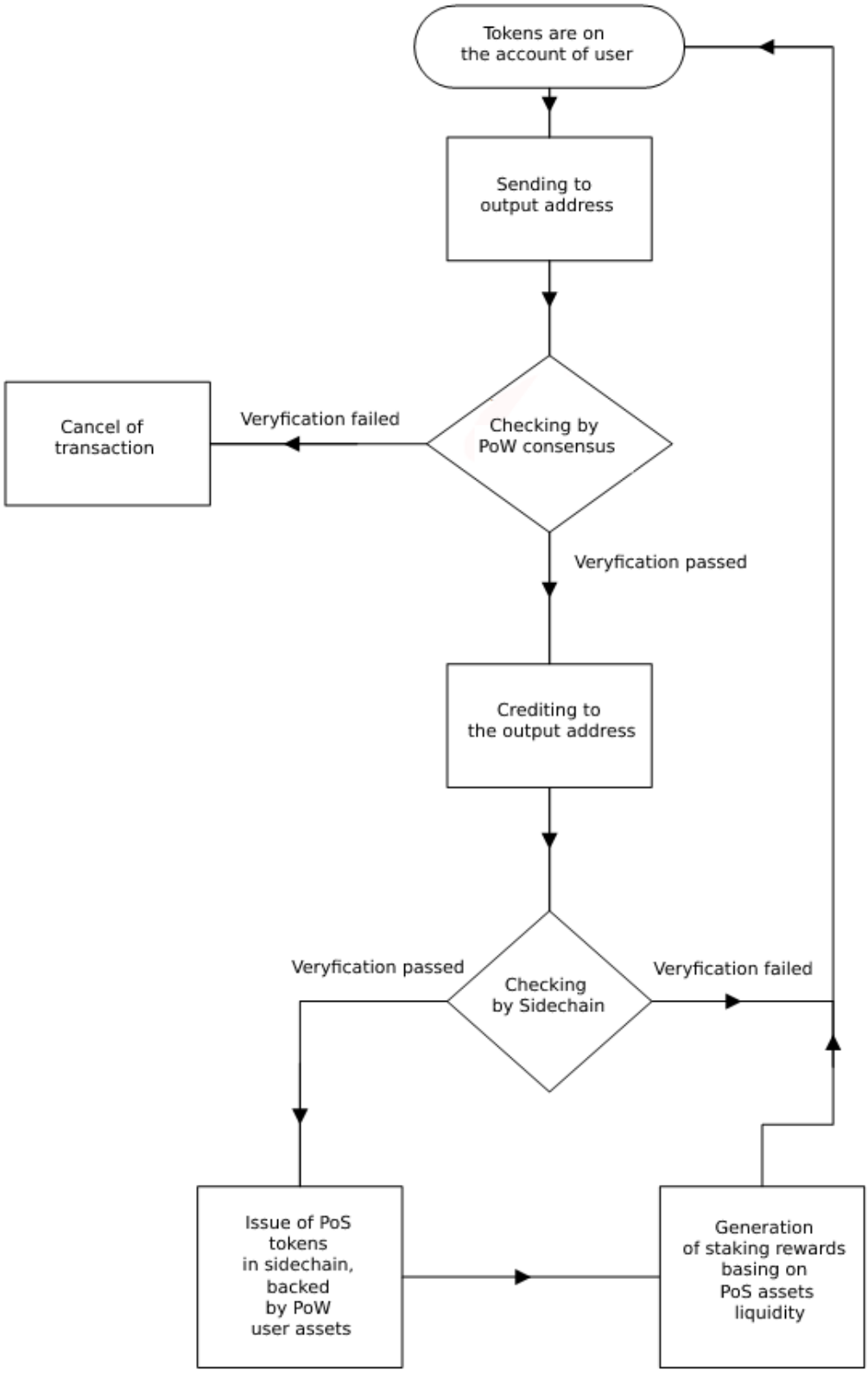

Tokens are on the account of user
Sending to output address
Checking by PoW consensus
Veryfication failed
Cancel of transaction
Veryfication passed
Crediting to the output address
Checking by Sidechain
Veryfication passed
Veryfication failed
Issue of PoS tokens in sidechain, backed by PoW user assets
Generation of staking rewards basing on PoS assets liquidity

Fig.5 Transactions and Security in Cross Staking.

