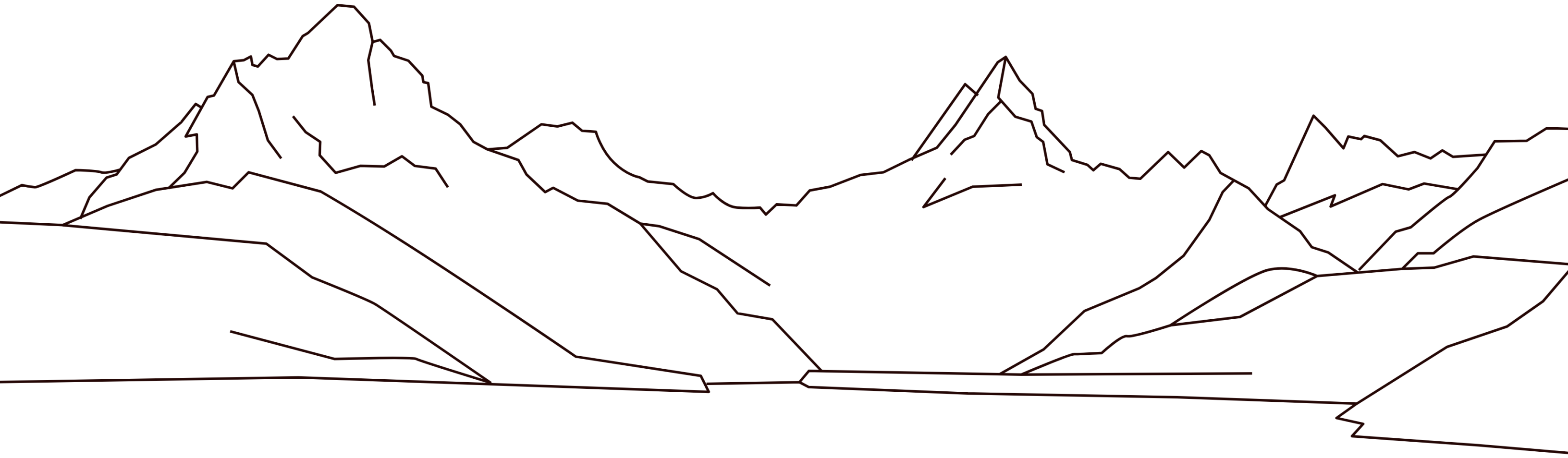
swisstronik

Whitepaper

Version 3.1.1



Notice

This paper and all documents related to this paper are a description of future developments within the Swisstronik ecosystem. The information in this document should be reviewed to familiarize yourself with the project and is subject to change in the future.

Contents

1. Preamble

Introduction

Over the past decade, blockchain as a complex of technical and financial tools has experienced its birth and rapid development. The size of the blockchain technology market reached USD 4.9 billion in 2021, and is expected to grow to nearly $70 billion by 2026 at a CAGR 68.4%. [1]

The global blockchain market started in 2008 when the Bitcoin whitepaper was published, and evolved to the first purchase of goods for a cryptocurrency made in 2010. Today, the blockchain market by component includes networks and services. There are 5 largest networks (ecosystems of blockchains): Ethereum, Polkadot, Solana, Cosmos, Bitcoin - of which Ethereum is the largest one with more than 50% TVL (total value locked) of the global blockchain market [2]. Primarily because Ethereum is not just a system for storing account balances: it was the first fundamental network to introduce tools for performing different functions in the blockchain environment - smart contracts.

Today, on its revolutionary development, the blockchain market is facing several key challenges that need to be addressed for the everyday life adoption of this technology. Which, in turn, is Swisstronik's end goal.

Blockchain interoperability is one of the key challenges impeding large-scale adoption.

Interoperability is the ability of different blockchain networks to exchange and leverage data and to move unique types of digital assets between one another. It contributes significantly to scalability and decentralization in the crypto space and allows users to seamlessly interact with apps on different chains.

This functionality is not exactly available at the moment, but a few projects are working on making it happen. Polkadot and Cosmos are the two best examples. Both ecosystems are attempting to build a meta-blockchain that hosts an open network of interoperable blockchains on top of it. But Cosmos grows faster, with 72% year-on-year growth in the number of developers against Polkadot's 47%[8]. It also allows better scalability and provides a consensus mechanism, network infrastructure, and application layers to form a blockchain. This is done by using SDK, where developers can start their own network that would run parallel to the main network. This makes the Cosmos network secure and solves the congestion problem.

On the other hand, the largest ecosystem in the blockchain market is still Ethereum, and most of the decentralized applications (dApps) are implemented on it. Hence other blockchains' compatibility with EVM (Ethereum Virtual Machine) is becoming crucially important for interoperability. Ensuring such compatibility expands the possibilities for emerging blockchains to attract developers to their ecosystem by reducing the time it takes to launch new Dapps. Some blockchain ecosystems with EVM compatibility are Avalanche, BSC, and Polygon.

But even though a few projects do provide solutions on interoperability and EVM compatibility, they do not address another challenge on the way to blockchain mass adoption.

Personal data protection and privacy issues hinder blockchain adoption in everyday life.

a) Anonymity vs Privacy:

Anonymity has always been the key philosophy of decentralized blockchain products. However, the issue is that while being anonymous, all operations (transactions) are still publicly available and traceable on the blockchain. The users' anonymity only remains intact unless someone knows their wallet number - but that would almost always be the case, eventually.

Moreover, even if blockchain networks provide some level of anonymity, what they certainly lack is privacy. Privacy means the right of the user to choose if any of his personal information is available to the general public or not. Recent research highlights that 86% of users care about data privacy and want more control over it, and 79% of users are willing to invest time or money to better protect their privacy [3]

b) Privacy vs Usability:

The rising demand for privacy has resulted in the emergence of projects aiming to prevent malicious data tracking: Monero, Dash, Aztec, etc. But their privacy enhancement procedures and user experience are too complex for an ordinary user to implement and require advanced knowledge in crypto/DeFi. That is one of the key reasons why the privacy tokens market size is just a small fraction of the cryptomarket at the moment, despite the demand. [4,5]

c) Compliance with the data protection regulations as a prerequisite for the everyday life usage:

While the user-friendliness must be a relatively easy thing to fix, there is one more challenge. Due to the non-transparency of such applications, the regulators often see them as a tool for illegal purposes, such as money laundering and financing unwanted organizations. [6] [7]

This wasn't an issue for the early stages of the blockchain market development though. Particularly because the use cases back then were rather narrow - such as trading, staking etc which didn't require a strong connection to «real life» where regulators would be able to interfere. But in order to fulfill the true potential of blockchain technology, it needs to extend to everyday life operations - including those run by corporations: supply-chain management, client data processing and so on. And for this, the blockchain world has to cope with the existing legal framework - particularly data protection regulations and KYC (Know Your Customer) procedures. Yet currently, there are no major public blockchains that would meet these standards, especially for enterprise usage. Same with KYC approaches: today KYCs are mostly done in a centralized way, which goes against the very philosophy of the blockchain field and compromises users' privacy.

Key takeaways

Eventually, the above challenges force potential users to make a hard choice: either sacrifice their data privacy or go into the gray area and lose the connection to the compliant "real-world" operations. In turn, this divides the blockchain world from the global banking system and everyday life operations, restricting both the blockchain market's growth and the overall progress of the economy.

But what if there was a solution that would allow regulators to ensure that operations in crypto are legal without taking away people's privacy? A solution that would solve the interoperability issue and be user-friendly while staying true to the original philosophy of decentralization? That is precisely what Swisstronik aims to bring to life.

2. Swisstronik concept

Concept

Swisstronik aims to foster real-life blockchain adoption by developing the network that addresses all of the above challenges - interoperability, data privacy, and legal compliance. Swisstronik will become the preferred solution for developers, individual users and enterprises. For anyone in the crypto community and beyond who cares about data protection and privacy while staying true to the spirit of decentralization.

Swisstronik network will leverage programmable and cryptographic privacy protection methods storing users' data private and ensuring interoperability with other blockchains. This approach, enables customizable, multi-level security for all sorts of blockchain applications, as well as fast and cheap transactions.

The Swisstronik platform will be developed on Cosmos SDK, benefiting from its interoperability and efficient transaction processing. It will also be EVM-compatible.

