Whitepaper

Version: 3.0

Date: 1st July 2018

Stakenet

Table of contents

1. Executive Summary

As we move through a 3rd generation wave of blockchains it is important to understand which technologies, communities and Decentralized Ledger Technologies (DLT's) will separate themselves from the rest, pushing through the noise of constant ventures entering the crypto-sphere. Instead of a "one chain rule" however; we believe the future will instead be the formation of a global backend - a 4th generation blockchain mesh consisting of every chain, technology and service created thus far. A united network of different tech from different chains fully communicating as one entity executing synchronously. A future where one powers software to run their vehicle, buys groceries, or signs contracts instantly using different chains will be amongst us, constantly evolving to fit users' needs on the fly. This conversion will be completely unbeknownst to end users as swaps will be done case by case on the backend, not seen, realized, or even chosen by the user.

Stakenet (XSN) is building an integrated decentralized ecosystem to create a suite of effective investment tools for investors and the world's first truly decentralized cryptocurrency bank. The front-end consumer interface, Stakenet.io, is scheduled for release in June 2018. The Stakenet blockchain is powered by its own native coin XSN, which can be used to pay for all the services and products within our ecosystem. The Stakenet ecosystem will be comprised of the following elements:

Trustless Proof of Stake (TPoS): TPoS is a Stakenet invention. 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. Rewards flow to the coin owner while the coins remain offline. TPoS is fully operational and available for everyone who owns XSN. This technology will be available for cross chain purposes upon implementation of CCPoS, described below.

Decentralized Exchange (DEX): XSN will create crypto's first truly decentralized cryptocurrency exchange run by masternodes. These masternodes will be rewarded through trading fees and will act similarly to Stakenet.io in that once XSN cedes control, the masternodes will run the network and cannot be shut down by XSN or any third party.

Masternodes with multiple sources of income: XSN masternode owners will have three sources of income: regular blockrewards, DEXs' trading-fees and fees for running TOR-network services.

Investment Agility due Cross Chain Proof of Stake (CCPoS): Another XSN innovation under development is CCPoS. With this technology we aim to enable users to stake XSN and receive rewards in any other coin. Herewith individuals will be enabled with flexibility to switch rewards on the fly to that new "hot coin", if they so desire.

Profit-sharing, buy-back-burns and Revolving Stake Bonus (RSB): All profits will be given back to XSN coin owners one way or another. Some options being explored are coin buy-back-burns and air drops to existing coin owners. Other options will be distributing the service-fees to all involved parties. At least XSN will reward coin holders via an RSB mechanism, which is a proof of burn technology for service- and business-provider who use the XSN network.

Convenience due a new multi-currency wallet: Stakenet multi-currency wallet will enable users to stake and earn rewards from one location, rather than as currently where a wallet is required for each specific coin.

Cold storage exchanging from a hardware device: In 2018 Q4, users will have the ability to trade Ledger and lightning network compatible coins through our DEX without the coins ever leaving the security of cold storage.

TPoS Marketplace: Stakenet.io will host a merchant marketplace where coin owners can hire merchants to trustlessly stake their coins using TPoS, while the coins remain on a Ledger or Trezor hardware wallet, or any other cold storage. Furthermore, it will also be possible to be your own merchant without any restrictions.

Security: Stakenet will initially be centralized but will thereafter run entirely by masternodes. This decentralization removes the risk of obstruction or being shut down by third parties. Furthermore, our TPoS consensus ensures the maximum level of network security along all existing PoS solutions.

Privacy: XSN is building crypto's first internal TOR network run by masternodes. Whereas TOR has been utilized in crypto by coins like XVG, those methods are fundamentally flawed due to exit node relay detection. Our TOR masternode network won't have this vulnerability and will allow truly obfuscated transactions. Moreover, the Stakenet blockchain utilizes coinmixing and will encrypt transactions due to the zK-SNARK protocol.

Coin metrics:

Consensus: PoS & TPoS
Coinage: enabled, 24h
Algorithm: X11
Block time: 60 seconds
Difficulty retargeting: 40 minutes
Swapped supply from POSW to XSN: 73.000.000 XSN
Blockreward distribution: 45% masternodes, 45% staking, 10% treasury
Masternode requirement: 15.000 XSN

PoS rewards breakdown:

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

PoS Phase 01: [000.000 – 020.000]	00 XSN
PoS Phase 02: [020.001 – 063.200]	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

Staking reward calculation:

Your daily chance to validate a block and being rewarded is:

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

Masternode reward calculation:

Your daily chance being rewarded for providing your services is:

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

a = number of coins you hold
b = number of masternodes 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

2. Disclaimer

PLEASE READ THIS DISCLAIMER SECTION CAREFULLY. IF YOU ARE IN ANY DOUBT OF THE ACTION YOU SHOULD TAKE, YOU SHOULD CONSULT YOUR LEGAL, FINANCIAL, TAX, OR OTHER PROFESSIONAL ADVISOR(S).

This document is a whitepaper setting out the current and future developments of the Stakenet Network and Stakenet Ecosystem. This paper is for information purposes only and is not a statement of future intent. Unless expressly specified otherwise, the products and innovations set out in this paper are currently under development and are not currently in deployment. Stakenet makes no warranties or representations as to the successful development or implementation of such technologies and innovations, or achievement of any other activities noted in this paper, and disclaims any warranties implied by law or otherwise, to the extent permitted by law. No person is entitled to rely on the contents of this paper or any inferences drawn from it, including in relation to any interactions with Stakenet or the technologies mentioned in this paper. Stakenet disclaims all liability for any loss or damage of whatsoever kind (whether foreseeable or not) which may arise from any person acting on any information and opinions relating to Stakenet, the Stakenet Platform, or the Stakenet Ecosystem contained in this paper or any information which is made available in connection with any further inquiries, notwithstanding any negligence, default or lack of care.

Stakenet, its directors, employees, contractors, and representatives do not have any responsibility or liability to any person or recipient (whether by reason of negligence, negligent misstatement, or otherwise) arising from any statement, opinion or information, expressed or implied, arising out of, contained in or derived from or omission from this paper. Neither Stakenet nor its advisors have independently verified any of the information, including the forecasts, prospects and projections contained in this paper.

Each recipient is to rely solely on its own knowledge, investigation, judgment, and assessment of the matters which are the subject of this report, and any information which is made available in connection with any further inquiries, and to satisfy itself as to the accuracy and completeness of such matters.
Whilst every effort is made to ensure that statements of facts made in this paper are accurate, all estimates, projections, forecasts, prospects, expressions of opinion, and other subjective judgments contained in this paper are based on assumptions considered to be reasonable as of the date of the document in which they are contained and must not be construed as a representation that the matters referred to therein will occur. Any plans, projections, or forecasts mentioned in this paper may not be achieved due to multiple risk factors including without limitation defects in technology developments, legal or regulatory exposure, market volatility, sector volatility, corporate actions, or the unavailability of complete and accurate information.

This white paper does not constitute a prospectus or offer document of any sort and is not intended to constitute an offer of securities or a solicitation for investment in securities in any jurisdiction. This white paper does not constitute or form part of any opinion on any advice to sell, or any solicitation of any offer by the distributor/vendor of the STAKENET (the “Distributor”) to purchase any XSN Coin, neither shall it or any part of it nor the fact of its presentation form the basis of, or be relied upon in connection with, any contract or investment decision. The Distributor will be an affiliate of STAKENET (“STAKENET”) and will deploy all proceeds of the sale of the XSN Coin to fund STAKENET cryptocurrency project, businesses, and operations. No person is bound to enter into any contract or binding legal commitment

in relation to the sale and purchase of the STAKENET, and no cryptocurrency or other forms of Payment is to be accepted on the basis of this white paper. Any agreement as between the Distributor and you as a purchaser, and in relation to any sale and purchase, of STAKENET (as referred to in this white paper) is to be governed by only a separate document setting out the terms and conditions (the "T & Cs") of such agreement. In the event of any inconsistencies between the T & Cs and this white paper, the former shall prevail. You are not eligible, and you are not to purchase any STAKENET in the STAKENET Technologies Initial Token Sale (as referred to in this white paper) if you are a citizen, resident (tax or otherwise) or green card holder of the United States of America or a citizen or resident of the Peoples Republic of China.

No regulatory authority has examined or approved of any of the information set out in this white paper. No such action has been or will be taken under the laws, regulatory requirements, or rules of any jurisdiction. The publication, distribution, or dissemination of this white paper does not imply that the applicable laws, regulatory requirements, or rules have been complied with. There are risks and uncertainties associated with STAKENET Network and/or the Distributor and their respective businesses and operations, the STAKENET and the STAKENET Network Wallet (each as referred to in this white paper).

This white paper, any part thereof and any copy thereof must not be taken or transmitted to any country where distribution or dissemination of this white paper is prohibited or restricted. No part of this white paper is to be reproduced, distributed, or disseminated without including this section and the following sections entitled "Disclaimer of Liability", "No Representations and Warranties", "Representations and Warranties By You", "Cautionary Note On Forward-Looking Statements", "Market and Industry Information and No Consent of Other Persons", "Terms Used", "No Advice", "No Further Information or Update", "Restrictions On Distribution and Dissemination", "No Offer of Securities Or Registration" and "Risks and Uncertainties".

To the maximum extent permitted by the applicable laws, regulations, and rules, STAKENET Network and/or the Distributor shall not be liable for any indirect, special, incidental, consequential, or other losses of any kind, in tort, contract or otherwise (including but not limited to loss of revenue, income or profits, and loss of use or data), arising out of or in connection with any acceptance of or reliance on this white paper or any part thereof by you.

Stakenet may provide hyperlinks to websites of entities mentioned in this paper, however the inclusion of a link does not imply that Stakenet endorses, recommends or approves any material on the linked page or accessible from it. Such linked websites are accessed entirely at your own risk. Stakenet does not accept responsibility whatsoever for any such material, nor for consequences of its use. This paper 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 state, country or other jurisdiction where such distribution, publication, availability, or use would be contrary to law or regulation. STAKENET and/or the Distributor does not make or purport to make, and hereby disclaims, any representation, warranty or undertaking in any form whatsoever to any entity or person, including any representation, warranty or undertaking in relation to the truth, accuracy, and completeness of any of the information set out in this white paper. No information in this white paper should be considered to be business, legal, financial, or tax advice regarding STAKENET Trading Technologies, the Distributor, STAKENET network, and sale of XSN Coin on exchanges. You should consult your own legal, financial, tax, or other professional advisers regarding

STAKENET Network and/or the Distributor and their respective businesses and operations, the XSN Coin. You should be aware that you may be required to bear the financial risk of any purchase of XSN Coin for an indefinite period of time.

2.1 Restrictions for distribution and designation

This paper is only available on www.xsncoin.io and may not be redistributed, reproduced, or passed on to any other person or published, in part or in whole, for any purpose, without the prior, written consent of Stakenet Network. The distribution or dissemination of this white paper or any part thereof may be prohibited or restricted by the laws, regulatory requirements and rules of any jurisdiction. In the case where any restriction applies, you are to inform yourself about, and to observe, any restrictions which are applicable to your possession of this white paper, or such part thereof (as the case may be) at your own expense and without liability to STAKENET Network and/or the Distributor. Persons to whom a copy of this white paper has been distributed or disseminated, provided access to or who otherwise have the white paper in their possession shall not circulate it to any other persons, reproduce or otherwise distribute this white paper or any information contained herein for any purpose whatsoever nor permit or cause the same to occur.

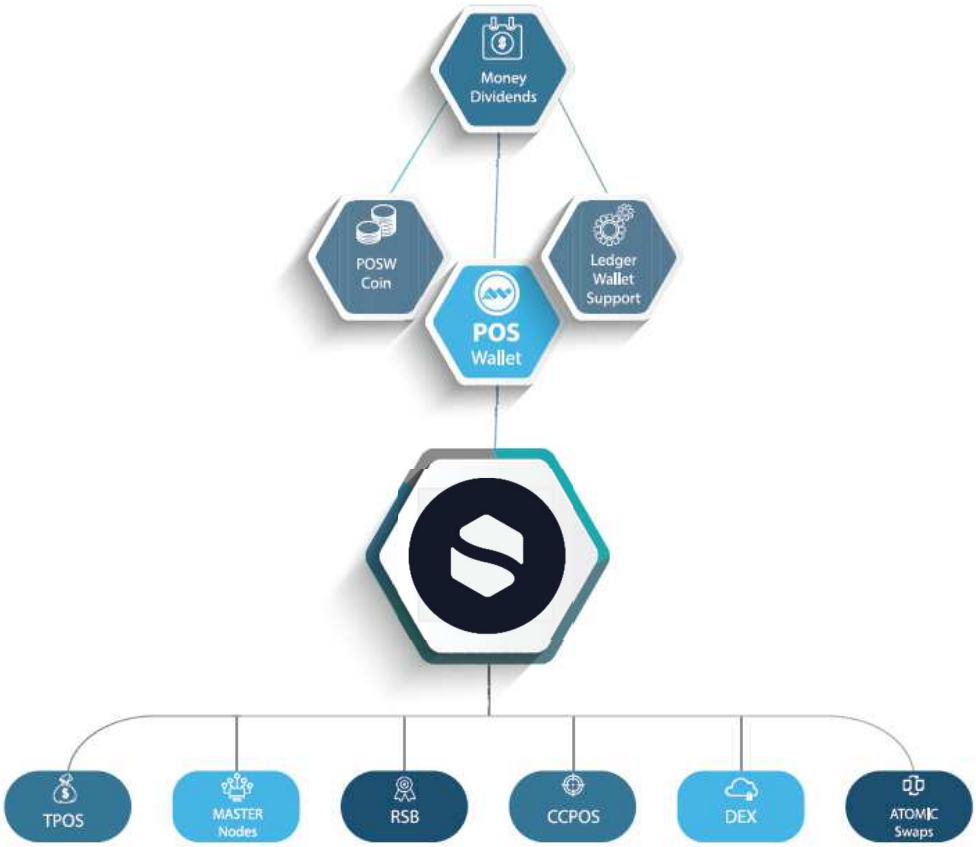
2.2 Risks and uncertainties

Prospective purchasers of STAKENET (as referred to in this white paper) should carefully consider and evaluate all risks and uncertainties associated with Stakenet Network, XSN Coin, the Distributor, merchants, and their respective businesses and operations. If any of such risks and uncertainties develop into actual events, the business, financial condition, results of operations and prospects of STAKENET Network and/or the Distributor could be materially and adversely affected. In such cases, you may lose all or part of the value of the STAKENET.