The difference between usual PoS consensus and improved PoS

The principle of operation of the usual PoS consensus: users extract new coins through staking, a special mechanism that allows you to add new blocks by proving ownership of the cryptocurrency of this network. The probability of the formation of the next block in the blockchain by the user is proportional to the share that the accounting units of this cryptocurrency belong to this user from their total number.

In enhanced PoS consensus, no one technically mines blocks and no rewards are provided, however, users receive a transaction fee as a proof of stake reward proportional to the coins they staked. A winner is randomly selected to update the block based on the share of the bid provided. Thus, the staking reward is formed and a percentage of the blocked funds is paid. Below the mathematical method by which the user's reward is calculated will be shown.

Participants in the staking process update blocks with a certain probability and accordingly receive a reward based on the condition below:

$$hash(prevBlocksdata, timeInseconds, txout_A) \leq d_0 * coins(txout_A) * timeweight(txout_A)$$

where:

timeinseconds - current time, in this inequality limits hashing attempts and blocks the creation of the next block;

txoutA is the result of the transaction;

coinstxoutA - the amount of unspent cryptocurrency of the transaction;

timeweight(txoutA) — time elapsed since the result of the txoutA transaction was included in the block. The probability of generating the next block immediately after generating the previous one is very small, but it increases with time. This avoids an exponential distribution between payouts, increasing the chances of users holding a small amount of cryptocurrency.

prevBlocksdata - data of the previous block;

d0 is a constant that is adjusted so that blocks are generated every few minutes on average.

The proof-of-stake protocol places limits on the possible values of timeinseconds. For example, if timeinseconds cannot differ from the UTC time of the hosts by more than an hour then the user can try no more than 7200 timeinseconds values. Thus, expensive calculations are not used in the stake confirmation process.

In a usual PoS consensus the lower and upper limits of block creation are limited, while in the improved PoS consensus the lower is always set to the average block time over the last N blocks, and the minimum timeweight(txoutA) intervals are set in seconds which allows you to make the speed of confirming a new block several times faster than the main network.

The time required to find a block for address A is exponentially distributed with the parameter bal(A)/D. Therefore, the implementation of stake confirmation is fair: the probability of generating a block is equal to the ratio of the address balance to the total amount of currency in circulation. The time it takes for the entire network to find a block is exponentially distributed with the parameter ∑a bal(A)/D. Thus, if the money supply of the currency ∑A bal(A) is fixed or grows at a predictable rate, the complexity of D must be known in advance:

$$D = \frac{1}{timeweight(txout_A)} \sum_A \quad bal(A)$$

timeweight(txoutA) — time elapsed since the txoutA transaction result was included in the block;

bal (A) — user A's cryptocurrency balance;

D is the complexity of updating a new block;

In a normal PoS consensus difficulty D must be adjusted based on recent blocks because not all currency holders participate in staking. In the case of PoS consensus used in Cross Staking, the variable "D" is known in advance, since all users who have tokens participate in staking.

The difference is that usually ICO or other types of initial offerings are used for the initial distribution of tokens in PoS blockchains. In the case of Cross Staking PoS consensus, the primary information about the tokens transferred to the sidechain from the main network is realized through a group of notary nodes that add information from the first chain of blocks to the second.

7. Transactions

The staking process begins with the transfer of assets from the main blockchain by sending coins to a special address. These coins are blocked there and after the appropriate checks (described in the section above), the corresponding amount is allocated on the PoS sidechain. Below we will show a typical example of how transactions occur when using the Cross Staking technology.

Transaction example

1) Suppose a user has five coins in the main PoW network, let's call them *powcoins*. The owner of the coins wants to stake them.
2) The staking provider provides him with an output address where the user sends his *powcoins*.
3) In this address the coins are blocked, then the corresponding amount of coins, let's call them *sidecoins*, is reserved on the sidechain. The deployed PoS

sidechain uses two-way pegging which allows the staking provider to transfer user assets from the main chain to the side chain and vice versa.