Privacy and data protection will be ensured by Swisstronik's unique combination of hardware and software encryption levels:

- programmable protection technology, based on Intel SGX
- cryptographic protection technology based on Zero-knowledge proofs (zk-SNARKs)

The Swisstronik network aims to provide numerous benefits for both end users and developers:

- For end users:
  - Data protection and enhanced privacy in compliance with regulations
  - Security: decentralization of blockchain-based services and service providers to reduce risks of intentional data loss or service stability breach
  - Low transaction fees
  - High transactions speed: transactions in native and Cosmos based tokens at least 10 times faster than in Ethereum
  - Convenience: users can utilize their favorite Cosmos and Ethereum dApps thanks to Cosmos SDK usage and EVM-compatibility of the network, as well as access Swisstronik native applications in one spot

  - Decentralized communication via serverless (servers in form of nodes will be used only for routing) messenger with calling features
  - Participation in the network governance via the on-chain governance mechanism.

- For developers
  - Easier and faster networks and dApps development: compatibility with EVM allows to use the same tools for testing and development as for Ethereum
  - Enhanced security: Random Number Generator secured by SGX
  - Business process automation via Smart contracts
  - Access to real world data through oracles

The Swisstronik network will also have the potential to be applied in a non-crypto environment for businesses, where data protection and privacy are of utmost importance.

Equally important is the compliance of the network's services with the existing and future requests of regulators worldwide - in an unprecedented mix with privacy enhancement techniques:

- Verification of network users, fight against money laundering and terrorist financing
- Verification of service providers on the network, fight against fraud
- Ensuring transparency of transactions on the network, fight against money laundering
- Automatic communications filtering - preventing the use of private communications for abusive materials distribution using on device automated tools

This will make the network reliable for the decentralized user applications that operate within the legal framework - and therefore ready for the imminent tightening of regulations around the blockchain applications and large-scale adoption. Just as Switzerland has traditionally been a mediator in international relations and a pioneer in international law, Swisstronik will be a pioneering network and a set of tools for bringing top-notch blockchain solutions to the legal field and everyday usage.

Swisstronik in a nutshell:

Main goal of Swisstronik is to foster real-world blockchain adoption by letting developers, individual users and enterprises be compliant with data protection regulations and only share the data they feel like sharing in blockchain applications.

To reach this goal, Swisstronik is creating a secure decentralized network for blockchain applications with enhanced multi-level data protection, where compliance will be ensured by a distributed network of independent data controllers and systems based on machine learning.

3. Blockchain

Overview

Swisstronik network is a layer one solution that is built using the Cosmos SDK and leverages Proof-of-stake (PoS) using Tendermint's Byzantine fault-tolerant consensus algorithms. Every node in the network performs computations for verifiability, security, and consensus purposes. As a layer one solution, Swisstronik is an independent chain interoperable with many networks thanks to the Cosmos Inter-Blockchain Communication Protocol (IBC).

For greater ease of use of the blockchain and the development of the ecosystem, the network will be EVM compatible. This will allow applications developed on Swisstronik to take advantages of both ecosystems - a well-developed ecosystem of applications on Ethereum (and utilize ERC-20 tokens or Ethereum compatible contracts, such as contracts for DEX-es and bridges) and a relatively new, but rapidly developing Cosmos ecosystem.

To achieve privacy, the Swisstronik network utilizes key management, cryptographic protocols, and a Trusted Execution Environment (TEE), which are the part of the hardware specification of all validating nodes on the network. TEEs guarantee that nodes cannot view computations taking place in a trusted environment, thereby protecting the confidentiality of the underlying data during computations.

Tendermint consensus

Tendermint can be described as a fractionally synchronous BFT (Byzantine Fault-Tolerance) consensus protocol based on DLS (Dwork, Lynch, and Stockmeyer) consensus algorithm (http://groups.csail.mit.edu/tds/papers/Lynch/jacm88.pdf). Tendermint is renowned for its fork-accountability, performance, and ease of use. A consistent set of validators, where each validator is identifiable by their public key, is required for the protocol to function. Validators goal is to reach consensus on one block (list of transactions) at a time. Rounds of voting are conducted to get an agreement on a block. A block proposal is made by the round-leader or proposer of each round. The proposed block is then put to a vote, and validators decide whether to accept it or advance to the next round. A round's proposer is picked deterministically from the validators' set following their voting power.

The security of Tendermint comes from its use of super-majority (greater than 2/3) voting and a locking mechanism to provide excellent Byzantine fault-tolerance. They together make sure that:

- To violate safety when more than two values are violated, more or equal to 1/3 of the voting power must be Byzantine.
- The protocol can be used to identify any group of validators who actually violate safety or even make an attempt to do so. Both voting for conflicting blocks and broadcasting invalid votes fall within this category.

Despite security complexity, the performance of Tendermint is extraordinary. Performance of well over a thousand transactions per second is maintained even in situations where validators crash or intentionally broadcast incorrect information.

Validators & Delegators

Overview

Nodes with non-negative voting power that secure the network by cryptographically signing blocks are called validators. Block proposals with BFT consensus are executed through a series of votes by validators using the broadcasted cryptographic signatures. Swisstronik's default number of validators is 70, and there is room for additional nodes to join the network if agreement on protocol parameter changes (during the governance process, which is described further). Validators in the Swisstronik network will be represented by nodes owned by independent entities. Validators earn rewards from transaction fees and block rewards. The more native tokens tied to any given validator, the greater the likelihood that said node will be selected for block proposal. If a validator commits malicious actions or does not validate a block on time, the network charges a fine from this validator in native tokens. Individuals may delegate native tokens to validators and earn rewards proportionally from the amount of delegated tokens for this kind of support - these individuals are called delegators.

Validators

Since Swisstronik is built on Tendermint, it secures the network with a set of validators. Validators are responsible for running a full-node and participating in consensus by broadcasting votes containing cryptographic signatures signed with their private keys. Validators commit new blocks in the blockchain and are compensated for their efforts. They must also vote on proposals in order to participate in governance. Validators are assigned a weight based on their total stake.

It is worth mentioning that Sigma Assets GmbH or its subsidiaries will never act as Validators in order to keep the network as independent as possible.

Staking

Since Swisstronik is a public Proof-Of-Stake (PoS) blockchain, weight of validators is determined by the number of staking tokens (SWTR) bonded as collateral. These SWTR can be staked directly by the validator or can be delegated to the validator by other SWTR holders.

By sending a "declare-candidacy" transaction, any user in the system can declare their intention to become a validator. They are then considered validator candidates. A candidate's weight (i.e. total stake) determines whether or not it is a validator, as well as how frequently he must propose a block and how big reward he will get. Only the top 70 validator candidates with the most weight will be validators initially. SWTR staked by validators (including SWTR delegated to them) can be destroyed or “slashed”, if they double sign, are frequently offline, or do not participate in governance.

Each validator's staking pool member earns rewards from:

- Block provisions: To produce block provisions, the native token is inflated. These provisions are in place to encourage SWTR holders to bond their stakes, as non-bonded SWTR will be diluted over time.
- Transaction fees: Swisstronik keeps a whitelist of tokens that can be used to pay fees.

The collected rewards pool is divided among validators' staking pools based on their weight. The revenue is then divided among delegators in proportion to each delegator's stake within each validator's staking pool. The validator applies a commission to delegated revenue before it is distributed.

Staking reward distribution

Block provisions are distributed to all validators in proportion to their total stake. This means that even if each validator gains SWTR with each provision, all validators retain equal weight.

Consider the following scenario as an example:

> We have ten validators with equal staking power and a 1% commission rate.
>
> Assume that a block has a provision of 1000 SWTR and that each validator has 20% self-bonded SWTR. These tokens are not given to the proposer directly. Instead, they are distributed evenly among validators. As a result, each validator's pool now has 100 SWTR.
>
> These 100 SWTR will be distributed based on the stake of each participant:
> Commission: 100*80%*1% = 0.8 SWTR

> Validator receives: 100*20% + Commission = 20.8 SWTR
> All delegators receive: 100*80% - Commission = 79.2 SWTR
>
> Then, in proportion to their stake in the validator's staking pool, each delegator can claim their share of the 79.2 SWTR. It should be noted that the validator's commission does not apply to block provisions.