3. Introducing Stakenet

In the last few years, the cryptocurrency community has steadily grown. However, the fact remains that this community is still in the early stages of expansion and is a continuously expanding market which offers great opportunities for traders all around the world. Presently, there are over 1,600 cryptocurrencies, above 10,450 markets and a total market cap of nearly $400 billion as per statistics available at coinmarketcap.com (date: 1st June 2018). In 2017, the prices of popular virtual currencies such as Bitcoin and Ethereum soared to record highs amid increased investor interest. There are now hundreds of cryptocurrencies to choose from - with more appearing each passing day. Choice paralyzes - this adds cost, complexity and the need for advice. Given that cryptocurrency can be high risk, has extreme volatility, and can be difficult to buy and store safely. An effective and diverse portfolio of coins can be a complex problem especially, when you like to store them at a safe place and claim their individual features for a passive income.

Stakenet, with the ticker XSN, is a Trustless Proof of Stake (TPoS) blockchain that addresses the issue of cryptocurrencies for nontechnical people by providing a simple user interface to access all the features of our 4th generation meta network. Stakenet allows users to stake various cryptocurrencies in one single wallet, to trade at a decentralized exchange, which is entirely provided by masternodes and empowers its users to execute atomic swaps between different blockchains. Stakenet focuses on technology, that ensures and truly decentralized and secure network. That's why we created the TPoS consensus, due to this XSN holders can earn staking rewards for protecting the blockchain, while their coins remain offline in a coldwallet. Because Stakenet is based on the Bitcoin.core blockchain architecture, it's also complete SegWit activated and can use all the Bitcoin achievements, such as the Lightning Network. We aim to develop tech, that really pushes the boundaries of our trustless profit-driven economy, so that XSN stays relevant and can be a store of value.



3.1 Purpose of Stakenet

Stakenet is aimed to be a truly high secure and profit driven inter-chain ecosystem for almost every cryptocurrency. Therefore, Stakenet will enable a meta network of cross chain agreements and contracts. This network will be powered by the Stakenets native coin XSN and managed by the Stakenets masternodes. Based on this interchain architecture, we will create one single secure and intuitive platform to access the features and services of every blockchain within our ecosystem and trade all these coins at our decentralized exchange. Stakenet will be that one blockchain to unite all beneficial chains into one single ecosystem of blockchains.

3.2 Our vision

A vision statement should reveal what a company – or in our case – what a community hopes to be and wants to achieve in the long term. By keeping it smart and simple, the easiest way to express our vision is, to use the following words:

"Restoring trust in crypto's store of value by offering profitability, privacy, security & inter-chain-ability"

Our goal for Stakenet is to create the world's first trustless, profit-driven economy with the use of TPoS, the highest level of network security - and with the help of masternodes, the highest level of providing network services for a truly decentralized world.

3.3 Our mission

Stakenets mission is to make the XSN framework an ecosystem for cryptocurrencies, to access all their features from one single place, that can't be hacked, shut down, corrupted or abused. All in all, we like to sum up our mission that way:

"Creating a truly decentralized, private and trustless profit-driven economy for cryptocurrencies"

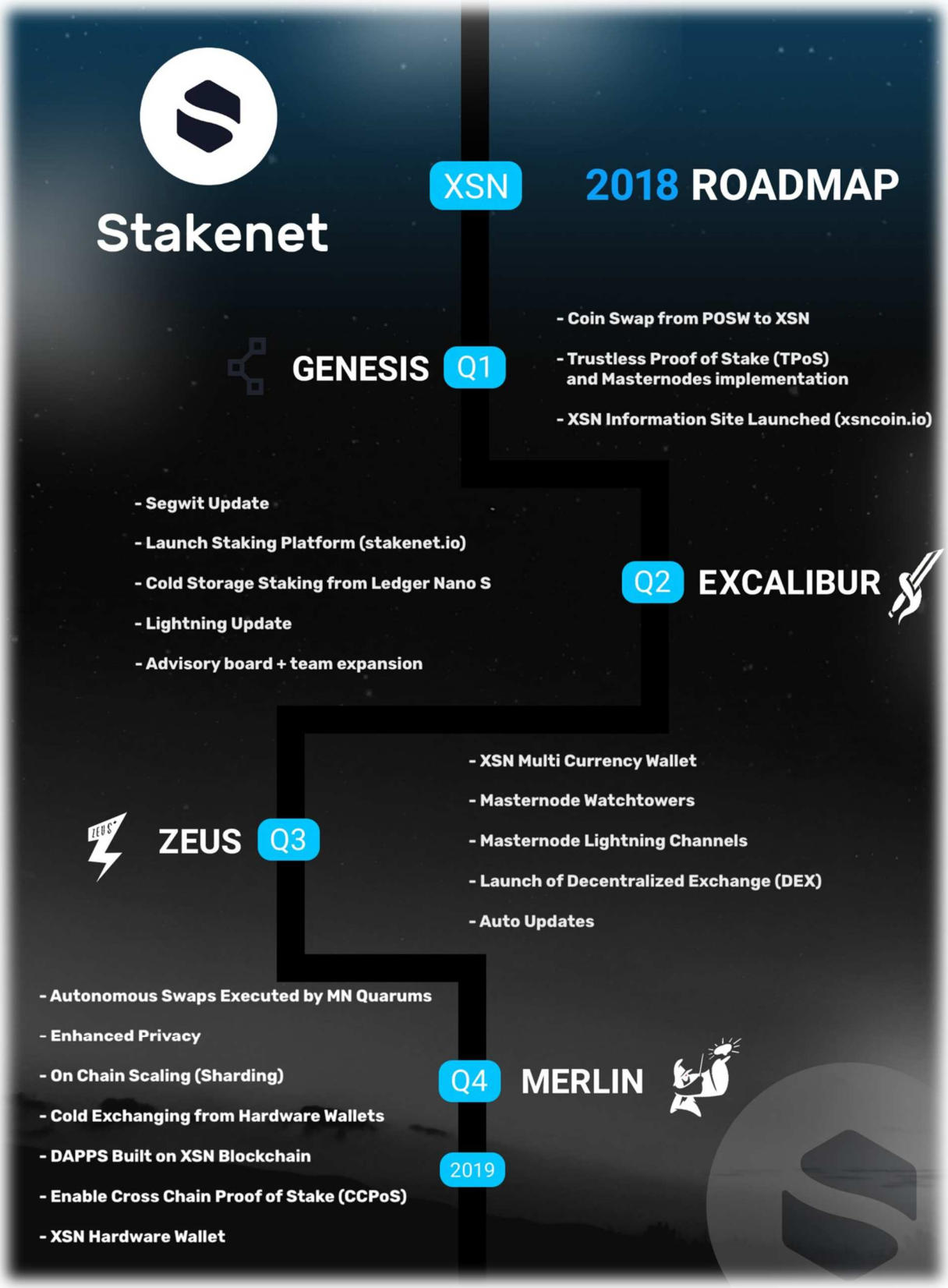
We already accomplished the fundamental for such an ecosystem by the creation of Trustless Proof of Stake consensus in a Bitcoin.core based blockchain architecture. We are now pushing boundaries to expand our ecosystem of the XSN services and products, to enable an internet of blockchains and to make crypto assets more accessible and secure for the average user around the world.

3.4 Our core objectives

The idea of Stakenet is to achieve these five following main goals:

Security using Trustless Proof of Stake and our decentralized exchange.
Immediacy over Lightning Network and masternodes.
Innovations creating XSN sidechains and new technologies.
Profitability from XSN services and applications.
Privacy by using state of the art features such inter TOR network and bulletproofed algorithms.

3.5 Our roadmap for 2018



3.5.1 Q1 – Genesis

Coin swap from POSW to XSN: From the 1st March till the 1st May the POSW blockchain swapped to the XSN blockchain. The POSW blockchain is shut down and no longer supported since the 1st May. All nodes have been shut down.

Trustless proof of stake (TPoS) and masternode implementation: The new blockchain architecture of Stakenet is a 100% minting Proof of Stake blockchain, which also enables cold staking with the help of a merchant node. In this course, the Stakenet masternodes were also implemented in the network; to provide the current network services, such as instant send, and enable further functions, such as hosting the Stakenets' decentralized exchange

XSN information site launched (xsncoin.io): https://xsncoin.io/ is the new website for all information and resources related to XSN.

3.5.2 Q2 – Excalibur

SegWit update: Segregated Witness, so called SegWit, is the name used for an implementation in the transaction format of the Bitcoin.core blockchain architecture. The implementation of this new protocol in the Stakenet blockchain architecture will be fundamentally for many more functions within the Stakenet ecosystem.

Launch staking platform (Stakenet.io): https://Stakenet.io/ will be Stakenet's own staking platform. With the help of this platform, users can stake various coins from one single place. Furthermore, Stakenet.io will provide services such as masternode hosting, managing pooled masternodes and enable atomic swaps between different coins.

Cold storage staking from nano ledger S: Ledger is the world's leading cryptocurrency hardware provider. Stakenet is one of the few coins and tokens (to date) that are supported by the Ledger Blue and Nano S hardware wallets. The integration of the offline staking features with the help of trustless Proof of Stake will be implemented soon.

Lightning update: The lightning network is dependent upon the underlying blockchain architecture. By using real Bitcoin.core based blockchains and using their native smart-contract scripting language, it is possible to create a secure inter-chain network of different participants. The implementation of this ability will be fundamental for the 4th generation meta-network, provided by Stakenet.

Advisory board + team expansion: Stakenet is still in the expansion phase. We will continue to involve qualified and talented individuals in the development process, just as we did with Frank Amato who is current Block 5 Capital Co-Founder and former executive Director of JP Morgen.

3.5.3 Q3 – Zeus

XSN multicurrency wallet: Allowing our network to hold databases and run full nodes of multiple chains we will be able to securely send, receive, and confirm transactions on separate chains from our own. These 3rd party chains will be held on our second layer which, will communicate with first layer nodes allowing our users to hold multiple wallets in one place – the XSN multi currency wallet.

Masternode watchtowers: Watchtowers have an important job. They are backbones of our cross chain ecosystem and are fundamental for our trustless cross chain swaps.

Masternode lightning channels: There will be requirements for XSN masternodes to have light channels open totaling a minimum of X amount of XSN per IP. As we expect ~2000 masternodes to be online, this will give our network a robust backbone to provide instant transactions to occur and liquidity on our lightning network.

Launch of decentralized exchange: Our masternodes will hold decentralized hashing tables or DHT's, which will be the precursor in allowing our network to be used as a DEX; holding and executing buy/ sell orders as a service. All required tech can be done in-house on the XSN chain, while XSN is accepted as a fee for powering these services.

Auto updates: Due to the rapid rate of technological advancement, soft- and hard-forks are a natural part of any emerging network. We will incorporate an optional auto update system for our users, that allows core team to update nodes automatically. Stakenet will secure that auto update system with state-of-the-art technology to ensure stability and reliability and to protect the master nodes from malicious updates and man-in-the-middle attacks. This way our investors can passively run nodes without having to constantly concern themselves with mandatory upgrades during initial periods of rapid network development.

3.5.4 Q4 – Merlin

Autonomous swaps executed by masternode quorums: Once Zeus is in place, we will begin programming our second layer to trustlessly handle cross chain light swaps utilizing masternode quorums. As of now, a human or merchant is needed to convert your TPoS stakes into a new currency. With Merlin this will be autonomously done by the network with no human needed.

Enhanced privacy: Utilizing Lightning Network and an inter TOR network we will be able to give our users the option when converting wealth to do so publicly or privately in real time. These can also be combined with emerging tech such as bulletproofs and zk-SNARKs.

On chain scaling (sharding): On chain scaling is a technique that allows the network to be divided into several shards. This sharding mechanism can improve the on chain capacity and throughput, allowing DApps and high tx functionalities.

Cold storage exchanging from hardware wallets: Once cold staking XSN from a hardware wallet is enabled, the next step will be executing cold storage exchanging. This allows users to trade and convert coins with the security provided by hardware devices.

