Tenzorum Project

A key management protocol for the decentralized web

DRAFT 1

Daniel Bar, Moritz Neto, Radek Ostrowski, Maciek Zielinski, Mark Pereira

Abstract

Cryptocurrencies and the Blockchain technology space has been evolving at a tremendous pace. However, despite the increase in awareness, the market has failed to produce solutions to support mainstream adoption of the technology, thus causing a plateau in user base growth.

The infrastructure to support real world products which will lead to mass adoption is the major missing piece of the Blockchain ecosystem. Inconvenient management of keys and access modes are currently some of the major obstacles in providing optimized experiences to the next generation of adopters entering the decentralized web.

Tenzorum is a key management protocol for the decentralized web. It is created from the ground up as the infrastructure to allow people to manage their keys and access different blockchains in a ubiquitous way. Tenzorum is developing:

- A personal multisignature smart contract to facilitate access management.
- A web of trust to enable the recovery of ownership.
- A Blockchain-agnostic framework to empower the next generation of applications with delightful and self-sovereign user experiences.
- A decentralized peer-to-peer network with its own token economy, to decrease the barrier of adoption when utilizing Blockchain solutions.

Table of Contents

1. Introduction

The awareness, technical developments, and market capitalization of distributed ledger technologies and cryptocurrencies have undergone tremendous growth since its inception in 2009 with P2P decentralized money - Bitcoin [1], to the implementation of Turing complete Smart Contract platforms such as Ethereum [2], Nebulas [3] or Cardano.[4]

With the evolving and dynamic nature of the industry, the development of self-sovereign, user-friendly key management systems are the turning point between a purely speculative dream and a truly equitable and decentralized future.

Despite the excitement for the potential of Blockchain to change the way society and the underlying financial systems communicate with one another, the industry is yet to create solutions that are widely adopted beyond the niched cryptocurrency communities.

Furthermore, the current management of private keys and access modes is typically handled in primitive and inefficient manners resulting in the rise of controlling, censoring and centralized custodian entities. This trend in essence defeats the purpose of decentralization at its core element: access and keys.

To ensure that the future of the digital realm is free and the access to decentralized technologies is not censored, controlled or stopped, dedicated public infrastructure has to be developed to guarantee decentralized access and support the next generation of people that will be empowered by experiencing true digital freedom.

Tenzorum is developing the platform that businesses, institutions, families, students, entrepreneurs, and regular users will use to control the ownership of their digital assets, permissions, and access to the decentralized world, while interacting with different Blockchains.

1.1. Tenzorum Project

Tenzorum is an unstoppable platform for self-sovereignty key management in the blockchain era. It is building the stack to guarantee unrestricted access and support mainstream adoption, allowing every user to interact with applications across multiple Blockchain networks and to interface with decentralized technologies in a seamless and secure way.

At the application layer, Tenzorum consists of Personal Multisignature Smart Contract which facilitates the management of ownership of digital assets and access while providing optimized experiences. At the middleware level, Tenzorum consists of the Interplanetary Access System (IPAS), a framework with APIs and SDKs (software development kits) to fuel the next generation of decentralized applications allowing them to provide seamless experiences to their users, supporting security, freedom and usability across the web. Lastly, at the infrastructure layer, Tenzorum consists of a decentralized p2p service node network that supports the relaying of gasless transactions and telemetry services (notification systems) which will consequently eliminate the need to deal with numerous types of tokens to interface with different Blockchain applications.

Tenzorum removes the need for a trusted party to manage user access across different applications. It provides personal self-sovereign management of keys as well as recovery for lost access. Tenzorum is set to build the foundation for mass consumer adoption of Blockchain technologies.

1.2. Key Components

- Personal Multisignature Wallet

  A usability driven personal multi-signature smart contract wallet.

- Web of Trust

  A social network that binds public keys to owner identities.

- Social Recovery Protocol

  A protocol to leverage the Web of Trust in combination with Time-Lock functions to serve as a recovery mechanism for lost keys.

- Inter-Planetary Access System

  A Blockchain-agnostic framework to provide decentralized access across the web.

- Tenzorum Service Node Network

  A p2p decentralized network responsible for relaying gasless transactions and executing telemetry services within the Tenzorum ecosystem.

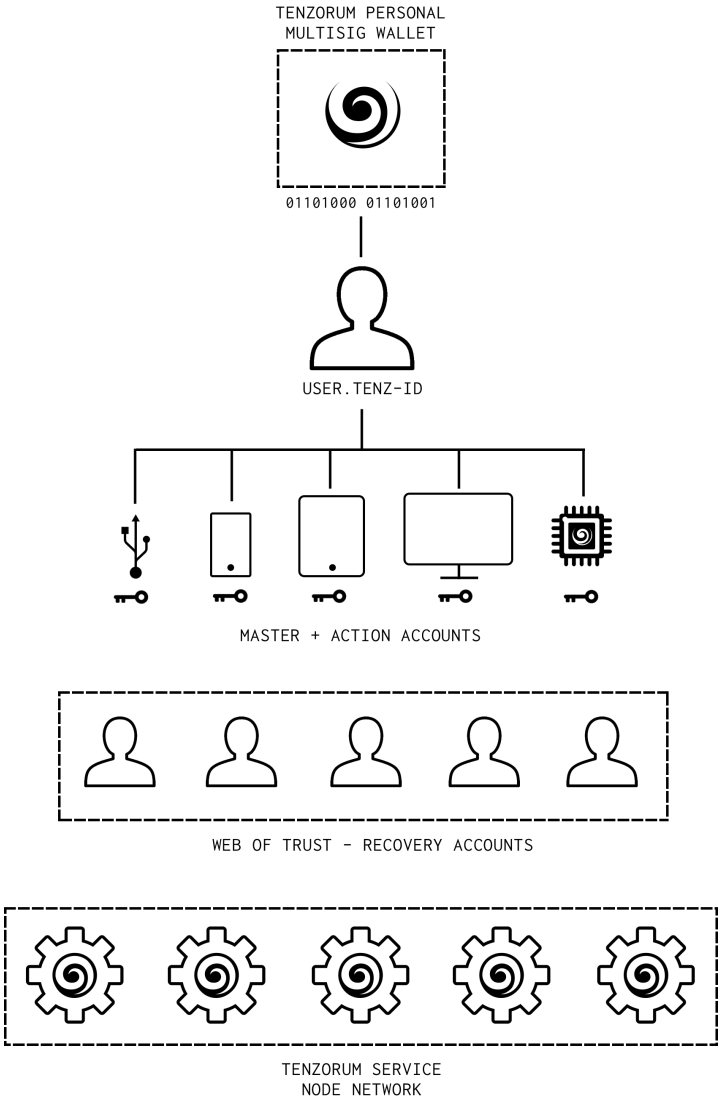

Figure 1: Tenzorum high-level architecture diagram

2. Tenzorum System Design

2.1. Personal Multisig Wallet

Tenzorum offers a personal multi-signature smart contract wallet which is referred to '*the wallet*'. There is one instance of the smart contract wallet per user. These are the key terms used when describing the Personal Multisig Wallet:

- *Master Account*
- *Action Account*
- *Recovery Account*
- *Time-lock*
- *Sender*
- *Service Node Relayers*

2.1.1. Master Accounts

A user account with full permissions, including editing the wallet configurations and is owned by the user. The administrative role can be granted to a single address (Single Key Mode) or granted to multiple addresses that are required to confirm transactions (Multisig Mode). The latter mode allows users to define the number of addresses required to accept transactions. This role is referred as the Master Account and will allow the users to customize their personal wallets to their security measures preferences.

2.1.2. Action Accounts

A user account with limited permissions, capable of performing certain actions on the multisig wallet such as small value transfers, login authorizations, and multi-signature signing. Action accounts give the ability to authorize other parties to perform and govern certain assets and actions. This can be for either Single Key Mode or Multisig Mode accounts.

2.1.3. Recovery Accounts

These are authorized Action accounts, owned by trusted third parties within a user's selected Web of Trust. These accounts participate in the Social Recovery event when a user has lost access to all of his keys.

2.1.4. Time-Lock

A parameter representing the time required to elapse before an action can take place. In the context of Social Recovery, there is a minimum inactivity time on the personal wallet, before the recovery process can be started. Master account owner can dynamically update the time-lock parameter at anytime and the start of the time-lock countdown is pushed forward after every interaction within the wallet.

2.1.5. Sender

Any account that wants to execute a transaction and pay for it in tokens. They sign a message of intent and send it to a Service Node.

2.1.6. Service Node Relayers

Nodes that provide a service for executing transactions on behalf of other parties by invoking relay smart contracts. Anyone can become a Service Node Relayer and compete with others based on their reputation ranking and low transaction fees. Service Node Relayers will be required to stake TENZ to operate.

Example permissions per account type	**Master**	**Action**	**Recovery**
Add new key at anytime	Yes	No	No
Add new key during social recovery state	Yes	No	Yes
Login	Yes	Yes	No
Small value transfer	Yes	Yes	No
High value transfer	Yes	No	No

These permissions need to be authorized by the Master Account and is similar to Github and Twitter's process of third party application authorisation. Granted permissions can also be revoked by the Master Account at anytime. This facilitates the design pattern where every device possesses its own key pair and limits access to certain assets on the wallet. Additionally, Action Accounts can be authorized to confirm transactions if multifactor transactions are enabled.

2.2. Web of Trust & Social Recovery

Social Recovery is the process of restoring access to your Master Account by enabling a set number of Recovery Accounts to vouch for your public key/account association. Through the Personal Multisig Wallet interface, this account recovery process is facilitated through the decentralized model of the "Web of Trust". Drawing inspiration from Phil Zimmerman PGP concepts [5] and the application of social recovery in WeChat [6] and Facebook [7] , the Web of Trust is a network of trusted parties who confirm n amount of requests to help the lost Master Account recover their credentials.

When assigning the Recovery Accounts in their Web of Trust, the Master Account owner will also define a desired amount of TENZ tokens to be burned by the Recovery accounts if their keys are lost. This is done in order to assure that the web of trust is conscientiously vouching and do not approve recovery requests without considerable assessment. If Master Accounts wants to set value to 0, recovery accounts will not have to burn any tokens.

All burnt TENZ tokens will cease to exist after this process and this mechanism will have marginal impact on TENZ total supply.

The successful scenario of recovering access to the Master account is as follows:

1) Master Account owner waits until the required lock period has elapsed, referred to as the Proof of Paralysis (PoP) [8] state, to initialize Social Recovery with the nominated Recovery Accounts in their Web of Trust.

2) Master Account owner generates a new key pair/account.

3) Master Account owner uses an external channel to communicate to n Recovery Account owners that the old key has been compromised and he/she requests authorisation for a new key pair/account.

4) If the Recovery Account owner is convinced of the request, they burn an X amount of TENZ tokens previously defined by the Master Account owner and authorize an on-chain action for a new public key/account.

5) If the number of Recovery Accounts authorising new public key reaches the required threshold of n requests, then this new key pair/account replaces the entire layer of lost accounts. Subsequently, Master Account owner can use it to access the wallet and the old keys are no longer valid.

6) The Master Account will have access to all previous assets under the new key pair/account and will be required to connect to new peripheral devices for future access and recovery.

