Factsheet

Trustless Proof of Stake

Stakenet

Factsheet

1. Trustless Proof of Stake

TPoS is a Stakenet invention and is fully operational and available for everyone who owns XSN. While crypto investors currently use offline storage such as Ledger or Trezor for mere storage, TPoS transforms these cold storage devices into profit generating devices which also secure the network by validating the blockchain. The Staking rewards flow directly to the coin owner while the coins remain offline. Furthermore, Trustless Proof of Stake allows people to offer Staking as a business, where a merchant can stake other people's coins and generate a commission-based income from the rewards created, opening new opportunities for businesses to arise from our invention.

1.1 Background of Proof of Stake

At its very core, the modern banking system is based on a simple paradigm - trust. We give our money to banks and they provide us with services in return (deposits, loans and investments). While we could perform these services ourselves, it has proven much more convenient to use this centralized, trust-based system. To mitigate the potential for abuse presented by such a global centralized system, decentralized blockchain based assets, such as Bitcoin, have been introduced. To secure a decentralized network and ensure users cannot double-spend their funds, Bitcoin utilizes a Proof of Work (PoW) algorithm, which requires miners to prove through distributed consensus - a large pool of people who are geographically segregated agreeing on transactions or blocks that are valid/invalid to be added/rejected to the blockchain - have spent a certain amount of computational resources to make an attack on the network uneconomical. The computing power required to carry out the cryptographic calculations only ever increases, as the difficulty increases, thus consuming greater amounts of electricity. In the long run, this would be counterproductive to the health of a cryptocurrency, as miners would have to sell substantial portions of their coins for fiat currency to foot the electricity bill, devaluing the price of the cryptocurrency. Thus, it can be deduced that PoW networks are not financially ideal as only miners can receive block rewards and transaction fees in return for precious resources, whereas regular users do not see any rate of interest from holding their coins.

This is where Proof of Stake (PoS) networks come in. PoS is a typical computer algorithm through which a cryptocurrency achieves their distributed consensus. It is also a better alternative to the PoW algorithm because it achieves the same distributed consensus at a lower cost and in a more energy efficient way. The transaction confirmation mechanism shifts from a burden of proof of the expenditure of resources over to total stake held, where transactions are confirmed by simple nodes who hold large balances, and the greater the balance the user holds, the more likely they are to receive fees and block rewards. While this significantly reduces the number of resources required to confirm transactions and effectively allows the average user to see positive ROI on balances held, this system still requires a user to maintain connectivity always, have a high-bandwidth connection, and for their wallets to be unlocked 24/7. During any time, frame in which all or any of the conditions are not met, the user is skipped by the network and does not receive their fair share of stake rewards.

1.2 Previous PoS solutions

To fully understand the meaning of Trustless PoS, developed by Stakenet, it is necessary to deal with the historical developments of different blockchain variations. Starting with the blockchain-family, based on Bitcoin.core, the consensus mechanism of the PoS, so-called minting, developed by Peercoin, will be explained first. After that, the Nxt's created PoS variant, the so-called forging, is presented with which it was possible for the first time to stake offline by lending the own balance to another node. To make this possible, the Nxt blockchain architecture has been redesigned from scratch and is based on

its own core, the Nxt.core. Based on the PoS solutions of Peercoin and Nxt, a further variation of the staking was then developed by Bitshares, the so-called delegated PoS, which also enabled offline staking via democratically elected delegates. Once you understand all these things, you can finally understand why trustless PoS is so special.

1.2.1 Peercoins' minting PoS

The Peercoin development team had the goal to find a consensus algorithm for a digital currency that does not require as much energy as the previously known PoW. For this purpose, the basic characteristics of the Bitcoin.core were assumed and, in some cases, slightly modified. The PoS in the new type of blocks is a special transaction called coinstake (named after Bitcoin's special transaction coinbase). In the coinstake transaction block owner pays himself thereby consuming his coinage (in Bitcoin the coinage is used only for the prioritization of transactions) , while gaining the privilege of generating a block for the network and minting for PoS. Therefore, a new minting process is introduced for PoS blocks in addition to Bitcoin's PoW minting. A PoS-block mints coins based on the consumed coin age in the coinstake transaction. The protocol for determining which competing block chain wins as main chain has been switched over to use consumed coin age. The block chain with highest total consumed coin age is chosen as active chain (in Bitcoin the chain with the highest accumulated PoW is chosen as the main chain). The main criticism of Peercoin is the use of the coinage for the validation of the blocks, because unspent coins can become extremely old in the Peercoin blockchain. As a result, there is an incentive to temporarily deprive your coins of the blockchain, resulting in fewer stakers online to protect the network.

