Politecnico di Torino

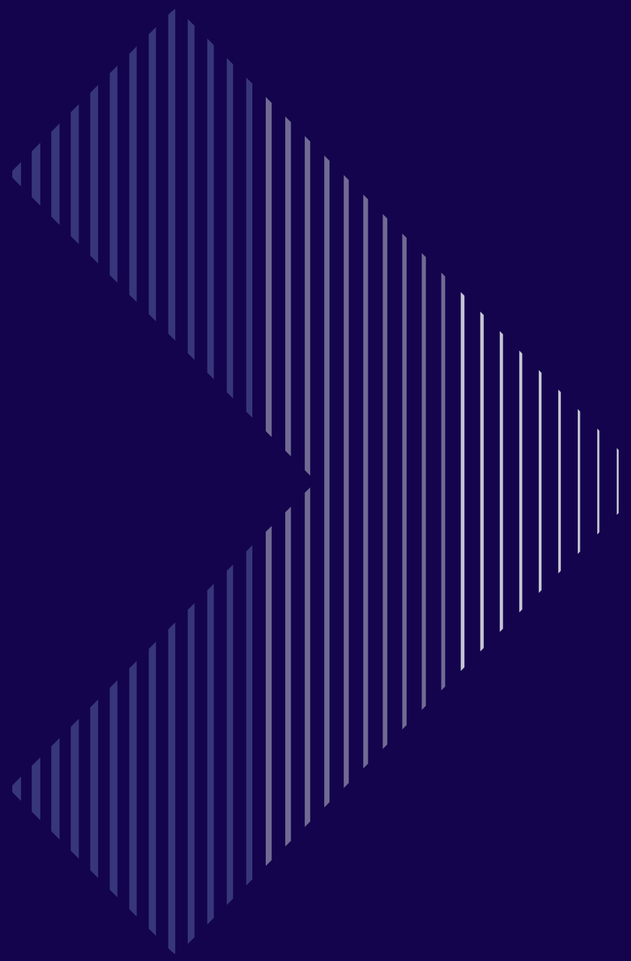
FONDAZIONE links PASSION FOR INNOVATION

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

MASTER'S DEGREE IN COMPUTER ENGINEERING
CYBERSECURITY FOCUS

Candidate: LUCA ROTA
Supervisors: D. Bazzanella, A. Favenza, S. Meneguzzo

Contents



Introduction

- Increasing digitization reshapes our conception of identity, necessitating new approaches to identity management.
- Growing computational power exposes weaknesses in centralized systems, posing risks to user's data security.
- Decentralized, user-centered models offer greater control, ensuring a more resilient digital identity ecosystem.

Digital identity management

Siloed identity management

One account for each service.

Centered identity management

One account, multiple services, same identity provider.

Federated identity management

One account, multiple services, different identity providers.

User – centric indentity management

Users control their personal data.

Self-Sovereign Identitiy (SSI) model

Decentralized Identifier (DID)

- Unique, user-controlled identifier.
- DID Document (DDO).
- Stored in a distributed ledger.

Verifiable Credential (VC)

