Decentralized Identity Management: Building and Integrating a Self-Sovereign Identity Framework

Candidate: Luca Rota
Supervisors: Prof. Danilo Bazzanella,
Company Supervisors: Dr. Alfredo Favenza, Dr. Silvio Meneguzzo

1 Introduction and Objectives

The concept of identity has been prominently redefined throughout digital transformation, and now is the time to talk about digital identity. In today's society, where our physical and digital lives often overlap, identity management has become indispensable. Mainstream centralized systems might as well be powerful, but possess basic problems, like lack of user control and susceptibility to data breaches. In response to these challenges, the concept of *Self-Sovereign Identity* (SSI) emerged, as a suitable alternative. *SSI* is embedded on the decentralized concept and user-centric system, which allows individual to make assertive decisions, regarding their identity data. Unlike traditional identity management systems, *SSI* introduces an entirely new and secure paradigm, employing blockchain technology, that eliminates the need for third parties and prevents theft of identities.

That being said, the long road towards fulfilling *SSI*'s potential, does not come without its own challenges. Centralized and federal models, although as resilient as ever, keep failing to cope with the changes and evolution of the digital epoch. The challenges push forward a paradigm shift to a user-centric model, whereby people maintain authority over their identities. An implementation of this paradigm shift is the *SSI* model, which is founded on the notion of individual sovereignty and control.

The primary objective of this master thesis is to explore the field of digital identity, with particular attention to the *SSI* standards and the design. This solution makes use of tools, like Metamask and the Ethereum blockchain as part of its architecture specifically geared towards handling identity management challenges in an apt, secure and user-friendly manner. Next, the framework was seamlessly integrated into our Data Cellar project at Links Foundation, showcasing the overall applicability and usefulness of this framework to the real world.

2 Research Area

In addition to brief insights into blockchain technology, the history of identity, and a brief exploration of cybersecurity and cryptography in this area, the focus of this thesis has been on a state-of-the-art of the *SSI* model.

The birth of the idea of the *SSI* paradigm for digital identity management can be traced back to the early 1990s, when cryptographic techniques such as *Pretty Good Privacy* (PGP) were introduced. Christopher Allen's publication in 2016 then contributed greatly to the development of that model, which later evolved into a mature system that can grant people control or that grants people authority over their digital identity. Additionally, the integration of blockchain technology, has greatly boosted the growth of *SSI*, which offers a concrete framework to manage digital identities, due to its decentralized and immutable nature. Today, the *SSI* model stands as a leader in its field, enabling individuals to manage their digital identities themselves, providing a high level of privacy and security for its users.

The core components of *SSI*, which enable secure and reliable exchanges within the identity ecosystem, are:

- **Decentralized Identifiers (DIDs)**: *DIDs* form the basis of the *SSI* infrastructure, where every person, organization or entity will be uniquely identified in a decentralized manner. Unlike conventional identifiers, such as usernames or e-mail addresses, *DIDs* provide greater security and privacy because they do not require centralized authorities. A central element of *DIDs* is the *DID Document* (DDO), which represents information about a particular *DID*.
- **Verifiable Credentials (VCs)**: *VCs* are cryptographic certificates issued by a trusted authority that allow individuals to prove their attributes through verifiable claims. *VCs*, stored in digital wallets, offer users the advantage of controlling what information is disclosed to the public, ensuring that privacy and security are maintained. Starting with information from one or more *VCs*, users can make selective disclosures using *Verifiable Presentations* (VPs).
- **Blockchain**: Blockchain technology, within the *SSI* model, acts as a decentralized, verifiable ledger in which immutability is guaranteed. Blockchain establishes a system of transactions, including *DIDs* and *VCs*, making trust and integrity a fundamental part of the identity ecosystem. Through the use of consensus mechanisms and cryptographic functions, blockchain technology enhances security and transparency, while the chronological and tamper-proof

nature of blockchain transactions safeguards the secure storage and validation of data, thus ensuring the principles of a decentralized identity system.

At the center of the decentralized architecture used by the *SSI* model is the Trust Triangle. The three main actors at play, which form the foundation of trust and integrity within this decentralized identity management system, are: Holder, Issuer and Verifier. The Holder, representing the individual user, uses a digital wallet to generate unique *DIDs*, which serve as cryptographic identifiers and to hold the *VCs* that will be issued to him. Issuers are regarded as trusted entities and are responsible for issuing *VCs*, signing them with their private keys to establish authenticity and integrity. At the time of interaction, Holders provide *VPs*, which are attestations containing some information from one or more *VCs*, to Verifiers. By validating the cryptographic signatures embedded in the credentials and confirming the credibility of the issuer through public *DIDs* on the blockchain, the Verifiers ensure the integrity of the shared information.

