WHITEPAPER

FreeTON Self-Sovereign Identity Framework

By HugeSurge

https://github.com/Tkareder/FreeTON-SSI-Framework
sashatkachev@protonmail.com

2021

Contents

Glossary

SSI - Self-Sovereign Identity

DID - Decentralized Identifiers

CJM - Customer Journey Map

Abstract

The document describes the main actors, functionality and technologies of the Self-Sovereign Identity Framework based on the FreeTON blockchain. The proposed system forms the technical requirements user paths based on the interaction of users, issuers and verifiers thru the external API and the blockchain network. The proposed architecture allows you to quickly and safely identify a user when solving problems of varying degrees of complexity - government services, financial transactions, healthcare procedures and any processes where user identification is required.

A mechanism is also provided for the inclusion of institutions in the number of trusted verifiers through the voting of network participants. Described proposed customer journeys for user identification and verification, issuer registration, and verifier approval. The advantages of the proposed solutions are the scalability of SSI and the transparency of its functioning for all participants in the identification process.

1. Intro

The document describes the main actors, functionality and technologies of the Self-Sovereign Identity Framework based on the FreeTON blockchain. The proposed system forms the technical requirements user paths based on the interaction of users, issuers and verificators thru the external API and the blockchain network. The proposed architecture allows you to quickly and safely identify a user when solving problems of varying degrees of complexity - government services, financial transactions, healthcare procedures and any processes where user identification is required.

A mechanism is also provided for the inclusion of institutions in the number of trusted verifiers through the voting of network participants. Described proposed customerjourneys for user identification and verification, issuer registration, and verifier approval. The advantages of the proposed solutions are the scalability of SSI and the transparency of its functioning for all participants in the identification process (fig.1).

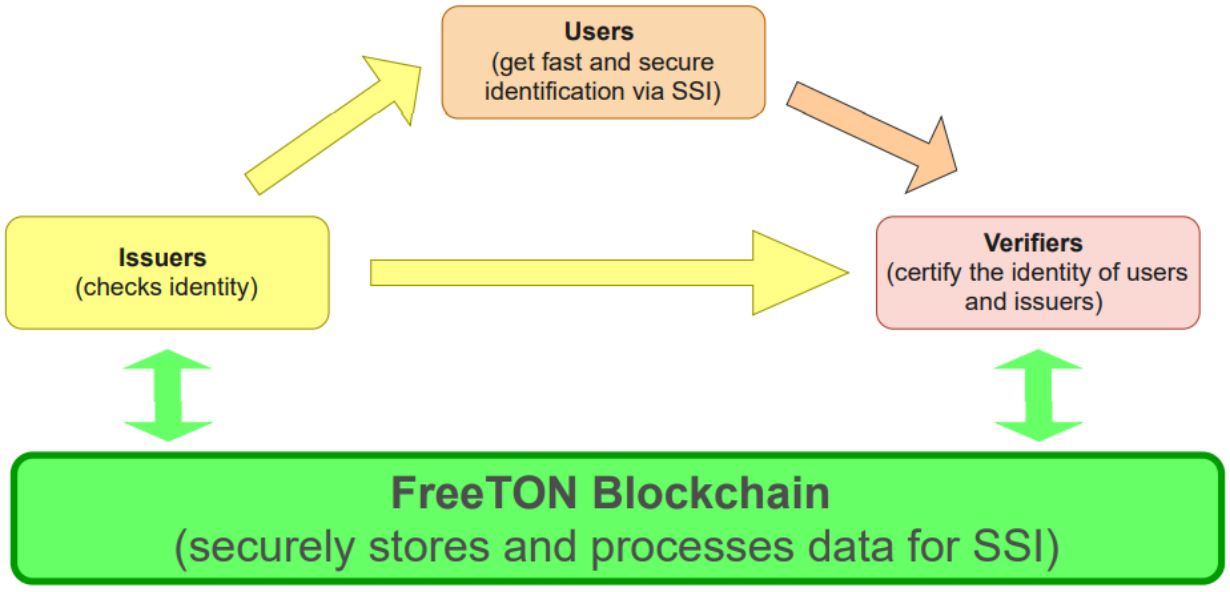


Fig.1 Self-Sovereign Identity common structure

The formation of trust between the verifier and the issuer occurs without additional actions, only based on the user's status in the FreeTON network. The presented architecture solves the problem of maximum simple and effective logic of

interaction between the participants in the SSI process.

