LIGHTPAPER

TENZORUM

The unstoppable machine for self-sovereign key management and access to the decentralized world.

PROPOSAL 1.0 - 23/04/2018

TABLE OF CONTENTS

DISCLAIMER

This Lightpaper is a dynamic proposal. **It can and will be changed** as the project matures and research is developed towards achieving the full vision for Tenzorum Project.

This document is not to be counted as a sales prospectus or solicitation of any digital asset distribution. It is a suggestive description of Tenzorum Project and the associated technological aspects related to key management in decentralized networks.

For any future involvement with the project participants should take into account that the decentralized technologies industry is in its infancy. The pioneering stage of development means that there are significant risks in interacting with cryptographic assets as described in the Lightpaper.

Specific details about the terms and conditions as well as the various ways to get involved in Tenzorum Project will be published on our websites and communication channels at a later stage.

KEYS & EXPERIENCES

When discussing the user experiences and consumer adoption of decentralized technologies, one fundamental interaction all Blockchain technologies have in common, is the individuals use of keys. Relatable examples that demonstrate this range from the simple use case where people transact cryptographic tokens (e.g. bitcoin, ETH, ZCash) to more advanced use case interactions with DApps, or personal address space that provides people with decentralized personal computing resources such as Urbit (Urbit.org). Historically, key management systems are used in various enterprise use cases. However, individual consumers do not have many options unless they have high technology literacy which has its own challenges.

The lack of user oriented key-management protocols and inadequate frameworks to interface with the various Blockchain networks, resulted in obscene cryptocurrency losses throughout the year of 2017. Over $225 million were stolen through phishing scams, over $100 million were frozen due to human-errors transacting to the wrong addresses, and more than $1 billion dollars were lost due to hacks. If this issue is not addressed and further security measures and mechanisms are not further developed for the average user, more catastrophic incidents are bound to occur as the networks grow. This increased amount of fear, uncertainty and doubt among all stakeholders in the Blockchain space could potentially jeopardize the future of public Blockchains.

There is a clear problem in the current management model that users and service providers use to control, store and manage their seeds, private keys and other modes of access and credentials to interface with the distributed Ledger. While scalability is understood as the current major issue to be solved in the public Blockchain space. It is evident that the designed user-experience and users interface to private keys, login portals, digital and hardware wallets, funds and keys storage, are the major factors that are hindering the mass adoption of Blockchain decentralized technology and hence the major inhibitor for real decentralization to take place.

Tenzorum Project is committed to the self sovereignty of key management systems. To achieve this, protocols need to be developed, integrated and be bridged through APIs to general third party decentralized products. The reason self sovereign key management systems are so important is that end user ownership and control of keys is at the heart and the basis for truly decentralized technology interfaces and user experience, without making compromises to the original cypherpunk values of creating trustless models.

BACKGROUND

How people are managing keys today?

WEB3.0 **HARDWARE WALLETS**

+Robust Solution.
+No internet connection
+High security user-cases.

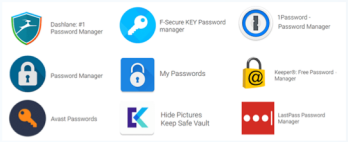
-Paper wallet dependent.
-Huge Technological Friction.
-Inconvenient
-Only suitable for long term storage.

WEB2.0 **APPLICATION ACCESS**

+Social Recovery
+Holistic Solution

-Surveillance tool
-No privacy

WEB2.0 **PASSWORD MANAGERS**



+Optimized User Experience
+User Friendly Mechanisms

-Centralized.
-Counter-party risk.
-Leaks and Hacks several times.
-Stoppable.

WEB3.0 **PAPER WALLET**

+Not Hackable

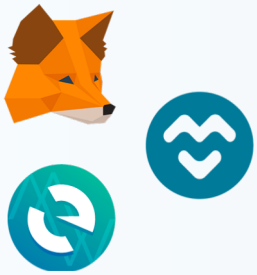
-We can do better
than paper.

Hybrid **Keys Manager**

+End-to-end encrypted
+Holistic Solution

-No incentive model.
-No access focused.
-Only suitable for verification.

WEB3.0 **ACCESS**



+It's the only
thing that works

-Paper Wallet dependent
-Fragmented Solutions
-Not consumer oriented
-Only Ethereum
-Only web3 compatible pages

THE PAIN

"To deal with cryptographic assets in todays crypto-landscape, you basically have to become completely paranoid about your private-keys. That's fundamentally a bad standard."