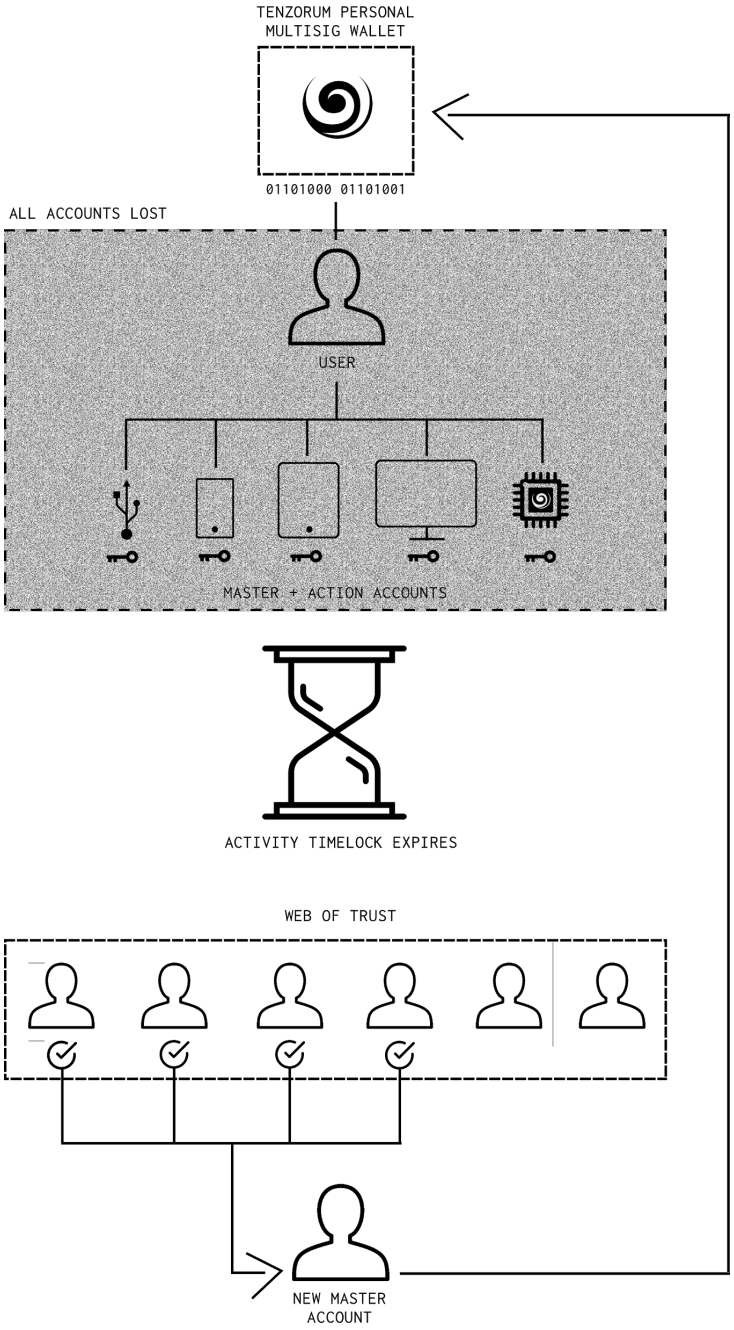

Figure 2: Social Recovery request

3. Tenzorum Service Node Network (TSNN)

Tenzorum Service Node Network is a p2p network responsible for relaying gasless transactions and auxiliary protocol services. Gasless transactions allows users to execute transactions and calls on the Blockchain without needing to have gas or different cryptocurrencies in their account.[9][10][11] The responsibility of paying gas fees is instead conditionally delegated and carried out by a third party decentralized application (dApp).

With current smart contract platforms such as Ethereum, on-chain transactions require users to facilitate validation using gas. This is a huge impediment for new users to Blockchain platforms because of the technical knowledge required to execute a transaction.

Tenzorum service nodes will spend gas executing the transaction on behalf of the users and will receive an equivalent amount of TENZ tokens as payment. The nodes will be setting their own rates and the users have the option to choose which Tenzorum services nodes they want to use. Tenzorum will provide a TSNN dashboard with a reputation ranking system.

Some of the benefits for gasless transactions are:

1) **Accounts do not require gas to execute transactions:** Gasless transactions removes a layer of friction for cryptocurrency users, especially new users to the Blockchain ecosystem. Users can transact cryptocurrencies through the use of dApps and other Blockchain platforms without requiring different cryptocurrencies. This removes the barrier of friction around adoption and opens up the user market of dApps and Blockchain platforms up to the rest of the world. It opens up the possibility of dApps giving Sybil verified users free gas tokens to conduct free transactions, resulting in a greater potential of onboarding new users, especially users who don't have gas or cryptocurrency.

2) **Simpler mental model for gas**: Gasless transactions enables dApps to be designed so users can pay for gas using tokens as opposed to gas units such as ether. This also enables users to pay gas in the denomination of a token as opposed to traditional gas. A dApp can also facilitate token creation and only charge their users in its internal currency for any Ethereum transaction. The currency units can be rounded so it looks closer to the actual amount of transactions with a standard transaction always costing one token and a very complex transaction costs exactly two etc.

3) **Experimentation dApp business models:** Gasless transactions enable the experimentation of different business models. The cost of the gasless transaction will be carried out by the dApps where they can accept the conditional delegated carry of the gas execution fees. This will enable dApps and businesses to experiment with different ways of monetizing their gasless dApps.

Example scenario one:

A social media dApp can create a monthly pre-paid subscription by creating a certain limit for the platform's usage. These subscriptions can then permission certain private keys the ability to execute transactions without the need for gas. A local device key can be generated and then assigned to the subscription without the need for the private key to ever leave the device. If another device requires the same level of access, identities can be linked. The dApp then signs transactions with the key on the device with a gas price of 0, sends them to the dApp which then can execute transactions if that key is associated with an identity/account that has paid for the subscription and/or have the correct permissions to execute gasless transactions.

Example scenario two:

Organisations such as charities and non-for-profits can delegate and permission certain keys access and usage of certain dApps without needing the keys to actually hold any gas or Ether. Key management options can be configured to cover all expenses incurred by a set of private keys, reducing the risk of embezzlement while enabling members of an organisation permissioned access of dApps and other instruments. This scenario can be applied to corporate governance and decrease the amount of trust required to operate an organisation.

3.1. User Flow

In order to further incentivize the network, participating TSNNs will be eligible to earn additional TENZ tokens for performing their duties. The incentive mechanisms will be implemented at a future point over TSNN's independent development.

Personal Multisig Wallet allows for the mentioned features to be executed in a gasless fashion and would follow a user flow of:

1) User of the wallet creates a new transaction including the amount of TENZ tokens they are willing to pay for relaying.

2) User sends signed transaction to Service Node (relayer).

3) Service Node executes transaction on Ethereum Blockchain, pays gas (Ether) and earns TENZ tokens.

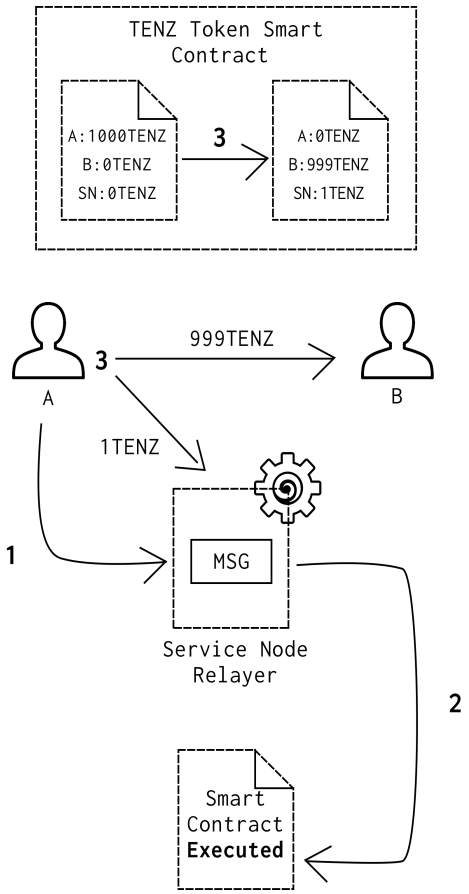

Figure 3: Gasless transaction implementation

The following potential malicious behaviours have been identified:

A Service Node might agree on relaying a transaction, but would not execute it in the future. This creates uncertainties in a user's understanding of whether a transaction will go through.