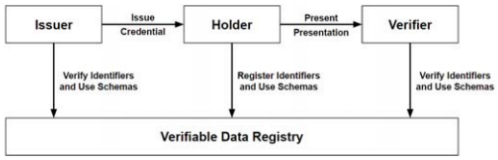

Figure 1: The Trust Triangle's workflow.

3 Contributions of the thesis

This master thesis is a contribution to the field of research in *SSI* studies, specifically in practical application, by examining the best fit solutions for the realization of decentralized identity management frameworks using the *SSI* model and blockchain technology. The main goal was to build an independent framework in the form of a browser *Decentralized Application* (DApp) built using React to create a user-friendly frontend, and JavaScript to create a robust backend. Next, this authentication system was integrated in an existing real project to demonstrate its practical applicability.

3.1 Solutions adopted

After an analysis of the solution adopted by the major *Identity Management System* (IDMS) based on blockchain, such as ShoCard, Sovrin Network, and uPort, and the most widely used libraries in the *SSI* domain, such as did-indy and algo-did and ethr-did, the latter was chosen as the basis for *DID* management, given its robustness and well-documented nature. This library is also developed within the Ethereum ecosystem, which has been found to be the perfect blockchain for this purpose, given its widespread adoption and for its support of smart contracts, which are essential for decentralized identity management. In addition, the decision to integrate MetaMask was fundamental, as it enabled simplified transactions on the blockchain, improving *DApp* development with Ethereum and ensuring secure storage of users' private keys. This tool then allows users to conveniently and quickly use the smart contract, that serves as the registry for the system, which is written in Solidity and has been deployed on Ethereum's testnet, namely Sepolia and Goerli, using Truffle. It provides functions for registration, de-registration, and user state verification; the first two for a fee, as they require the blockchain to change state.

Next, the focus shifted to the management of *VCs*. The initial idea was to use the *VCs*, to certify user information and create immutable credentials, that are issued and signed by the browser *DApp*, in order to guarantee user registration on the blockchain and to keep immutable the information provided by the user. However, two significant challenges emerged: the lack of *VCs* issued by the certified bodies, thus requiring manual entry of user data during registration, and the fact that, non-proprietary wallets, that can store and manage *VCs* in a secure way, in order to allow users to make selective disclosure, are not currently available. Given these limitations, after some research on what possible tools to use for managing these *VCs*, such as Masca, the final choice was to use the did-jwt-vc library for creating and verifying *VCs*; they will be released from the *DApp* browser, and then kept in a secure storage by the user.


```
{
  "credentialSubject": {
    "name": "Luca",
    "surname": "Rota",
    "email": "lucarota@gmail.com",
    "profession": "Studente",
    "country": "Italy",
    "region": "Liguria",
    "id": "did:ethr:0x539:0x7CDB5903C9caB36a5B0bF7F205500865608c2672"
  },
  "issuer": {
    "id": "did:ethr:0x539:0x2F506eaaFfe39edD456cA74F13c74D6d80768Eb0"
  },
  "type": [ "VerifiableCredential" ],
  "@context": [ "https://www.w3.org/2018/credentials/v1" ],
  "issuanceDate": "2024-01-30T18:40:27.000Z",
  "proof": {
    "type": "JwtProof2020",
    "jwt": "eyJhbGciOiJFUzI1NkstUiIsInR5cCI6IkpXVCJ9.eyJ2YyI6eyJAY29udGV4dCI6WyJodHRwczovL
  }
}
```


Figure 2: The VC emitted by the SSI framework.

3.2 The SSI framework created

The framework created allows, following the guidelines of the *SSI* model, for decentralized management of users' digital identity. Created in the form of a browser *DApp*, it is supported by HTTPS, to ensure secure storage of authentication tokens, within session cookies. This is done through SSL certificates, generated using the OpenSSL and mkCert tools. This framework thus allows to offer an authentication process, consisting of three main phases: access, sign-up and sign-in.