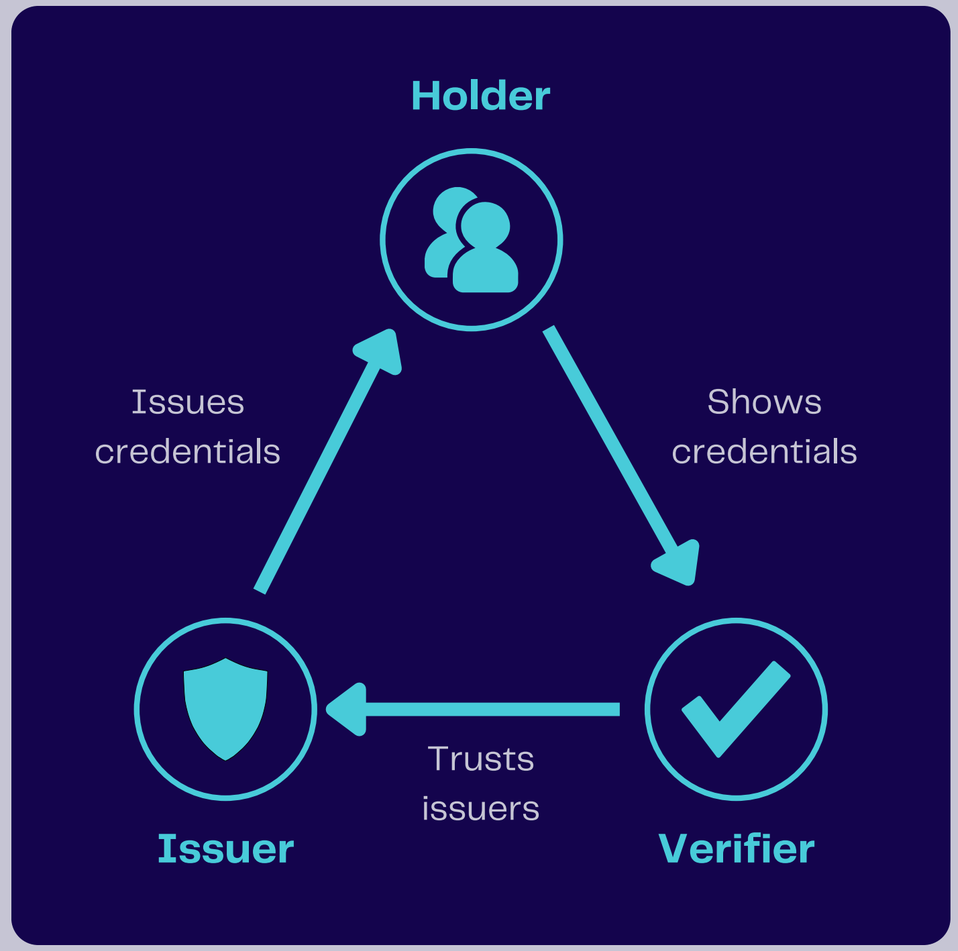
- Claim about a user's identity.
- Verifiable Presentation (VP).
- Proof ensures authenticity.

Blockchain

- Distributed Ledger Technology.
- Immutability, tamper-proof.
- No central authority.

Trust Triangle

- **Holders:** Own their DIDs, store VCs in digital wallets, control information reveal.
- **Issuers:** Confirm users information, sign VCs with their private key.
- **Verifier:** Check VCs, rely on blockchain to confirm issuer credibility.