Fees are distributed similarly, with the exception that the block proposer can receive a bonus on the fees of the block it proposes if it contains more than the strict minimum of required precommits.

When a validator is chosen to propose the next block, it must include at least two-thirds of the previous block's precommits in the form of validator signatures. However, there is a bonus for including more than two-thirds of the precommits. The bonus is linear, ranging from 1% if the proposer includes 2/3rds of the required precommits (minimum for the block to be valid) to 5% if the proposer includes 100% of the required precommits. Of course, the proposer must not wait too long, or else other validators will time out and move on to the next proposer. As a result, validators must strike a balance between waiting for the most signatures and risking missing out on proposing the next block. This mechanism aims to incentivize non-empty block proposals, improve networking among validators, and reduce censorship.

Let’s have a look at a specific example to demonstrate the aforementioned concept.

> In this example, each validator has an equal stake. Each charges a 1% commission and has 20% self-bonded SWTR. Now comes a successful block that earns 1025.51020408 SWTR in fees.
>
> To begin, a 2% tax is levied. The corresponding SWTR are allocated to the community pool. The funds in the community pool can be used to fund bounties and upgrades through governance (using social signaling mechanics).
> 2% * 1025.51020408 = 20.51020408 SWTR go to the community pool.
>
> 1005 SWTR are still available. Assume that the proposer's block contained 100% of the signatures. As a result, it receives the full 5% bonus.
> To find the reward R for each validator, we must solve the following simple equation:
> 9*R + R + R*0.05 = 1005 <=> R = 1005/10.05 = 100
>
> For the proposer validator:
> The pool obtains R + R*5%: 105 SWTR
> Commission: 105*80%*1% = 0.84 SWTR
> Validator's reward: 105 * 20% + Commission = 21.84 SWTR
> Delegators' rewards: 105 * 80% - Commission = 83.16 SWTR (Each delegator will be able to claim their proportionate share of these rewards.)
>
> For each non-proposer validator:
> The pool obtains R: 100 SWTR

Commission: 100*80%*1% = 0.8 SWTR
Validator's reward: 100 * 20% + Commission = 20.8 SWTR
Delegators' rewards: 100 * 80% - Commission = 79.2 SWTR (Each delegator will be able to claim their proportionate share of these rewards.)

Slashing

Slashing is an event that causes a loss of stake percentage based on the type of network violation and affects the safety of other participants. It is a measure to prevent the "nothing at stake" problem as well as a financial reason to act properly.

There are two types of events leading to stake liquidation:

- Downtime occurs when a validator is unavailable and does not sign more than 5% of the blocks in a row of 10,000. This situation results in a loss of 0.01% stake not only for the validator but also for the delegators who are bonded to him. Furthermore, this validator leaves the consensus and do not earn block rewards for at least 10 minutes. After resolving the issues, the validator can rejoin the set of validators by sending an un-jail transaction.
- A double-sign can have even more negative consequences than the previous one. It may result in double-spend or even chain fork. The most common causes of this type of slashing are incorrect validator's infrastructure setup or key compromise. In this case, stake is penalized by 5%, and the validator loses the ability to propose blocks and earn rewards while being imprisoned. This validator's delegators all enter the unbonding period, which lasts 21 days.

Delegators

Delegators are SWTR holders who are unable or unwilling to run validator operations on their own. Any user can delegate SWTR to a validator and receive a portion of its revenue in exchange by using the Swisstronik command line interface or any other user interface.

Delegators share responsibility and revenue with their validators because they share revenue. If a validator messes up, each of its delegators will have their stake slashed in proportion to their stake. This is why, before delegating, delegators should conduct due diligence on validators. Delegators are vital participants in the system because they are in charge of selecting validators. Being a delegator is more than just delegating: Delegators should constantly monitor their validators' actions and take part in governance.

EVM Compatibility

Swisstronik blockchain will be EVM compatible. That means that creating apps on Swisstronik does not differ from building on Ethereum, it will be as easy as copy pasting the code from one network to another. The difference and benefit would be faster execution time and privacy layer provided by SGX.

Developers will be able to:

- Deploy same source code for smart contracts that was used for Ethereum
- Reuse Ethereum compatible tools (i.e. Remix)
- Connect Ethereum compatible wallets (i.e. Metamask)

TEE

Trusted Execution Environment is a neutral party, represented as a hardware for secure and private computing. A TEE is hardware that resides in an isolated area on the device's main processor, separate from the main operating system. TEE ensures that data is stored, processed and protected in an immutable trusted environment. The remote attestation process allows new nodes registered on the Swisstronik protocol to verify the validity of their hardware and TEEs.

All smart contracts within the Swisstronik network operate within SGX, which ensures a high degree of security for user data and reduces the likelihood of system manipulation.

Intel's Software Guard Extensions (SGX) are a set of security-related opcodes built into special Intel CPUs that enable TEE. Swisstronik network currently is using Intel SGX as TEE, with plans to migrate to an improved version of SGX that has no known CVEs (Common Vulnerabilities and Exposures) - Intel TDX in the near future.

If desired, the network can use other TEEs with space for potential future implementations such as secure multi-party computation (MPC).

The consensus seed is stored in each validating node's TEE, allowing encrypted inputs to be decrypted and computed in a secure hardware environment.

Swisstronik token

Swisstronik token (SWTR) is a native token of Swisstronik. SWTR will be used for paying fees within the network and ensures the operation of the consensus mechanism. Since Swisstronik network uses a DPoS (delegated proof of stake) consensus algorithm, holders of SWTR have the opportunity to delegate their SWTR to one of the validators and receive part of the rewards of this validator. Any Swisstronik user who stakes SWTR can become a network validator (in a competitive system) and receive rewards for mining blocks, as well as receive a part of the network fees.

SWTR is also used as a governance token.

Overall SWTR supply is not limited, and is defined by the network.

Tokenomics

Due to Swisstronik being built with Cosmos SDK, Swisstronik's monetary policy is in most aspects common with the one of Cosmos'. The token is designed to balance security and liquidity by focusing directly on staking rates. When the amount of staked SWTR is changing, the protocol will adjust issuance to balance the changes. For example: less SWTR is staked, more SWTR is issued, until staking will increase to the point that protocol will reduce issuance to the desired ("stable") level. The same logic will be applied to the situation when the amount of staking is too high - the issuance rate will slow down.

Issued tokens will be:

- Distributed among active validators and delegators - as validation rewards, in order to secure the network operations
- Donated to Swisstronik Treasury - in order to stimulate the network's security and value. Treasury will be used only to cover the Swisstronik network expenses and fulfill its operations. Treasury fair usage will be secured by Swisstronik itself and an independent non-commercial entity, having the right and instruments to restrict over spending.

Distribution proportion will be defined by the governance mechanisms, however it is expected that security-related issuance will decrease over time in order to keep the economy of the system stable and self-sustaining.

Governance

Overview

Staying true to the spirit of decentralization, Swisstronik offers an on-chain governance mechanism to approve text proposals, modify consensus parameters, and decide on the usage of the community funds.

SWTR acts as a governance token. Validators backed by SWTR from other network users have the responsibility of participating in the network's ongoing governance.

Proposal types

Swisstronik supports three different categories of proposals:

- Parameter proposal - Change to a key on-chain parameter (i.e. rewards distribution proportion), is executed on chain.
- Community Pool proposal - A plan to use tokens from the community pool for a significant undertaking (i.e. new service/feature development). However, the decision to follow such proposals and to effectively execute the transactions lies at the sole discretion of the Swisstronik Network (social signalling). Community pool fair usage will

also be secured by an independent non-commercial entity, having the right and instruments to restrict over spending.
- Text proposal - Request for acceptance of a specific plan, strategy, commitment, upgrade, or other declaration. Text proposals do not really bring any changes, but they will serve as an important source of community ideas for future Swisstronik development.

Each proposal contains the following information:
- Author of the proposal
- Parameter change amount OR Amount of funding
- Deliverables and/or schedule
- Potential risks and benefits
- Short essay regarding the proposal setup, future impact if it is implemented etc

On-chain proposal mechanism

The Proposal process is divided into two periods:
- Locking Period
- Voting Period

Locking Period

The moment a user publishes his proposal indicates the start of the locking period for this proposal. This period lasts either 14 days or until the locked amount of funds under the offer reaches the value of the recommended locked amount (constant SWTR amount) indicated by the network rule.