In the access phase, users communicate with the MetaMask extension to connect to the *DApp* and unlock their wallet to make interaction with the blockchain possible. After successfully connecting, users are granted limited access to the *DApp*'s functionality. The application is able to constantly detect the presence of the connec-

tion to MetaMask and which network is selected within it, so that it can return the user to the initial state, should it be necessary. The sign-up process includes submitting the user's data through a form, which will be considered, given the limitations highlighted earlier, as trusted and will constitute the payload of the *VC* that will be issued by the *DApp* browser, through the server, following the user's registration in the smart contract registry. This registration is done through a transaction in the blockchain, upon payment of a fee, and through the MetaMask wallet. After registration, users are required to download the *VC* issued to them and save it themselves in a secure location. In the sign-in phase, users authenticate with their selected account within the MetaMask wallet, providing the *VC* that was issued to them during the sign-up phase and signing a message, containing a nonce (useful for avoiding replay attacks), with their private key. The *DApp* browser will then check the validity of the *VC* received, and then the server will instead check the validity of the user's signature, which guarantees that the request is from the owner of the *VC* provided. Once the user's identity has been verified, the server will respond with a signed JWT token containing information taken from the provided *VC*, which will be stored in session cookies and provide the user with access to *DApp* functionality based on his authorizations.

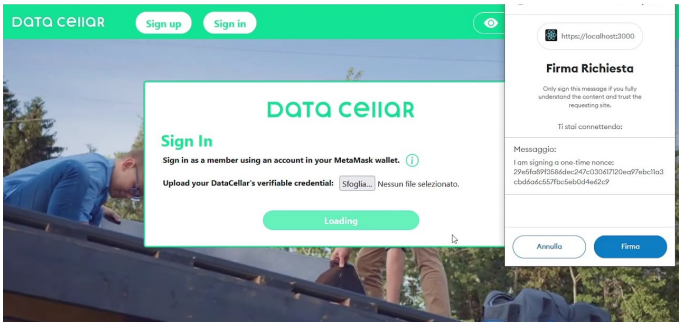

Figure 3: The Sign In page with sign message pop-up.

3.3 Project integration

The integration of the self-sovereign Identity (SSI) framework into the Links Foundation's Data Cellar project requires an adaptation of the previously created decentralized identity management system and the development of an entire *Graphical User Interface* (GUI) for the *DApp*. Data Cellar is an EU-based energy data center leading the development of a federated energy data space for local energy communities. Initially, data center services were centralized, but the purpose of this project is precisely to decentralize various aspects for greater security and efficiency, including that of user identity management. The initial project setup encompassed smart contracts for the energy data digitization, a backend written in NestJS, and a frontend generated via Swagger. The development environment uses Docker containers for simulation, which include Ganache for Ethereum blockchain simulation, Postgres for off-chain database, and Redis for queue handling.

The integration process consisted primarily of a modification to the Docker container, adaptation of the *SSI* framework for use with Ganache, and configuration of MetaMask for interaction with it. Numerous changes were then made to the code, to switch API functions from backend to frontend so that Metamask could be used for signing user transactions, thus completely eliminating the need for a centralized database and queue management. The final *DApp*, with a dynamic frontend, offers enhanced security and usability for the user. Features include user registration, dataset display, license management, token balance display, and so on. The backend was still NestJs, which focused on user authentication and credential generation. The frontend, based on React, offered easy-to-use navigation and smooth interaction with blockchain features. The application's main pages are the marketplace for data transactions and the user profile page for data uploading, license management, and account settings. Users can create, edit, and delete datasets and licenses, purchase licenses and consume purchased licenses. The *DApp* also provides an account deletion feature, hence users can remove their accounts from the platform.

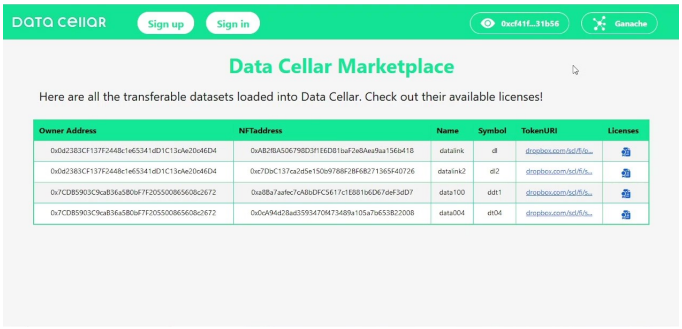

Figure 4: The Data Cellar marketplace's Home page.

4 Conclusions and Future Work

In conclusion, this thesis has examined the prospect of *SSI* and how it can be applied to identity management digitally. Even if *SSI* is a powerful alternative to centralized systems, it should also be mentioned that both *SSI* and blockchain technology are still developing. The thesis put forward the idea of a decentralized model for managing *SSI*, through the implementation of a framework for managing the entire user authentication process and its integration into a real project. Addressing limitations identified during implementation suggests two key advancements: the use of *VCs* from accredited organizations and the development of non-proprietary wallets for credential management.

In summary, although this thesis has provided the groundwork for future work on identity management, there is a lot more that needs to be done to boost this emerging field. Recognizing the limitations identified and exploiting the research opportunities, will take us a step closer towards a secure and privacy preserving digital identity ecosystem.