In order to avoid the scenario above, the protocol proposes:

1) Service Node locks TENZ tokens.
2) User of the wallet creates new transaction including:
   a) amount of TENZ tokens for relaying;
   b) amount of TENZ tokens for compensation;
   c) maximum time allowed for executing the transaction.
3) User sends signed transaction to Service Node.
4) Service Node agrees on the transaction's terms, signs the transaction and sends it back to the user, as a confirmation.
5) Service Node relays transaction as quickly as possible.
6) If the Service Node successfully executes transaction within the specified time limit, it earns TENZ tokens.

7) If Service Node does not execute transaction within requested time, user can use the confirmation to receive compensation from locked contract's service node's balance.

A user might send the same transaction to multiple Service Nodes and intend for all of them to compete for TENZ tokens. This would require all of them to send Ethereum transactions to Ethereum miners. Only the first one with confirmed transactions will execute and reward a Service Node's account with TENZ tokens.

This can be solved by requiring the user to lock some funds which would be lost in case the above scenario happens. Alternatively, Service Nodes are allowed to keep track of users who behaved this way and refuse them the service in the future.

Service Nodes have an option to register itself in the Service Node Register Smart Contract, by providing IP or a list of IPs of its service. The user interface of the Personal Multisig Wallet integrates with the Register and allows users to discover the best price for a gasless transaction, by simply querying all services.

3.2. Token Minting

In order to further incentivize the network, participating nodes will be eligible to earn additional TENZ tokens for performing their duties. The incentive mechanisms will be implemented at a future point over TSNN's independent development.

Following calculations are based on the estimated amount of TENZ tokens issued at the token generation event (TGE). At the time of writing, 1 ether is equivalent to 8200 TENZ and the total amount of tokens including incentives is expected to be 768,977,777.8.

The number of TENZ tokens minted at any given period (10 minutes) is defined by the following geometric progression:

$$a_t = \begin{cases} b & \text{if } t = 0 \\ d \cdot r^{t-1} & \text{if } t > 0 \end{cases}$$

Where:

- b is the estimated amount of TENZ tokens minted at the completion of TGE: 768,977,777.8.
- d is the amount of TENZ tokens issued at the first issuance period after TGE
- r determines the total amount of TENZ tokens issued over time.

The total supply of TENZ tokens will be capped to double the amount of TENZ tokens minted at TGE:

$$\text{total\_supply}(n) = \min\left(\sum_{t=0}^{n} a_t, 2 \cdot b\right)$$

Parameters r and d are chosen so that:

- 5000 TENZ tokens will be issued at the first issuance period after TGE
- The total supply of TENZ tokens will be reached 20 years after TGE.

Specifically:

- $d = 5000$ TENZ
- $r = 0.999993504905839$

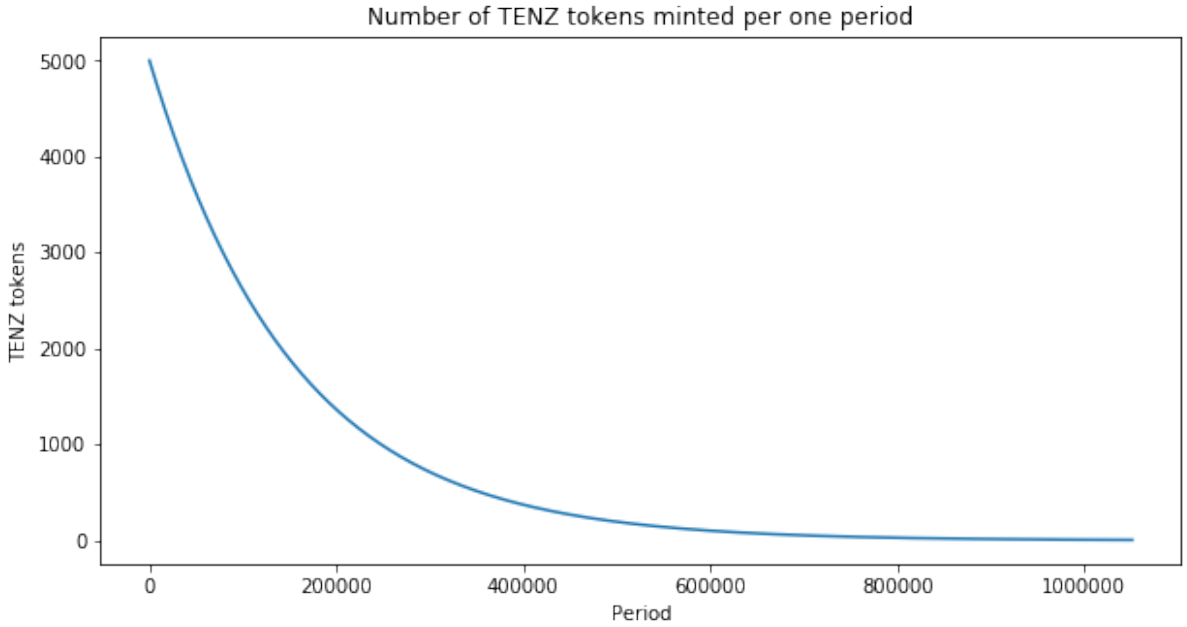

Figure 4: TENZ Token Minting

TENZ tokens expansion over time:

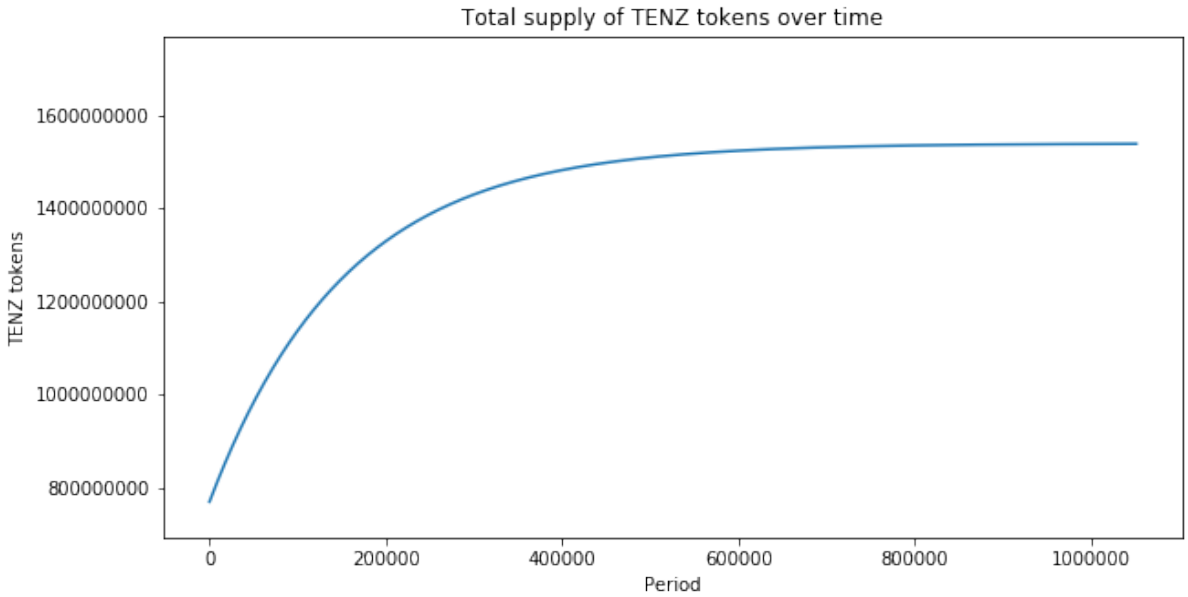

Figure 5: Total Supply of TENZ Token

The proposed dynamics in supply does not include the tokens being burnt as part of the Social Recovery process, which is independent to the minting process and is expected to cause marginal impact on the total supply.

3.3. Transactions with Multisig and Time-Lock

To provide added security to a user's funds, there are three main features integrated into Tenzorum's Personal Multisig wallet.

- Daily transaction limits.
- Multiple signatures per transaction.
- Transaction time-locks for transfers with an extremely high value.

Every method of transferring assets, granting and revoking permissions provided by the Personal Multisig Wallet can be secured by adding an additional confirmation step by either requiring multiple keys or a time-lock.

Example of requiring two confirmations is depicted below:

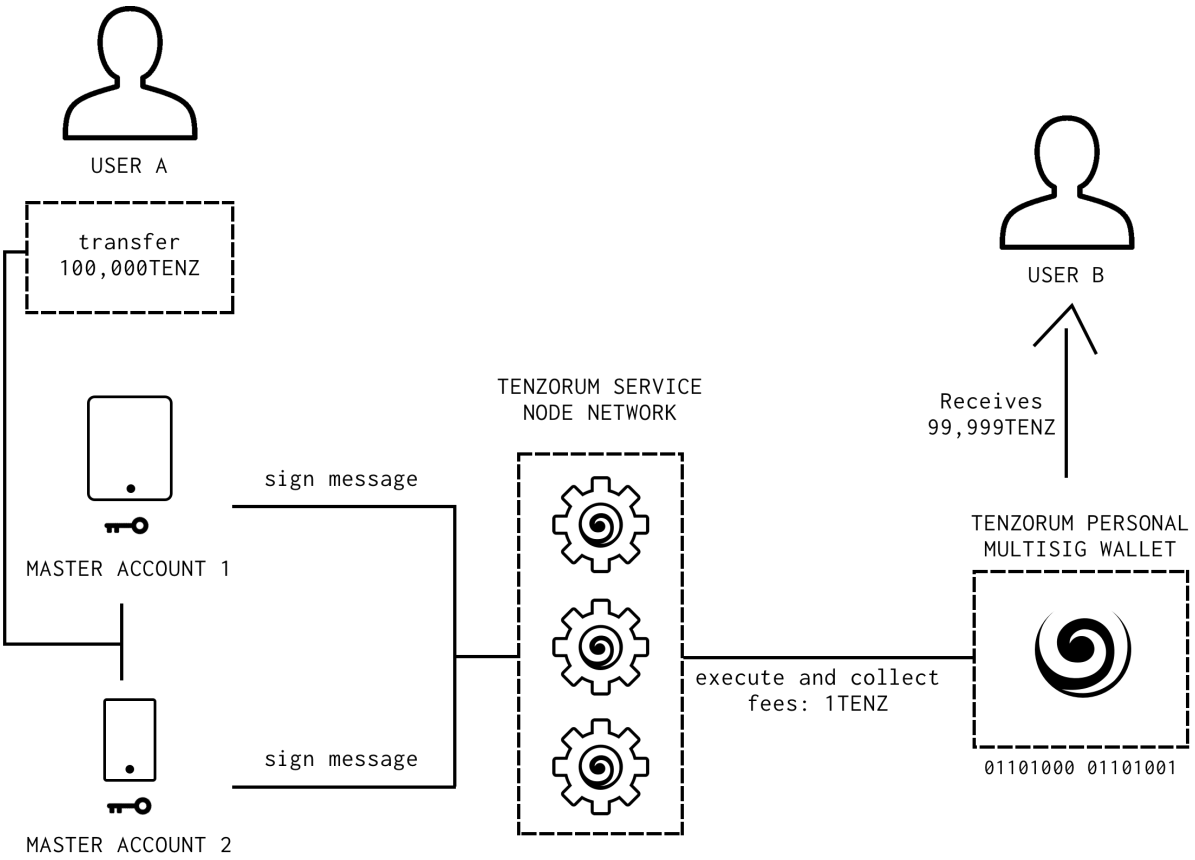

Figure 6: Multiple signature transaction.

Transactions requiring a time-lock, enter a pending state where a user can cancel by authorized keys.

Once time-lock expires, to complete the transfer another confirmation transaction is required and can be performed again by TSNN.