Contribution of the thesis

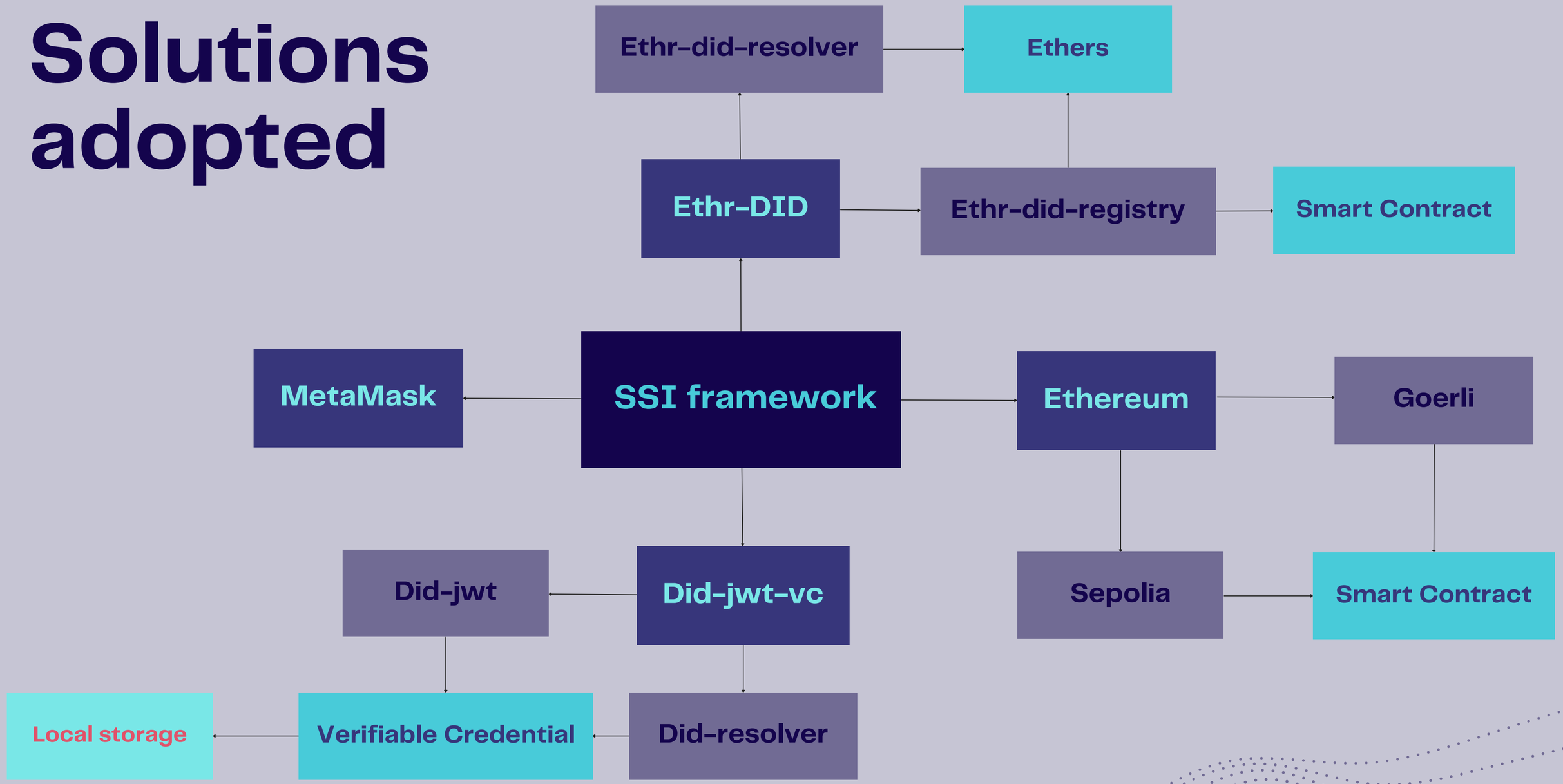
Creation of the SSI framework

The first goal was to build the standalone framework for the decentralized user identity management, applying the SSI models, based on blockchain technology. In this model, the identity management process consists of authentication and authorization procedures that do not rely on centralized systems or databases. Blockchain, smart contracts, DIDs and verifiable credentials are used for this purpose.
Built using React and JavaScript. Secured by HTTPS.

Integration in a real project

The second objective was to demonstrate the real utility and effectiveness of the previously created decentralized identity management SSI framework. To do that, it was integrated, as authentication process into an ongoing project at Links Foundation, known as DataCellar. Later, in addition to the integration of this system, the entire GUI of the application was also developed.
Built using React, JavaScript and NestJs.

