Securing Digital Identities with Blockchain and Smart Contracts

Lucía Muñoz, Álvaro Fernández, Daniel Paredes

Lucía Muñoz Solanas,
VICOTMECH

lmunoz@vicomtech.org

SHORT BIO

LUCÍA MUÑOZ SOLANAS

Education

- **Mathematics** Degree from the University of Zaragoza.
- Master's Degree in **Artificial Intelligence** from the Valencian International University.

Current role

- Working at **VICOMTECH** (since 2022) in the Digital Security department.

Specializations

- **Cryptography** and **encryption** techniques.
- **Identity management**.
- **Blockchain** technologies (Ethereum, Hyperledger-Fabric).

CONTENTS

01

INTRODUCTION

02

SELF-SOVEREIGN IDENTITIES

03

VDR AND SMART CONTRACTS

04

CONCLUSION AND FUTURE WORK

INTRODUCTION

DIVINE

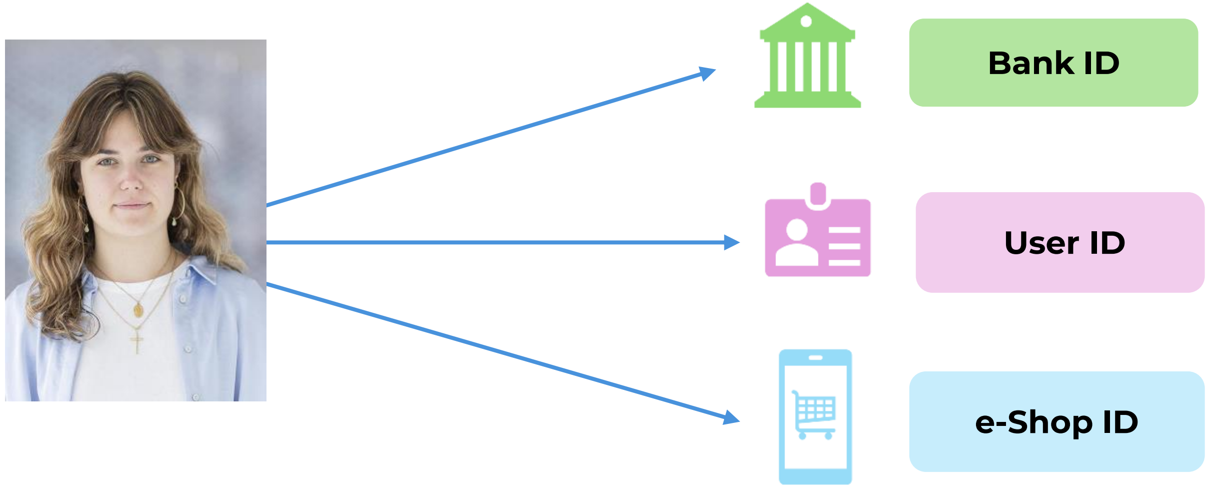
- **European Project** of the **agri-food** sector.
- Based on the creation of a **Data Space ecosystem.**
- It provides participants with **access** to a variety of **resources**.
- Owners provide **specialized agricultural applications**.

OBJECTIVE

- Develop an advanced Self-Sovereing Identity (**SSI**)-based Identity Management System (**IdM**), focused on authentication and authorization, for this Data Space that alings with European regulations (**eIDAS2, GDPR**).

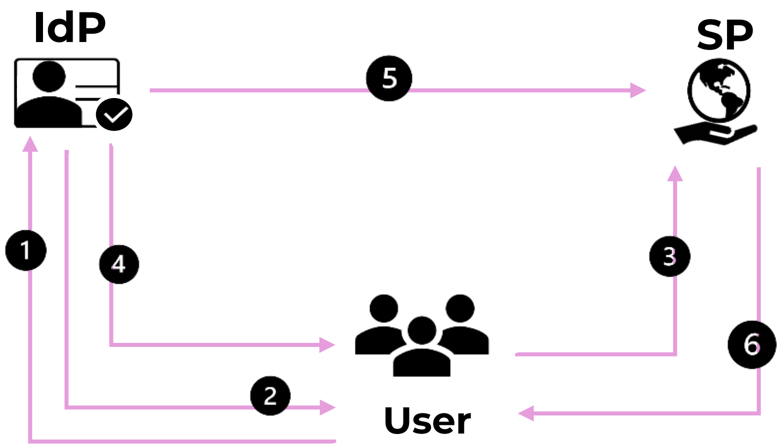
DIGITAL IDENTITY AND IDM

- **Online representation of individuals**, used for identification and authentication purposes.



