Factsheet

Privacy and Security

Stakenet

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

Factsheet

1. Privacy and Security

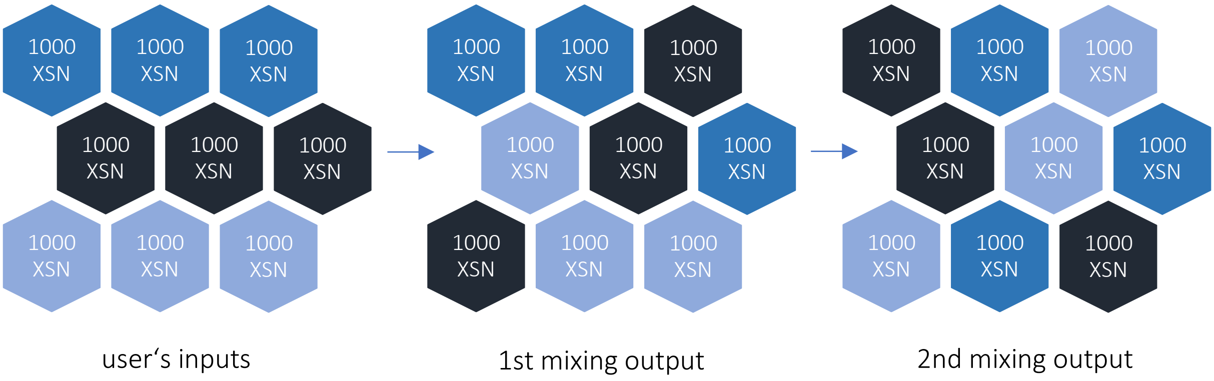
Privacy and security should be a fundamental feature of every blockchain, especially in times like this, when politicians begun to discuss about criminalizing those who "hide" cryptocurrencies. This can certainly evolve into broader criminalization of all holders at some point and time. What does this 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.

1.1 Privacy of Stakenet

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.

1.1.1 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.

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

1.1.2 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_λ (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.

1.1.3 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

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

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.

1.1.4 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.

1.1.5 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.

1.2 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.

1.2.1 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!

1.2.2 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.

1.2.2.1 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.

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

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?

1.2.2.2 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 you 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

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

- 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!

1.2.2.3 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.

1.2.2.4 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

1.2.3 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.