Factsheet

Blockchain architecture

Stakenet

Factsheet

1. Blockchain architecture

Stakenet is a trustless PoS blockchain, which provides a truly decentralized, highly secured and profit driven inter chain meta network for cryptocurrencies. Stakenet is powered by its native coin XSN and is managed by its own masternodes.

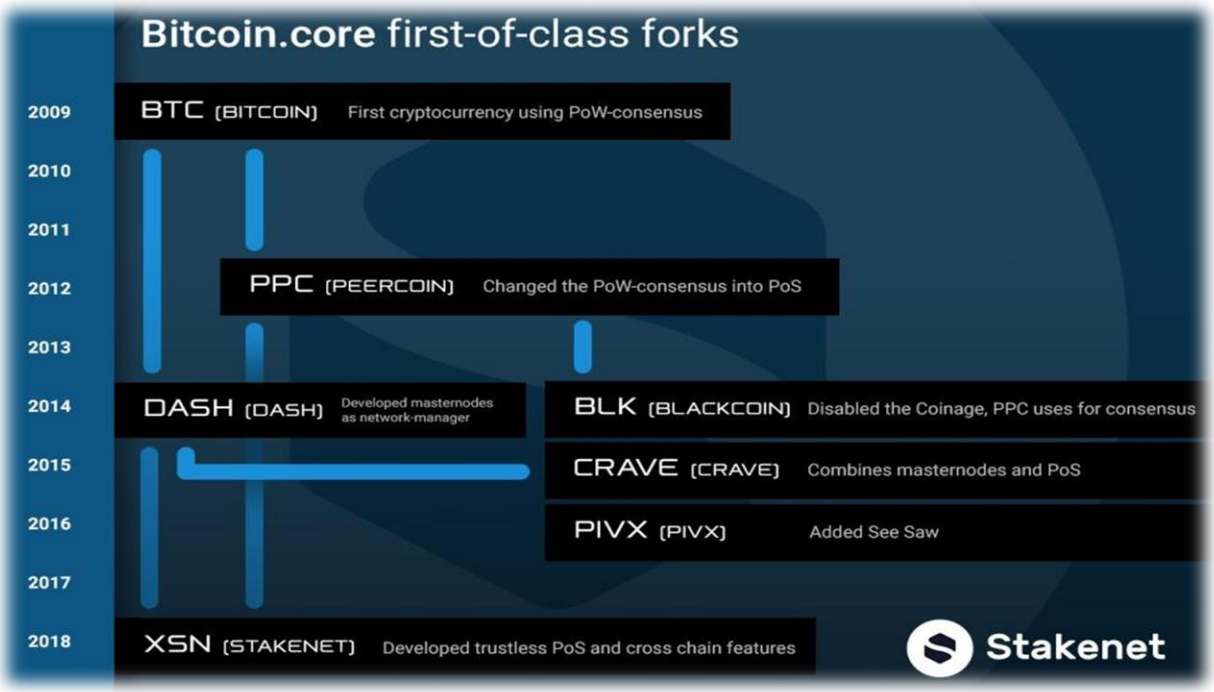
1.1 History

A coin swap from POSW to XSN created the Stakenet blockchain. The new blockchain architecture is based on the Bitcoin.core and has been modified as needed by the development team.

1.1.1 POSWallet

POSWallet was an online staking wallet serving up more than 100 of the most common PoS altcoins along with block explorers and faucets for each coin. The initial market supply of POSW was capped at 250.000.000. The previous team decided to reduce the final supply by burning coins from the developers address, so that the initial supply was reduced to only 70.000.000 POSW with an interest rate of 1% per year. After a hack of poswallet.com the old team left POSW. In summer 2017 the X9 Core-Devs took over the development putting together a completely new team. They rebuilt the underlaying blockchain architecture from scratch and have expanded their features and use cases, to finally wipe out all connections left to the former POSW blockchain. From that day on, XSN was born and finally launched its completely new dedicated blockchain at the 1st March 2018.

1.1.2 Bitcoin.core fork table



Stakenet was created to build an ecosystem, that allows easy and secure offline staking and cross chain communication. For this purpose, the basic characteristics of Bitcoin, Dash and Peercoin were assumed and slightly modified. XSN uses the same core as Bitcoin, an improved Dash masternode architecture and an adjusted coinage, like Peercoin for the validation of new minted blocks, down to 24h.