A locked amount is an amount of funds that can burn out - but without it, the transition of the proposal to the voting stage is impossible. The locked amount can be submitted by any participant of the network.

If the proposal goes to the voting stage, the locked amount will be returned to the participants who submitted it at the end of the vote. The only case when the locked amount will be burned is when the proposal ended up being vetoed (in case more than 1/3 of participants voted as “NoWithVeto”).

Voting Period

This period lasts 2 days. During this period, the network participants can select a voting option from one of the following:
- Abstain - the voter is satisfied with any outcome of the vote
- Yes - the voter supports the proposal
- No - the voter does not support the proposal

- NoWithVeto - the voter considers the proposal being a spam or dangerous for the network

Voters can change their vote any time until the vote is still ongoing.

The proposal is accepted if all 3 parameters are in place:
- 33.4% of the network voting power participated in the vote
- More than 50% voted with “Yes” option
- Less than 33.4% voted with “NoWithVeto” option

At the end of the 14-day voting session, stake weight determines voting power, which is proportional to the total number of SWTR taking part in the vote. A governance proposal's vote power is only tallied for bonded SWTR. A vote or quorum will not include liquid SWTR.

Inactive validators may vote, but if they are not in the active validators set at the end of the voting session, their vote (and the support of their delegators) will not be counted. This means that user’s stake-weight won't count in the vote if he delegates to a validator who is now banned or has a poor stake-backing ranking.

Network fees

Network transaction fees are collected by the Swisstronik network and then split between the community pool, validators and delegators. The distribution proportion will be defined by governance mechanisms.

Any token type, or any combination of token types, can be accepted by Swisstronik validators as a form of payment for processing a transaction. As long as the block's gas limit is not exceeded, each validator is free to choose which transactions to accept and determines its own subjective exchange rate.

Every hour, the bonded stakeholders receive a percentage of the collected fees (minus taxes mentioned below) in accordance with their bonded SWTR.

A delegated validator also receives a commission from SWTR holders who assign their voting authority to other validators. Each validator may choose their own commission.

2% of the transaction costs will be allocated to the community pool. This tax is added to improve the Swisstronik network's security and value. The proposals made via the governance system can affect how these funds will be allocated.

4. Utilities kit

Overview

To support the development of the ecosystem within the framework of the goals defined in “Swisstronik concept”, Swisstronik network plans to provide a number of tools available to all developers of decentralized applications for both Swisstronik and other blockchains. The use of standardized core tools will allow greater synergy between applications and ease of development of new products.

As noted earlier, all commissions and payments made within the framework of the blockchain and utilities operating within it can be executed in any cryptocurrency.

Swisstronik Digital Identities

Introduction

Physical and digital documents are easily forged, and this is becoming a global issue. Fake diplomas alone are a multibillion-dollar business, and supply chain fraud is widespread. When unqualified people work in fields such as medicine or engineering, they can cause injuries, company liabilities, and even death. Data manipulation is easy with centralized databases and old vulnerable systems.

People do not fully own and control their identities when using centralized and federated digital identity systems (such as using a Google account to sign in), and their information is vulnerable to privacy breaches. People's data is frequently shared with third parties without their permission, and a user account can be terminated by the provider any time.

Swisstronik DI

Verifiable Credentials and decentralized identity technology can help to solve these issues. Swisstronik DI (SDI) enables organizations to quickly generate and validate fraud-proof Verifiable Credentials. Verifiable Credentials will be implemented using Reducible Signatures (https://eprint.iacr.org/2019/1201.pdf), which allow users to prove signatures correctness without disclosing all signed data.

Using decentralized identifiers, individuals can fully own and control their digital identities (DIDs). Individuals can use DIDs to securely manage and share their verified data while avoiding data tracking. Without the permission of the holder or issuer, no one can take away their DIDs or gain access to the content behind the DID.

Components of the SDI

- **Identity owners**

Entities with a DID (https://www.w3.org/TR/did-core/) on the chain.

The DID (Decentralized Identity) has a public key associated with it. This key can be used to authenticate the DID or verify assertions made by the DID, either on or off-chain.

- **Issuers**

Entities that use the Swisstronik DI module to issue credentials.

Credential issuers can be organizations, developers, businesses, or government entities. The issuers sign the DID Documents with their DID, which can be verified by any verifier to ensure the credential's authenticity.

- **DID Documents**

A DID is described by a unique set of data.

A passport, for example, contains information such as the date of birth, citizenship, visas, and so on. This document includes custom data, the controller's signature, and a verification mechanism. The default verification mechanism is a controller's digital signature, but issuers can choose other methods. W3C docs (https://www.w3.org/TR/did-core/#dfn-did-documents describe DID Document in greater detail. Following the creation of a DID Document, it is encrypted and stored in the DID Registry, with the full content accessible only to the issuer and holder. You can see an example of a minimal DID document below:

```
{
  "@context": [
    "https://www.w3.org/ns/did/v1",
  ],
  "id": "did:swtr:123",
  "authentication": [
    {
      "id": "did:swtr:123#z6MkecaLyHuYWkayBDLw5ihndj3T1m6zKTGqau3A51G7RBf3",
      "type": "ReductableVerificationKey",
      "controller": "did:swtr:123",
      "publicKeyMultibase": "zAKJP3f7BD6W4iWEQ9jwndVTCBq8ua2Utt8EEjJ6Vxsf"
    }
  ]
}
```

The document may also include fields that will limit the scope of its application. For example, in some countries, certain smart contracts or services may not be legal (e g fraudulent contracts, Ponzi schemes etc), so an Accredited Issuer (an entity that checks a document and issues a confirmation) can blacklist these contracts. Similarly, a document can be issued exclusively for a certain type of contracts or services, and its use will be possible only within a certain network address.

It is also important to note that the document can be made publicly available if the user so desires. This can be useful for verifying the identity of public figures (the verified name is visible to its subscribers), linking a mobile phone (to simplify the search for a user by his contacts when sending funds), and so on.

- Holders

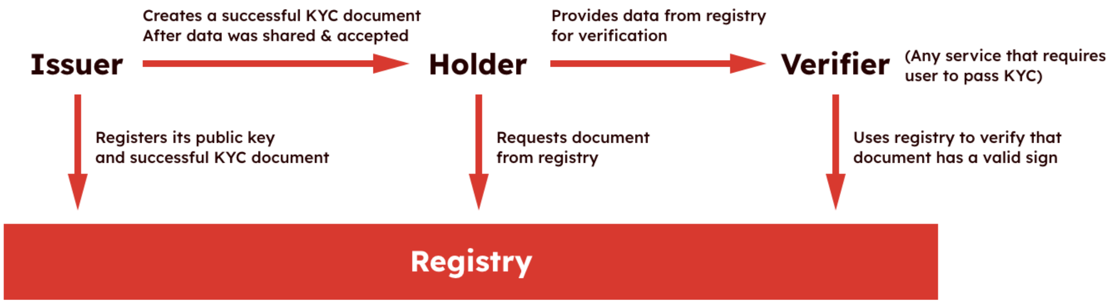
Entities that acquire credentials from issuers

Holders, like issuers, are exempt from having an on-chain identity if their public key is always available (or embedded in the credential). Holders can use the credentials they have received to create representations (links to DID with a proof of age, identity, ownership, etc.).

- Verifiers

Entities that verify the holder's received representations.

These are generally organizations that require the holder to verify certain conditions in order to engage, transact, or provide services to holders. The credentials used in the representation provide verifiability.


Creates a successful KYC document
After data was shared & accepted
Provides data from registry
for verification
Issuer
Holder
Verifier
(Any service that requires
user to pass KYC)
Registers its public key
and successful KYC document
Requests document
from registry
Uses registry to verify that
document has a valid sign
Registry

- **Revocation authorities**

Entities with the authority to revoke (or, in some cases, terminate the revocation of) issued credentials.

For a credential, the issuer can select one or more revocation authorities or choose to be the authority himself. Each credential specifies who has the authority to revoke it. The revocation authorities must have an on-chain identity, which is their DID, because the revocation registry is maintained on-chain. The revocation registry does not contain any personal information, but it is used by Verifiers to determine whether a credential has been revoked.