4) Once the coins have been converted into sidecoins, they become available for staking.
5) If Flexible Staking is chosen, then the user can stop staking whenever he sees fit. Interest will accrue until he submits an application to withdraw his tokens from the network. In this case the sidechain tokens are withdrawn and the corresponding amount is returned to the user in the main network.
6) If Locked Staking is chosen, then the user will be able to receive his funds only after the end of the staking period.
7) In both cases the user will be able to withdraw the interest accrued according to the staking schedule.

While coins are brought in from the external network and withdrawn back to it with two transactions, many different transactions with coins can be performed in the additional network.

In the process of transferring tokens from one type to another, generating interest from staking, withdrawing them or transferring them again to a certain type of staking, withdrawing tokens and fixing profits, a commission is charged. Due to the technical features of the PoS sidechain the cost of the transaction itself is much lower than in the main network and the speed is higher. This allows the staking provider to charge an increased commission during the staking process, distribute the reward in the form of interest accordingly, and thus earn income.

8. Information security and threats

The architecture of a blockchain project system is quite complex, and when developing a security policy, it is necessary to take into account the vulnerabilities

of all components of the IT infrastructure: servers, web and mobile applications for clients, blockchain nodes, etc. It is also necessary to consider the security of the main L1 blockchain. All these measures should be taken into account when building a general threat model for a blockchain project. When developing a security policy for a project, it is necessary to take into account international and local information security standards, guidelines and best practices in the field of cybersecurity.

This document will outline the most common threat vectors that are specific to all PoS sidechains (and Cross Staking technology in particular). It will also indicate the information security measures that must be taken to avoid threats and problems.

1) Initial distribution problem

Problem: In systems using PoS, there is always a threat that the initial coin holders will not be interested in spending their coins, since their balance directly contributes to their wealth.

Solution: In the case of Cross Staking technology all PoS coins are backed by the coins of the main PoW network and their value relative to fiat currencies grows accordingly. This factor does not motivate large coin holders to keep and not exchange the coin.

2) The problem of "nothing at stake" (the “Nothing at Stake” attack)

The “nothing at stake” problem: in case of a consensus error validators lose nothing by voting for multiple chain branches. This fact prevents a consensus from ever being established. In the case of the PoW proof-of-work algorithm, this behavior will be irrational, since by dividing resources into different blockchain branches, the miner reduces the likelihood of finding a block on each of them. The

optimal strategy in a PoW system is to always work on the same branch. In the PoS share confirmation algorithm, unlike PoW, the probability of finding a block does not decrease if the user tries to work on several branches of the blockchain, but increases.

Solution: In the case of Cross Staking technology, delegated PoS algorithms are used to solve this problem, where the validator loses his funds if the blockchain branched, and he himself was seen confirming blocks on both branches.

3) Attack from afar
(the “Long Range” attack)

Problem: In a system with PoS negotiation an attacker with sufficient computing power can try to build an alternative blockchain starting from the very first block.

Solution: One of the reasons why Cross Staking is designed specifically for staking providers is this type of attack. In order to control the network and confirm fraudulent transactions the node must own a larger stake in the network which is known as a "51% attack". In this case the staking provider ensures the scale of the network attracting a significant amount of liquidity to it, which makes the implementation of this type of attack much more difficult.

4) Attack "double spend"
(the "double spending" attack)

Problem: Chain formation is low resource intensive so any user can abuse trying to double spend “for free”. The attacker transfers or withdraws tokens to some address, then waits for the transaction to be considered confirmed, after which he announces a reward for confirming a new block that does not include the transaction

in question. In a standard PoS algorithm validators that validate new blocks have nothing to lose if the attack fails.

Solution: This type of attack is solved in a similar way to the "nothing at stake" problem, where the validator loses its funds if it is seen validating the attacker's blocks.

9. Technological aspects

Cross Staking technology uses standard L2 solutions (sidechains) but has its own completely innovative advantages over classic PoS sidechains.