1.2.2 Nxts' leasing PoS

Nxt is a 100% PoS cryptocurrency, constructed from scratch in opensource Java. Nxt's unique PoS algorithm does not depend on any implementation of the coinage concept used by other PoS cryptocurrencies. A total quantity of 1 billion available tokens were distributed in the genesis block. Since the full token supply already exists, Nxt is redistributed through the inclusion of transaction fees which are awarded to an account when it successfully creates a block. This process is known as forging and is akin to the "mining" concept employed by other cryptocurrencies. Nxt transactions are based on a series of core transaction types that do not require any script processing or transaction input/output processing on the part of network nodes. These transaction primitives allow core support for an asset exchange, storage of small data, digital goods and account control features. There are two different types of nodes in the Nxt-network. The normal nodes and the hallmarked nodes. A hallmarked node is simply a node that is tagged with an encrypted token derived from an account's private key; this token can be decoded to reveal a specific Nxt account address and balance that are associated with a node. The act of placing a hallmark on a node adds a level of accountability and trust, so hallmarked nodes are more trusted than non-hallmarked nodes on the network. The larger the balance of an account tied to a hallmarked node, is the more trust is given to that node. If you like to stake offline, you need to lease your balance to a trusted hallmarked node. These accounts with leased forging power generate blocks more often and earn more transaction fees, but those fees are not automatically returned to lease accounts. With a bit of coding, however, this system allows for the creation of nearly trustless forging pools that can make payouts to participants. In the Nxt blockchain ecosystem, the trusted hallmarked nodes are responsible for block validation and all full nodes are responsible for the network services. The historic progression of the Nxt network has shown that hallmarked nodes with a high leasing

balance have become more and more powerful over time. For example, 5 individual nodes control over 70% of the Waves network, which backend is nearly 1:1 based on the same Nxt.core.

1.2.3 Bitshares' delegated PoS

Delegated Proof of Stake (DPoS) was created as new method of securing a PoS cryptocurrency's network. DPoS attempts to solve the problems of both Bitcoin's traditional PoW system, and the PoS system of Peercoin and Nxt. Therefore, DPoS implements a layer of technological democracy to offset the negative effects of centralization. The fundamental feature of DPoS is that shareholders remain in control. Bitshares argues, that if they remain in control it is decentralized. As flawed as voting can be, when it comes to shared ownership of a company it is the only viable way. Fortunately, if you do not like who is running the company you can sell, and this market feedback causes shareholders to vote more rationally than citizens. Every shareholder gets to vote for someone to sign blocks in their stead (a representative if you will). In Bitshares, anyone who can gain 1% or more of the votes can join the board (in Lisk for example only the Top 101, in EOS only 21 delegates are on board). The representatives become a "board of directors" which take turns in a round-robin manner, signing blocks. These delegates are the only authoritarian individuals within the blockchain that can produce and broadcast blocks. Producing a block consists of collecting transactions of the P2P network and signing it with the delegates signing private key. Delegates are also responsible for creating all network services. The biggest problem with DPoS is that the delegates can also get together in groups. For example, the complete Lisk network is determined by 3 groups. As the delegates have the power and decide how much they give their voters from their blockrewards, a DPoS blockchain ecosystem turns to quickly "eat or die" mentality with less privacy.

1.3 Introducing TPoS

One of the main criticisms of a PoS system has been that it is only maximally safe when all the coins are online and authoritative staking nodes are avoided. All previous staking and offline staking solutions could not meet these conditions. Stakenet has devised a solution to the problems being faced by users of decentralized networks today: Trustless Proof of Stake. TPoS essentially allows users to own a stake in Stakenet and use any other node to do the staking for them using their high bandwidth, continuous, connectivity, while not having to share any spendable balance or private keys with the node. Your funds are yours and yours alone. They will safely and securely grow over time and protect the network even while you sleep. This feature was created with the intention of allowing users to securely stake XSN coins in cold storage form a hardware device and produce, validate and move a blockchain at the same time. Increasing security for both the network and the user.