In an IdM there are **two key components**:

- **Identity Provider (IdP):** Authenticates users and provides identity information to other systems.
- **Service Provider (SP):** Provides services to users, relying on identity information from IdPs.



CONTENTS

01

INTRODUCTION

02

SELF-SOVEREIGN IDENTITIES

03

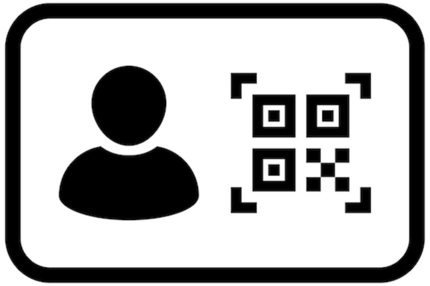
VDR AND SMART CONTRACTS

04

CONCLUSION AND FUTURE WORK

SELF-SOVEREIGN IDENTITIES

- Digital IdM that gives user **full control** over their **credentials** without relying on centralized authorities.
- **No need to directly verify credentials** with trusted third parties thanks to verifiable data registries (VDR).
- Uses **cryptographic techniques** to ensure data integrity and authenticity.
- **Secure and transparent recording** of all transactions through database replication and computational trust.
- **Digital wallets** securely store private keys, authenticators, and digital credentials securely and reliably.



ENTITIES IN THE SSI ECOSYSTEM

HOLDER

- Responsible for **storing** and **presenting** the credentials.

ISSUER

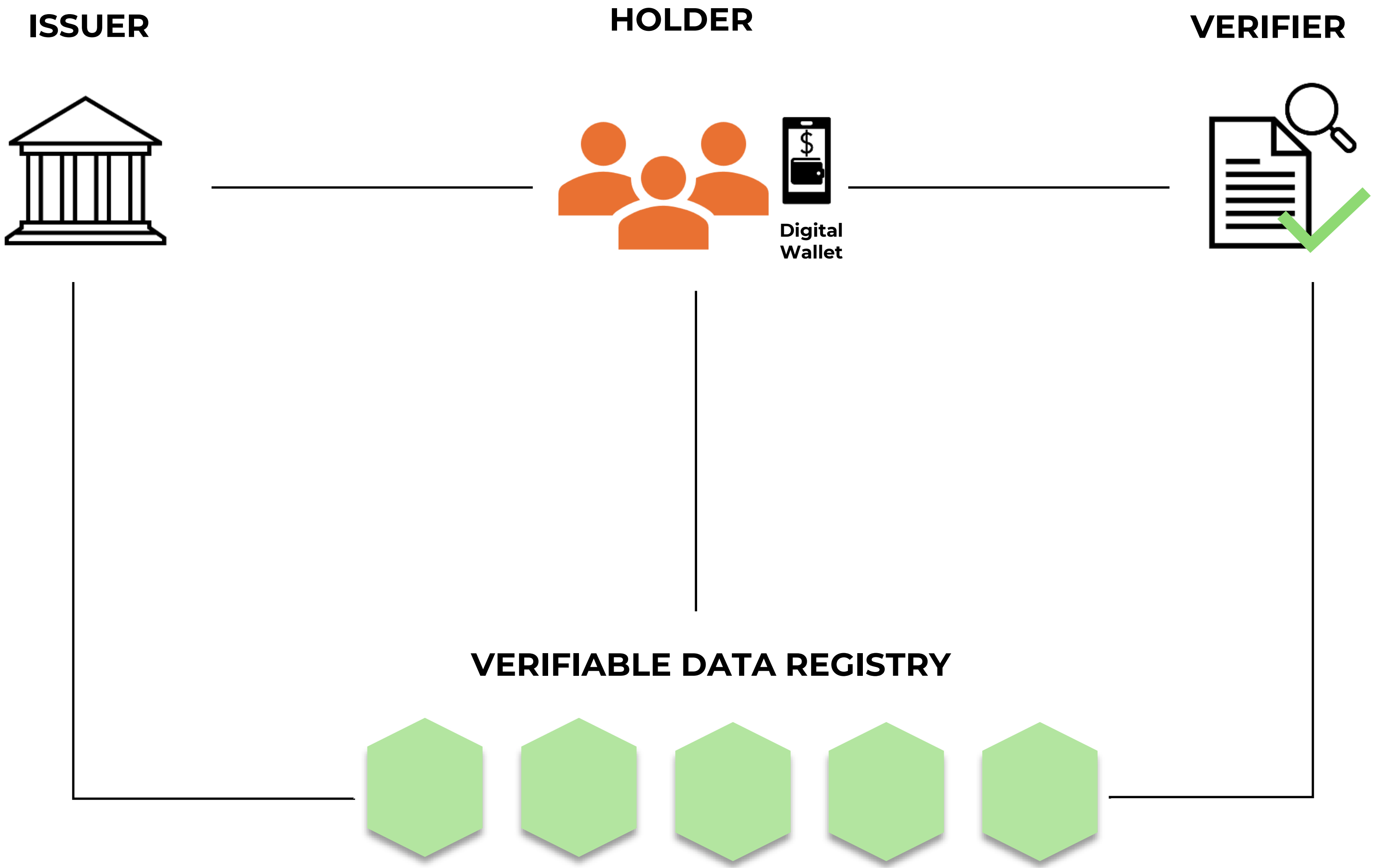
- Trusted entity or individual authorized to **issue** and **sign** the credentials.