DApps build on XSN blockchain: DApp is an abbreviation for a Decentralized Application. The backend code of our DApps will be running on the Stakenet's decentralized peer to peer network. The DApps frontend code and users interface can be written in any language that can make calls to the backend. The Stakenet's DApp framework will enable 3rd parties to develop powerful tools to provide their service in and for Stakenet.

Enable cross chain proof of stake: Cross chain proof of stake enables users to stake XSN and other lightning compatible coins and receive rewards in an entirely different coin within the Stakenet ecosystem. By offering this service, Stakenet enables its users to flexibly and autonomously switch staking rewards, if they so desire.

XSN hardware wallet: XSN will be dedicating a hardware division to solve the problem and bridge the gap between the blockchain digital world and the real world. These devices will be more than just a wallet – they will be the user's medium to access the features of all supported blockchains.

3.6 Key characteristics

Trustless Proof of Stake: Trustless Proof of Stake is a minting PoS consensus to validate, move and secure a blockchain, even if your coins are stored in a cold wallet.

Masternodes: Masternodes are powerful nodes which acts as manager and service provider for the Stakenet ecosystem.

Instant: Due the lightning network, transactions can be processed within milliseconds to seconds.

Virtually unlimited transactions per seconds: With Lightning, XSN will be empowered to execute millions to billions of transactions per second.

Nearly fee-less: By using off-chain technology, Lightning ensuring exceptionally low fees for the Stakenet ecosystem.

Private: XSN provides enhanced privacy features, like bulletproofed algorithms and an internal TOR network run by masternodes.

Secure: Using trustless PoS consensus results in the highest level of security among existing PoS Networks.

Revolving stake bonus: The RSB mechanism is a proof of burn technology for generated profits within the XSN ecosystem.

Atomic swaps: This technique allows any XSN user to swap assets between different blockchains instantly and anonymous.

Cross chain: Using cross chain PoS and cross chain Masternodes, holders can passively proliferate their XSN and receive rewards in other coin.

4. 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.

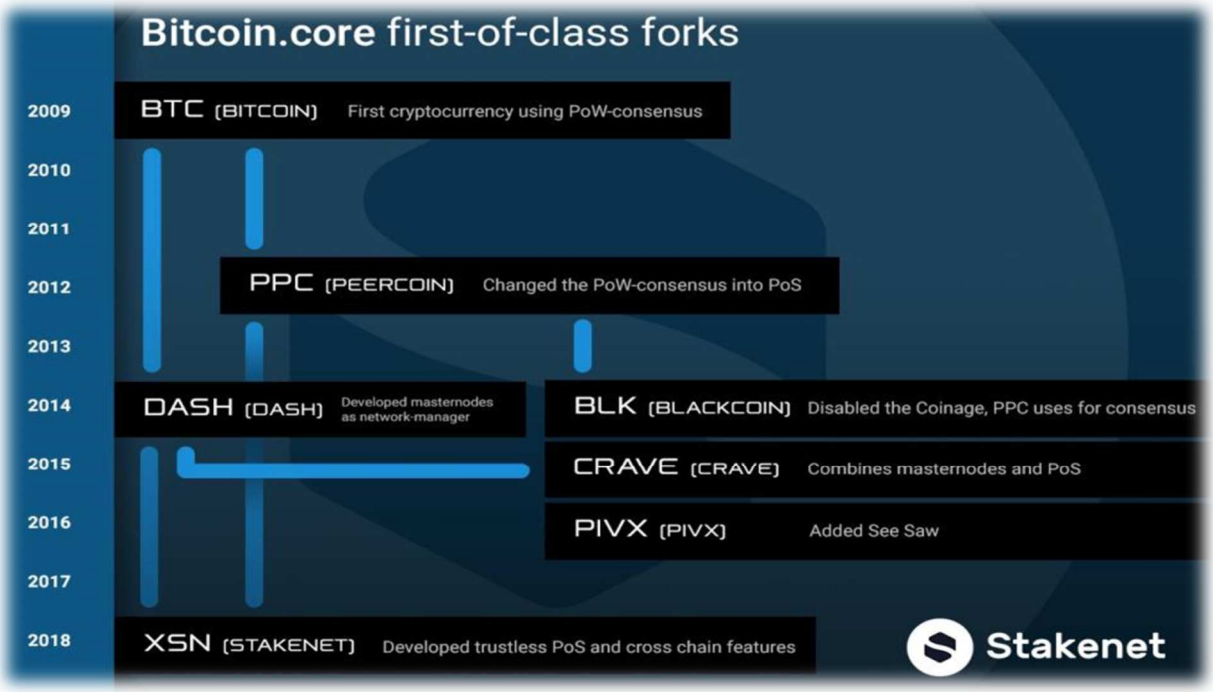
4.1 History

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.

4.1.1 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.

4.1.2 Bitcoin.core fork table



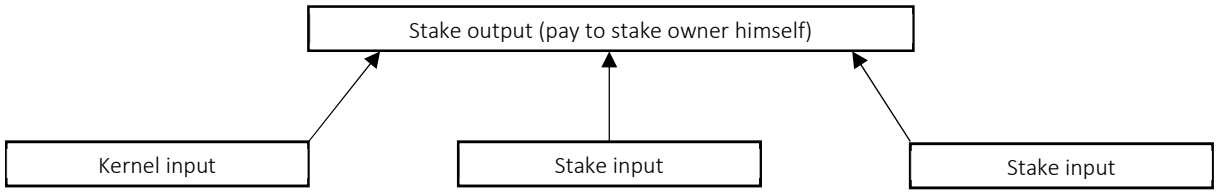
Stakenet was created to build an ecosystem, that allows easy and secure offline staking and cross chain communication. For this purpose, the basic characteristics of Bitcoin, Dash and Peercoin were assumed and slightly modified. XSN uses the same core as Bitcoin, an improved Dash masternode architecture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

4.2 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.

4.2.1 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

4.2.2 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.

4.2.3 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

4.2.4 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.

4.2.5 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.

4.2.6 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.

4.2.6.1 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

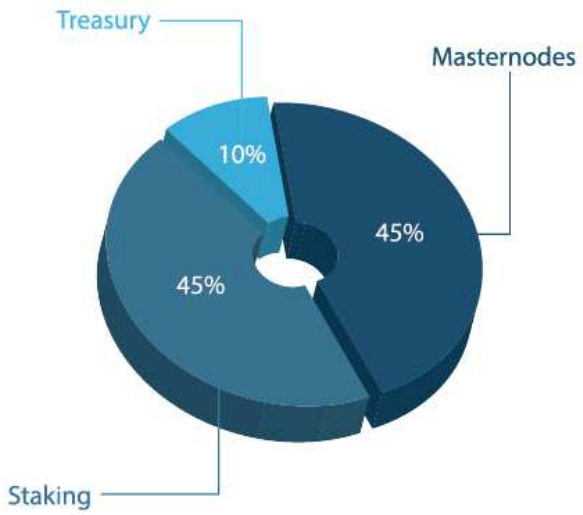
PoS Phase 01: [0 – 20.000] 00 XSN
PoS Phase 02: [20.001 – 63.200] 50 XSN
PoS Phase 03: [063.201 – 106.400] 45 XSN
PoS Phase 04: [106.401 – 149.600] 40 XSN
PoS Phase 05: [149.601 – 192.800] 35 XSN
PoS Phase 06: [192.801 – 236.000] 30 XSN
PoS Phase 07: [236.001 – 279.200] 25 XSN
PoS Phase 08: [279.201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

4.2.6.2 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.



4.3 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.

4.3.1 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.

4.3.1.1 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.

4.3.1.2 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.

4.3.1.3 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.

4.3.1.4 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.

4.3.1.5 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.

4.3.1.6 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.

4.3.2 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.

4.3.2.1 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.

4.3.2.2 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.

5. 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.

5.1 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.

5.2 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.

5.2.1 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.

5.2.2 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.

5.2.3 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.

5.3 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.

5.3.1 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.

5.4 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.

5.4.1 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

5.4.2 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 }

5.4.3 RPC calls

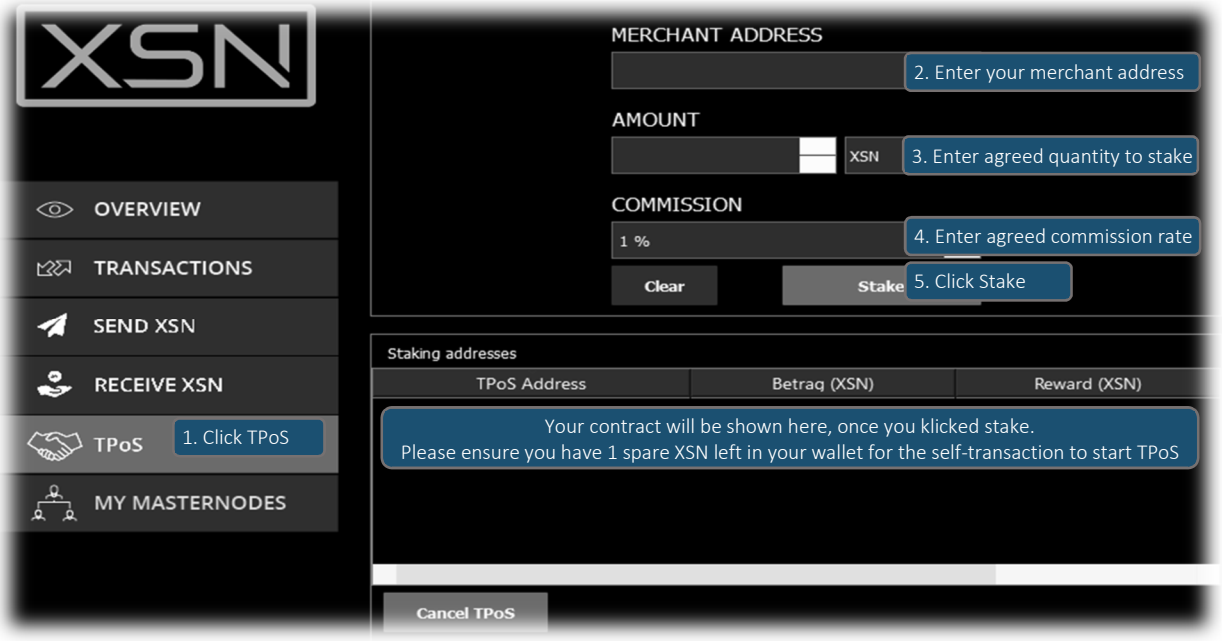
We have created RPC calls to create a TPoS contract and submit it to the network:

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.

5.4.4 Sample “one click” TPoS UI

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



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

5.5 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.

5.5.1 Use case

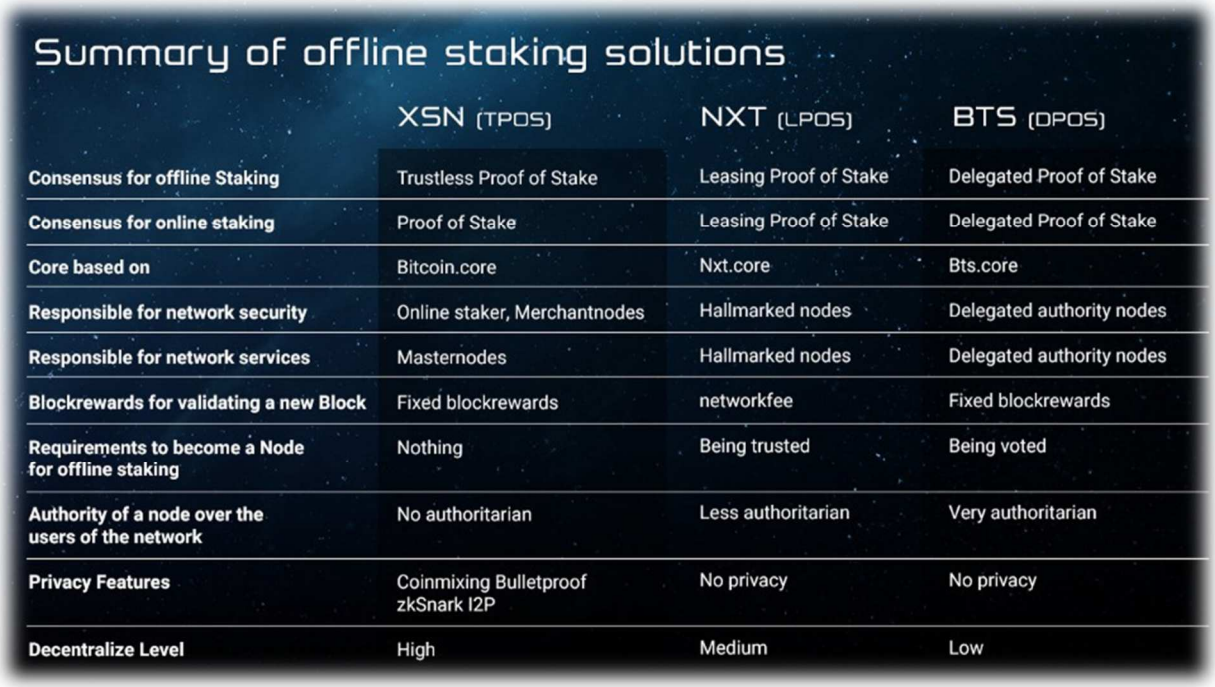
Say a merchant wants to gain a competitive edge and offer added services on top of their regular staking. So, they could instruct the owner to input 99% commission at the time of their TPoS creation, then agree to send the reward in a currency of the owner’s choice to an address of their choice. The 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.