Gaining access to decentralized technologies require handling of keys, currently the options available to consumers are limited, unpleasant and the landscape is therefore very fragmented and inefficient. This means that Blockchain technologies is not accessible for mainstream consumers on large scale and that there are major risks associated to managing keys.

On the Blockchain, everything is about your keys.

Keys give you:

- ACCESS
- IDENTITY
- RIGHTS
- BENEFITS
- COINS
- OWNERSHIP
- MORE COINS

IF YOU LOSE OR FORGET ANY OF YOUR 64 RANDOM CHARACTERS KEY YOUR MONEY IS GONE FOREVER.

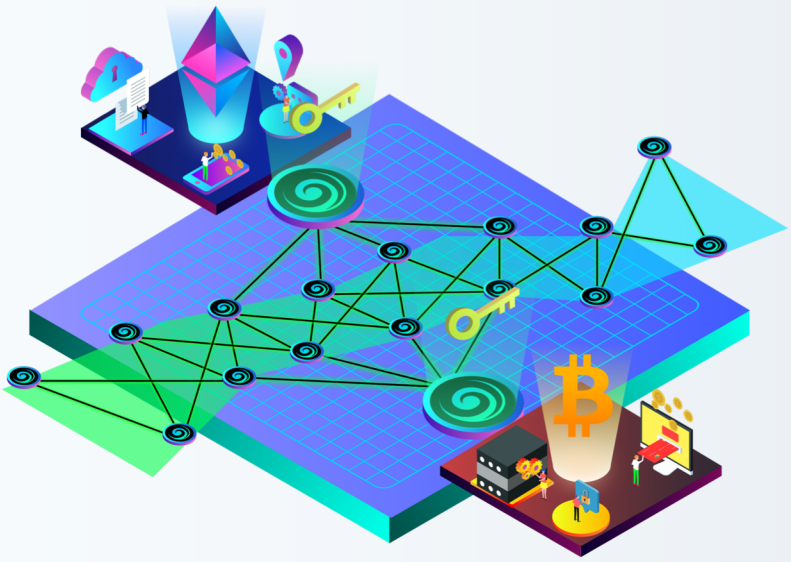
- **Risks too high for average users.**
- **Immense technological barrier.**
- **Integration is virtually inexistent.**
- **Solutions are fragmented.**
- **UX has been neglected**

The user-experiences around key management are today the biggest problem with Blockchain technologies.

"The delight factor of any winner solution, comes down to the experiences that users have with your products"

TENZORUM PROJECT

Tenzorum is set to become a general purpose decentralized key management system that serves as the backbone to support and connect users between decentralized networks.



Tenzorum protocols are being created from the ground up, to abstract and simplify the way people manage their keys and accounts on decentralized applications. It provides the infrastructure to allow every user to interact with decentralized applications across multiple chains.

To take the next step and establish the necessary elements required for the decentralized public networks to be accessible for an extensive user base, we need to address specific fundamental elements: key ownership and access control must always be achieved through a self-sovereign manner.

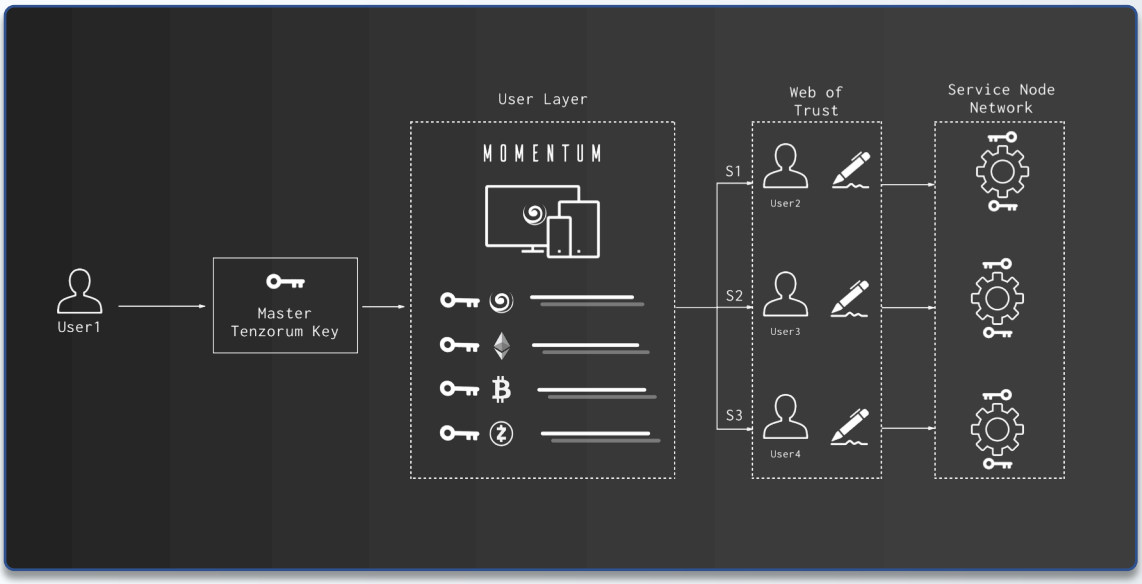
Tasks to be achieved in a self-sovereign manner:

Login Abstraction	Access Control	Recovery Mechanism

ARCHITECTURE

The protocol layer will interface with existing decentralized networks such as Ethereum, Urbit, Nebulas, Bitcoin, etc.

The Project is addressing the fundamental key management experiences elements by bringing together protocols such as secured login, recovery mechanism and access control that allows users to take control of the way they interact with decentralized technologies.



Web of Trust

The new privacy and personal data mishandling by centralized social networks have exposed the importance of having self-sovereignty over our data. Although the concept of Web of Trust was pioneered a long time ago, is yet to be successful in reaching mass consumer adoption.

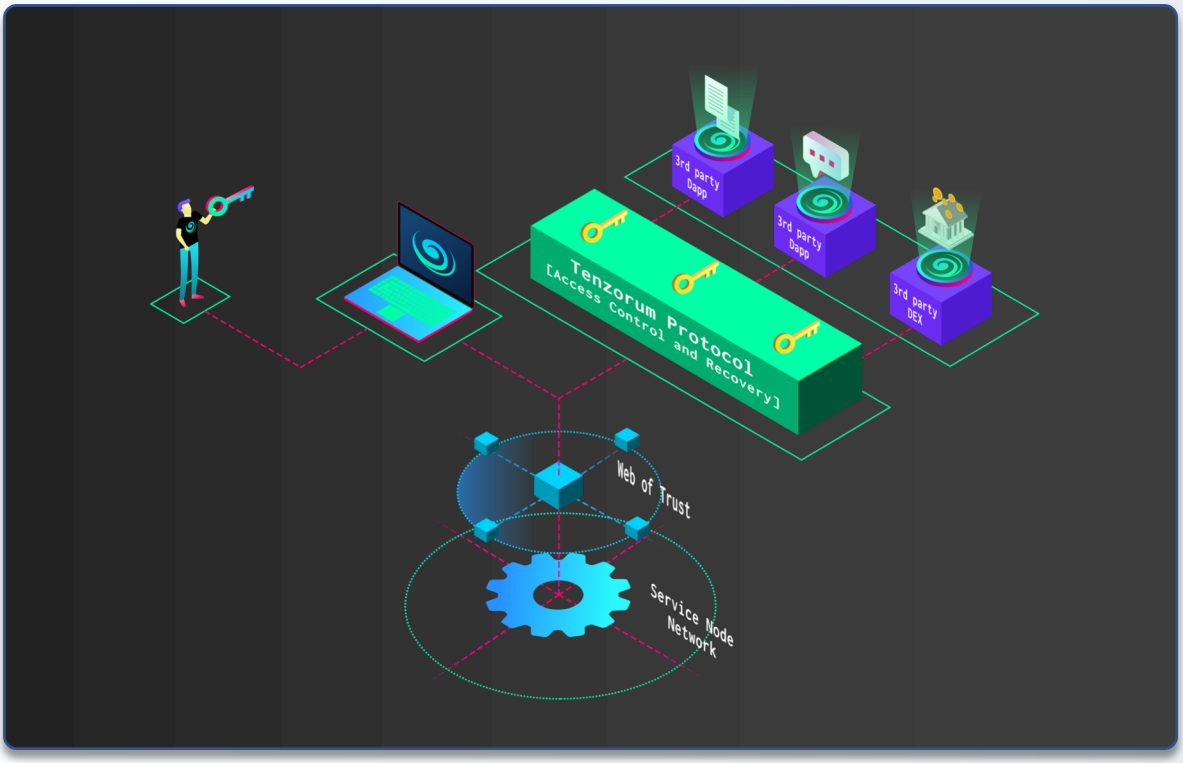
Tenzorum Project is powered by a web of trust as a social network and proposes to use crypto economic incentive mechanisms to harness this dominant protocol. Users can verify and vouch for each other to activate access to secured storage, edit and recovery functions and rely on their web of trust peers to serve as their key guardians in case vouching is required.