The most numerous are users - who can be both members of the FreeTON network and third-party users of other SSIs (this is why it is proposed to develop an identification application as an intermediate data processing layer and a multi-platform solution for fast SSI scaling.

The second largest category is issuers. They get the ability to quickly check the user's credentials, and can be any organization, entrepreneur or company, as well as government agencies and financial institutions. They get quick access to user data.

The smallest category in terms of the number of network participants is Verifiers. In this scheme, they perform the functions of an independent party, which had reliable data about the user prior to his identification in the FreeTON network. In the process of scaling the proposed SSI ecosystem, Verifiers and their efficient operation are the main limiting factor for scaling and rapid distribution.

2. Technical stack

A common feature of the developed SSI technical architecture is that all three categories have their own accounts in the identification application (fig.2).

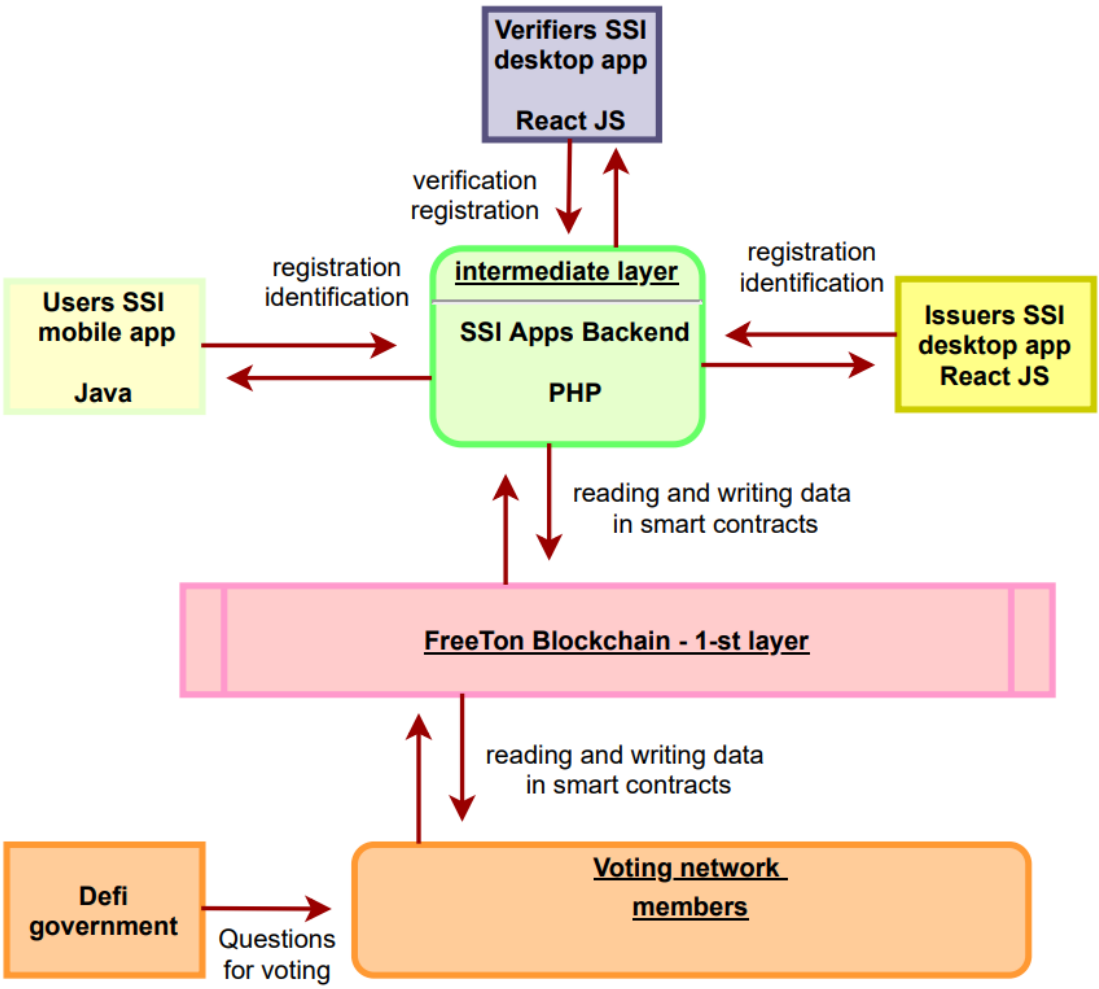


fig.2 interraction between actors and app with 1-st layer blockchain

The framework's technical solutions are based on a three-part approach:

Smart contracts - based on the existing FreeTon network, which surpasses the best blockchain networks in terms of security and performance;

Integration layer - processing of commands received from the frontend and from the blockchain in the php backend of the application for identification. What is the advantage of having an intermediate layer allows you to connect the fast and reliable Free TON blockchain with a flexible application interface for the user.

User interfaces - built in Javascript and Java programming languages.

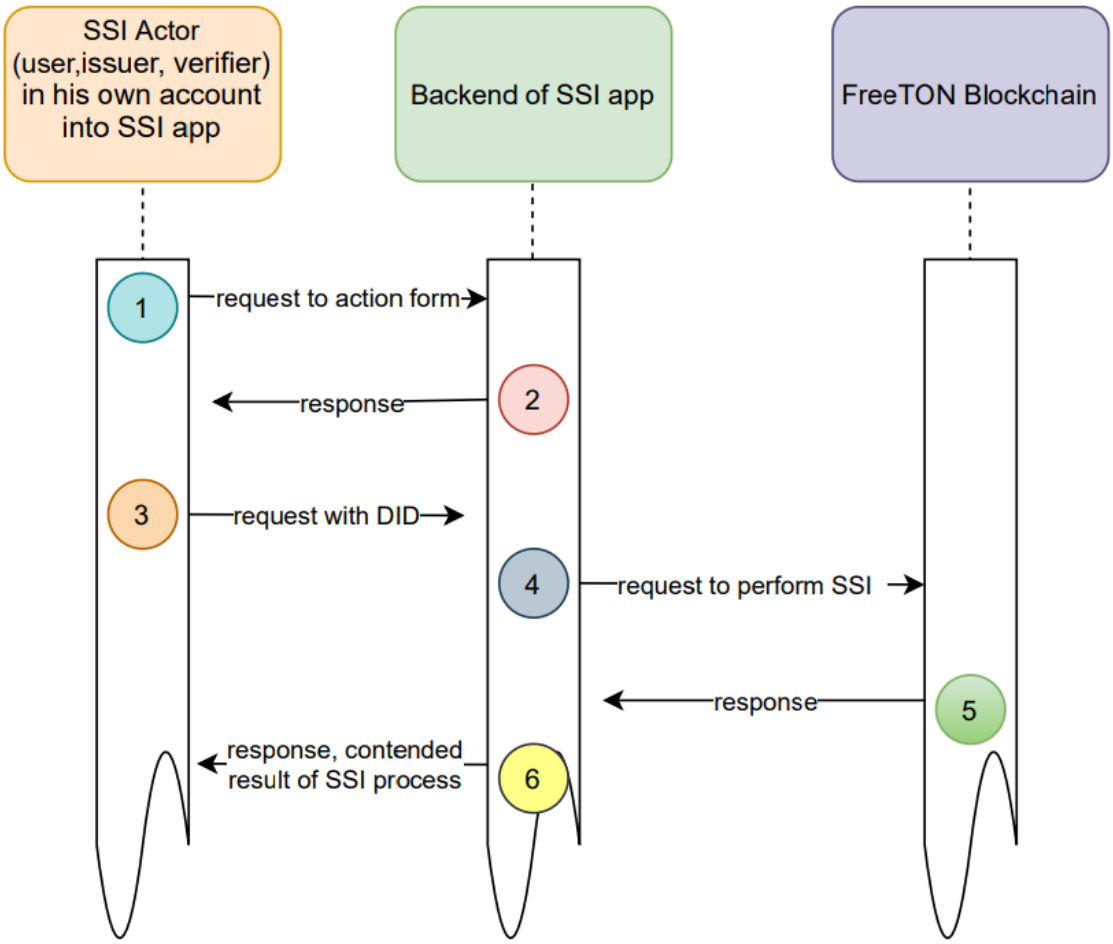


Fig. 3 interaction between actors and 1-st layer blockchain within application responses and requests

As can be seen in the interaction between SSI actors diagram (fig.3), the first level is the Frontend, namely the user interface of the mobile and desktop versions of the application for integration. The second, intermediate level is the application backend, which two-way transmits and receives data from users of the framework to the blockchain and back.