Stakenet was created to make an ecosystem that allows easy and secure offline staking to increasing security for both the network and the user. For this purpose, the basic characteristics of Bitcoin and Peercoin were assumed and in some cases slightly modified. XSN uses the same core as Bitcoin and an adjusted coinage, like Peercoin for the validation of new created blocks, down to 24h. The trustless staking is realized by the invention of so-called merchantnode. The requirements to set up a merchantnode offline staking are zero. In contrast to all previous solutions, the merchantnodes have neither an advantage in the block generation and the blockrewards, nor a decisive influence on the blockchain. They have only the right to validate the blockchain for you. Just imagine you are putting your money inside of a virtual bank that cannot fail, get robbed, go bankrupt, become insolvent or shut down. Just imagine you can withdraw or move 100% of your funds at any time, day or night, no questions

asked, and no withdrawal limits imposed. With Stakenet you do not send over your money, you send the right to grow your money for as long as you like.

1.3.1 Purpose

An XSN TPoS contract is a special agreement made on our blockchain, which allows an owner of a given address ("owner") to give staking permission to a separate address ("merchant"). The owner of this merchant address does not have permission to move funds in the TPoS address, only the right to stake the balance of that address. The owner can move his funds out of the TPoS address at any time, giving him complete control of his funds during and throughout the execution of this contract.

1.4 Technical documentation of the TPoS contract

The contract is a special transaction with OP_RETURN that holds data specifying the terms. The contract is created by a user sending 1 XSN to himself. This transaction will also broadcast the terms of the contract to the network. This 1 XSN needs to be made lowest priority when user spends XSN. To cancel the TPoS contract the user simply needs to move all his funds into a new address or just unlock and move the 1 XSN, which includes all contract information.

1.4.1 Required information of the TPoS contract

Required information in the contract are as follows:

1. tposAddress, Address owned by creator of contract (this balance will stake via TPoS)
2. merchantAddress, owner of this address will have the ability to stake the balance in "tpos address"
3. commission, (value between 1 - 99%) tells the protocol how to split staking rewards minted from tpos address (allowing owner to auto pay commission to merchants)
4. signature, signature by creator of the contract showing proof that he is the owner of the tpos address

1.4.2 Sample contract

A sample contract within the XSN blockchain looks like this:

out 0: { tposaddress : 1 XSN} (deposit)
out 1: { OP_RETURN XoX31nLRYeteYLHMibYmHALCV7bE2PPRH6 Xp944knpdSSWex2uH2he5CKZg2sN12 bbPS 10 65_bytes_signature }
out 2: { changeaddress: changeamount }