Tenzorum Service Node Network [TSNN]

TSNN is proposed as an unstoppable public utility that can run independently of any central service provider and provide the essential business logic associated with key management protocols. TSNN will run the protocols to enable general purpose key management services for various decentralized technologies and by that serve as a utility network that connects between different decentralized networks.

Some of TSNN functionality will be:

- Handling encryption tasks such as key fragments packets.
- Securing access to data through ownership verification of Web of Trust.
- Distributing rewards for successful keys ownership calls through consensus mechanism.
- Assuring integrity and disincentivizing improper behaviour.



Token Reward Mechanism

Service nodes stake collateral tokens through an escrow smart contract. The stake nodes hold reflects the maximal proportional amount key management associated tasks they will be allocated through Tenzorum protocol. Rewards are distributed from prepayments made by consumers who lock funds to an escrow smart contract system. Another source of income for service nodes is through rewards issued as newly minted tokens at a rate that compensates for contribution and ‘uptime’. Uptime should be regularly measured.

A penalty policy slashes out service nodes escrowed stakes and burns those tokens if service nodes prove to provide inadequate key management tasks work.

To compare the quality of output tasks rewards would only be issued after reaching a given task has been performed and produced the same result on several service nodes on the network.

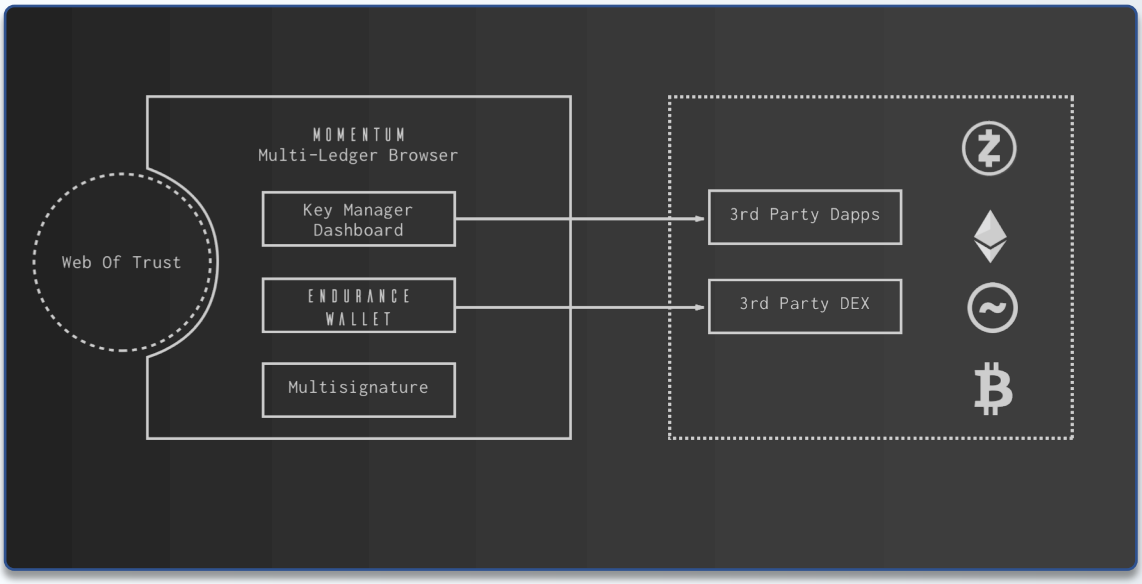
Social Reward Mechanism

The Tenzorum recovery mechanism is fundamentally attached to the responsiveness of the user’s web of trust, meaning that for a user looking to verify keys, it’s crucial that other users from the web of trust respond to their vouching call as fast as possible. In order to incentivize such behaviour, the users who respond to the vouching request will be awarded a portion of the tokens that were held in an escrow smart contract.

FRONT-END CLIENT • MOMENTUM

A multi-ledger browser, to become the unstoppable foundation of an ecosystem of user-friendly Blockchain products.