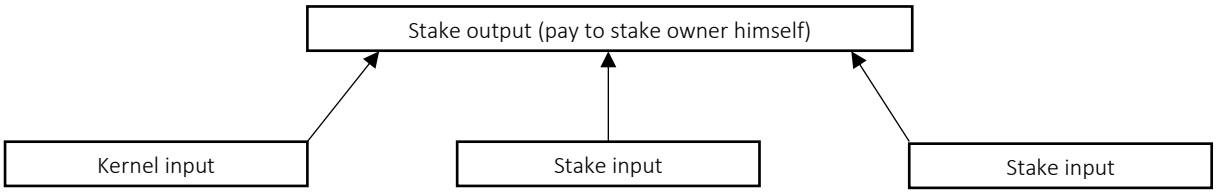
Disclaimer: As with any crypto-currency, there is inherent risk. While XSN endeavors to implement to the best of their abilities, they make no representations as to future value and individuals purchase XSN at their own risk.

1.2 XSN blockchain metrics

Stakenet is a cutting-edge utility blockchain and ecosystem created to provide a truly decentralized, highly secure and profit-driven interchain meta network for cryptocurrencies. This economy is backed by Stakenets own coin named XSN. It utilizes the X11 algorithm, has powerful Masternodes providing the network services and is secured by a Trustless Proof of Stake (TPoS) consensus. All this results in the highest level of security amongst existing Proof of Stake networks.

1.2.1 Consensus

The consensus in a decentralized digital currency is a fundamental for the validation of the newly generated blocks and moving the blockchain. Expressed in a simple way; it's a software component that the validator of a blockchain uses to vote on whether a story about the past is true or not. For this proof, Stakenet uses a Proof of Stake (PoS) consensus. In the PoS consensus, the block generation is done with a special transaction, called coinstake. In this transaction the coin owner pays himself, thereby consuming his coinage (up to 24h), while gaining the privilege of generation a block for the network.



The first input of the coinstake transaction is called kernel. In doing so, it must satisfy a specific hash target protocol, turning the generation of PoS blocks a stochastic process. The hash target that the coinstake transaction must satisfy is defined as a target per unit coin age that needs to be reached, before its subsequently consumed in the kernel. In contrast to Proof of Work solutions, the hashing operation is done over a limited search space instead of an unlimited search space. Therefore, the block generation time within the Stakenet is 60 seconds, while the difficulty retargeting is set to 40 minutes to avoid such long adjustment periods like in the Bitcoin blockchain. The daily chance for a staker to find and validate a block within the Stakenet blockchain is:

$$\frac{a}{(x - 15.000 \cdot y) \cdot z} \cdot 1.440$$

a = number of coins you hold
y = number of all masternodes
x = total supply
z = percentage share of all staking coins (0,0:1,0) usually between 0,5 and 0,7

1.2.2 Algorithm

Each information bit within a blockchain has undergone a process known as cryptographic hashing. For this purpose, Stakenet uses the X11 algorithm. This is a cryptographically algorithm, which uses a chained combination of the following eleven hashing functions. All of these differ by their output size. The implementation defines for the output sizes 224, 256, 384 and 512 bits.

#include "sha3/sph_**blake**.h"
#include "sha3/sph_**groestl**.h"
#include "sha3/sph_**keccak**.h"
#include "sha3/sph_**luffa**.h"
#include "sha3/sph_**shavite**.h"
#include "sha3/sph_**echo**.h"
#include "sha3/sph_**bmw**.h"
#include "sha3/sph_**jh**.h"
#include "sha3/sph_**skein**.h"
#include "sha3/sph_**cubehash**.h"
#include "sha3/sph_**simd**.h"

The enhanced complexity of chained hashing solutions, like the X11 algorithm, provides a higher level of security and longevity for store of value for digital currency compared to other single hash solutions, which all have one single point of failure. If someone breaks the single hash – the entire network is threatened till it hard forks to another cryptographic hash. This scenario is less critical for X11, because all eleven algorithms needs to be broken at the same time to threat the network.

1.2.3 Masternodes

While a staking node is defined as an active electronic device that is attached to the Stakenet network and responsible for validating the blockchain, a masternode is a full node of the network that provides several services. Each masternode within the Stakenet blockchain needs a collateral of 15.000 XSN. This was made to avoid a wild growth of the nodes. Thanks to the masternodes, the Stakenet blockchain becomes an ecosystem in which no single entity can governance the entire network. The Masternodes and their collateral requirements empower the XSN blockchain to perform highly sensitive missions in a truly trustless way. By selecting randomly masternodes to solve a task, these nodes act like oracles, so that not the entire network needs to get it done. We believe that previous masternode networks are not even doing 1% of what is possible. Because of that we will empower the Stakenet masternodes to become much more, than just coin mixer, instant sender or governance provider. With the help of periodic masternode challenges our nodes will step by step evolve into more and more powerful nodes, that provide high end services, such as hosting a decentralized exchange. Since the Stakenet blockchain uses its revolutionary Trustless Proof of Stake (TPoS) consensus, significantly more independent Stakers secure the network and many more Masternodes can be online than with previous solutions. The daily chance for a masternode node to get rewarded with a share of a blockreward is:

$$\frac{b}{y} \cdot 1.440$$

b = number of masternodes you hold
y = number of all masternodes

1.2.4 Governance

Stakenet is a decentralized autonomous organization that is run through unbreakable rules encoded and maintained on our blockchain. Stakenet doesn't have a centralized leader; instead we created a management mechanism, that takes credit for the needs of all involved individuals. The Stakenet Self-Governance will ensure that every proposal made by the community is democratically legitimatized by itself. Stakenet masternode owners have voting rights - one masternode equals to one vote.

1.2.5 Treasury

The treasury is a cryptographically sealed public address that holds money automatically allocated to it by the network. Exactly 10% of the block rewards go to the treasury. It's used to fund any related XSN project such as further coin developments, marketing campaigns, bounties and other related use cases. No centralized entity owns or have access to the money in the treasury. To obtain funds from the treasury, a proposal must be submitted and voted democratically by the masternodes. It's effectively owned by no one and everyone at the same time.

1.2.6 Supply

The Stakenet initial supply is caused by the swap from POSW to XSN. Therefore, 76.000.000 XSN were created within the genesis block. Right after the swap ended, 3.500.000 unswapped XSN coins were sent to the following burning address: XmPe9BHRsmZeThtYF34YYjdnrjmcAUn8bC.

Disclaimer: As with any crypto-currency, there is inherent risk. While XSN endeavors to implement to the best of their abilities, they make no representations as to future value and individuals purchase XSN at their own risk.

1.2.6.1 Blockreward breakdown

The Stakenet blockchain was truly fair launched with empty blockrewards for the first 10 days, respectively for the first 20.000 blocks, to avoid asymmetric gains and offering everyone a fair chance to swap their coins and set up staking nodes and masternodes. The PoS block rewards will be decreased step by step every 63.200 blocks, which is a timeslot of around 30 days, by 5 XSN each, down to 20 XSN.

PoS Phase 1 fair launch start date: 6th Mar. 2018

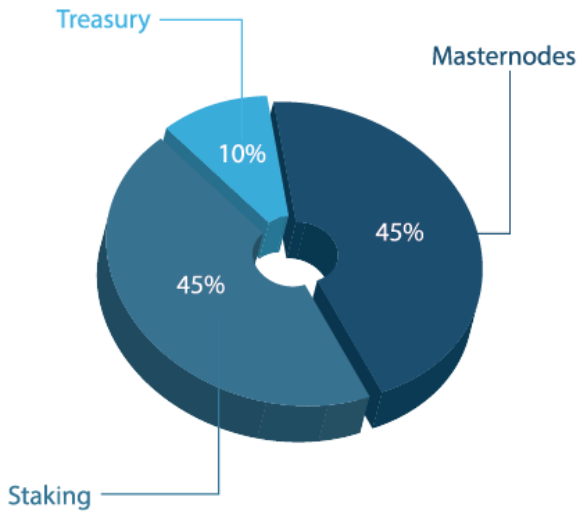
PoS Phase 01: [0 – 20.000] 00 XSN
PoS Phase 02: [20.001 – 63.200] 50 XSN
PoS Phase 03: [063.201 – 106.400] 45 XSN
PoS Phase 04: [106.401 – 149.600] 40 XSN
PoS Phase 05: [149.601 – 192.800] 35 XSN
PoS Phase 06: [192.801 – 236.000] 30 XSN
PoS Phase 07: [236.001 – 279.200] 25 XSN
PoS Phase 08: [279.201 – infinity] 20 XSN

PoS Phase 8 estimated start date: 20th Sep. 2018

Since the total block reward for XSN will stabilize at 20 XSN, the supply is theoretically unlimited. Therefore, Stakenet burns every transaction fee within the network and is building businesses that provide more value to XSN. Either by burning the profits of those thus decreasing the supply of our coin or by sending this money to the treasury to fund more projects, it's ensured that all profits within the Stakenet ecosystem will end up benefiting XSN. This Proof of Burn mechanism fulfills the purpose of a counterpart to the increasing supply.

1.2.6.2 Blockreward distribution

The Stakenet blockchain is powered by two types of nodes: Staking nodes and Masternodes. We believe that network security and network services are equally as important as to have a robust and powerful infrastructure, so we do not discriminate any for their work. That's why the staker and masternodes are equally rewarded, each with 45% of the block rewards. This way we don't incite false to disbalance the blockchain. Finally, 10% of the blockrewards are sent to the treasury to fund the further development of Stakenet.