1.4.3 RPC calls

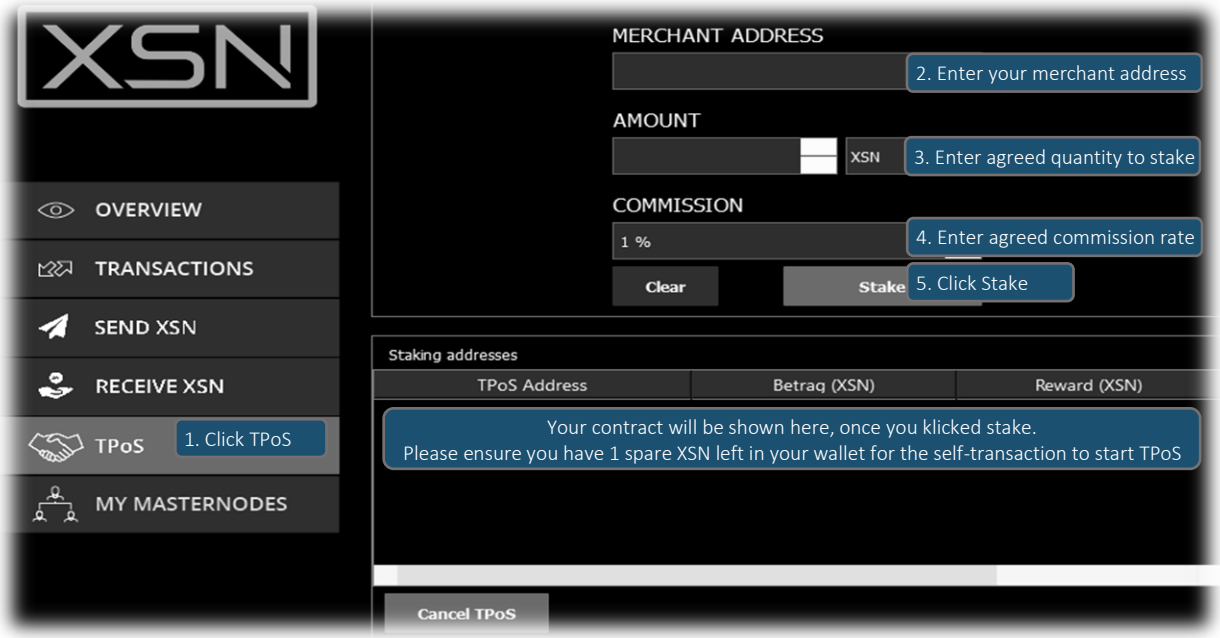
We have created RPC calls to create a TPoS contract and submit it to the network:

RPC call 1 tposcontract create [tpos_address] [merchant_address] [comission]
#this call will return a hex encoded contract, which can be sent to the network using RPC call 2.
RPC call 2 sendrawtransaction [hex encoded contract]

In this snapshot you can see how a contract is being created and broadcasted on our network via RPC.

1.4.4 Sample “one click” TPoS UI

The image below is an example of an “one click” TPoS UI taken from the XSN desktop wallet.



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.

Once the user fills the required fields and clicks “stake” the backend executes this for steps:

1. Generates the new tposAddress for the owner
2. Generates the TPoS contract using the entered merchantAddress
3. Broadcasts the contract to the network
4. Send the amount of XSN to the tposAddress of the owner for staking

1.5 Staking as a business

The Stakenet blockchain was created to be the world’s first truly trustless, profit-driven economy where everyone can offer TPoS services as a 3rd party to other individuals, who use the XSN blockchain. Therefore, the XSN TPoS protocol includes a commission features, which makes it possible for everyone to run staking as a business.

On the surface, the commission is simple. A merchant provides a service and charges a fee for said services. However, in our case this entire negotiation is handled directly on the XSN blockchain. The TPoS protocol itself is smart and knows exactly how to split the new minted coins. All done without any human involvement through a series of cryptographically signed messages broadcasted when the contract first created. We engineered this feature to avoid predicting market rate or demand but allow the two parties to settle among themselves a split from 1 to 99%. This will also allow alternative forms of services to arise, such as willingly giving the merchant all the rewards in exchange for certain goods.