The decentralized web is bringing us a different connectivity paradigm and rapidly transforming centuries old value exchange methods. Interacting with decentralized technologies has many differences to interacting with standard web products. The most fundamental aspect is that for proper public decentralized networks, consumers are tasked with key handling, thus far it is a somewhat inconvenient process that has not enough decent consumer grade products.



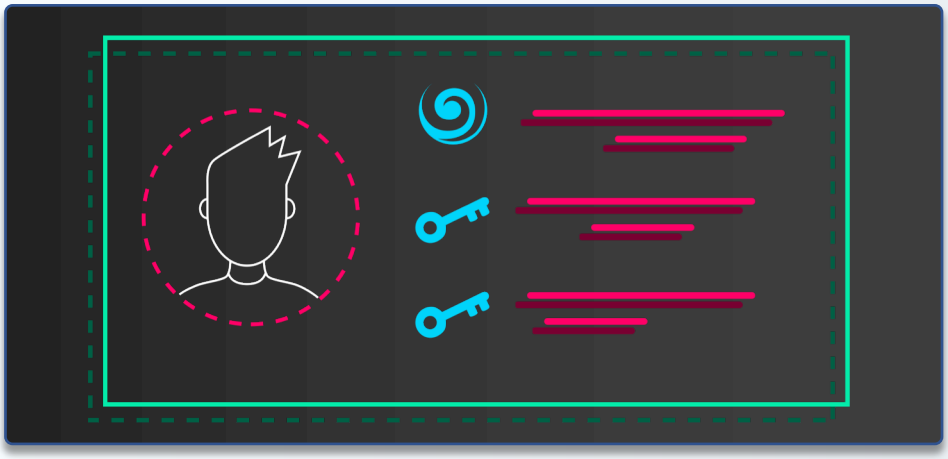
Momentum browser will contain the fundamental elements required to allow users to manage their keys securely, control how they interface to external services, recover keys in case of loss and activate more advanced key signing features such as multisig applications down the line.

CORE ELEMENTS

Keys Manager & Access Control

The main user dashboard is an equivalent to the ‘preference’ or ‘settings’ panel, this is where users load or generate their keys in, 3rd party public accounts can be verified (GitHub, Reddit, Twitter etc) and public addresses of Blockchain networks can be set to be shared as well.

Interacting with Blockchains typically requires message and transaction signing. The key management service supports these features, manages to interface to 3rd party Dapps like a decentralized exchange and handles master key storage and recovery functions. The key manager is essentially the control centre for all those events.



Secret Sharing

In the decentralized technology realm, as self-sovereign key ownership is an essential requirement, there’s fundamental need to build and integrate recovery mechanisms. Using Shamir secret sharing, keys are being divided into fragments and are encrypted using the web of trust properties so that a user would be able to rely on their web of trust in case they’d need to gather the k out of n secret fragments to regain access to the associated crypto assets.

Endurance Wallet

As the decentralized web grows, more complex scenarios are emerging, examples range from a fund that requires multisig to manage crypto asset to DAOs that handle their operations using various crypto assets and so on.

Endurance wallet is where the relevant info is being displayed and from where transactions status would start or end.