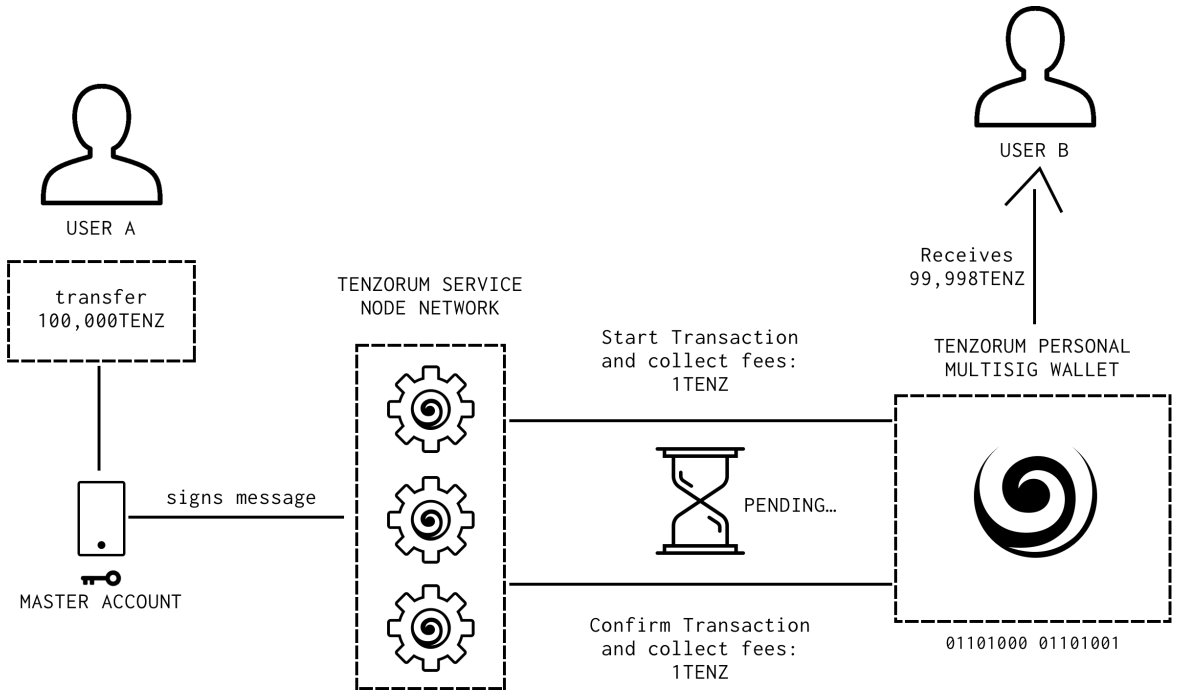

Figure 7: Time-lock transaction.

Time-lock features are especially important in attack scenarios where private key credentials are stolen. Tenzorum provides an additional service (Telemetry Service) described later in the document.

Telemetry Service works by keeping wallet holders informed about every transaction taking place in their personal multisig wallet, sending updates through personal notifications, SMS or Email. This is done to guarantee malicious behaviours can be identified, tracked and neutralized.

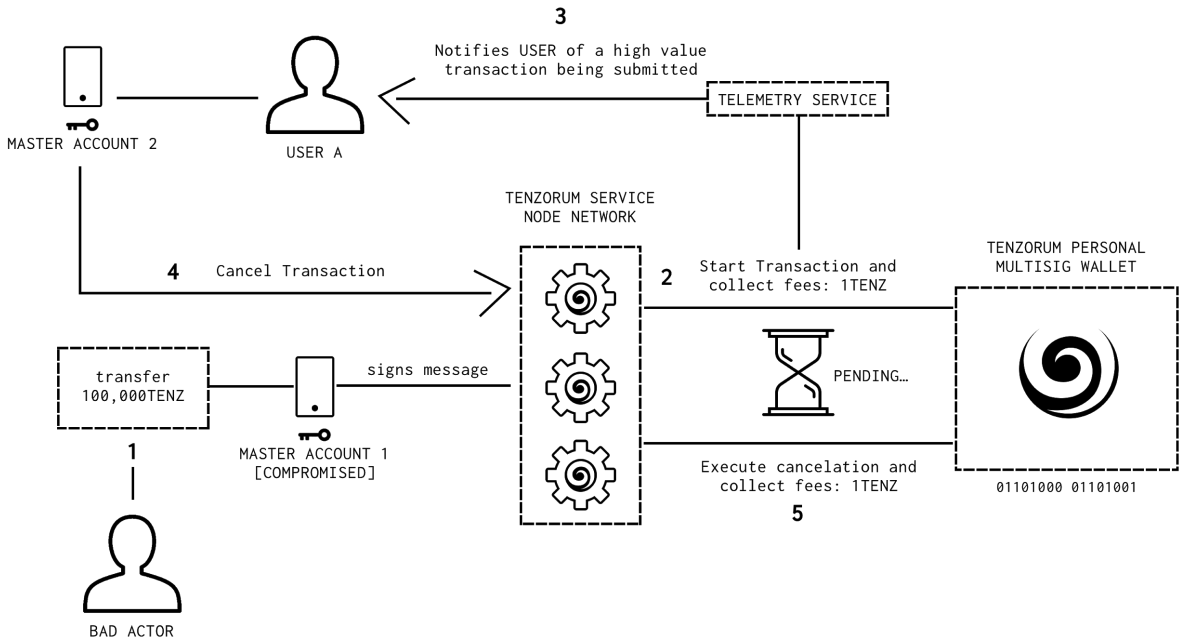

Figure 8: Telemetry service activated on a malicious request.

To further prevent malicious behaviours, the wallet requests can only be modified or cancelled according to the following hierarchy:

1) Master Account owner backed by more than 50% of Action Accounts

2) Master Account owner

3) Action Account

I.e. Master can cancel requests from a Recovery Account or requests created by another Master key, but cannot cancel a transaction if it was created by the master key and approved by more than 50% of the Action Accounts.

3.4. Upgradable Token

At the time of the crowdsale, TENZ token will implement only ERC-20 compliant methods. More functionalities will be built into the token's Smart Contract in order to operate gasless transactions. Degrees of upgradability are required to meet and achieve this, so there will be a split in the logic, created in two smart contracts:

- Interface smart contract - A publicly available, ERC-20 compliant interface that users can use to interact with their tokens. It implements access and permission layers between users and Tenzorum's secondary contract, the Balances Smart Contract.

- Balances smart contract - Keeps track of account balances and allowances. It implements the storage layer where only one approved Interface smart contract can do transfers and approvals and has full privileges to change all the data. This contract also allows the Tenzorum Team to propose new Interface smart contracts deployed on another address.