The advantage of such a

Self-Sovereign Identity Framework actors:

- users;

- verifiers;

- issuers;

- participants of the FreeTON network participating in decentralized voting /

The big advantage is the structure of the distribution of powers in the decentralized SSI system. As a result, one and the same person can be both a user (consumer of SSI services) and a participant in the management of the new identification ecosystem (participants of the FreeTON network participating in decentralized voting).

This allows you to close the architecture and solve the problems of developing and maintaining the system in parallel.

Based on the listed groups of actors (categories of users by the new framework), the developed scheme assumes 6 main functions of the SSI framework:

User verification (actors: user, verifier)

User identification (actors: issuer, user)

Verifier registration (actors: participants of Free TON network, verifier)

Verifier validity state cheking (actors: participants of FreeTON network, verifier)

Issuer registration (actors: issuer, verifier)

Issuer identification (actors: issuer, verifier).

3. Governance stack

Members of the Office of the proposed SSI system have their own responsibilities and capabilities.

For the expansive distribution of the proposed identification technology, the following parameters must be taken into account:

- financial motivation - the use of SSI should be cheaper than using traditional identification systems, and other SSIs offered by competitors;

- ease of use - clear and convenient user interface, and available recommendations for the use of the system;

- reputational motivation - SSI should be seen as a sign of commitment to the most progressive technological community;

- motivation to improve security - the reliability of SSI should allow increasing the protection of user data and counteraction to malicious actions.

After the implementation of SSI, it is necessary to achieve a viral spread of the technology for all categories of users.

A critical parameter for the dissemination of SSI among verifiers (government and financial institutions) is its compliance with the state legislation of all countries. In this regard, at the implementation stage, it is required to conduct a study of the difference in the legislation of individual countries and the formation of a manifesto on the compliance of the SSI procedures implemented with the legislation on the protection of user data, privacy, personal data processing and copyright. The basic advantage of the system is the use of the Free TON blockchain in the first layer of data storage as the most secure and secure way of storing data, and the depersonalization of network users. This minimizes the risks of data misuse in the proposed SSI system and provides advantages over centralized identification methods.

Existing identification systems focused on the implementation of the most modern technologies should not be considered as competitors, but as possible participants in the network. To do this, it is necessary to provide for the possibility of

their connection to the application API.

Such systems include:

Sovrin

Uport

MOBI

RealME

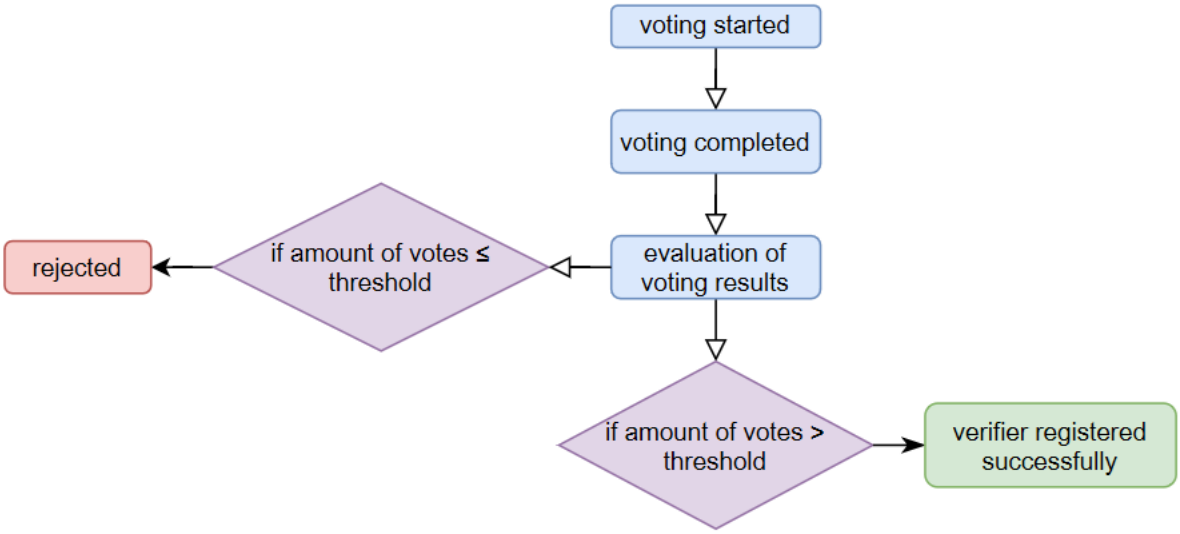
Verimi

Itsme

Verified.me

As a result, the strategy of involving competitors in the FreeTON ecosystem will be implemented and the subsequent explosive growth in the number of users of the proposed SSI.

The Verifier obtains the authority to approve the user through a vote of the



TON Crystal network participants (fig.4)

Fig 4. Voting Scheme for SSI Verifier status

The proposed voting procedure avoids duplicating verifiers and adding an invalid verifier. In addition, control over Verifiers will allow the use of SSI as a method of identification, which removes a person's identity from excessive

government pressure, and increases the level of personal freedom and information security.

4. Proposed customerjourneys

In this section, we will look at the basic CJMs in the proposed SSI system. This allows you to evaluate how the logic of the main SSI execution of the 6 main functions of the SSI framework, described in section 1 of this document.

User interaction with the SSI system begins with registration, which consists of five sequential steps in CJM (fig.5).

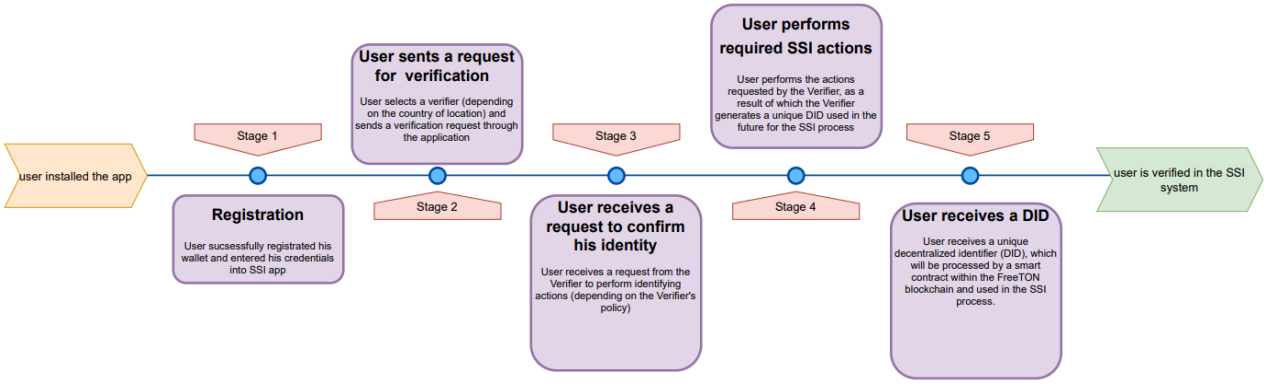


Fig 5. User verification (actors: user, verifier)

As you can see from the diagram, after installing the SSI application, the user is registered.

The user then submits a verification request (stage 2).

After the verifier has received a request from the user, it sends instructions to confirm the user's identity, and the application receives an incoming request for primary identification (stage 3).

After that, at stage 4, the user performs verification, as a result of which the Verifier forms a record in the FreeTON blockchain on the correspondence of the user's identity and the issued unique identifier (DID).

The fifth and final stage of the user verification process is obtaining a DID, which is further used in the SSI process, the most frequent process in the proposed

framework (fig.6).

The mechanism of user identification, presented in Fig 6. It is based on the simultaneous and independent receipt by the user and the Issuer of a confirmation from a smart contract, previously generated after verification of the record and about the user in the FreeTon blockchain network.