Use cases

There are many ways to use decentralized identifiers, for example:

- Creation of digital documents, certificates resistant to forgery
- Verification of age or identity for applications (for example, for Internet banking, games or services whose users must be over 18 years old, etc.)
- Confirmation of ownership of an object (for example, crypto assets)

Registry of Accredited Issuers

To ensure the operation of DID, the presence of Accredited Issuers (for KYC and KYB, for chain analysis etc) connected to the system is required. Moreover, it is extremely important that issuers have a legal basis (are reputable and authorized to carry this kind of operations) for carrying out these operations in the same region where the user of the system or service is located.

To connect to the system, the Accredited Issuer will be provided with an API and a web interface for working with incoming information.

For data analysis, the Accredited Issuer will receive a reward (amount of tokens) that suits him (reward will be defined by issuer). Since it is assumed that there will be more than one suitable Accredited Issuer, the user will be able to choose the Accredited Issuer that suits him by cost, which will keep the cost of data analysis at an adequate level.

At the initial stage of the system’s operation, the list of Accredited Issuers will be provided by the Swisstronik network & its partners (providing such services on a regular basis, not necessary for blockchain products), but in the future possibility to accredit issuers by voting on the main blockchain will be added.

In order for the registry of the Accredited Issuers to be legitimate within any jurisdiction, it has to be decentralized between Accredited Issuers who become responsible for compliance. This way, they jointly become the ones to regulate the verification system and determine whether and to what extent the user is granted access to the system.

However, ensuring such decentralization implies the possibility of adding new Accredited Issuers to the system and removing them from such a system - which can undoubtedly lead both to the oligarchization of this service (if entry barriers are too dependent on existing members) and to the gradual marginalization of new participants (if restrictions will be too easy to follow or existing members of the registry will not have enough tools to control actions of new and other existing members).

To begin with, it is necessary to define the main qualitative criteria for Accredited Issuers:

- Countries in which an Accredited Issuer is eligible to work and public proof of his legitimacy
- Document types that the Accredited Issuer is able and authorized to process

These criteria allow Swisstronik to determine the list of countries and cases in which a user can use the services of an Accredited Issuer.

And also it is important to define the criteria that allows to evaluate the Accredited Issuers' quality of work over time:

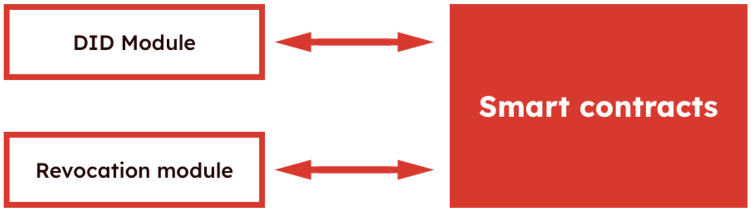
- The authenticity of verification of a special type of document (is it possible to get approval for fake or empty documents from the issuer)
- The speed of verification of a special type of documents
- The cost of verifying a special type of documents
- Number of fraud cases with users whose documents were verified by the given Accredited Issuer

These criteria allow the system to assign an Accredited Issuer rating in the processing of a particular type of document.

The formula that will determine the Accredited Issuer's access to the system and the scope of his rating, above which his access to the system will be limited, will be determined during meetings with representatives of the Accredited Issuer companies and will be unique for each of the countries and application cases. In some cases, such a formula will also require the participation of a local regulator. Once this formula is determined, it will be approved by a general vote on the blockchain (via text proposal) and approved for implementation as a decentralized Registry of Accredited Issuers.

Interaction with smart contracts

Swisstronik DI is made up of two modules: DID and revocation. The DID module stores all DIDs, public keys, service endpoints, and so on. Revocation registries and statuses are stored in the revocation module. Swisstronik implements a precompiled contract that allows smart-contracts and other applications to interact seamlessly with the DID and revocation modules. This precompiled contract allows smart-contracts and other applications to read and write data from the both modules.



Integration of third-party DID solutions

Swisstronik does not plan to be a solution that will only work within its ecosystem. Swisstronik will connect third-party DID solutions to SDI as well as port SDI to other DIDs. Each such integration will be made only after the implementation of the governance process on the network level (and the proposal should be accepted), as well as after the approval of this integration by voting among Accredited Issuers. Such an approach will, on the one hand, make Swisstronik and other DID solutions more versatile in use, on the other hand, it will allow Swisstronik to continue to provide the high level of regulatory compliance that the Network strives for.

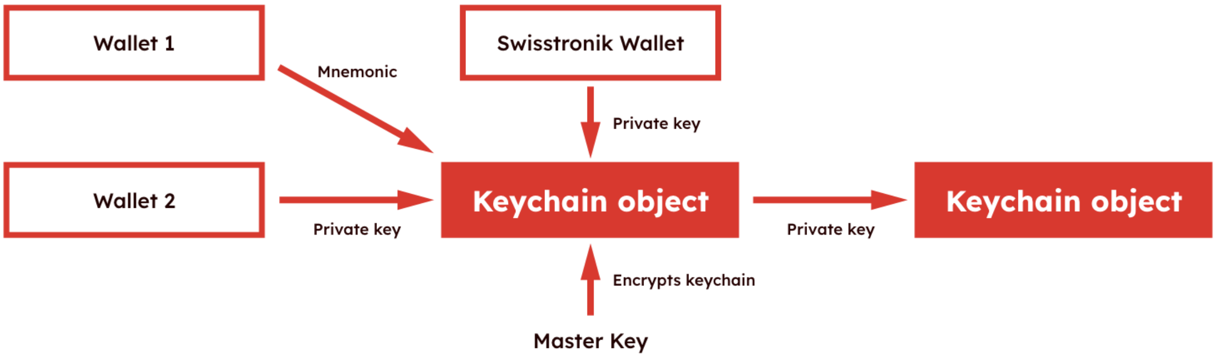
Regulatory compliance

To ensure compliance with country regulations, SDI will be adapted to local laws. In particular, users in Europe will be able to revoke their self-issued documents and initiate their deletion, as well as request a list of documents (that user previously sent to issuer) to view them (documents) using their private key. In countries where it is required to store user data locally (in the country of residence), Accredited Issuers are required to comply with these requirements. Country Compliance Principles are adopted by voting among the country's Accredited Issuers (via text proposals) and are publicly exposed as part of a user agreement when documents are reviewed. This approach allows the blockchain to keep data open and understandable for users, and ensures the high-quality implementation of local legislation through consensus regulation by qualified companies operating in the region.

SDI Keychain

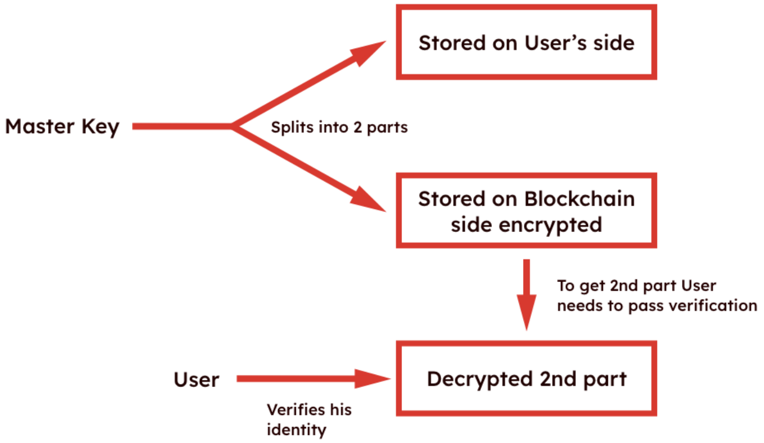
Using SDI, the user can link their third-party wallets to it - thus simplifying the management of funds. In essence, the service is a Single Sign On (SSO) solution. To do this, there is an SDI Keychain module within the SDI Utility. The module works like this:

The unique access tool (for example, private key) from the Swisstronik network or other desired private key (created when initializing the module) acts as a master key. All new wallets' private keys that the user adds to SDI Keychain are encrypted with the master key (which the user stores locally) and are added to the Swisstronik blockchain in encrypted form. For an additional layer of security, each of the wallets can be further encrypted with a word (password). When a user wants to log in on a new device, he drives in the master key from Swisstronik (and passwords if they were set up) and thus decrypts the keys from other wallets on the device, gaining access to them.