Disclaimer: As with any crypto-currency, there is inherent risk. While XSN endeavors to implement to the best of their abilities, they make no representations as to future value and individuals purchase XSN at their own risk.

1.3 Benefits of a Bitcoin.core blockchain architecture

Because XSN is based on Bitcoin.core, all the achievements of Bitcoin development, like SegWit and the Lightning Network, can be integrated in the Stakenet blockchain architecture without much effort.

1.3.1 SegWit

Segregated Witness, so called SegWit, is the name used for an implemented soft fork change in the transaction format of the Bitcoin.core blockchain architecture to include a variety of functions. Because most of them are very technical, the following pages will summarize the benefits of all these features for the Stakenet ecosystem. It should be noticed, that SegWit is much more than just a solution for the scaling problem – SegWit is the smallest common denominator for any cross chain communication. This sum up is based on BIP 140, 141, 143 and the current Bitcoin.core.

1.3.1.1 Linear scaling of sighash operations

In some transactions the signature hashing tends to scale more quadratically than linearly, depending on how these are structured. By just doubling the block size of a transactions, you would consequently also double the amount of data that needs to be hashed for the verification – which may cause an extremely longer validation time within the block generation process, especially when some of these large transactions are designed maliciously. Segwit solves this problem by adjusting the calculation of the transaction hash for signatures, by removing the quadratic scaling of hashed data for verifying signatures. Due to this change, each byte of a transaction never needs to be hashed more often than two times – so that the same functionality is achieved much more efficiently.

Benefit: By removing the quadratic scaling of hashed data for the verification signatures, also large transactions can be generated in the Stakenets meta network without facing the previous difficulties with the signature hashing, even if those transactions are lager or generated maliciously.

1.3.1.2 Signing of input values

Before Segwit was enabled, a hardware wallet needed a full node copy of all input transactions to verify the total amount being spent and sign the transaction. Thus, it was also necessary to hash all those data to ensure that no false data were fed, so executing withdraws from a hardware devise was not particularly cheap. SegWit solves this problem by only hashing the input value explicitly which makes it easier and safer for a wallet to sign the spending transaction, no matter how large or complicated it is.

Benefit: Hardware wallet user need to pay less transaction fees for executing secure and fast withdraws. Keep in mind, Stakenet will provide its own multicurrency hardware wallet in Q4 2018.

1.3.1.3 Increased security for multisig

Without SegWit, multisig payments were protected due to a pay-to-script-hash (P2SH), which is secured by the 160bit hash (HASH160) algorithm. However, this encryption can be violated by a well-resourced attacker, who tries to find a collision address through brut forcing. SegWit prevents this fraudulent act by using HASH160 only for payments directly to one single public key, while using an improved 256bit hash for the P2SH.

Benefit: This feature of the SegWit implementation will ensure extra security for everyone paying to a multisig address or smart contract within the Stakenet network or the cross chain ecosystem.

1.3.1.4 Script versioning

Every change to the Bitcoin.core script was developed to ensure improved security and improved functionality. However, the script design only enables backwards-compatible changes, caused by soft-forking, to be implemented by replacing one of the ten extra OP_NOP opcodes with a new one. This procedure is sufficient for most changes – but it is slightly hacky (for example, OP_CLTV usually needs to be accompanied by an OP_DROP) and cannot be used to enable such simple features as joining two strings. Therefore, SegWit implements version number for scripts to enable even opcodes that would have required a hard-fork to be used in non-SegWit transactions, just by increasing the script version.

Benefit: Making changes to script opcodes easier will cause an advanced scripting in all Bitcoin.core based blockchain architectures – so that supporting sidechains or creating even smarter contracts by using Merklized Abstract Syntax Trees (MAST) can be achieved much easier by Stakenet.

1.3.1.5 Reducing UTXO growth

The unspent transaction output (UTXO) database is maintained by each fullnode of a blockchain to review whether a new transaction is valid or fraudulent. To ensure a fast an efficient network, this database needs to be very quick to query and modify. This challenge becomes even harder the more users are using the blockchain, because every new user needs to have at least one individual UTXO entry. SegWit improves the situation by adjusting the signature data by reducing the UTXO group size by at least 75%.

Benefit: By reducing the UTXO size, the maintenance and the query of the UTXO database are reduced, which will counteract future limitations or performance problems and improves the current situation for everyone, who runs a fullnode within the Stakenet ecosystem.