VERIFIER

- Entity or individual who **validates** the **credentials** that **are presented** by the holder.

VERIFIABLE DATA REGISTRY (VDR)

- System or database where the **public keys and necessary data are stored to verify** credentials, without relying on Issuer (Blockchain).



CONTENTS

01

INTRODUCTION

02

SELF-SOVEREIGN IDENTITIES

03

VDR AND SMART CONTRACTS

04

CONCLUSION AND FUTURE WORK

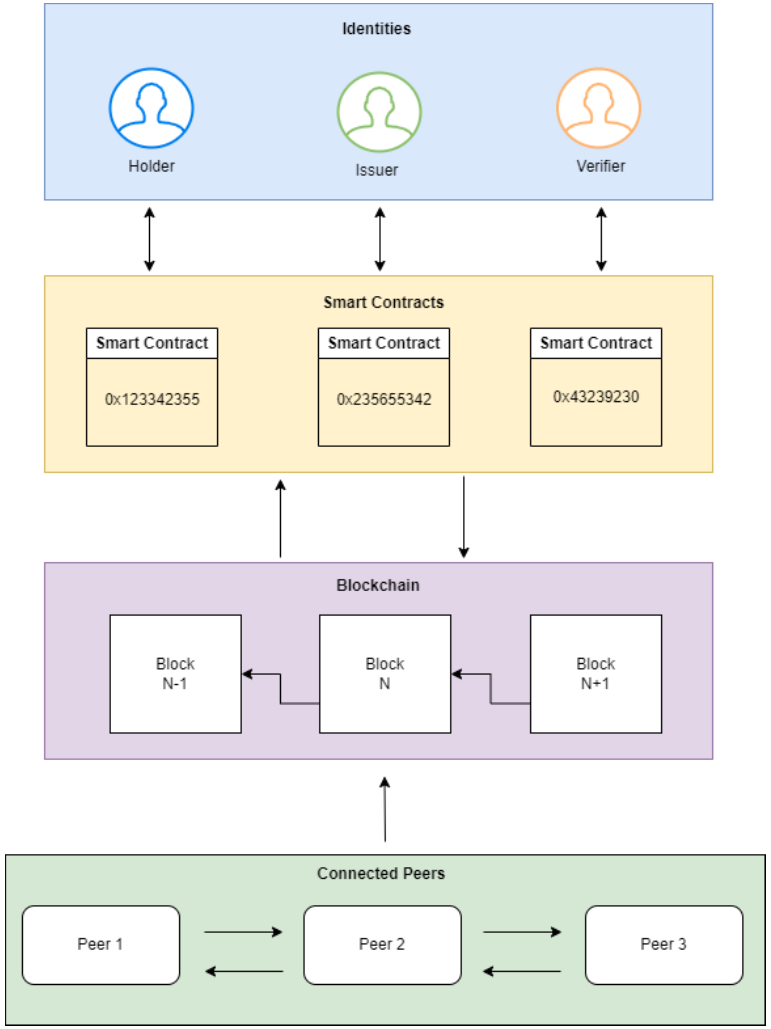
ETHEREUM VDR

- The **VDR** is a **blockchain-based registry** that is immutable and transparent.
- Stores credential data, enabling **Verifiers** to authenticate information without direct contact with the **Issuer**.
- Registered data is **unmodifiable**, ensuring credential integrity.
- Operates on a **private Ethereum blockchain** with three nodes.
- Uses Proof-of-Work (**PoW**) as its **consensus mechanism**.