5.5.2 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.

5.6 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.

6. Stakenet Masternodes

Normally, launching a masternode is a highly technical process and generally goes way beyond the scope of non-technical user's abilities. Stakenets masternodes platform will solve this issue by providing a simple to implement masternode hosting service that allows users to launch a masternode with incredible ease and no advanced technical ability required. Masternodes or Bonded Validator Systems can simply be termed as the servers of a cryptocurrency. A Stakenet masternode can be any computer that runs on a Virtual Private Server (VPS) and has the Stakenet wallet with 15000 XSN as a collateral number of coins required to run the masternode. Unlike normal nodes that help the miner in generating new coins, Stakenet masternodes are utilized for verifying transactions, voting system mechanism, etc. In a way, the masternode serves the Stakenet blockchain as well as other blockchains that will be integrated via cross-chain support. For users, who do not understand the complex mechanisms of cryptocurrency trading and still want to have a passive cryptocurrency income, owning a masternode means that they are involved and making gains even when not trading.

Stakenet masternodes are dedicated hardware nodes that reside on servers around the world to ensure network decentralization and needed redundancy. Masternodes serve a critical role in adding a self-governing, service-providing layer to the network as well as supporting the Stakenet vision and mission statement by performing network-related functions. Trustless Proof of Stake essentially allows users to own a stake in XSN and have merchants do the staking for them using their high-bandwidth continuous connectivity (to ensure maximal rewards distribution) while not having to share any spendable balance or private keys with the merchant. Your funds are yours and yours alone and will safely and securely grow over time even while you sleep.

6.1 How do XSN masternodes work?

Each masternodes will store an exact replica of the Stakenet blockchain, thus allowing average users to use thin SPV web, phone, and PC/Mac wallets. Statistically speaking, the average user will tend to want to use thin wallets for greater usability. To achieve the mass adoption, we have planned a reduced barrier to entry will need to be introduced to our users. Masternodes help eliminate the requirement for running a copy of the blockchain on a user's machine as wallets will connect to masternodes directly and securely.

Masternodes will require a set amount of Stakenet coins as collateral, fully redeemable should the owner ever wish to take their node offline. This is to reduce the financial viability of performing malicious attacks on the network by setting up malicious nodes as well as guarantee that only stakeholders in the Stakenet Network can vote on proposals, thus ensuring their quality.

The Stakenet project regards user anonymity and financial privacy as a core value. For a global payment network to be ready for mass adoption, payments between users must be confidential and untraceable, so a public address used to store funds cannot reveal a user's balance. To illustrate this point, failing to do so will result in vendors' inability to set prices and negotiate effectively as both suppliers and customers will be able to see their transaction history, what they charge and what they pay. This is clearly an undesirable outcome that we seek to prevent.

6.2 Masternode config

XSN Core allows controlling multiple remote masternodes from a single wallet. The wallet needs to have a valid collateral output of 15.000 coins for each masternode and uses a configuration file named masternode.conf which can be found in the following data directory (depending on your operating system):

- Windows: %APPDATA%\XSNCore\
- Mac OS: ~/Library/Application Support/XSNCore/
- Unix/Linux: ~/.xsncore/

Masternode.conf is a space separated text file. Each line consists of an alias, IP address followed by port, masternode private key, collateral output transaction id and collateral output index.

Example:

>alias< >IP:Port< >masternode private key<

mn1 127.0.0.2:62583 93HaYBVUCYjEMeeH1Y4sBGLALQZE1Yc1K64xiqgX37tGBDQL8Xg

7603c20a05258c208b58b0a0d77603b9fc93d47cfa403035f87f3ce0af814566 0

>collateral output transaction id< >collateral output index<

If you like to add more remote masternode to your local wallet, just add a new line, structured the same way, in the masternode.conf.

6.3 Masternode budget API

Stakenet supports full decentralized budgets that can paid directly from the blockchain via superblocks once the proposal is submitted by the network. Budgets go through a series of stages before being paid:

1. **prepare** - create a special transaction that destroys coins to make a proposal
2. **submit** - propagate transaction to peers on network
3. **voting** - lobby for votes on your proposal
4. **get enough votes** - make it into the budget
5. **finalization** - at the end of each payment, proposals are sorted then compiled into a finalized budget
6. **finalized budget voting** - masternodes that agree with the finalization will vote on that budget
7. **payment** - the winning finalized budget is paid

Note: A Proposals must be active on the network at least 1 day and needs to receive 10% of the masternode network votes to qualify.

6.4 Several sources of income

To secure the long-term health of the Stakenet Network, masternode operators will have financial incentives to keep their nodes running for extended periods of time, primarily by getting paid for services rendered. These will include the following:

Blockrewards: Masternodes are rewarded with 45% of all blockrewards.
DEX trading fees: Masternodes will be paid with 100% of all DEX trading fees.
TOR service fees: Masternodes will receive 100% of all fees for TOR services, they provide.

Calculation:
This calculation is based on the latest PoS breakdown reward period with a stabilized blockreward of 20 XSN for every newly minted block, because this period will last forever. Let's assume X Masternodes, Y DEX volume, Z TOR and $$ price for 1 XSN. Keep in mind, that the DEX and TOR volume will be more volatile than the blockreward.

$$Daily\ reward = \frac{1440 \cdot Blockreward \cdot 0{,}45 \cdot \$\$\ 1\ XSN}{X\ masternodes} + \frac{Y\ DEX\ volume\ \cdot\ fee}{X\ masternodes} + \frac{Z\ TOR\ volume\ \cdot fee}{X\ masternodes}$$

6.5 Watchtowers

As of now the underlying technology powering swaps would require so-called "watchtowers" — entities that need to be relied on, holding multi chains, watching and punishing any bad actors involved in cross chain communications. Watchtowers are an important job and a backbone of this cross-chain ecosystem. Our XSN masternode network is aiming to be amongst the first decentralized watchtower network providing services not just for our own chain but others could plug into our network and securely and safely rely on it — allowing groundwork for trustless cross chain swaps and trustless cross chain communication to occur as well. Each of these watchtowers will provide lightning channels for the Stakenet network and other supported blockchains like Bitcoin. There will be requirements for XSN masternodes to have light channels open totaling a minimum of X amount of XSN per IP. As we expect ~2000 masternodes to be online this will give our network a robust backbone to provide instant and private transactions to occur and liquidity on our lightning network.

6.6 Masternode challenges

Rather than see-saw the Stakenet core team decided it best to implement masternode challenge requirements (sending masternodes a challenge to solve in under a certain amount of time if they exceed challenge runtime often it will result in a ban). This can be raised to lower masternodes (increase staking) and lowered to raise the number of masternodes (decrease staking). All masternodes would need to update together. There are a few working models currently we can go off to ensure stability. This challenge runtime would need to be updated often, maybe once a year or even longer if at all. The idea is, that masternodes would need to upgrade their specifications — however this would allow many more responsibilities we can give to the masternodes and key features in our roadmap (for example cross chain proof of stake, light atomic swaps, TOR implementation on the masternode network would be services provided by masternodes) These may need to be a minimum level of power to handle heavy traffic as we believe these will be very popular features.

To compensate the masternodes for this extra power we have the option of implementing fees on the user when they use these given features which go to the masternodes providing the service. If masternode owners believe this feature will be popular then it is well worth to upgrade as the long term interest rate will be much higher. In addition, TPoS will result in the entire network being more secure than tradition PoS, as cold storage and offline wallets will be constantly staking and adding extra active pos security to the network, putting less importance on needing active stakers at a given time.

7. Privacy and Security

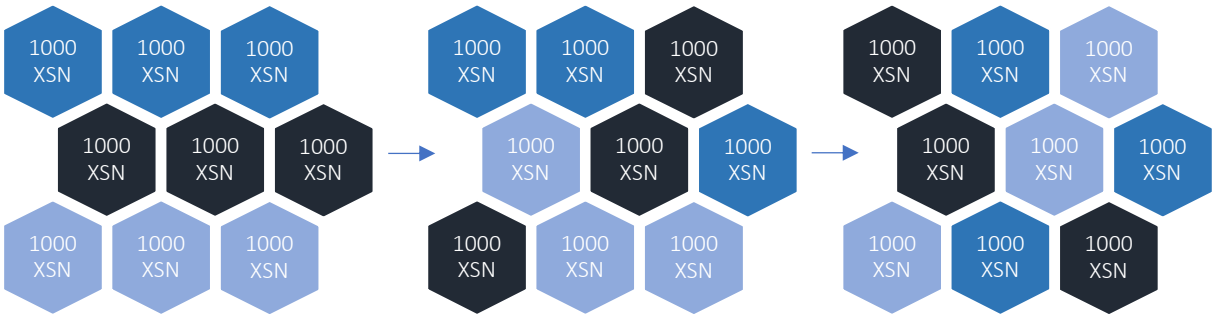
Privacy and security should be a fundamental feature of every blockchain, especially in times like this, when politicians begun to discuss about criminalizing those who “hide” cryptocurrencies. This can certainly evolve into broader criminalization of all holders at some point and time. What does this mean for us? For most of us we have never had to worry about criminalization regarding personal IP’s, web traffic or general behavior with our online crypto portfolios. However, this activity may be used as an evidence for conviction and proof of guilt under possible prosecution in a not so distant future. Any activity online related to cryptocurrencies is threatening to be classified as a criminal offense entering this next era. We believe, that it will be of high value for our users to “remain” their funds cold and stay private within our blockchain meta network, which avoids exclusive rights and cannot be shut down by the government or any other party. The Stakenet ecosystem will ensure a truly privacy and secure network with the best state of the art technologies.

7.1 Privacy

One of the main problems of the Bitcoin.core is, that the Bitcoin-protocol itself is not anonymous, because all transactions are recorded in the blockchain. By combining the structure of the transactions graph with real world informations, such as value, dates and the blockchain exit points you can easily deanonymized the pseudonyms the Bitcoin-users use. Furthermore, Bitcoins are not fully fungible. Thus, all coins have the same value in the Bitcoin protocol itself, each coin has a history that can be traced in the blockchain. This knowledge can influence your ability to spend your Bitcoins, especially then if they were part of a previous crime (e.g. Wannacry ransomware). As solution for Bitcoins privacy issues, the Stakenet uses several lines of privacy. The Stakenet blockchains includes a built-in coin mixing that makes it nearly impossible to trace transactions. This privacy feature will be enhanced by utilizing the zero-knowledge protocol and the TOR network to offer the XSN users the ability to convert their wealth privately in real time.

7.1.2 Coin mixing

If you like to send a private transaction, you send a mixing request to the masternodes. Then, one masternode broadcasts your request to the network and matches you up with other mixing requests happening at the same time. After this mixing, the masternode passes your transaction to another masternode to mix your coins with other transactions again. This process will be run several times.



To ensure that the Stakenet masternodes cannot learn the details of the transactions to rebuild the mixings, the XSN blockchain will be upgraded with the zero-knowledge protocol.

7.1.3 ZK-SNARK

ZK-SNARK is the abbreviation of "Zero-Knowledge Succinct Non-Interactive Argument of Knowledge", which is a proof construction technology where someone can prove possession of certain information like a secret key without revealing that information and without any interaction between the prover and verifier. ZK-SNARK guarantees strong privacy due to shielded transaction which are fully encrypted on the blockchain while the transaction will still be verified as valid under the network's consensus rules.

Zero Knowledge: The client (verifier V) learns nothing but the validity of the computation
Succinct: The proof is tiny compared to the computation

- the proof size is constant $O_\lambda(1)$ (depends only on the security parameter λ)
- verification time is $O_\lambda(|f|+|u|+|z|)$ and does not depend on the running time of f

Non Interactive: Proofs are created without interaction with the client and are publicly verifiable strings
Arguments: Soundness is guaranteed only against a computationally bounded server (prover P)
of Knowledge: The proof cannot be constructed without access to a witness

What sounds difficult at first is easy to understand on an abstract level. If two parties want to verify each other without revealing the secrets needed for the process they can use zk-SNARK. The sender (the one who needs to proof his identity) could show the receiver (the one how wants to verify the identity of his partner) a hash value of a random number without revealing the random number itself. zk-SNARK is using a non-interactive mode. That means the sender only sends a single message to the receiver. The current problem is to generate proofs using zk-SNARK which are short enough to be posted on the blockchain. At the moment it can only be done by generating a common reference string shared between sender and receiver. This reference string is known as the public parameter of the system.

7.1.3 Internal TOR network

Tor is an abbreviation for "The Onion Router". It is used to build up anonymous communication networks by sending network traffic on routes comprised of randomly selected Tor relay nodes. Each node removes his layer of encryption and afterwards sends the rest of the encrypted message to the decrypted address of the next node in the chain. That process slows down traffic and is challenging to use with real time applications where deviation of mean transfer times matter. The ultimate goal of Tor is making network traffic leaving an exit node looking like its origin is that exit node and thereby in theory preventing tracing the traffic back to its originator.