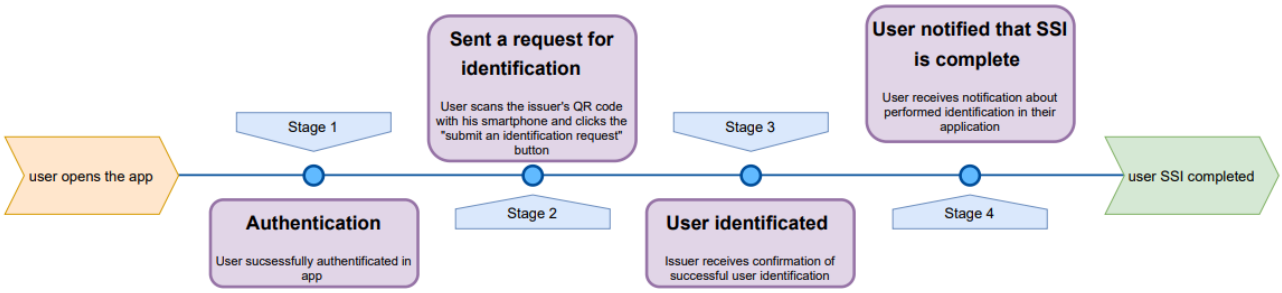


Fig 6. User identification (actors: issuer, user)

Let's take a closer look at the stages of the main user path in SSI.

At Stage 1 User sucsessfully authentificated in app.

Then, he sends a request for identification - User scans the issuer's QR code with his smartphone and clicks the "submit an identification request" button (second stage of identification)

The transition to the third stage occurs if the User was previously successfully verified in the blockchain network and uses a valid DID. If these conditions are met, then Issuer receives confirmation of successful user identification - stage 3 has been successfully completed.

In the fourth stage (which occurs simultaneously with the third) User receives notification about performed identification in their application.

The result of these four steps is the successful identification of the user and the receipt of services, information or goods from the Issuer. The versatility of the developed approach to SSI will greatly simplify its practical implementation and implementation, as well as the understanding of the stages of the process by operators and end users.

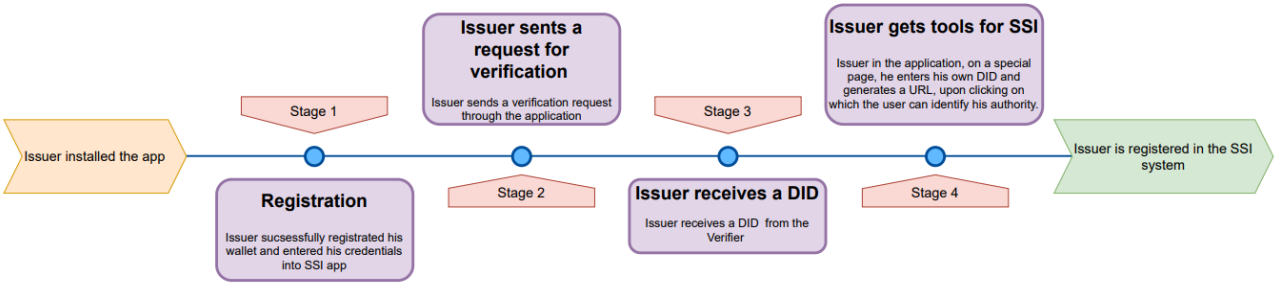


Fig 7. Issuer registration (actors: issuer, verifier)

After installing the SSI application, the Issuer account is registered in the application.

Next, the Issuer sends a verification request (stage 2).

After the verifier has received a request from the Issuer, if the Issuer belongs to real legal entities or organizations, the Verifier generates an Issuer record in the FreeTON blockchain and sends a unique identifier (DID) of the issuer, which is used in further interaction with users.

The fourth and final step in the issuer verification process is generating a URL that the user opens in the application as a string or as a QR code, which is then used in the SSI process (fig.7).

Thus, the presented CJMs form an idea of the technical design of the SSI system, in which the choice of screens and interfaces will be built to implement the chain of actions of users and other participants in the identification process.

Conclusion

The proposed Self-Sovereign Identity Framework has advantages over currently widespread identity systems. SSI makes life easier for users, speeds up government processes, and opens up new business opportunities. The subsequent development of the system requires maintaining the principles of scalability, universal access to data, decentralized management and minimal disclosure of user data. Safety and convenience - the main motivation of future users will allow to achieve the viral effect of the spread of SSI. Technological compatibility with existing identification systems will accelerate the integration of companies and government institutions into the proposed SSI concept.