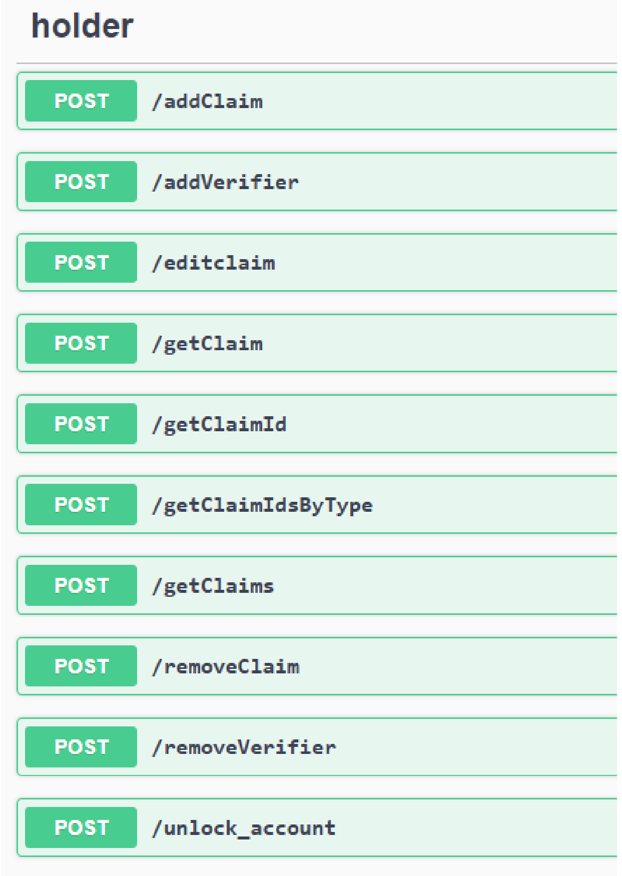
ethereum

SMART CONTRACTS

- **Self-executing programs** operating on the Ethereum blockchain, following predefined rules.
- **Custom** Smart Contracts in **Solidity** developed for each **participant** in the SSI ecosystem.
- Automates the **issuance** and **verification** of credentials.
- Based on the Ethereum **standards ERC-735** (Credential Management) and **ERC-725** (Key and Permission Management).