It is possible to run XSN Core as a Tor hidden service and connect to such services. The following directions assume you have a TOR proxy running on port 9050. Many distributions default to having a SOCKS proxy listening on port 9050, but others may not. The TOR Browser Bundle defaults to listening on a random port. If you configure your Tor system accordingly, it is possible to make your node also reachable from the Tor network. The directory can be different of course, but (both) port numbers should be equal to your xsnd's P2P listen port (9999 by default). Starting with Tor version 0.2.7.1 it is possible, through Tor's control socket API, to create and destroy 'ephemeral' hidden services programmatically. XSN Core has been updated to make use of this. This means that if TOR is running (and proper authorization is available), XSN Core automatically creates a hidden service to listen on, without manual configuration. This will positively affect the number of available onion nodes. This new feature is enabled by default if XSN Core is listening and a connection to Tor can be made. Because the Stakenet masternodes are using the same XSN core like the Staking nodes, we can provide a truly inter

TOR network with untraceable transactions across the Stakenet network. That way we will avoid the exit node relay problem every other TOR coin without masternodes like Verge XVG faces.

7.1.4 The hash algorithm

The main part of every crypto currency and the first line of defense against deanonymization is the hash algorithm used. XSN is based on X11 which is comprised out of eleven different hash algorithms which are chained together. The main advantage is that every single algorithm needs to be broken for the whole blockchain to be compromised. X11 consists of the following algorithms:

- Keccak is the winner of the NIST hash function competition and is further known as SHA-3.
- BLAKE, Grøstl, JH (Hongjun Wu) and Skein were finalists in the NIST hash function competition
- Blue Midnight Wish (BMW), Luffa, CubeHash, SHAvite, SIMD and Echo didn't make it to the final round of the competition, but it was noted that "none of them was clearly broken".

As you can see X11 has a reasonable security margin because all used algorithms have been thoroughly analyzed and some of the best cryptographers have been involved in the design of these algorithms.
Quantum computing *is said to kill* known hash algorithms soon. Grover's algorithm is normally used to test the quantum resistance of those algorithms. If you take available information on quantum computing into account and according to recent studies *SHA-3 256* is quantum resistant as it would take 10^{32} years to break it. So, we can safely assume that during the lifetime of SHA-3 256 and Stakenet quantum computers won't pose a real danger to the blockchain — despite it is commonly accepted that quantum computers will ruin normal asymmetric encryption standards.

7.1.5 Your behavior

All features you implement in a crypto ecosystem have clear borders: They can't protect against failures of the user. For a safe and private use of Stakenet please consider at least the following:

- Use a new address for every transaction. If you use only one address and post this address e.g. on social media platforms you make yourself traceable by everyone knowing that address.
- Stick to the security standards when you are using computers. Stakenet can't protect you if the platform you are using Stakenet on gets compromised. Use an up to date anti-malware tool, firewall and anti-virus.
- Encrypt your wallet! If your platform gets compromised and the attacker gains access to your unencrypted wallet your savings are gone!

Stakenet can effectively ensure private transactions by coin mixing, zk-SNARK and the optional Tor connection. But it can never foresee all kinds of failures done by the users of the system.

7.2 Security aspects of TPoS

This abstract will deal with the most important security aspects of crypto currency networks and how Stakenet will deal with this threat by using the sophisticated Trustless Proof of Stake System. Even if you are new to the crypto industry you will have heard about the "51 % attack" threatening the networks. To get a handle on that, we start repeating some basic knowledge about blockchains.

7.2.1 Blockchains and the 51% scenario

At first the blockchain belongs to the so called “distributed ledger” technologies. If we describe it in layman's terms think about your data on your hard disk drive. If you replicate that data multiple times, store it on different computers which are geographically separated and afterwards you ensure that all those replications are synchronized with all changes done to any location, you have built your own distributed ledger. Easy, isn’t it? That example above works flawlessly because only you are responsible for and interacting with it. Now imagine you want other people to interact with your distributed storage. Every person you add can have adverse effects on your system. So, this is when the need for a consensus emerges. All actors need to determine the changes which are valid and interact with each other in a way like a peer-to-peer network is doing it. If you want to get a basic understanding I recommend reading publications regarding the Byzantine Generals problem. Imagine initially three persons each having one vote are representing the consensus. If one person plays rogue the other two can still decide what is right and wrong. Now the rogue person finds a way to make his vote count two times. Now he can block the other two persons from keeping the environment sane and safe. He can block all votes because no one will achieve the needed 51 % majority. The consensus has an inherent flaw which is called the 51 % attack scenario. If you own more than 51 % percent of the resources (the votes in the example above) you have the majority in the consensus and you can determine on your own what is right and wrong — even backwards!

7.2.3 The different consensus algorithms

In most of the cases the consensus determines what is correct and what is not, and a healthy decentralized system will be immune to any 51 % attack scenario. It assumes, that transactions and states available on the blockchain are valid. This can be done in different ways which we will now analyze in detail.

7.2.3.1 Proof of Work

Proof-of-Work is the oldest mechanism used and we will use Bitcoin to explain it. In a Proof-of-Work (PoW) crypto currency new blocks are mined by solving a cryptographical hash puzzle. The solution must be of a higher difficulty than the target set by the network. The difficulty in the network is adjusted to keep the average time needed for a new block to be mined as close as possible to the 10 minute mark. The solution is found by brute force. That means that after the start of a new round every miner in the network will try to solve the puzzle by trial and error. The difficulty ensures that statistically every 10 minutes in average a block is mined. That also means that block times can vary. You can have a round that is solved after one second and the next one takes hours to complete. If no new blocks are mined no transactions on the network are carried out. If you want to get a better chance on winning the competition you just have to add more hardware or develop more specialized items. It all began with CPU mining in 2009 followed by GPUs. GPUs where made obsolete by FPGA and those were becoming obsolete by Application Specific Integrated Circuits (ASIC). Just like an arms-race the difficulty has sky rocketed and the Bitcoin Network use more electrical power than same major countries – and it is still rising!

PoW coins solely rely on the computational power and the hope, that it is dislodged geographically (paired with wide spread ownership) so no entity will ever own more than 51 % of the computational power and gets in a position to manipulate the entire network. An entity may also be a mining pool comprised of thousands individual miners. The owner of the pool controls the network and Bitcoin has

already experienced pools exceeding the 51 % mark. Luckily those always decided to block new miners from joining the pool or urged people to change the pool.

To sum it up: PoW coins rely on computational power. Computational power can be bought by FIAT money. So, any actor with enough FIAT money could join in one day, take over the entire network because the difficulty adjustment takes too long to react, and the currency is dead. Maybe no rational person would ever do that, but the danger is imminent.

PoW advantages:

- Established mechanism since 2009

PoW disadvantages:

- Waste of energy
- Danger of 51 % attack
- Inefficient use of the worlds resources (mining equipment, power consumption, cooling)
- Tends to be highly centralized
- Equipment lifetime limited & coupled to the development of the lithography used for it
- production (new smaller processes make old hardware obsolete very fast)
- High financial risk for new players

Excursion: Can you see it coming?

Can you see a 51 % attack coming in a PoW ecosystem like Bitcoin? Maybe, but any half skilled attacker would build up his force in the shadows and would be trying to distract you. Currently 80 % of the mining pools are based and China and 40 % of the hash rate in the network is controlled by a single company in that country. What does it tell us? Currently the biggest mining pool is controlling 25 % of the network hash rate. So, most would say everything is looking fine. But this is a deception and a fallacious security. If one day some of these big pools decide to fusion their hashing power into one pool the 51 % attack is no any longer a theoretical possibility but a real scenario and danger. So obviously the idea of Proof-of-Work in its real world implementation has failed hard.

Also, you don't even need to build up real 51 % hashing power to overtake the network. Let us combine that thought with a few hacking skills and a nice undetected Zero Day Exploit (ZDE). According to recent studies the average undetected (meaning not publicly known) lifetime of a ZDE is almost seven years! And in most cases the ZDE is resolved by a software update including a code refactor. That means a developer has changed a few lines in the code and rendered the ZDE ineffective – but he never intended that as he never knew of that ZDE.

Now let a big mining pool (around 25 % of the hash rate will be enough) poison the well by infecting other pools control servers with that ZDE and at a certain time he takes them all offline – here we have it! The perfect 51 % attack without even having 51 % of that current hash rate needed. Sure, the difficulty will stay high (if developers stick to Bitcoin's more than 2000 blocks of adjustment time and didn't tune that down to a few blocks or minutes) and if the attacking pool is unlucky he will not find a new block fast enough to overtake the blockchain before everyone is aware of the attack and actions are taken. But eventually he is fast enough and rewrites the blockchain in his favor.

Why should he do this you will ask? The only way to turn back that wheel of time will be a hard fork of the crypto coin ecosystem and this needs time. In the meantime, of a few hours before everyone could react (close the crypto exchanges for that coin for example) he could have dumped large amounts of coins and made a lot of money which he afterwards mixed into more private coins. Of course, we have to admit, that scenario is not that probable. But that it is even possible in theory should really make us start thinking. Did anyone use that “cyber warfare” buzzword?

7.2.3.2 Proof of Stake

Proof-of-Stake is a counterpart to Proof-of-Work. New blocks are created in a process called “minting”. PoS based currencies determine the node that creates the next block in the chain by using a pseudorandom formula. That formula differs between different implementations and can take in consideration:

- Wealth (e.g. Nxt): A node which owns more coins has a higher chance to be chosen.
- Coin Age (e.g. Peercoin): The product of the numbers of coins held multiplied with the days those where owned.

What you need to now is that only coins which are held by nodes that are currently connected to the network can be chosen as creators of the next block. As soon as you take your wallet offline the formula doesn't affect you.

PoS ecosystems tend to centralization too as most people won't keep their wallets online 24 hours a day and seven days a week. Thus, they also don't benefit from new blocks because passive staking will not reward them. Active nodes in contrast will grow bigger as time goes by and the bigger their stake the faster they grow because they have a higher chance of minting a new block. Thus, PoS systems have an implemented tendency to centralization like real world money.

A PoS blockchain has the same risk exposure to 51 % attacks but with one difference: You will never see it coming before it happens! Any skilled attacker would use hundreds of wallets to store the coins needed for the attack and not until shortly before the attack would he transfer them to a single node. Attacks can be much more fast paced that the hash rate growth in a PoW network. You can't add 100 % of mining power to the Bitcoin network at its current level in a few hours.

PoS shifts the resources needed for an attacker from buying the necessary hardware to pure buying of the coins. In theory any attacker trying to accumulate the coins needed for an attack like this would cause high prices at the exchanges due to a shift in the bid and ask relation. At least in theory because if he is clever (as we see it daily in the traditional stock market) he will silently accumulate over a long time to gain control of the network.

PoS advantages:

- More energy efficient compared to PoW
- The design of the formula can build a healthy system (or prevent it)

PoS disadvantages:

- Danger of 51 % attack
- Tends to get centralized as time goes by

- Only coins in an active online wallet are producing security for the network
- Healthiness of the network is dependent on the start of the ecosystem and the way the first coins were distributed.

Excursion:
Security in Proof-of-Stake or how we get average Joe's help in saving the network! As we learned above the network security of PoS coins is only guaranteed by the coins which are “hot” (in an active online wallet). Let us determine a few metrics to set a lower limit of active coins needed for a healthy network:

- Coins of a potential attacker have a Coin Online Ration (COR) of 100 % which we define as <number of coins> · 1,0.
- Independent securing entities (ISE) in the network get a COR of 100 % as defined above, too.
- The silent mass of the coin holders gets a COR of 25 % with the above formula.

Let us assume a hypothetical coin with 1.000.000 coins available. The attacker managed to accumulate 25 % of it, 10 % are in the independent entities and 65 % are divided to the common holders. The stake of the attacker and his influence in the network thereby is: (1,0 · 250.000) / (650.000 · 0,25 + 100.000 · 1,0 + 250.000). The attacker in this scenario already has 48 % of the active stake in the network. If we take in consideration that most PoS ecosystems don't have independent security entities a 51 % attack becomes a very plausible scenario.

But what is the motivation behind that? Of course, any attacker would harm himself by doing any attack like this, but it would be a probate instrument of killing potential rivals in an early stage where the money needed for an attack like this is nothing that really matters. If we look at the formula we can determine two possibilities to defend against attacks. The first would be to increase the activeness of the broadly distributed masses of the coins. But then psychology kicks in and 99 % of those people (take the 1 % enthusiasts for granted) will not be willing to keep their machines running all year (e. g. power costs) or they were just looking for that investment to give them their new muscle car fast. Also, the populace will never be willing to pay for a pure payment system and its security (at least not directly). The second possibility is the installation of ISEs, but these would consume up coins and could lead to a high inflation due to limited coin supply at the exchanges. All in all, PoS already has excelled PoW, but it also becomes clear; we need to motivate the average person to keep his coins online to secure the network!

7.2.3.3 Delegated Proof of Stake

The most obvious idea to solve that problem is to integrate independent entity to perform validation and signing of new blocks. That entity needs to be trustworthy and reliable. Delegated Proof-of-Stake (DPoS) tried to achieve this by porting the principle of democracy on a PoS coin ecosystem. In DPoS the power is seen to be held at the populace like in real world democracy. But, in reality it is just a consensus to empower the richest and suppress the network. The more coins you own, the more votes you have - to select a delegate (even yourself). In other words: The more coins you own, the less democratic is the entire blockchain. Those coin owners elect two types of entities:

- The delegates, which propose and realize change requests affecting the network in total. They don't receive any compensation for their duty. If a change is implemented depends on the final vote of the coin holders.