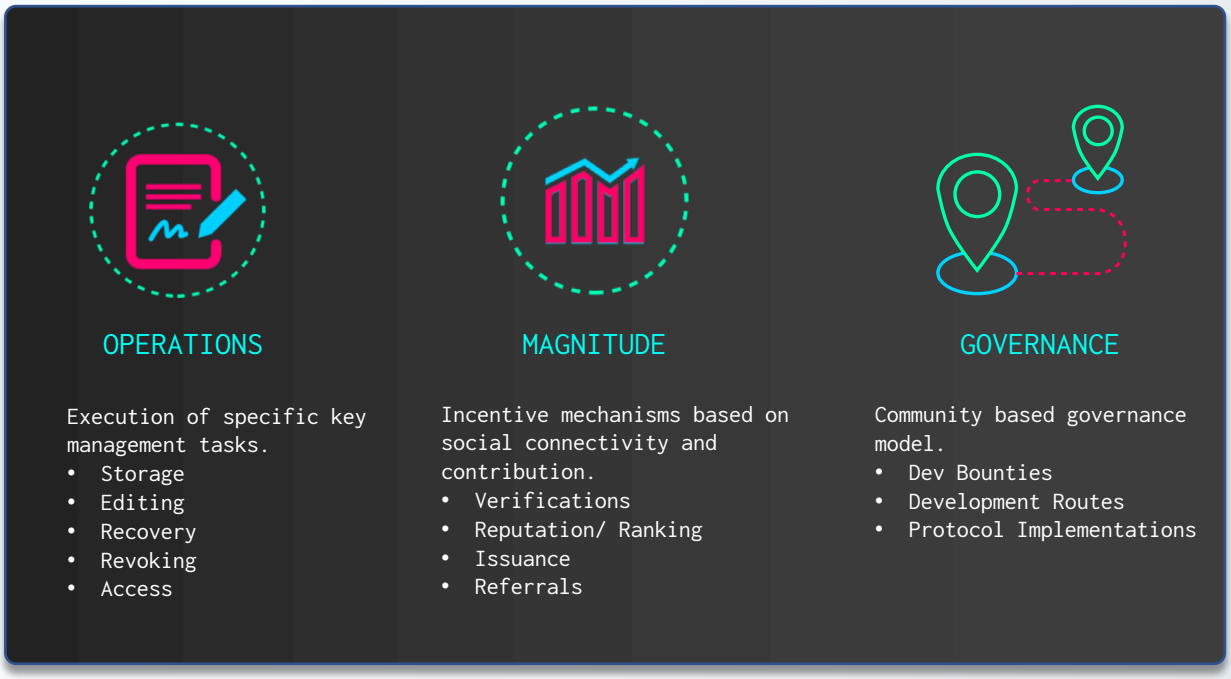
Endurance will contain the fundamental features to support a healthy decentralized ecosystem of user-friendly Blockchain solutions.

Fundamental Features:

Multi-Signature	Native DEX access

PROGRESSIVE CRYPTO ECONOMICS

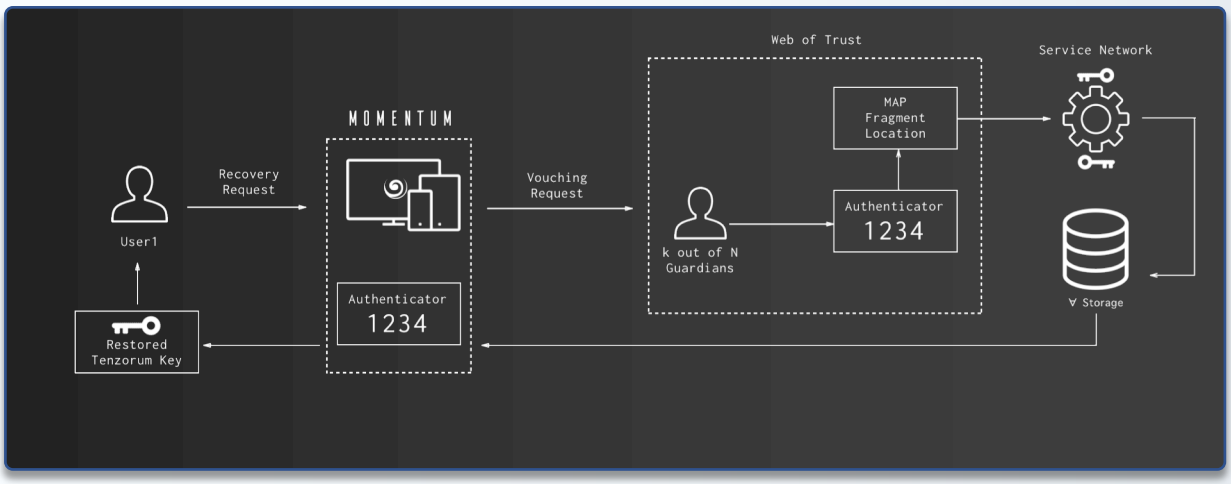
Tenzorum Token [TENZ]



Inception • Stage 1 • ERC20

At first, an ERC20 token will serve as a unit of exchange to activate core contract with few business logic functions associated to key management services: storage, edit and recovery of keys. These tasks are intended to be facilitated by web-of-trust network that has cryptographically verifiable relationships.

1st Implementation • Recovery Protocol



Liberation • Stage 2 • Tenzorum Service Node Network Token

The ERC20 tokens issued at the INCEPTION stage will be used to gain access to the future Tenzorum network that will be used as the inter-ledger network. This will be established as a public network with its own native token and associated issuance rate to reward infrastructure contributors.