1.3.1.6 Efficiency gains when not verifying signatures

Bitcoin.core based blockchains do not check signatures for transactions prior to the most recent checkpoint by default. Furthermore, even some SPV clients don't check signatures themselves at all, because they trust the validation by other nodes. However, the signature data is an essential proportion of the entire transaction. Due to SegWit, every node that is not interested in signature data can skip those data to avoid downloading it to save resources.

Benefit: Because more transactions are proceeded using SegWit addresses, everyone who is running a pruned or SPV node in the Stakenet network needs less bandwidth and disk space to operate.

1.3.2 Lightning

One of the main objectives of introducing cryptocurrency was to make payment processing faster and cheaper. However, as mining operations started to become expensive, transaction fees for Bitcoin also started raising. A version of the technology that is meant to make cryptocurrency payments faster and cheaper, called Lightning Network, is a second layer solution to enable off-chain transactions on Bitcoin.core based blockchains and is expected to be a game changer in the evolution of the crypto currency. By solving the transaction malleability problem, SegWit eliminates a major barrier to implement such a second-layer solution, like the Lightning Network, on top of a blockchain. The second-layer dependents upon the underlying architecture of each blockchain, using their native smart-contract scripting languages to allow for a massive increase in the network capacity by moving the bulk of transactions off chain for quick processing. Once it is deployed across all nodes, the network will speed up transaction processing and decrease their associated costs. The Lightning Network allows Bitcoin.core based blockchains to open payment channels directly between two nodes. The parties can then conduct transactions without having to broadcast them to the blockchain, avoiding delays and costs that result from recording those transactions each time. Once the channel is closed, only the resulting balances are recorded on the blockchain, not the full transaction history of the channel, and only then fees (can even be nearly zero) were paid. There is no required time or transaction limit required to close a payment channel, so they can potentially remain open for even years.

The major problem some criticism see, is on how the sidechains within the Lightning Network work. They move the coins to a second-layer system, to not rely on the highly congested blockchain. In previous solutions, all transactions were needed to process by a trusted third party, without having to broadcast them across the entire network, which saves a lot of resources and time. Stakenet solves this problem by processing and managing these transactions by a trustless and decentralized masternode network called watchtowers, which provide lightning channels for the Stakenet ecosystem. As we expect ~2000 masternodes to be online, this will give our network a robust backbone to provide instant, private transactions to occur and liquidity on our Lightning Network.

1.3.2.1 Transactions for the future

The advantages of using the Lightning Network to cross communicate between all blockchains within the Stakenet meta network can be summarized very well by using the following four criteria.

Instant payments: Lightning-fast instant payments across the entire blockchain without any limitations caused by the block confirmation times. Due to smart contracts, the security of the transactions is ensured without the need of an on-blockchain transactions, so that a payment speed of milliseconds to seconds can be achieved.

Scalability: Allows the processing of millions to billions of transactions per second across the network. This capability outperforms all previous legacy payment rails and attaches a payment per action/click is now possible without custodians or third-party services.

Low cost: Using an off-blockchain transaction setting profits in exceptionally low fees in the Lightning Network. This enables completely new use cases such as instant micropayments.

Cross blockchains: Cross blockchain transactions will be possible if both chains are connected due a compatible second layer protocol or are supporting the same cryptographic hash function on their own. Given that, it is possible to execute trustless transactions between different blockchains.

1.3.2.2 Powered by blockchain smart contracts

Lightning is a decentralized network between several nodes which use smart contract functionality in the blockchain to enable instant payments between all participations.

How does it work? Lightning dependents upon the underlying architecture of each blockchain, using their native smart-contract scripting languages to create a secure network and allow for a massive increase in the network capacity by moving the bulk of transactions off chain for quick processing.

Bidirectional payment channels: At first, two individuals open a ledger entry on the blockchain, which requires both participants for further actions. Then, both parties need to create transactions which refund the ledger entry to their individual allocation without broadcasting this to the blockchain. This entry can be closed by each party at any time without completely trustless by just broadcasting the most recent version to the blockchain. If they've updated their individual allocations, only the most recent version is valid, which is ensured by a smart contract.

Lightning network: Due to the creation of a network of these two-party ledger channels, it is possible to find a path across the entire network. Because all the nodes along these paths are not trusted, the payment is ensured and secured by using a script which enforces the atomicity processing via decrementing time-locks.

Blockchain as arbiter: Because the blockchain itself is acting as an arbiter and intermediary, it is even possible to conduct off chain transactions with the confidence of an on-chain transactions. It’s just like making a legal contract with someone else without going to any notarian, because the smart contract ensures that no one can cheat. The court will only take actions in the event of non-cooperation to prevent fraudulent behavior.