1.5.1 Use case

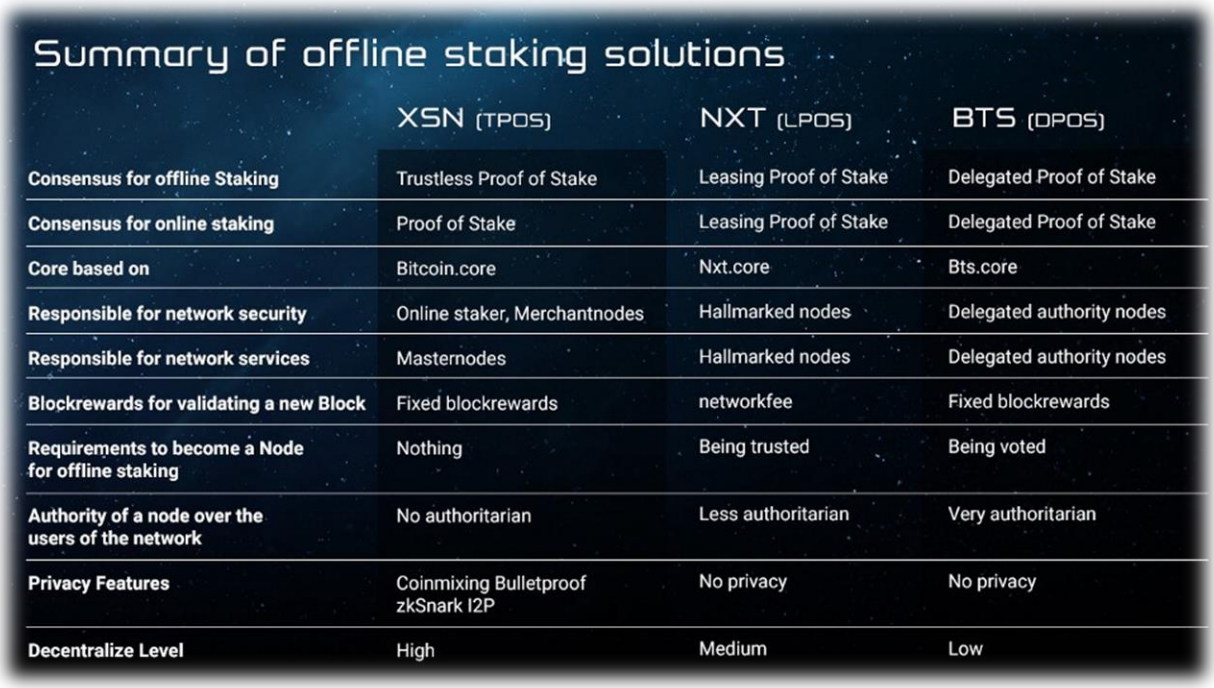
Say a merchant wants to gain a competitive edge and offer added services on top of their regular staking. So, they could instruct the owner to input 99% commission at the time of their TPoS creation, then agree to send the reward in a currency of the owner’s choice to an address of their choice. The owner could not only be staking his assets while offline but also be exchanging securely and safely, without lifting a finger. The exchanged rewards could hypothetically be translated to any form, like a BTC address, ETH, or even fiat (directly into a bank account) and could be used as a means of “cashing in” to an owner’s local currency. Once these services are established, it will drive large amounts of traffic and attention to our currency as we will be the first and only one with this unique functionality. In a world with increasing regulations this effect will be even more dramatic.

1.5.2 Seller ratings

Since the staking rewards would be in control of the merchant, this example of a hidden exchange would have to maintain a small degree of trust. We believe this will be easily mitigated by giving the merchant a rating based on the quality of service. Any dishonesty or underperformance would cost the merchant more in the long run than they would gain, like the effect of standard seller rating we are all familiar with before making an online purchase. This model works because the merchant will never be enabled

to make off with a significant amount of fund. The worst scenario is he steals a few small rewards but completely ruins his reputation in doing so, and if the owner is not comfortable with the service he can simply cancel the TPoS contract and redeem his funds at this discretion.

1.6 Comparing TPoS with previous PoS solutions



Summary of offline staking solutions

	XSN (TPOS)	NXT (LPOS)	BTS (DPOS)
Consensus for offline Staking	Trustless Proof of Stake	Leasing Proof of Stake	Delegated Proof of Stake
Consensus for online staking	Proof of Stake	Leasing Proof of Stake	Delegated Proof of Stake
Core based on	Bitcoin.core	Nxt.core	Bts.core
Responsible for network security	Online staker, Merchantnodes	Hallmarked nodes	Delegated authority nodes
Responsible for network services	Masternodes	Hallmarked nodes	Delegated authority nodes
Blockrewards for validating a new Block	Fixed blockrewards	networkfee	Fixed blockrewards
Requirements to become a Node for offline staking	Nothing	Being trusted	Being voted
Authority of a node over the users of the network	No authoritarian	Less authoritarian	Very authoritarian
Privacy Features	Coinmixing Bulletproof zkSnark I2P	No privacy	No privacy
Decentralize Level	High	Medium	Low

"One of the main criticisms of a PoS system has been that this is only maximally secure when all the coins are online and authoritative staking nodes are avoided." As you can see now, Stakenet is the only staking solution, which ensures the maximum of decentralization, privacy and security in a non-authoritarian network by providing high end services ensured through masternodes for the entire ecosystem at the same time.