- The witnesses, which perform control tasks and sign new blocks. There is a defined upper number of witnesses and they are elected by all coin owners. The winners of the election are chosen by the best ratio of up-votes from different voters (the more the merrier). Witnesses are compensated for their duty by receiving a share of transaction fees. The compensation is set by the delegates.

Does this really solve all the problems of PoS ecosystems? For sure it doesn't. As it is based on the democratic principle it only works out flawlessly in an ideal world. As the world itself is not an ideal, DPoS inherits all flaws of modern democracy – or should we better say politics? Most of its security features can be easily annulled:

- The election process of the witnesses relies on the idea, that a witness that gets voted on by a wide spectrum of the populace of coin owners must be trustworthy. As all crypto currencies are dependent on anonymity of their actors (mainly as a marketing feature) the determination of the different actors is just their wallet address and the coins held in there. The voting process shall prevent the voting of adverse actors and thus the witness with the highest count of votes is automatically selected.

How to break it? If you're an attacker, you just need to split up your coins to different wallets and your vote gets more weight. As the system can't determine that all those wallets belong to the same actor it must assume the witness you voted for is in the best interest of the populace.

- The election process of delegates relies on the idea, that delegates are elected by the populace of coin holders. Let us oppose this with a real world example: A common election in any major western country has a participation quota of 60 – 70 % - some have more, some have less, and we are talking about government elections here! Now ask yourself: Will the populace be willing to actively take part in the election process of witnesses and delegates in a system the average person uses just for payment? Will they monitor those technical proposals? Will they recheck which blocks their elected witnesses sign? How shall the populace determine if those nameless delegates and witnesses are performing as they should?

How to break it? There is no need to break something which is broken by default. The reason is the human mind and its integration in the modern world. A DPoS ecosystem will perfectly work in a community mainly consisting of enthusiasts which are willing to spend much time on controlling their delegates and witnesses. A crypto currency ecosystem aimed at the populace with the build-up as we see it in the world today will tend to have the same centralization of power like any modern democracy paired with lobbying and hidden interests. If you don't believe it look at the newspaper and current scandals in politics.

DPoS advantages:

- Adds two pseudo independent entities for controlling duties and signing of new blocks
- Perfect system for an ecosystem dominated by enthusiasts featuring common sense and deep knowledge

DPoS disadvantages:

- Danger of 51 % attack enhanced because only a small number of entities needs to be corrupted
- Tends to get centralized as time goes by
- Security of the network is directly attached to the witnesses and delegates
- Shares the same flaws with modern politics
- The populace of that ecosystem (coin holders) may not be willing to spent time on elections for a payment system

To sum it up: DPoS is a nice idea and it will for sure work if you have enough enthusiasts in your ecosystem. In real world application interaction with the populace it will not work out and will be even more exposed to 51 % attacks.

7.2.3.4 Trustless Proof of Stake

Trustless Proof-of-Stake (TPoS) is a type of consensus which is implemented in XSN (Stakenet) for the first time to solve all the shortcomings of pure PoS and DPoS crypto currencies. It is aimed at activating the populace to secure the network by using coins in offline (cold storage) wallets and eliminating the need to vote in election processes. At its core Stakenet is also a PoS based crypto currency. 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. 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 it's 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 one. 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. As it is a PoS based ecosystem we need to deal with the problems we identified in that context and need to find a way to mitigate them. Stakenet and TPoS do this by:

- Implementing an ISE which is called the treasury. 10 % of the block rewards are passed on to the treasury which is a cryptographically sealed public address. As this is an always-online wallet a reasonable amount of coins is always online and staking thereby securing the network. This poses an additional hindrance for attackers trying to achieve 51 % majority.
- In TPoS a coin holder can keep his coins in cold storage but can pass the staking rights to a merchant node. Thereby all coins affected by a TPoS contract are counted as "hot" and can actively take part in the process of securing the network. In contrast to DPoS the populace of the ecosystem profits by handing over their staking rights to a merchant node because the merchant node rewards them for doing so with a part of the staking rewards of the merchant node. This is a psychological effect because humans tend to interact with things they can benefit from Also the process of signing a TPoS contract is much more easily achieved than voting on delegates and witnesses.
- Centralization of coins is prevented by dividing each block reward in three parts. Staking nodes receive 45 %, Masternodes receive 45 % and the treasury receives 10 %. A possible attacker now has to participate in the staking nodes and the Masternodes to accumulate coins passively. The treasury is out of his reach. Each Masternode needs a collateral of 15.000 XSN coins to be recognized. This shared distribution actively reduces the free float of XSN coins as every 1000

Masternodes bind 15 Million of coins. If you assume that 10 % of the coins are bound in the treasury and currently 2000 Masternodes exist, you already set an upper limit of free float coins of roughly 50 %.

In total at least 60 % of coins are always-online in Masternodes and the treasury. If we achieve a 50 % COR of the free float coins using the merchant nodes and their reward scheme we have a COR of the whole ecosystem of 80 %. We consider this the lower limit needed to secure the network!

TPoS advantages:

- Coins in cold storage are actively securing the ecosystem
- Cold storage coin holders will still receive rewards for holding their coins
- Danger of 51 % way less compared to PoW/PoS or DPoS
- Populace of the coin ecosystem gets motivated to participate by a reward scheme

TPoS disadvantages:

- Stakenet is the first implementation of this idea
- If TPoS is not accepted by the populace shares the same risks with normal PoS crypto currencies

7.2.4 Security summary

51 % attacks pose a real problem for all PoS based crypto currencies and its variants. Everyone stating his system is totally immune against that attack scenario is not telling the truth. Stakenet identified the shortcomings of other PoW and PoS ecosystems and did its best to mitigate them. Of course, we can't assure you a total security, because no actor or company on the IT sector can do that. But we are convinced that Stakenet and its Trustless Proof-of-Stake is the best technology available currently to build a safe and sane ecosystem for everyone – including the whole populace! Also, every security expert knows today, that security in an IT application depends on the hardware/software and - if not even more important - the social aspect of the users of that system. You can have the best firewall and encryption if one of the users is successfully attacked by social engineering (like Phishing). Therefore, Stakenet relies on technical security but also pays attention to the social aspect because even a simple phishing campaign for the coins of the users of your network can be the first indicator of a 51 % attack.

Finally, Stakenet is the only solution that allows users to delegate the right to grow their funds without needing to hand over custody over them. This is a groundbreaking technology and cannot be seen anywhere else. By using a dedicated blockchain, Stakenet records each user’s balance and stores it forever until they choose to move it around. The Stakenet blockchain is cryptographically secure meaning that no one can access anyone’s funds unless they have their private key (unique password). Furthermore, the Stakenet network is fully decentralized meaning it is not owned by any party who can choose to arbitrarily change the rules.

8 Cross chain communication

The value of blockchain is its concept of immutability. This strength however brings real world complexities difficult to manage in use cases, as blockchain was not conceived to adapt easily and faces challenges working with rigid models limiting its agility. For a new breakthrough to be adopted, a coin must often change its “rules” and undergo what is called a “Hard Fork”. In a large network this can be very damaging as it requires consensus amongst all nodes to run new software, possibly fragmenting its community and sometimes changing its history. There is also nothing to stop forks from occurring again and again at any point in the future, diluting a coin’s value and market capitalization. There may be solutions however using recently developed technologies and advancements. In this abstract we will discuss a few. If we can achieve these goals, it would give teams a better and smoother model to conduct operations.

Through this mechanism of CCPOS, Stakenet is creating programing protocols that themselves will interact with the ‘rules’ on separate chains other than their own. This ability would allow communities to utilize new technology, inventions and advancements ensuring they are able to adapt and adopt easily as well as remain competitive.

8.2 How do we get there?

A requirement and first step towards a chain participating in this cross chain “meta network” will be the ability to autonomously swap fluidly back and forth between assets in a trustless instant manner. We will first transform our chain into a multi-currency wallet which will enable it to hold, send and receive balances and will provide us with our solid foundation. This foundation will allow smooth transitions into cross chain capabilities and thereafter this functionality will be enabled onto our chain known as a Decentralized Exchange (DEX).

8.3 Atomic swaps

Atomic Swapping might be the closest thing to magic we have experienced thus far. It allows any user on one blockchain to ‘swap’ his asset with a peer he has never met on a completely different chain - 100% trustless, instant, and with little to no fee involved. It is also the closest solution in protecting privacy while acquiring and trading assets. There is a catch however as Atomic Swaps still require assets to be “hot” and by nature all information associated with these transactions are required public for it to work properly. This is a step in the right direction as a peer to peer system is much more secure than a centralized point of exchange, but still not a perfect system. It is not difficult to spot identities in a P2P market, and with that being considered we figure a user may not want to spend or transact any more than necessary on these platforms. As XSN will have a compatible off chain network of our own, our features can be utilized to provide extra value to this network. This is where our chain comes into play - by instantly atomic swapping into an XSN TPoS address, your newly swapped funds will automatically be safe offline and gain interest, without the need to perform extra steps in sending, receiving, or activation of any kind. Rewards gained from these addresses can also be exchanged into a different currency of your choice.

For example, if Alice owns 1 Bitcoin but desires to have 10.000 XSN instead to generate a passive income, she would need sign up at an exchange, which provides trusted trading services as a third-party. However, with atomic swaps, if Bob owns 10.000 XSN and likes to take his profits in 1 Bitcoin instead,

then Bob and Alice could make a trade without any need of a trusted third party due the trustless atomic swaps feature, provided by Stakenet.

To prevent any fraudulent behavior, our atomic swaps utilizes what is known as hash time-locked contracts (HTLCs). HTLCs enforce that the entire atomic swap process is truly trustless by ensuring both trading parties fulfill the requirements of the swap. HTLCs forces the recipient of a payment to acknowledge the receiving payment within a set timeslot by generating a cryptographical proof, we call proof of payment. Otherwise the recipient risks losing his right to the claim the set trading conditions to execute the swap.

In our trade example between Alice and Bob, consequently both parties need to submit their transaction to their respective blockchain (Alice on the Bitcoin blockchain, Bob on the XSN blockchain). For Alice to claim Bobs' 10.000 XSN, she must produce a number that is only known by her to generate the cryptographic hash value to provide her proof of payment. For Bob to claim Alice 1 Bitcoin, he must specify the same number used by Alice, to generate the cryptographic hash to provide his proof of payment.

By entitling a HTLC as linking two blockchains together, the Lightning Network can be entitled as linking payment channels between the involved blockchains. To transact with each other, Alice and Bob must be linked through these payment channels., which are provided by the Lightning Network.

8.4 Cross chain Proof of Stake

An atomic swap is essentially proof — a user is proving he has transferred funds from one account to another and thus its contract terms are satisfied. A verification mechanism on the other end is observing making sure the first user does act honestly and is true to his promise. If all is good the contract can execute, if not they are able to refute — cancelling the contract. Using this method, a user could also move funds to himself — proving he owns a stake in the 1st chains currency. This proof could be broadcasted on chain #2 (and verified using atomic swap functionalities) that our user does indeed possess a stake in the 1st chain. The second chain's protocol might then allow for an appropriate response considering this 'proof of stake'. This could be in the form of unlocking privileges, rewards or access to special features. Ownership on the first chain could even be used as "fuel" for its sister chains, creating a hierarchy while avoiding fragmentation. This would increase the origins (1st chain's) value greatly as any new advancements can be adopted into the ecosystem, using the stability, infrastructure and community from the original chain. What would result is an intra-network of blockchains we call "Inter Chain Clusters".

8.5 Interchain cluster

These Clusters have interdependent traits to one another, giving additional value to users within a given network. They still would however be able to communicate, sync, and partake in all other features allowed through those running on a lightning network. If the lightning network is analogous to an "internet" allowing communication to different blockchains, this would be like a 'LAN' — a group of local chains having special rules relative to one another, but also able to communicate to the outside world. Because lightning nodes are custom built to each chain, one could reprogram and construct rules from scratch with specialized interdependence in mind. So long as the new chains have code to be both lightning compatible as well as cluster compatible it will allow room for flexibility in all other aspects of

building and programming for experimentation and invention. This will allow new technologies to be quickly integrated as a framework will exist satisfying all pre-requirements needed allowing developers room to operate quickly and freely.

We should stress that this goes radically beyond the concept of ICOs being run on the Ethereum chain for example, as new projects wouldn't be restricted to being token-based solutions on the same chain. Instead, they'd have their own chains, and subsequent chains for secondary purposes, with virtually unlimited flexibility. As they'd be 'tethered' to our main chain — holders, masternode operators, and core team members will all benefit.

8.6 Why has this not been done?

One of the main limitations of atomic swaps is the user must have 2 blockchains — his own as well as that which he intends to interact with to verify the terms of his contract are met. He needs both, so he can physically refute if terms are not met or allow it to execute if he sees nothing wrong. This method causes limitations however as a human is needed for this entire process to function. For cross chain proof of stake to be possible it requires complete autonomy on the part of the protocol.

In our case utilizing masternode functionalities to both monitor and verify will solve this issue**.** Allowing masternodes to contain databases of 3rd party chain**s,** (specifically our sister chains) while watching for and verifying specific actions allows us to autonomously cross chain communicate via the protocol. In addition to CCPOS this would also enable an ability for users to "light-swap" (atomic swap without having to DL an entire 2nd blockchain) directly on our protocol, without the need of a 3rd party centralized service.