3.5. Multiple Chains and Cross-Chain

Tenzorum is a Blockchain agnostic project. It aims to support interaction and collaboration across multiple networks. The vision is to abstract and simplify the nuances in key management across all major blockchains for the end user. We have architected our solutions to suit schematic descriptions presented by interoperability projects such as Polkadot [12] and Cardano.

The major components in our interoperable chains are:

- Multi-Network, Multi-Signature Wallet
- A Relay System
- Atomic Swaps / Cross Chain Trading
- Side Chains / Parachain Schematics

3.5.1. Multi-Network, Multi-Signature Wallet

Our Personal Multisig Wallet features are designed to suit a canonical, standardized interface. This equips users and developers with the capability to build and implement on every immutable ledger that has a Turing complete virtual machine. It is also possible to implement the wallet using Bitcoin's Script.

3.5.2. Relay System

Tenzorum's Service Node Relayers facilitates gasless transactions through a relay protocol. This decentralized, relay protocol network executes Ethereum based token transfers via publishing signed transactions to the TSNN. TSNN will expand to multi-network based Tenzorum tokens via atomic swaps.[13]

3.5.3. Atomic Swaps / Cross Chain Trading

For our relays to operate agnostically, a mechanism to discourage cheating or collusion across system transactions by withholding one side of the deal while another is essential. Atomic swaps will facilitate and prevent such scenarios over cross chain transactions.

3.5.4. Side Chains / Parachain Schematics

Tenzorum's Service Node Network will lead the build to architecting operable side chains or parachains. The decentralized microservices of our TSNN will morph into a fully fledged network through the integration of segmented, modular infrastructure provided by multi-chain frameworks.

4. Application Layer

Tenzorum will provide various interfaces to interact and manage keys. A web based dApp, a mobile application for Android and iOS, a desktop application and a browser-based web extension will be created to cater for users at the application layer. All interfaces will allow them to interact with all the features provided by the wallet Smart Contract and Telemetry Service.

Tenzorum Service Nodes can easily be deployed on local hosts by anyone, to provide access modes to other users on Tenzorum's network. Transactions can be signed via dApps with the use of the Tenzorum browser-based wallet, the Tenzourm mobile phone application or hardware wallets.

4.1. Inter-Planetary Access System - IPAS

IPAS is the framework to provide decentralized access across the web. Tenzorum will be developing open source SDKs, APIs, modules, packages and other tools for developers to use within their decentralized applications to seamlessly integrate into the Tenzorum ecosystem.

IPAS enables application users to access Tenzorum Action accounts which are built upon the use of public/private key cryptography. Additionally, IPAS has accessed the extensibility of portable devices, such as smartphones and laptops, to allow you to interface with multiple Blockchains and decentralized applications. Through trusted, secure enclave environments, IPAS enables interface level code to be safely executed.

IPAS does this through decoupling code that runs on the interface level from code that manages cryptographic signing and secure storage. This gives Tenzorum the confidence to build out well-architected, visual experiences with the brute force that lower level languages provide.

By open-sourcing these features, Tenzorum aims to enhance the user experience of Blockchain solutions and open accexfss to them by providing interfaces to seamlessly integrate and utilize the power that distributed ledgers and Blockchain technologies provide.

4.1.1. Device Specific Keys

Each device running Tenzorum's application will have their own private key associated to its native encryption environment. The ability to access wallets via the web, smartphones and personal hardware will give users the experience needed for leveraging the numerous benefits of decentralized systems.

4.1.2. Universal Login (OAuth)

Tenzorum's use of public/private key cryptography, alongside cryptocurrencies, pioneers a new form of self identity while browsing both decentralized products but alongside the web2.0 architecture. We will provide well documented SDKs and APIs for developers to integrate IPAS' Universal Login authentication features into their dApps.

We aim to utilize the ability to remain as an anonymous user browsing the web by integrating an OAuth solution which acts as an universal login similar to what companies like Facebook and Google provide, however without having to give away targetable and utilizable data to corporations.

The added benefit for third party apps using Tenzorum's Universal Login is user access to wherever they have their portable devices and it provides easier access to their digital assets.

4.2. Telemetry Service

Tenzorum Service Node Network also requires telemetry services to relay information to the respective Master, Action and Recovery Accounts regarding any Wallet transaction or activity. The Telemetry Service layer facilitates this with a monitoring and notification system. This information services provide a channel for communication through e-mail, push notifications and SMS services. This component will be a premium service and paid for in TENZ tokens. The source code will be open-sourced so everyone can setup private instances. It will be available for use on multiple instances to reduce redundancy.

5. Token Mechanism

TENZ token is deployed on Ethereum and implements an ERC-20 interface. Main uses of tokens can be described in the following categories.

5.1. Web of Trust

Users can designate TENZ tokens to be paid by the Recovery Accounts to participate in the process of setting a new master key. It is an optional feature and intended to discourage collusion. The amount required, if any, is chosen by the user. For well defined use cases such as cryptofund custody or insurance the amount can be pre-configured in correlation to the associated assets stored in a Tenzorum multisig account.

5.2. Tenzorum Service Node Network

Tenzorum Service Nodes provide a crucial service to users on the Tenzorum network, which is the facilitation of seamless, feature-rich user experiences. This is facilitated through the usage of TENZ tokens in exchange for gas on particular networks which will incentivize Service Nodes to contribute relaying transactions on the network.[14] Transactions facilitated by the Service Nodes allow them to be rewarded in a similar way to mining or collecting transaction fees.

TENZ tokens are minted at a predefined rate (as described in the Token Minting section) as an extra incentive for Service Nodes performing their duties. In exchange, users of the Tenzorum network are able to interact with the network without owning ether or other ERC20 tokens.

Service Nodes are required to lock TENZ tokens as compensation in the event of malicious behaviour or attack vectors.

5.3. Voting

Tenzorum has the intention of implementing Masternodes to decentralize the project governance to vote on the proposed improvements made by the core team and the community. TENZ tokens will be used as a voting mechanism, to upgrade Tenzorum smart contracts.

5.4. Telemetry Service

TENZ tokens can be used as payment method for the Telemetry Service which monitors all wallet operations and sends users notifications and reminders.

6. Security and Recovery Scenarios

6.1. One Master Account

When a user onboards with the Tenzorum platform, the first thing they create is a Personal Multisig Wallet smart contract. There will be a factory contract available and a user friendly UI to hide the complexities and allow users to create the personal multisig with one single call. Tenzorum team will be working on adjusting the smart contract to be as economical and gas efficient as possible.