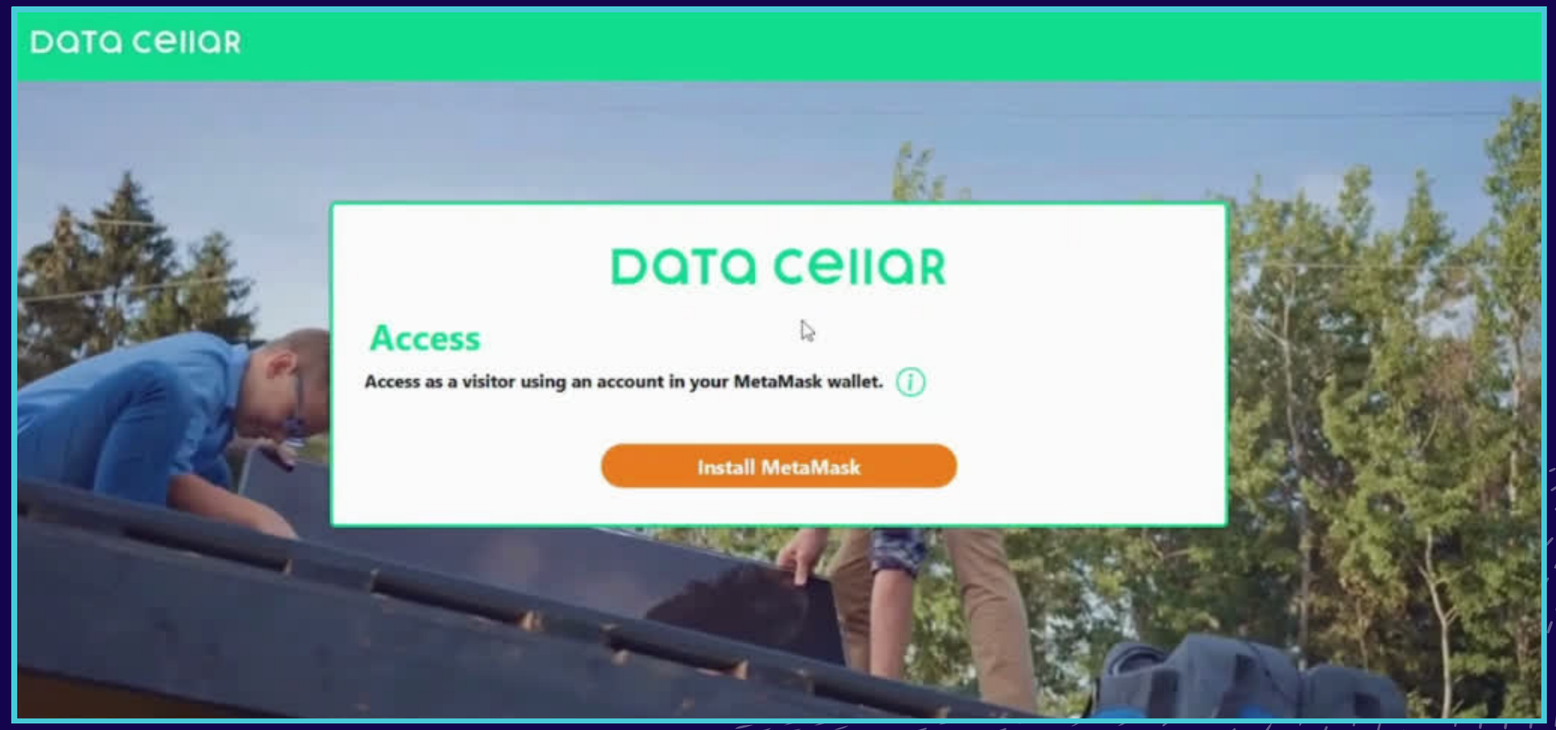
Solutions adopted



The SSI framework's user interface

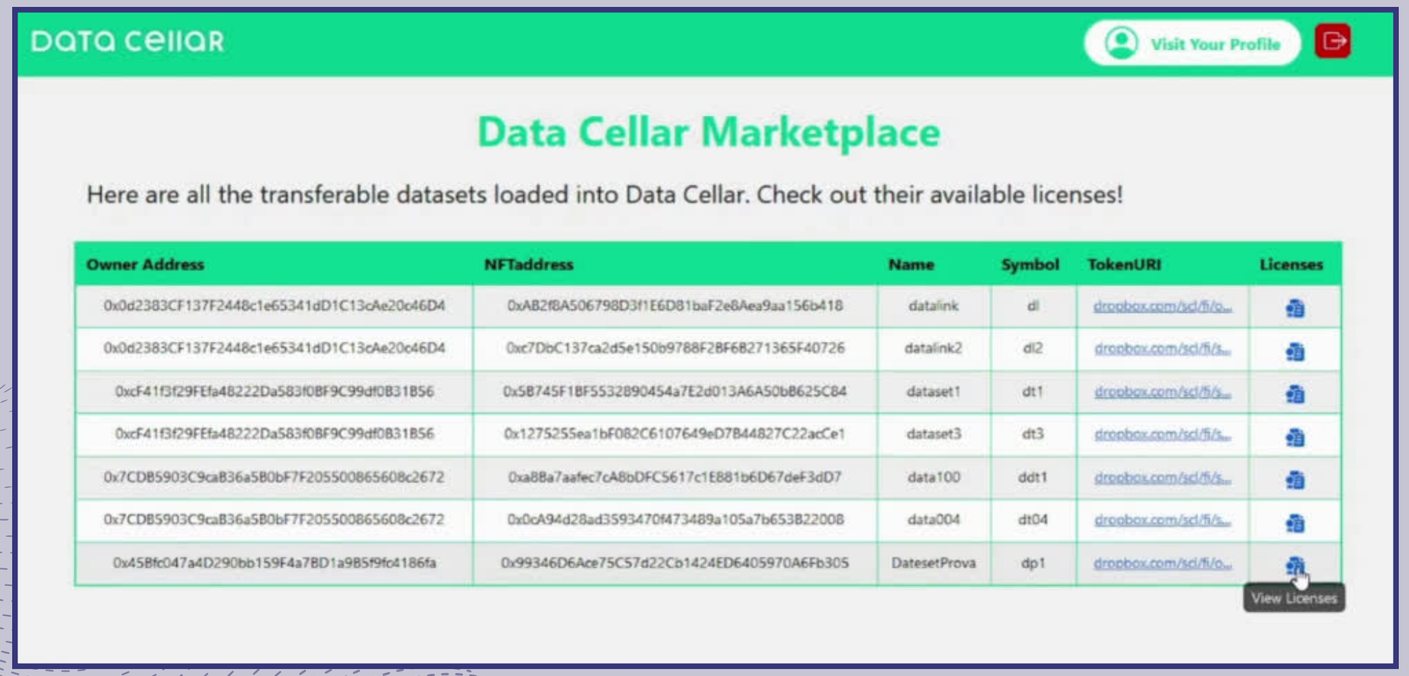
The Authetication process

- Access Phase: User connects his MetaMask wallet to the browser DApp to access as visitor.
- Sign-Up Phase: User provides his data, makes a transaction to register, and the browser DApp returns the VC to him.
- Sign-In Phase: User provides the VC, signs a message, and the dApp, if verifications are successful, generates a JWT to be placed in session cookies for authorizations. The user is authenticated.



Project integration

The target project for integration was DataCellar. DataCellar is an EU-based energy data center leading the development of a federated energy data space for local energy communities.



Project before integration

- Smart contract's API in the backend
- Docker : Ganache, Postgres and Redis
- No user interface (Swagger)

Project after integration

- Decentralized authentication process
- Smart contract's API in the frontend
- Docker : Ganache / No Database
- New user-friendly interface
- Introduced deregistration function

Conclusions and future works

Thesis's contributions

- Researching the best solutions in the SSI ecosystem
- Creation of the SSI framework
- Integration in a real project

Limitations found

- Absence of VCs issued by the certified bodies
- Lack of wallets capable of making selective disclosure

Future works

- Find trusted VCs
- Build a non-proprietary wallet to manage VCs
- Develop DataCellar's functions

Politecnico di Torino

FONDAZIONE links
PASSION FOR INNOVATION

Thank you for your attention

Presented by Luca Rota