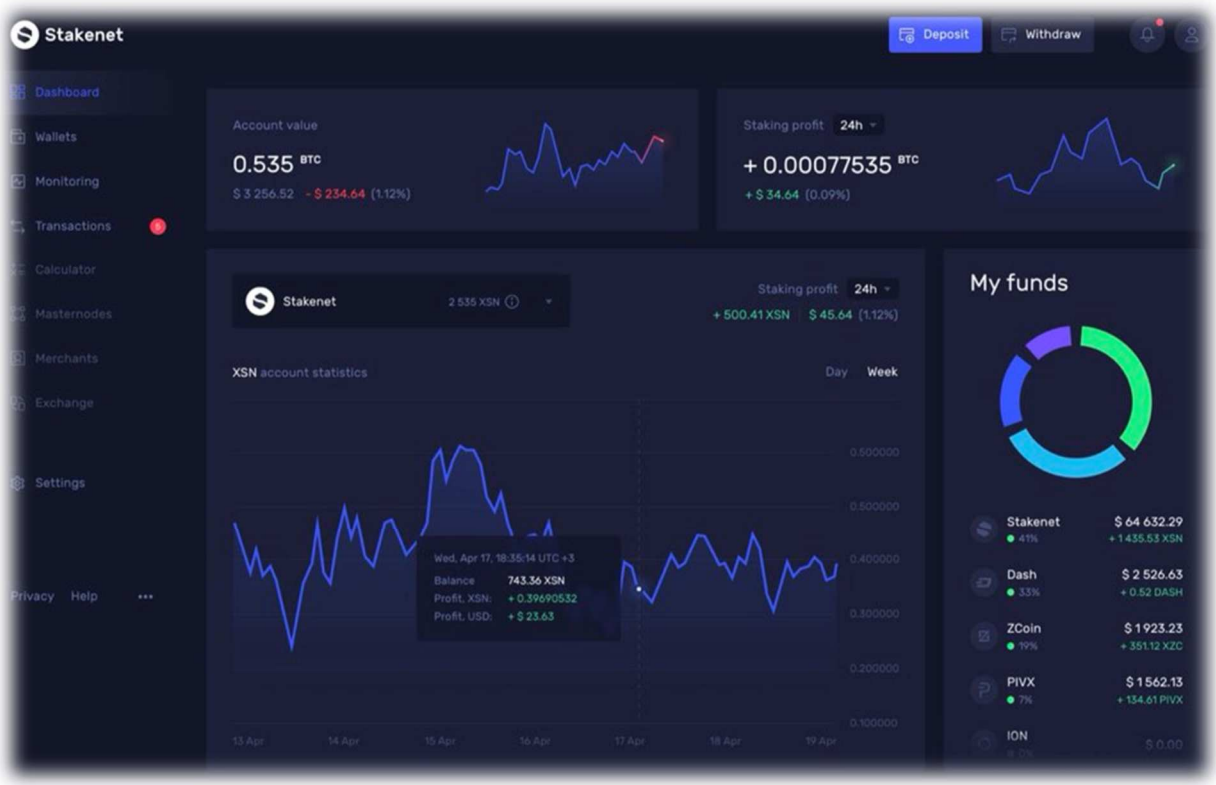
Delegating CCPOS responsibilities to masternodes would also provide an added income stream as new fees and rewards would exist associated with these cross-chain verifications. If a sister chain increases in popularity and demand, ROI on main chain masternodes would rise as proving your stake on chain #1 would be the only way to unlock given actions on chain #2 — & utilizing our masternodes would be the only way to accomplish this proof.

8.7 Maintaining agility

In a world of open source, it can be difficult to protect new innovations from being forked, spun, and implemented in new and sometimes better models. As we diverge from traditional ownership (patents, copyrights, …) we must learn to preserve value in this new environment. No better could this be done through engineering protocols themselves to respond to original decentralized master chains. The result would be not centralized control but a hierarchical control (HC) with masternode owners from an origin chain determining the direction, development, and purpose of the given inter chain cluster.
Platforms will soon rise eclipsing bitcoin, and ability for chains to adapt and evolve will be critical, as those that cannot will fade, be replaced and forgotten. We will see chains begin to combine into greater cohesive bodies where at its core lies a decentralized system growing proportionately with breakthroughs and advancements in the greater field of cryptocurrency. Rather than combat disruption we will position ourselves to adopt disruption — our community will secure future value and exposure to new trends simply by holding our asset, and our masternode owners will also benefit as their added service in verifying these cross-chain proof of stakes would increase fees, rewards, and overall ROI giving us definitive value moving forward.

9 XSN Businesses

Stakenet is building businesses that provides even greater value to XSN. Either by burning the profits of these businesses 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. The Stakenet team is building a platform in which users would be able to keep their holdings safe, stake their major PoS (proof of stake) coins, and trade coins via a decentralized exchange (DEX) all in one single place. For existing solutions to get staking rewards for your PoS coins, you need to run the wallet(s) and keep it online 24/7 continuously which most users find unpleasant. XSN solves this problem by providing a secure environment to store your coins and stake them at the same time, so you do not have to keep your computer running. The picture below is a preview of the user's graphical interface to access our businesses and manage his funds.



Businesses include the "XSN Cloud" or the "XSN Decentralized Exchange" powered by the Stakenet Masternodes whom will directly earn all the fees from it, effectively owning an exchange where you will trade your coins in a truly decentralized, secure and anonymous way. Also, the "XSN DApp framework" (Decentralized Application) that will enable third parties to develop powerful tools to provide their services in and for Stakenet, or the "XSN Hardware wallet", allowing you to store and operate with your coins safely within our very own hardware wallet. Because the Stakenet economy is powered by our native currency, XSN will be used to pay for all these services within our ecosystem.

9.2 XSN Coin

XSN is digital money that powers the Stakenet economy. It can be used to pay for all the services and products within our ecosystem. Created with the future in mind, it uses the most secure PoS blockchain with our Trustless Proof of Stake consensus and Lightning Network compatible, allowing instant and virtually fee less transactions with an output of billions to theoretically infinite transactions per seconds.

XSN has cross chain (between different blockchains) capabilities. So, it will be able to interact with any other coin. This opens a wide broad of opportunities. For example, our Cross Chain Proof of Stake (CCPoS) technology will allow you to stake XSN and earn the rewards in Bitcoin (BTC) trustlessly, with no intermediates or risks involved. Due to the Lightning Network, you will be able to seamlessly pay anyone in any currency just by having XSN, e.g. automatically pay invoices in BTC by using your XSN. Our objective is for XSN is to be the only coin you ever need to own and to be the most secure one by always being able to operate with it in a trustless environment. You can generate XSN by staking your coins, providing a merchantnode to enable trustless cold staking for others or by running a masternode. In summary, you earn XSN by securing or providing services to the Stakenet network.

9.3 XSN Cloud

This expansion is in anticipation of the launch of our official “Staking as a Service” platform stakenet.io, where you will be able to trustlessly stake XSN, regular stake major POS coins, host masternodes and execute atomic swaps via our coming Decentralized Exchange built with XSN Masternodes. The future will move towards platform centered, trustless utility and cross chain developments. Introducing “XSN Cloud”, the new generation of coin staking. As we believe Proof of Stake coins are the future, so we created a suite of staking tools you can capitalize on. Profits from 'XSN Cloud' will be burnt or sent to the treasury to further benefit XSN.

Multi currency wallet: Storing your coins in an online wallet and benefit from group staking. You will receive staking rewards, no matter how much coins you are staking.

Pooled staking: Your coins, stored the XSN Cloud, will automatically stake. Earn staking rewards every few minutes no matter how many coins you have.

Pooled masternodes: Share ownership and rewards of a masternode even if you don't have enough coins for it. Hereby we wipe out all barriers to enable you to earn profits.

Masternodes as a Service: We setup and maintain your masternodes. Notice, you are still always in control of your coins, while earning profits for providing network services.

TPoS marketplace: Find the best merchants to stake your coins trustlessly. Stakenet.io will monitor merchant contracts and let you rate them based on your experience.

Monitoring services: Monitor all your masternodes (even the ones you are not running with us) and your Trustless Proof of Stake contracts. To make sure your masternodes and TPoS contracts are working properly, you will be notified via email in case something goes wrong.

9.4 XSN Decentralized exchange

The power and implications of a decentralized exchange are often overlooked. The ability to morph assets instantly from one chain to another in a trustless manner gives massive power to the individuals of a given system as well as the system itself. Think of how difficult it is to convert assets in our current financial model, let alone done peer-to-peer - nearly impossible. To this point exchanges have been swapping assets tailored specifically for accredited institutions to oversee by central authorities — they have been financial vehicles and not much more. Due to utility traits of tokens and the fact that ownership is never conceded, the entire definition of an “exchange” changes. When a user executes an exchange for example, it will empower him instantly with all features and functions that come with the resulting swap. When sleeping, working, cooking, driving etc there will be certain chains that enhance different human experiences. A given individuals net worth will constantly be evolving form to accommodate its owner in the most efficient way possible. XSN sees the future of wealth in a new light - as alive, intimately involved enhancing our lives in real-time in a way that has never been realized yet. We understand there will be different utility needed in different situations and rather than compete with new tech, we will engineer ourselves to integrate new chains easily into our system.

Cryptocurrency exchanges are the backbone of the crypto currency market. They provide liquidity and the ability to trade your coins. The main problem with the current centralized exchange structure is, they are generally run from one central server in one location. Also, you are forced to provide personal information, that’s required for to set up an account. Coins that are sent to a centralized exchange are no longer your coins. You simply get a normal ticket to represent your deposit of coins or tokens. Owners do not benefit from any utilities or features of the coins. They even do not earn any staking rewards. Furthermore, security can be a big issue for centralized exchanges, because they can be hacked easier or shut down by the governance. All your coins hold on a centralized exchange can be lost at any time. These present unnecessary risks that Stakenet aims to solve with its own upcoming decentralized exchange, also known as a DEX. When using Stakenets DEX your coins never leave your position and you have unlimited access to them at any time. So, you benefit from all utilizes and features your coins and tokens offer you, including staking rewards. You remain anonymous , as you do not need to submit any personal informations to create an account.

The DEX cannot be shut down by any third party, even Stakenet cannot shut it down once it’s up and running. All trades are done on a peer to peer basis and require no centralized middle man so process the transactions. This means more security for all users and lower fees. You are maybe asking yourself: aren’t there lots of DEX’s out there? And you be right – there are some DEX’s – but all of them have one week point to centralization. They are run by several servers in several locations, but all these servers are still owned by one company. In contrast to all previous solutions, the Stakenet DEX will be the first in the worlds running entirely of masternodes and not just supported by masternodes. So, it won’t have any of those week points or limitations. While centralized exchanges have control over your coins, Stakenets DEX will empower users to trade simply and easy while maintaining absolute control over that coins, therefore using stakenets DEX is not only much safer, it’s also cheaper, faster and more reliable.

Furthermore, all current DEX's are just built from a technical point of view and not from a trading perspective. So silly things happen, like orders are violated and simple order types that exist in more established markets are not options, for example Stop-Limit orders. Stakenet is aware of the trader’s needs, so our DEX will offer you all state of the art order types and all needed tools for technical analysis.

9.5 XSN Decentralized application

DApp is an abbreviation for a Decentralized Application. The backend code of our DApps will be running on the Stakenet's decentralized peer to peer network. The DApps frontend code and users interface can be written in any language that can make calls to the backend. The Stakenet's DApp framework will enable 3rd parties to develop powerful tools to provide their service in and for Stakenet.

Imagen a world, where you get payed for providing content to the Stakenet ecosystem without anything left to do. Imagen a world, where people use your self-developed application based on the Stakenet blockchain and reward you with tips. Imagen a world, where no bank is needed to grow your money. That world is not far away.

Cryptocurrency and blockchain became more than just a store of value. A paradigm shift in the way we price software models has approached. First, Bitcoin made us trust in the value of an immutable and fungible encrypted piece of code. Now its time to sneak in the future: an interchain ecosystem supported by DApps. Although there is no consistent definition of a DApp, a DApp is essentially characterized these four properties:

- Decentralized. All records of the DApps operation should be stored encrypted on a blockchain, which avoids exclusive rights to be truly decentralized.
- Protocol. The community needs to agree on a hash algorithm and consensus to proof the store of value. For example, Bitcoin use Proof of Work and SHA256, while Stakenet uses Proof of Stake, Trustless Proof of Stake and the X11 algorithm.
- Open Source.: Ideally, a DApp should be managed autonomously. All changes must be made only by a consensus or majority. Therefore, it is necessary that the codebase is open source.
- Incentivized. Nobody works only for the idealism. That's why the validators, which protect the blockchain need to be rewarded block rewards, known as cryptographic coins or tokens.

The ever-increasing adaptation of the blockchain will make many previously known business areas and activities obsolete. Even if it looks strange, especially the financial services, like banks are threatening to be replaced by trust-less and decentralized networks in near future. The XSN DApps will play an important role in advancing this decoupling of the traditional banks and financial services.