Tenzorum Service Node Network (TSNN) will extends the functionality of the project to a general purpose key management service network. Access to any external decentralize technology (e.g. Urbit, Cardano, Nebulas, Bitcoin etc) will be powered by nodes that are being rewarded tokens according to predefined consensus rules to perform tasks that support Tenzorum as a self sustaining public network.

Sovereignty • Stage 3 • Tenzorum Masternode Network

Similar to Dash, Tenzorum aims to harness staking to establish inclusive governance. This will guarantee the governance of the open-source code base, protocol/UX features acceptance, organizational priorities, growth campaigns, partnerships and future vision direction.

GROWTH MECHANISMS

Most Dapps are using centralized solutions for key management and are openly eager to leverage decentralized infrastructure to execute such fundamental operations.
Tenzorum Project gained a lot of attention and requests come in from various services and projects that want to get early access to Tenzorum platform.

Tenzorum Architecture is being designed in order to become a fundamental element of the decentralized web, creating APIs to empower Dapps to leverage the Tenzorum decentralized infrastructure to provide the fundamental missing piece for consumer oriented key management functions like access control, key recover mechanisms, and login abstraction.

Mechanism 1 - Access Modes for Dapps: Seamless access, i.e. from Momentum Browser users will have instant key-free access to their services of choice.

Mechanism 2 - Web Of Trust: Dapps will be able to leverage the existent web of trust to integrate Social Media like features, Decentralized Social Games, and take advantage of Tenzorum platform to power their own systems.

Mechanism 3 - Access Modes for DEX • Seamless access, i.e. from Momentum Browser/ Endurance Wallet users will have instant key-free access to 3rd party DEX. This is a major industry need.

Mechanism 4 - Multi-signature implementation: Developers will be able to integrate multi-signature features in their applications using Endurance Wallet, nurturing the grounds to truly decentralized organizations.

INCENTIVE MECHANISMS

Tenzorum Mechanism Design is being created in order to assure that incentives are aligned towards network effect and product growth.

Issuance - For a decentralized public network to be self-sustaining, an incentive mechanism for network maintainers has to be put in place. In PoW networks, miners are being rewarded to validate transactions and solve the associated PoW problem. In Tenzorum Service Node Network the resource the network gives is processing key management events requests. As a public network, anybody can contribute resources and operate a service node if the necessary requirements are met. The reward will be given based on the number of tasks performed, the time the node is providing itself to the network and integrity of work.

Native Referral Mechanism - The platform will leverage existent social platforms to establish invites of new users to the Web of Trust. To unlock fundamental features like key recovery mechanism users will have to refer people, users will be incentivized to invite multiple trusted contacts to the platform.

Social Verification Rewards - Users will be rewarded to verify each other keys and enhance the network's integrity.

Developer Bounties - Independent Developers will be rewarded to complete development tasks on Tenzorum Project as well as to integrate the protocols into their own applications.

ROADMAP V1.1
[SUBJECTED TO DYNAMIC REVISION]

2018 [Q3 - Q4]

- Expand the core team and focus on Product, Protocols and Community Verticals.
- Develop initial strategic partnerships with Exchanges and Dapps and projects.
- Proof of Concept V1.0 - Recovery mechanism and secret sharing.
- Fundraising and public Initial Coin Offer.
- Tenzorum Suit initial product releases - Ethereum compatible.

2019 [Q1 - Q2]

- Protocol Fundamental Tasks Development.
- Protocol Architecture Research and Development.
- Tenzorum Suit Releases - Initial Protocol Integrations: Recovery, Storage, Edition.
- Design and Experiments for Liberation - Tenzorum Service Node Network.

2019 [Q3 - Q4]

- TSNN TESTNET
- Experiment Analysis with first group of partners and early adopters.
- Initiate integration studies with high frequency use Dapps - Production Version.

[BEYOND]:

- TSNN public experiment.
- Extend protocols to additional Blockchain Networks.
- Design and experiment TMGN and other governance models.
- Continue integrations with high frequency Dapps.

TOKEN SALE

Tenzorum.org/presale

Priority access to token allocation will be given to early signups and existing community members. Exact dates and further details about Tenzorum token distribution plan will be announced at a later time. Please fill the form if interested in participating in Tenzorum token distribution and want to be updated as more details are announced.

Find out more

Tenzorum.org

Join Tenzorum Project Telegram community

t.me/tenzorum