This can be useful for simplified storage of keys from multiple wallets - by connecting SDI to a non-custodial wallet (by entering a private key) the user also gets access to managing wallets on other networks. This mechanism preserves the security of user data, but at the same time allows to ensure the proper level of decentralization.

However, it should be noted that SDI Keychain module theoretically increases the risk of losing assets in case of loss of the master key - therefore, its use can be enhanced by methods such as additional identity verification, text password, biometrical verification (using decentralized methods) and so on.



SDI Simplified access

Losing the private key can be a significant problem, it is the only way to access the funds in the wallet. Although the private key is the most reliable means of protection, many services and users prefer more convenient access methods, such as a mobile phone or email verification. In general, this method is not secure, however, SDI users, if they consider it acceptable, can utilize such method.

This method can be created on the base of SDI Keychain - second part of the master key will be stored in custodial standalone service, or even the whole key can be stored in the standalone service. This method makes the use of the blockchain more casual, however, each user should take into account the risks of using this approach - centralized systems are convenient but vulnerable.

Swisstronik is not planning to develop such a service (Simplified access), the text above is supposed to serve as a referral note to developers.

Bridges & Cross-chain interoperability

Bridges are a way to transfer assets from one chain to another one. They connect two or more blockchains, and while being a neutral party allow the user of the bridge to safely exchange cryptocurrency on one blockchain for a specific amount of the same or the other cryptocurrency on the other.

In order to facilitate the usage of Swisstronik as an ecosystem of products and services, and to enhance the adoption of Swisstronik blockchain, Swisstronik will provide bridges to the most popular blockchains, like Ethereum, Bitcoin and Binance Smart Chain .

The users will be able to use existing ERC-20 tokens privately & securely on the Swisstronik blockchain, and to use their other assets for various applications.

Swisstronik also plans to simplify the usage of bridges for the developers, in order to enable the usage of different tokens & assets in their applications.

It's important to note that Cross-chain Bridges are different from Cosmos IBC (Inter Blockchain Operability) in a way that they allow exchanging assets from different chains, ones that are not necessarily part of the Cosmos ecosystem. Although Cross-chain Bridges present a different set of challenges, in comparison to Cosmos IBC, in terms of decentralization - they also present an open set of possibilities that allow a lot of use-cases for all members of the network.

It will be possible to harness the full power of Cosmos IBC together with the bridges, in order to use bridged assets on other Cosmos chains, and vice versa.

Bridges will also allow to swap different kinds of assets seamlessly and privately due to low commissions, fast transactions and the usage of TEE in the Swisstronik blockchain.

Decentralized Oracles Service

Oracles present a way for a blockchain or smart contract to interact with external data. They act like an API to the world outside of blockchain. There are many cases where outside data needs to be communicated to the closed blockchain system — particularly when smart contracts are connected to real-world events. Crypto oracles query, verify, and authenticate external data and then relay it to the closed system. That authenticated data would then be used to validate a smart contract. By leveraging many different data sources, and implementing an oracle system that isn't controlled by a single entity, decentralized oracle networks have the potential to provide an increased level of security and fairness to smart contracts.

Based on report (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7248830/), and having in mind that Swisstronik has TEE (SGX) integrated within the blockchain, decentralized and highly effective oracles system can be provided - DOS (Decentralized oracles service).

Main DOS traits:

- Data availability support is provided by a leader oracle server, which is chosen to facilitate cooperation among DOS's distributed oracle servers. Because of this, data availability is guaranteed even if one Oracle server fails.
- Oracle protocol with TLS and Intel SGX security: Through Intel SGX and Transport Layer Security (TLS) connectivity with external data sources, DOS ensures data integrity. Data tampering is not possible since DOS uses TLS connection to draw external data into each Oracle server's SGX enclave.
- Reputation system for oracles in DOS provides fast and stable response even if one of the oracles in the enclave is not behaving correctly.

ZK/ZKM tokens

Additional layer of privacy for token transfers will be guaranteed by usage of ZK (zero knowledge) proofs.

Overview

Zero-knowledge proofs, also referred to as ZK protocols, are verification methods that take place between a prover and a verifier. In a zero-knowledge proof system, the prover can prove to the verifier that they have the knowledge of a particular piece of information (such as the solution to a mathematical equation) without revealing the information itself. In the ZK token contract (described below), Swisstronik network utilizes zk-SNARKs as ZK proofs. The acronym zk-SNARK stands for "Zero-Knowledge Succinct Non-Interactive Argument of Knowledge," and refers to a proof construction where one can prove possession of certain information, e.g. a password, without revealing that information, and without any interaction between the prover and verifier.

ZK token contract

Using the mechanisms of the Swisstronik network, a user who has passed KYC with his DID can exchange cryptocurrency (funds that user is exchanging must be checked with chain analysis mechanism) for an equal amount of the ZK version of this cryptocurrency. The privacy of this cryptocurrency will be protected by both SGX and ZK proof mechanics. ZK versions of the cryptocurrency have high transaction speed and low commission rate. The issuance of these tokens is strictly limited with tokens bridged by users from other blockchains & networks. When ZK tokens are exchanged back for regular tokens, they (ZK tokens) are burned.

Diagram 1 shows the process of exchanging regular tokens to ZK tokens.

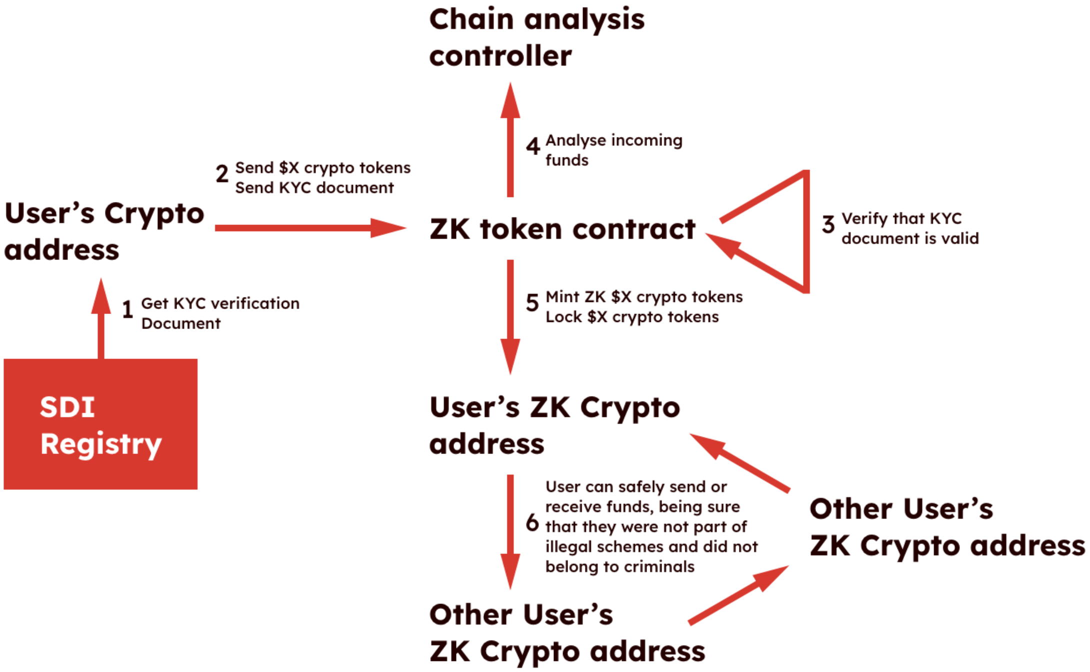

Chain analysis controller
4 Analyse incoming funds
2 Send $X crypto tokens Send KYC document
User's Crypto address
ZK token contract
3 Verify that KYC document is valid
1 Get KYC verification Document
5 Mint ZK $X crypto tokens Lock $X crypto tokens
SDI Registry
User's ZK Crypto address
Other User's ZK Crypto address
6 User can safely send or receive funds, being sure that they were not part of illegal schemes and did not belong to criminals
Other User's ZK Crypto address

Diagram 1

Here is the example of how this process works:

How to exchange USDT tokens to ZK USDT tokens

1. User passes KYC at the accredited controller with his SDI
2. User links USDT wallet to his SDI
3. User sends 500 USDT to the ZK tokens contract
4. User's 500 USDT are verified by the accredited controller (chain analysis)

5. User's 500 USDT are sent to the ZK contract fund. In exchange, 500 ZK USDT are minted and sent to his Swisstronik account linked to SDI

   ZK USDT tokens management

6. Being sure that the tokens did not participate in illegal schemes and did not belong to criminals, the user can safely send and receive ZK tokens, while keeping all the details of transactions private.