9.6 XSN Hardware multicurrency wallet

The XSN hardware multicurrency wallet is a securely programmed device that stores your private keys of the cryptocurrencies you own. This private key is needed, to sign your transactions and as well as to recover your address, known as wallet.dat. By using a hardware wallet to execute transactions, your private keys are always isolated from your wallet, even if you are connected to the internet.

Advantages of hardware wallets in general:

- Private keys are never exposed to your computer.
- The hardware is immune to computer viruses.
- Your hardware requires you to confirm a transaction on your device
- Hardware wallets are encrypted with a pin, which adds another layer security.
- The software is open source which allows users to validate the entire operation of the device.
- Hardware wallets can store multiple cryptocurrencies.

Special features only provides by the Stakenet multi currency hardware wallet:

- Cold staking XSN and receive cross chain proof of stake rewards in any other currency you desire
- Cold storage exchanging from our hardware wallet to convert assets with complete security provided by a hardware wallet.

The use of a hardware wallet can be clarified once more by the following scenario: Let's say you inadvertently download malware onto your computer. Once you open your Stakenet desktop wallet, because you do not use our hardware wallet, your coins are at risk because your private keys are now exposed to the hacker. Here are three ways how the attacker might steal your XSN coins:

- If your wallet isn't encrypted, the hacker can set a remote command to send your XSN to a specific address of his choice, as soon as you open your desktop wallet.
- If your wallet isn't encrypted with a very strong password, the hacker can try to encode your encryption by brut forcing. This is just a matter of time for him.
- If your wallet is encrypted with a very strong password, he still can watch your screen to see if you accidentally reveal your private keys or your wallets password on the screen. Once he sees this, he can steal your XSN.

All these options will not be a threat for you, if you use the XSN multicurrency hardware wallet. Keep in mind, our hardware wallet will enable you to store more cryptocurrencies then just XSN. That way we provide you a solution to ensure the safety of all your funds.

XSN will be dedicating a hardware division to solve the problem and bridge the gap between the blockchain digital world and the real world. These devices will be more than just a wallet – they will be the user's medium to access the features of all supported blockchains.

9.7 XSN Future use cases

Future use cases and business cases for the Stakenet are theoretically unlimited. Below are two more examples of Stakenet service briefly addressed

9.7.1 XSN Rental market place

A rental marketplace integrated with the Internet of things(IoT) technology allows a peer to peer connectivity between landlords and tenants by enabling them to rent out or acquire houses or rooms at best possible rates without deduction of any service fee or hidden charges. Furthermore, it works as a medium of dispute resolutions by ensuring both parties agree and act to a certain set of defined rules.

9.7.2 XSN Service hiring

A job market built on XSN Network platform that allows customers to find quality services from across the globe. It uses AI and Smart contract technology to address dispute resolution and ensure the client is delivered what they have paid for.

10 Revolving stake bonus

As citizens of the globe, we are most likely familiar with a process called 'inflation'— a common effect of governments and their ability to print and increase the money supply. Although, its meaning may get distorted through its use in politics, it is simple to understand — every holder of the currency at the time of this money creation (by choice or not) is transferring value from their personal holdings at the time of this money creation (by choice or not) is transferring value from their personal holdings to the destination these newly created monies end up. It is a collective transfer of wealth and extremely efficient form of taxation.

The opposite of inflation (deflation) can be just as powerful, simply working in reverse. It provides an efficient method of transferring wealth from one singular point to all holders of the currency of that time, a form of "reverse taxation". Deflation is the method using which Stakenet rewards its coin holders, executing this via the RSB mechanism. RSB "Revolving Stake Bonus" will build and support an XSN businesses or network business whose proceeds are sent to their respective and assigned burner addresses. The scope of these operations will be limited to properly incentivize businesses to perform the 'proof of burn'. Unlike modern nation states, where governments are the sole executors of the national monetary policies, XSN's monetary policy is based on hard-coded rules and consensus via our masternodes—any decisions of how inflation is used is left to the ones with large stakes. No group of people, whether elected or otherwise can unleash a tragedy of the commons. The possibilities that arise from this proof of burn model are limitless, with the very highest ones being prioritized and pursued on a strategic partnership and adoption level in the early stages. This is made possible due to XSN's unique economic model via our RSB coupled with treasury and API integration, creating a powerful multi-layer of financial protection and growth for its holders. Over the next few years we will see boundaries pushed on the disruption these self-governing communities have not just on their respective organizations but greater society.

There, then, can be a suite of applications built on top of these addresses— analyzing in real time— the health and statistics of the ecosystem. Holders will track exactly how much value these bonuses provide directly from within our wallet and which organizations are providing them. There are many models and layers you can build on this framework, let's start with a popular one — financial services. All profits will be given back to XSN coin owners one way or another. Some options being explored are coin buy-back-burns and air drops to existing coin owners. Other options will be distributing the service- and transaction-fees to all involved parties. At least XSN will reward coin holders via an RSB mechanism, which is a proof of burn technology for service- and business-provider who use the XSN network. All profits will be given back to XSN coin owners one way or another. Some options being explored are coin buy-back-burns and air drops to existing coin owners. Other options will be distributing the service- and transaction-fees to all involved parties. At least XSN will reward coin holders via an RSB mechanism, which is a proof of burn technology for service- and business-provider who use the XSN network.

10.2 Hedge funds

It is important to understand the effects that blockchain will have on the world of traditional financial services - especially in hedge funds. We are living in one of the most disruptive eras of growth in human history, with massive amounts of wealth being generated in relatively short periods of time. A hedge fund model is perfectly positioned to capitalize on hyper-growth industries, as they have appropriate risk assessment and diversification models to benefit from these gains taking place.

Our treasury (~.001% of the total XSN market cap a month) controlled by our masternode holders could, in theory, behave as an individual client of a chosen hedge fund. Through our budget/ proposal system, fund managers would accept a principal from our masternode holders and provide a transparent portfolio with auditable gains and losses. Once their proposal is approved, we (the community) assign them a burner address, which they use to send their agreed upon proceeds. There would be little of an incentive for a fund manager to 'run away' with our budget since we work with reputable names as RSB provides transparency and trust. For the fund manager, this will result in larger budget approvals for that given individual or firm as time goes on. There will also be reinventions of these funds along with all other financial service models. One is that we could soon start to see 'anonymous' hedge funds, where the individual identities are concealed but their brands are reputable, verifiable, and public. Just like an immutable blockchain being released in the wild, we could see portfolios released getting popular whose origins are not traceable but results famous.

10.3 Stakenet ventures

A common problem arising amongst treasuries is the oversight. It is difficult to find a model (outside of delegating core team members themselves) that allows ongoing diligence after a budget is paid. This causes inefficiencies, delays, and losses for investors. This current structure is also limited to shorter terms (months vs. years) and is problematic for projects requiring long-term development and growth.

A VC firm is a bit more dynamic vs a hedge fund as it deals with long-term business development, equity distribution, and higher risk/ reward ratios. Focusing on development that services the Stakenet community, however, will strengthen our long-term position and growth coupled with more traditional treasury operations. Using equity distribution mechanisms on the blockchain, coupled with smart contracts, ownership can be distributed accordingly to end users via the RSB burn, passing the value to the average users.

10.4 Stakenet services

Staking services, pools, masternode hosting etc. will easily integrate with our RSB model and will be the first to arise. Our proof of concept will be our very own xsncoin.io, whereby integration of our API into the QT wallet, we will not only be able to provide information on the RSB address, but also statistics relating to servers, nodes, and other relevant operations to users and investors directly, in real time. Imagine having an interface where you can see data on each bonus address, showing you not only the health and statistics of the given business but also the rewards it is providing to the holders of the currency as well.

10.5 Incentivized prizes

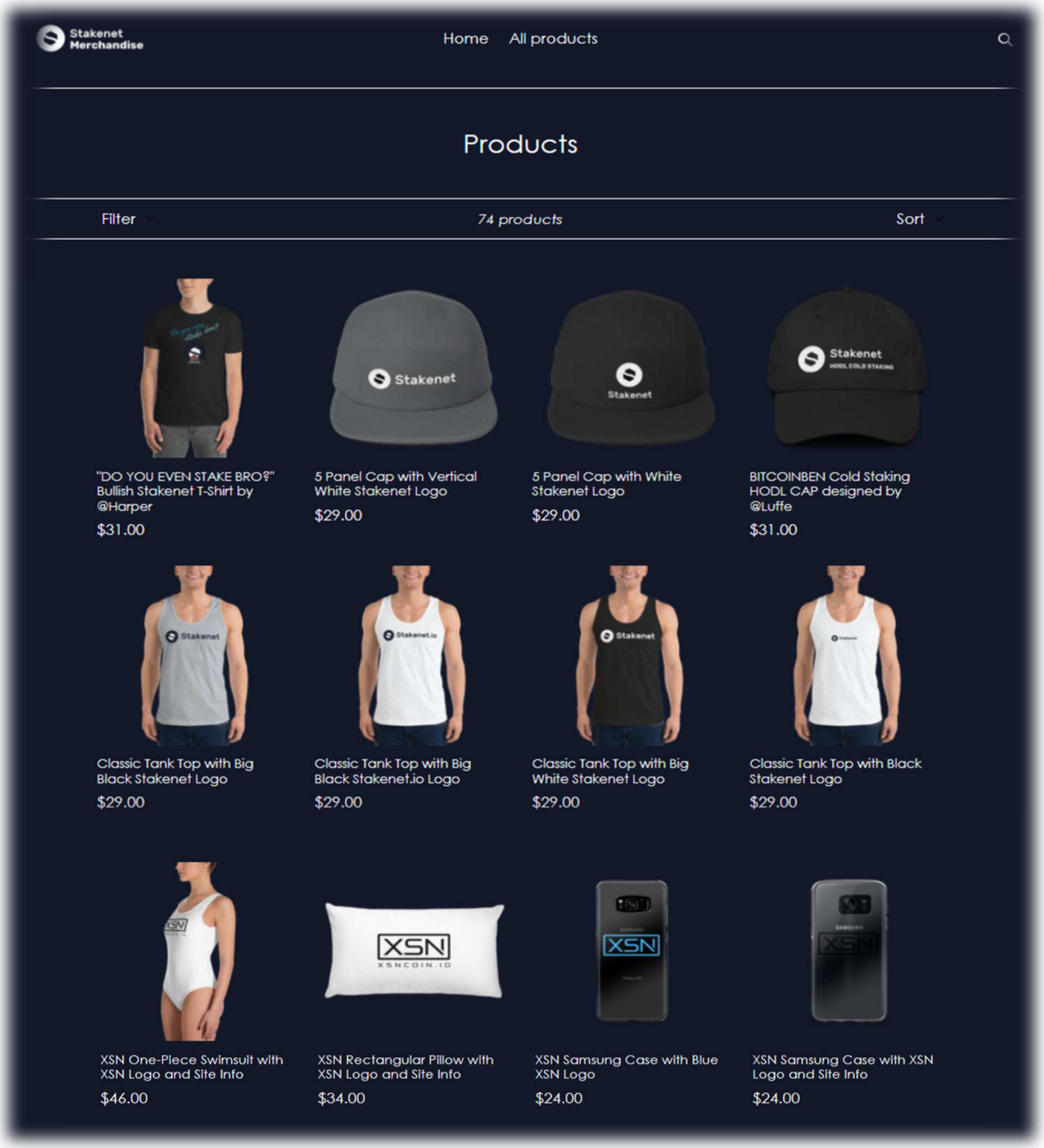
Why is the free market so efficient? It is because individuals are racing to get a prize - profits. They will put time, energy, and pain to get them. We can use this economic principle and put it on steroids offering 'X' amount from our treasury to whoever solves a given problem, adds a feature, or builds a service that helps our community. If the prize is big enough, there will be multiple teams competing against each other, building entire businesses just to obtain the prize alone. We could track the progress of everyone from within our RSB interface, giving real-time data and statistics as they race against each other to the finish.

11 Stakenet Community

As we know, how important a committed community is, we will introduce you right now community based services for the Stakenet ecosystem.

11.1 XSN Merch

XSNMERCH is an online store that offers various wearable accessories with various versions of the Stakenet logo printed on it, at extremely competitive prices. The mission with XSNMERCH is to offer our community a chance to wear what they love while spreading the word about Stakenet (XSN). Turnover from the merchandise store will help funding developments, exchange listings, and general partnerships. XSNMERCH is the go-to place for the absolute best Stakenet merchandise at unheard of, on-demand prices. Link: https://xsnmerch.io



11.2 StakeART

StakeART is a new series that aims to explore digital currencies by way of digital art work. The principle aim of StakeART is to complement our traditional articles by commissioning original, thought provoking digital art. In other words, we want to expand the engagement of XSN and digital currencies beyond the written word. Much of the work featured in this series will, naturally, call to mind Stakenet, and its native currency, XSN. One of the reasons why StakeART chose to focus on digital art work, that is inspired by digital currency, is because of the controversy inherent in both. Digital art is frequently snubbed by the traditional art world. When artists first started using computers instead of a palette and brushes, critics were less than impressed. Such elitism is unsurprising; Impressionist paintings were almost universally loathed before they were beloved. Thankfully, highbrow opinions of digital art are changing, albeit slowly. The rise of digital currencies is unfolding in a similar manner. First, digital currencies were considered to be worthless. Next, they were deemed to be the purview of criminals. Now, VC firms are falling over themselves to fund the next Oracle or Google.