Cross Staking takes all calculations off the main blockchain. Although transactions are processed in L2, data about them is recorded and stored in the main network which can significantly increase the efficiency of the sidechain. Also, the created sidechain does not even form blocks as such. In the improved PoS consensus used in cross staking, a sequence of entries is created, which are voted on by validators and generate a confirmation. Unlike other sidechens, Cross Staking technology allows you not to block data and not waste time on unlocking, i.e., the time between receiving the previous entry and validating it by the node is almost zero - the entry is confirmed immediately. Due to this, a high speed of the entire network is achieved.

In the current implementation the block confirmation speed is 2.5 - 3.5 times faster than in the main network which makes this technology even more attractive for staking providers as it will allow you to charge an increased commission. The technology will also attract token holders as their passive income can increase significantly.

10. Environmental aspects

The problem of environmental friendliness rises before all new technologies. Greenhouse gas emissions are on the rise, and technology requires more and more computing power. So, according to scientists at the University of Cambridge, during the production of bitcoins, 97.9 terawatt / hour of electricity is consumed per year. This is more than the Philippines (93.3 terawatt/hour) and Kazakhstan (91.7 terawatt/hour) consume per year, although back in 2018, energy consumption for bitcoin mining was almost 0.5% of the global one.

Cross Staking confidently copes with the environmental challenges of our time. The sidechain deployed by technology is based on the proof-of-stake consensus algorithm which minimizes its impact on the environment. So, at the Startmeup HK festival in Hong Kong, Ethereum co-founder Vitalik Buterin called the Proof-of-Stake algorithm a solution to bitcoin's environmental problems which requires much fewer resources to maintain. According to the Ethereum Foundation, the transition to Proof-of-Stake consensus will reduce Ethereum's energy consumption by approximately 99.95% after the network merge. This logic is fully applicable to other PoW blockchains which makes Cross Staking a solution for the transition of the crypto industry to a green development path.

11. Conclusion

According to the article published by Coindesk in 2022, sidechains have huge potential to expand the functionality and dynamics of blockchain technologies. In opinion of a financial journalist Stefan Roth, the prospect of blockchain technologies is a large chain with many side chains, each of which will have its own consensus algorithm, rules of operation and will solve strictly defined functions.

Cross Staking, with the help of sidechain deployment, makes possible what until recently seemed completely unfeasible - staking cryptocurrencies based on PoW consensus.

The introduction of CROSS STAKING technology will solve many problems that the classic blockchain has, namely:

– improve network scalability and performance;

– increase the level of security;

– reduce the energy costs of blockchain projects by several times thereby increasing energy saving and developing a “green economy’’.

It should be noted that the Cross Staking technology is under constant development, being modernized and improved over time, adapting to the constantly changing conditions of the post-industrial economy.

Technologies such as Cross Staking will become cutting-edge in the crypto industry in the near future and will set the direction for the development of the entire industry as a whole.

12. Materials used

1) https://blog.ethereum.org/2021/05/18/country-power-no-more/

2) https://www.coindesk.com/learn/an-introduction-to-sidechains/

3) https://academy.binance.com/ru/articles/proof-of-stake-explained

4) https://academy.binance.com/en/articles/blockchain-scalability-sidechains-and-payment-channels

5) https://www.researchgate.net/publication/335147247_Fair_Proof_of_Stake

6) https://en.wikipedia.org/wiki/Proof_of_stake

7) https://coinmarketcap.com/alexandria/ru/article/proof-of-work-vs-proof-of-stake

8) https://blog.ethereum.org/2016/12/04/ethereum-research-update/

9) https://academy.binance.com/en/articles/proof-of-work-vs-proof-of-stake

10) https://www.researchgate.net/publication/346761640_Evolution_of_Shares_in_a_Proof-of-Stake_Cryptocurrency

11) https://blog.ethereum.org/2014/10/21/scalability-part-2-hypercubes/

12) https://academy.binance.com/en/articles/proof-of-stake-explained

13) https://ethereum.org/en/energy-consumption/

14) https://www.investopedia.com/terms/p/proof-stake-pos.asp

15) https://www.researchgate.net/publication/319647471_Securing_Proof-of-Stake_Blockchain_Protocols