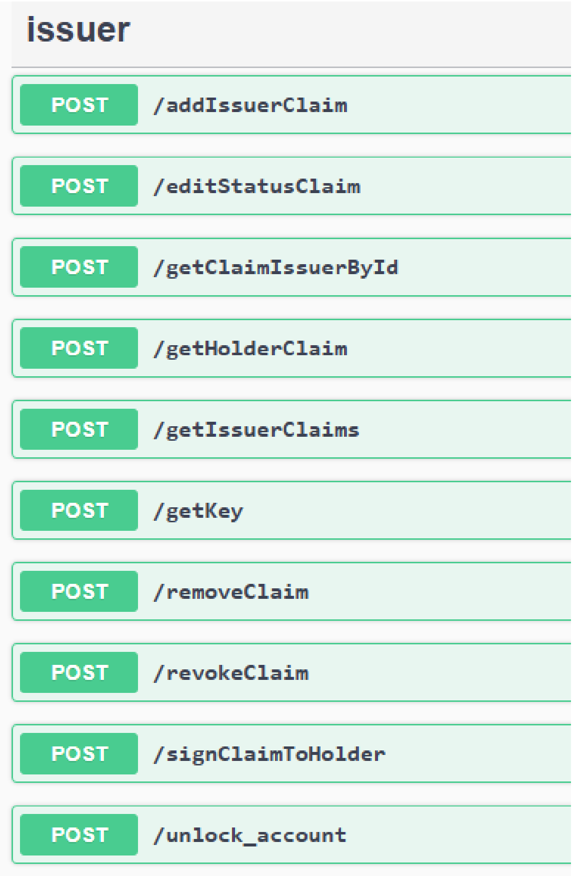


SMART CONTRACTS



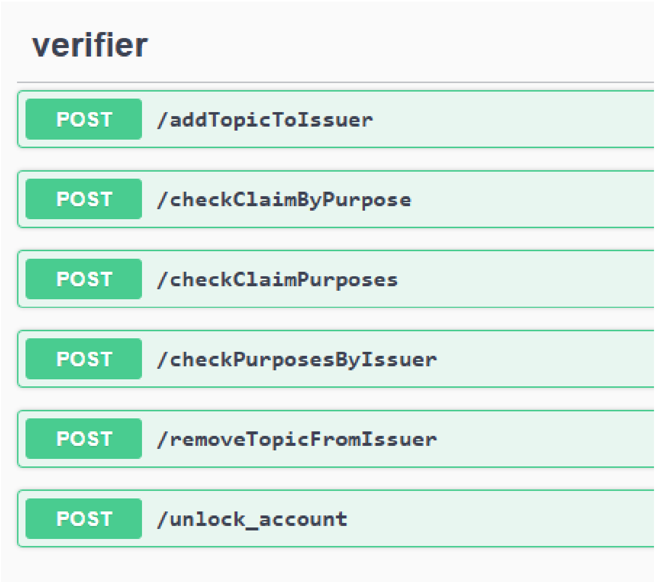
holder

- POST /addClaim
- POST /addVerifier
- POST /editclaim
- POST /getClaim
- POST /getClaimId
- POST /getClaimIdsByType
- POST /getClaims
- POST /removeClaim
- POST /removeVerifier
- POST /unlock_account



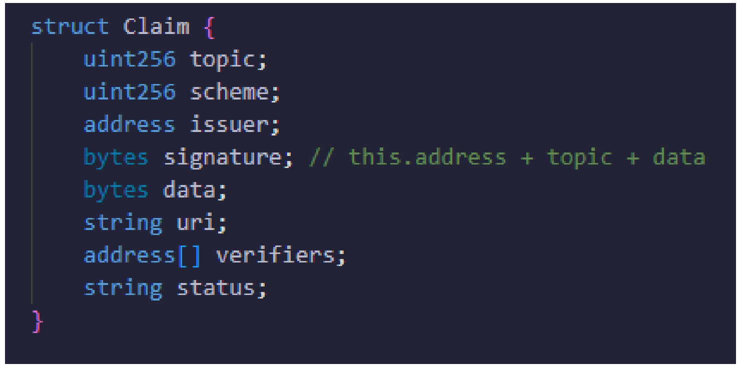
issuer

- POST /addIssuerClaim
- POST /editStatusClaim
- POST /getClaimIssuerById
- POST /getHolderClaim
- POST /getIssuerClaims
- POST /getKey
- POST /removeClaim
- POST /revokeClaim
- POST /signClaimToHolder
- POST /unlock_account



verifier

- POST /addTopicToIssuer
- POST /checkClaimByPurpose
- POST /checkClaimPurposes
- POST /checkPurposesByIssuer
- POST /removeTopicFromIssuer
- POST /unlock_account



```
struct Claim {
    uint256 topic;
    uint256 scheme;
    address issuer;
    bytes signature; // this.address + topic + data
    bytes data;
    string uri;
    address[] verifiers;
    string status;
}
```

USE CASE

1. Bob and Alice creates an account in the IdP→ **HOLDER** identity
2. Bob registers an application the IdP → **ISSUER** identity
3. Alice request access with a role in the application → **ADD CLAIM**
4. Bob receives the requests and sings the claim → **SIGN CLAIM**
5. Alice tries to access to the application → **GET CLAIM**
6. The IdP service (VERIFIER) checks the user credentials (user + password) and the claim → **VERIFY CLAIM**

CONTENTS

01

INTRODUCTION

02

SELF-SOVEREIGN IDENTITIES

03

VDR AND SMART CONTRACTS

04

CONCLUSION AND FUTURE WORK

CONCLUSION AND FUTURE WORK

CONCLUSIONS

- A **SSI-based** identity management system has been **implemented** and now is **functional**.
- For this SSI-based system we have a **digital wallet** for users to manage their credentials, both in web and mobile application format.

FUTURE WORK

- Migrate the blockchain format to align it with the **European Blockchain Services Infrastructure (EBSI):**
  - Change **credential format**.
  - Smart Contracts are replaced by DIDs.
  - Credentials are not stored in the blockchain. They are stored by the holder in the digital wallet.
- Transitioning from Proof-of-Work to Proof-of-Stake.

vicomtech

MEMBER OF BASQUE RESEARCH
& TECHNOLOGY ALLIANCE

THANK YOU!

✉ lmunoz@vicomtech.org

🌐 www.vicomtech.org