   How to exchange ZK USDT tokens back to USDT tokens

7. User sends 500 ZK USDT to the ZK tokens contract
8. User's 500 ZK USDT are burned, and 500 USDT from the ZK contract fund are sent to his USDT account.

Diagram 2 shows the process of exchanging ZK tokens to regular tokens.

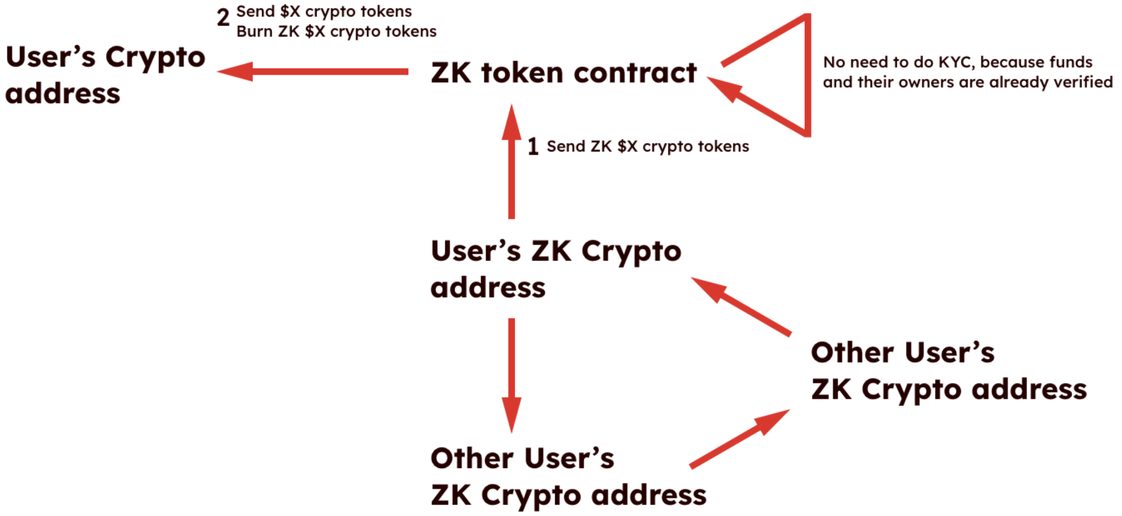

2 Send $X crypto tokens
Burn ZK $X crypto tokens
User's Crypto address
ZK token contract
No need to do KYC, because funds and their owners are already verified
1 Send ZK $X crypto tokens
User's ZK Crypto address
Other User's ZK Crypto address
Other User's ZK Crypto address

Diagram 2

ZK module will be launched only upon full decentralization of the SDI service. This approach will not allow users with criminally obtained funds, as well as users who want to exploit the service for malicious purposes, to interact with it.

Regulatory compliance

The ZK token tool should work differently in different regions. To comply with local crypto regulations, as well as adapt to future regulations that will appear in certain countries, user verification may not be enough - it may be necessary to disclose part of the transaction data. To do this, modified contracts for ZK tokens (ZKM) will be developed, in the process of exchanging funds there will also be an authority agent (AA) that will represent the regulator. Access to the use of AA will be obtained in each individual region by the local regulator based on the vote of Accredited Issuers operating in that particular region. This agent will also have a private key for decrypting transactions, however, access to decryption will be available only when signed jointly by the private keys of the authority and the Accredited Issuer that issued the SDI to the user whose transaction is being decrypted. Signing with two keys guarantees the ability to check suspicious users (for example, a user against whom legal proceedings are underway and the court requires the disclosure of his financial assets, a user included in the sanctions lists of individual countries, a user recognized as a terrorist, and so on), but will not allow to do this indefinitely for the purpose of illegal surveillance of users.

ZKM will be incompatible with standard ZK tokens, however, bridges will be created to enable interaction between them, the operation and launch of which, however, will be regulated by the Registry of Accredited Issuers and AA within individual regions. The bridge must first be approved by a Registry of Accredited Issuers and then by the AA.

ZKM pairs in different countries can be implemented in different ways and will be incompatible with each other, however, to enable interaction between them, bridges will be created, the operation and launch of which, however, will be regulated by Registry of Accredited Issuers and AA pairs of individual regions, between which compound. The bridge must first be approved by the registries of Accredited Issuers (in each of the countries), and then by the AA (in each of the countries).

Swisstronik wants to note that in many countries there are currently no significant restrictive regulations in the field of cryptocurrency control, and ZK tokens will work without AA. However, the potential chance of their appearance should be foreseen and for this there is a ZKM mechanism.

Decentralized communications app

Overview

DCA - Decentralized communications app is a serverless messenger with calling features. This is part of the Swisstronik network, which serves as an infrastructure for creating decentralized messengers and applications that require communication with the user (superapps, B2C services, chatbots etc).

Basic principles

DCA is a trustless end-to-end encrypted messaging application, where third parties cannot compel the network’s inventor to divulge information on users. The app routes communications through a random selection of Swisstronik network nodes.

Swisstronik DCA runs over a transport protocol that provides integrity, server authentication, confidentiality, and transport channel binding. To guarantee integrity, the messages are sequentially numbered and include the hash of the previous message, just like the good old Bitcoin blockchain works. If any message is added, removed or changed the recipient will be always alerted.

As the messenger can't access users data, it preserves the privacy of user profile, contacts and metadata and thus protects from advertising, price discrimination, and any kinds of prosecution due to innocent association.

Unlike usual P2P networks all messages in Swisstronik DCA are not sent via the servers, both providing better metadata privacy and reliable asynchronous message delivery, while avoiding most common problems of P2P networks. To prevent MITM attacks, DCA passes one time keys out-of-band when user shares an address as a link or a QR code.

Swisstronik DCA infrastructure has the following properties:

- Security against passive and active attacks - the parties have reliable end-to-end encryption and are able to detect the presence of an active attacker who modified, deleted or added messages.
- Privacy - DCA protects against traffic correlation attacks determining the contacts that the users communicate with.
- Reliability - the messages are delivered even if some participating network servers or receiving clients fail, with “at least once” delivery guarantee.
- Integrity - the messages sent in one direction are ordered in a way that sender and recipient agree on; the recipient can detect when a message was added, removed or changed.
- Asynchronous delivery - it is not required that both communicating parties (client devices, services or applications) are online for reliable message delivery.
- Low latency - the delay introduced by the Swisstronik network is not higher than 100ms-1s in addition to the underlying TCP network latency.

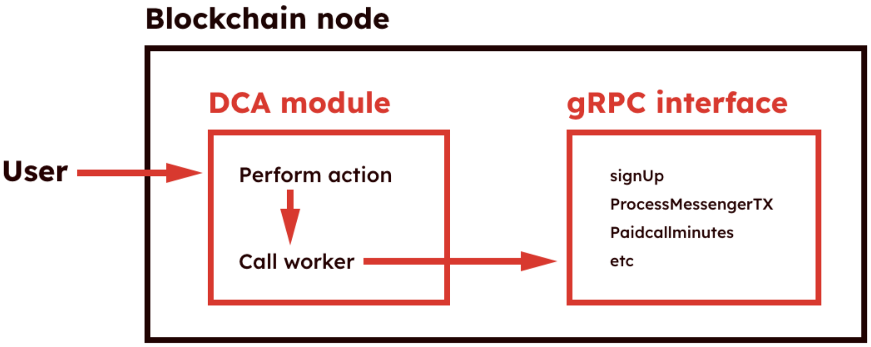
Messaging protocol

Messaging protocol of the app is based on SMP (Simplex messaging protocol, [https://github.com/simplex-chat/simplexmq/blob/stable/protocol/simplex-messaging.md], [https://github.com/simplex-chat/simplex-chat/blob/stable/docs/protocol/simplex-chat.md]), created to provide peer-to-peer communication with minimum amount of data processed on servers.