The address they use for the contract creation becomes the first and initial Master wallet address which has all the privilege rights.

Users will be instantly incentivized to add new device actions and Master accounts to their Personal Multisig as well as inviting new users to become a part of their Web of Trust.

6.2. Two or More Master Accounts

When the user adds one or more Master accounts, the Personal Multisig Wallet immediately increases its security reputation as it enables redundancy between the devices and a multi-factor approval of transactions. Users can enforce limits on the withdrawals of funds and require multiple approvals.

6.2.1. Recovery

In the event of losing key access (e.g. laptop hard disk gets corrupted or the loss of your mobile phone), the user is still in full control of the Personal Multisig and can add a new key/account using the spare Master account(s). With redundancy of keys/devices, the users can recover their lost access.

6.2.2. Attack Vector

If one Master private key is stolen and the recommended multi-factor confirmation is enabled, any action to withdraw the funds by the attacker would have to be confirmed by the owner of the account from another device, effectively blocking the transfers. Consequently, if the owner of the account had an additional permission layer (Master, Action or Recovery Account), only the majority would be able to authenticate such actions, thus stopping the attackers effort to gain access.

6.3. Master and Action Accounts

Excluding the fully privileged accounts, users can also have one or more Action accounts with limited access and capabilities. They can have an Action account on their mobile phone, which would become very convenient in many scenarios including two factor confirmations and everyday logins across Blockchain networks.

6.3.1. Recovery

Recovery of lost keys is as described in the previous section (Two or More Master Accounts).

6.3.2. Attack Vector

Let us assume that the user's mobile phone was stolen which had an Action Account private key on it. If the attacker manages to hack the phone and bypass the app security (face ID/fingerprint/pin), they would be only able to perform a limited amount of operations on the wallet such as login and minor withdrawals, as described in the Tenzorum System Design section. The user would also be able to quickly remove the permissions from the stolen account with the permissions of a Master Account.

6.4. One Master and Recovery Accounts

Following the example of an individual who was gifted a small amount of cryptocurrencies and has limited knowledge about the key management however still

wants to keep their Personal Multisig secure; they would usually have only one Master account. During their onboarding process, they can assign a set of arbitrary accounts to their trusted parties who effectively become their Recovery Accounts such as family and friends.

6.4.1. Recovery

If the Master key is lost and the specified amount of time since the Proof of Paralysis period has elapsed, the user can ask their Recovery Accounts to grant a newly generated key Master permission. Once a required number of signatures (set by the user's configurations) is reached, Master Account access will be recovered.

6.4.2. Attack Vector

To prevent collusion among Recovery Accounts, where they agree to take over a certain account, the recovery process would follow:

1) The required number of Recovery Accounts would perform Social Recovery to generate a new key pair.

2) Every malicious Recovery Account authorizes the new public key to replace the current Master Account's key. time-lock period begins.

3) Master Account receives confirmation of malicious behaviour and uses his private key to cancel the Social Recovery procedure.

4) Malicious Recovery Accounts get removed from the list of Recovery Accounts and their staked TENZ tokens get burned.

5) Master Account should find new friends.

Another attack scenario could follow a Master Account who has no Internet access and the time-lock period passes where a malicious Social Recovery is initiated. To prevent this, Personal Multisig Wallet requires a PoP period has elapsed from the Master Account before Social Recovery can be started. If Master Account plans to go on a two-week vacation, by simply increasing the required inactivity period to one month can secure their funds. Master Account can initialize Social Recovery at any time.

Tenzorum Wallet can also secure funds from the theft of a Master Account 's private key, only if two-step transactions and Social Recovery are enabled and follows the flow of:

1) Thief copies/steals the private key of Master Account without their knowledge.
2) Thief performs a malicious transaction. time-lock period begins.
3) Master Account gets a notification of the transaction and realizes that someone is trying to steal their private key.
4) Master Account cancels transaction during time-lock.
5) Master Account creates a new key pair.
6) Master Account sends new public key to every Recovery Account using a secure channel.
7) If Recovery Account is convinced that changing the Master Account's key is correct behaviour, then they perform an on-chain action of authorisation for the new public key as a new Master Account.
8) If at least 51% of Recovery Accounts authorize this action, then Master Account is able to request for the official change of their old key/account access to the new Master account. Master Account uses old private key to sign it. Time-lock period begins, but only Master Account with confirmation of at least 51% of Recover Accounts can cancel it. Attackers cannot do anything.
9) Master Account can use the new key/account to interact with their Personal Multisig Wallet and their old key/account is no longer active.

7. Roadmap

Q3 2018	• Whitepaper Release. • IPAS PoC code open sourced.
Q4 2018	• Tenzorum IPAS MVP release. • Personal MultiSig Deployed on Ethereum Testnet. • Web Extension Release. • Social Recovery Mechanism Release.
Q1 2019	• First IPAS module available for third party integrations. • TSNN - Gasless Transaction Relayers Release.
Q2 2019	• IPAS API and SDK Releases. • Telemetry Service Release.
Q3 2019	• Personal Wallet deployed on Ethereum Mainnet. • Desktop Application Release.
Q4 2019	• Cross-chain transactions with the use of multi-chain frameworks like Polkadot.

8. References

[1] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system.

[2] Vitalik Buterin. A next-generation smart contract and decentralized application platform.

[3] Nebulas team. The value-based blockchain operating system and search engine.

[4] Aggelos Kiayias, Alexander Russell, Bernado David, Roman Oliynykov. Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol.

[5] p2pfoundation, Web of Trust.

[6] Matthew Brennan, Lost your Phone? What about Wechat?

[7] Facebook, Delegated Recovery.

[8]Fan Zhang, Philip Daian, Gabriel Kaptchuk, Iddo Bentoc, Ian Miers, Ari Juels, (2017) Paralysis Proofs: Secure Dynamic Access Structures for Cryptocurrencies and More.

[9] Alex Van de Sande, ERC-1077 and ERC-1078: The magic of executable signed messages to login and do actions.

[10] BokkyPooBah, BokkyPooBah's Token Teleportation Service Smart Contract.

[11] Status, Gas economic abstraction in top of smart contracts.

[12] Dr Gavin Wood, Polkadot: Vision for a heterogeneous multi-chain framework.

[13] En.bitcoin.it, Atomic cross-chain trading.

[14] Uport Project, TxRelay.