Features provided via DCA:

- Private chats
- Group Chats
- Images, videos and files sending
- Voice messages
- Stickers

- Audio calls
- Video calls



However there will be 3 major changes in the architecture of the app:

- User profiles have IDs, and they are connected to SDI. Thanks to SDI nature, user ID stays secure and private. Users have to pass KYC procedures.
- Routing servers are implemented as on chain nodes and their operation is funded by DCA user actions (via transaction fees).
- Crypto payments are integrated within the communication framework.

Regulatory compliance

In order to comply with the regulations of individual regions, the DCA application must be adapted to local legislation (It can be referred to ZK-ZKM; DCAM - DCA modified). For example, in the European Union, the GDPR should be observed - for this, a special decentralized protocol for deleting messages will be developed (the right to be forgotten). To ensure the protection of the service from content that can harm users' mental health, or content that is inappropriate within a particular region, a system will be implemented on the client side to detect such content and block its loading into the application. In order for system to be transparent though effective - it will be open sourced and its integration (within app) will be executed after the consensus of the community will be met (via governance mechanisms, specifically text proposal).

The user's access to a particular server will be strictly limited by the SDI permission received from the credential issuer. This condition will not allow the appearance and active use of servers that bypass the laws of individual countries and serve the criminal purposes of malicious users.

5. Use cases

Overview

As an example of the Swisstronik blockchain and utilities usage, Swisstronik will develop and distribute several applications. These services will form the backbone of the Swisstronik product ecosystem and can be used as a reference for developers.

Swisstronik app (B2C use cases)

Swisstronik app will be a nice example of the revealed potential of the network. The application is going to provide the most important services a user would need for full-fledged crypto management. The app UX will be designed convenient enough to be used by newbies in crypto.

The application will be developed for iOS, Android and Web (standalone app and web extension) networks. All services developed within this section are fully decentralized products and will utilize SDI for user login in order to simplify the transition between platforms and perform KYC/AML checks where needed.

Wallet software

- **Non custodial wallet - supporting all major currencies, including Ethereum, Cosmos, Polkadot, Bitcoin based blockchains**

Having user-friendly features, high security, and cross-platform support make the Swisstronik wallet an excellent wallet both for beginners and more advanced crypto users. Since the wallet supports proof-of-stake blockchains, it offers an easy way for users to stake crypto assets directly within the wallet.

An aesthetically pleasing software and the wallets’ simple layout enable users to easily access, manage, and hold a large number of the most common cryptocurrencies. The wallet is free and does not charge additional fees for sending or receiving crypto assets, except blockchain network fees.

- **ZK tokens module implementation**

This technology enables users to make their transactions completely private adding a powerful extra layer of enhanced privacy to their on-chain activities. Thus users transactions, trading behavior, balances, and other sensitive information remains hidden from any third party.

ZK tokens rely on advanced cryptographic primitives that guarantee that the transmission of data is safe, secure and fully private. Thanks to this additional privacy layer and the versatile zero-knowledge proof system, ZK tokens enable totally private transactions, a key ingredient for the digital identity and self-sovereign identity use cases.

ZK tokens service will only be accessible for the users in specific regions with their KYC documents verified on their SDI.

- **DEX for crypto fiat exchange (connected providers and local exchange offers)**

This DEX will allow users to make on- and off-ramp payments and help economic value to securely flow from fiat money into crypto assets and vice versa. The DEX will make it much easier for users to enter into the decentralized, blockchain ecosystem and take advantage of this trustless area.

The main advantage of the Swisstronik DEX is that newly purchased coins and tokens will go directly to user's non custodial wallet, meaning user will have full control over crypto from the moment he bought it.

The software will be providing both online and offline exchange. In both cases, Swisstronik network will not be part of the deal and won't collect any commissions.

The online exchange will take place through third-party services connected to the platform, their operation in a particular region will depend on local regulations.

The software for offline exchange is a list implemented as a stream of messages in a special format with exchange offers. Users will be sending messages to this thread using the DCA mechanism, further communication with the counterparty takes place within the framework of this interface.

- **Lending DEX**

The Swisstronik DEX utilizes the best practices and inherits all the mechanics that DeFi market leaders have, including AMM trading liquidity pools and the possibility for users to easily lend and borrow cryptocurrency assets against collateral, creating their own high-yield passive income strategies.

The lenders on the Swisstronik DEX can benefit by earning interest, while the borrowers benefit by accessing a crypto asset instantly without going through any traditional financing sources. The main advantages of the Swisstronik lending DEX are:

Accessibility - borrowing a crypto loan is much easier than borrowing from traditional banks.

Speed - under normal circumstances, user can get a crypto loan with just a couple of clicks.

Flexibility - users can set their APR according to their desired value. The Swisstronik lending DEX will allow the borrowers to adjust APR based on the term of the loan, loan-to-value ratio, type of cryptocurrency and the amount of collateral.

To achieve a low risk of loans non-repayment, it is possible to launch an analogue of the Registry of Accredited Issuers, but for insurance companies or banking organizations. The operation of such a service will be built on the principles of decentralization, and through smart contracts it will allow to insure deposits by depositing funds for their issuance (sharing risks and profits between the borrower and the insurer on conditions that will suit both parties).

- Bank card issuance

This will allow users to easily and conveniently make purchases and pay for goods and services anywhere using their crypto. 24/7 access to digital assets, ubiquitous payments with cryptocurrencies, discounts, cashback, loyalty programs and withdrawals from any ATM in the world will be available to every Swisstronik bank card user.

Decentralized operation of this service may not be possible and may require the Swisstronik network to obtain a specialized license. The timing and availability of obtaining this license may affect the launch and operation of the service in specific regions.

DCA Messenger

The messenger will be built using DCA, routing users communications through a random selection of the Swisstronik network nodes. This system provides full privacy, reliability, integrity, low latency, and increased level of security against all kinds of attacks.

Governance portal

This is a service that will be one of the ways to interact with the network Governance portal, here users will be able to make their own proposals for the development of the network, as well as vote for others. This system will make it easier for users to explore new projects that are planned to be launched within the network, which will help determine which of them are the most promising, and help guide the Swisstronik network development. The projects and dApps that get the most votes from the community members are then funded from a community pool and integrated within the Swisstronik app.

Projects that are developed within the framework of these initiatives do not involve direct investment from network participants and do not lead to the payment of dividends. Voting is required to develop the network in a direction that is useful for users.

Swisstronik suite (B2B use cases)

Swisstronik plans to customize its services for the needs of crypto and non-crypto businesses, in particular such as:

- Distributed authorization system

The DID module allows companies to implement a decentralized authorization system, in which the user will be able to determine to whom and to what extent their data for authorization should be supplied.

It is also possible to create sovereign DIDs, where the user is both the issuer and holder of his DID, which allows the user to have full control over their data, as well as accounts - which will allow companies to use a tamper-proof / data loss-proof authorization system, since the data is completely controlled by the user and is stored in a distributed network.

- Secure corporate communications system

On premise messaging app built using DCA. Integration with corporate internal systems or additional features development (in order to suit specific needs of the company) may be applied.

- Secure computation execution platform

The solution is the use of Intel SGX combined with the modular Cosmos architecture for simultaneously distributed and secure computing. Swisstronik network supplies a module template that can be modified to perform any calculation.

After the required modifications to the template, the company deploys a Swisstronik subnet, which, through the use of native IBC from Cosmos SDK, will be compatible with the main network, but the processed data will not leave the subnet.

This solution is suitable for scientific computing, training ML models on private data, and other areas that require large computing power combined with data protection.

- Suite for a company’s assets tokenization

The system allows for the tokenization of the company's assets by issuing derivatives in the form of ZK tokens, provided that these tokens are linked to obligations (property or legal) under the guarantee of Verifiers from SDI.

Thereby the Swisstronik ecosystem creates additional value and business scaling sources by adding new technological use cases that connect digital and real-world assets through tokenization.

Users and businesses gain new opportunities for asset diversification, the new source of liquidity, and complete security and privacy of all financial transactions due to the use of blockchain and ZK technology.

Contacts

Legal inquiries

Chief Executive Officer:
Guggi Constantin
constantin@swisstronik.com

Product information

Chief Product Officer:
Brizhatiuk Valerii
valeryb@swisstronik.com