



UNIVERSITÀ
DI CAMERINO

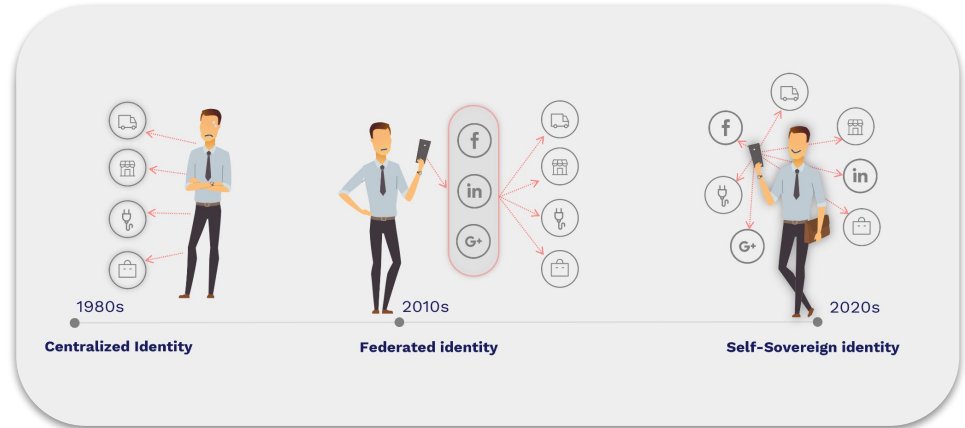
ChorSSI: A Model-Driven Framework for Self-Sovereign Identity on Blockchain

Tommaso Cippitelli, Alessandro Marcelletti, **Andrea Morichetta**
University of Camerino

Motivation

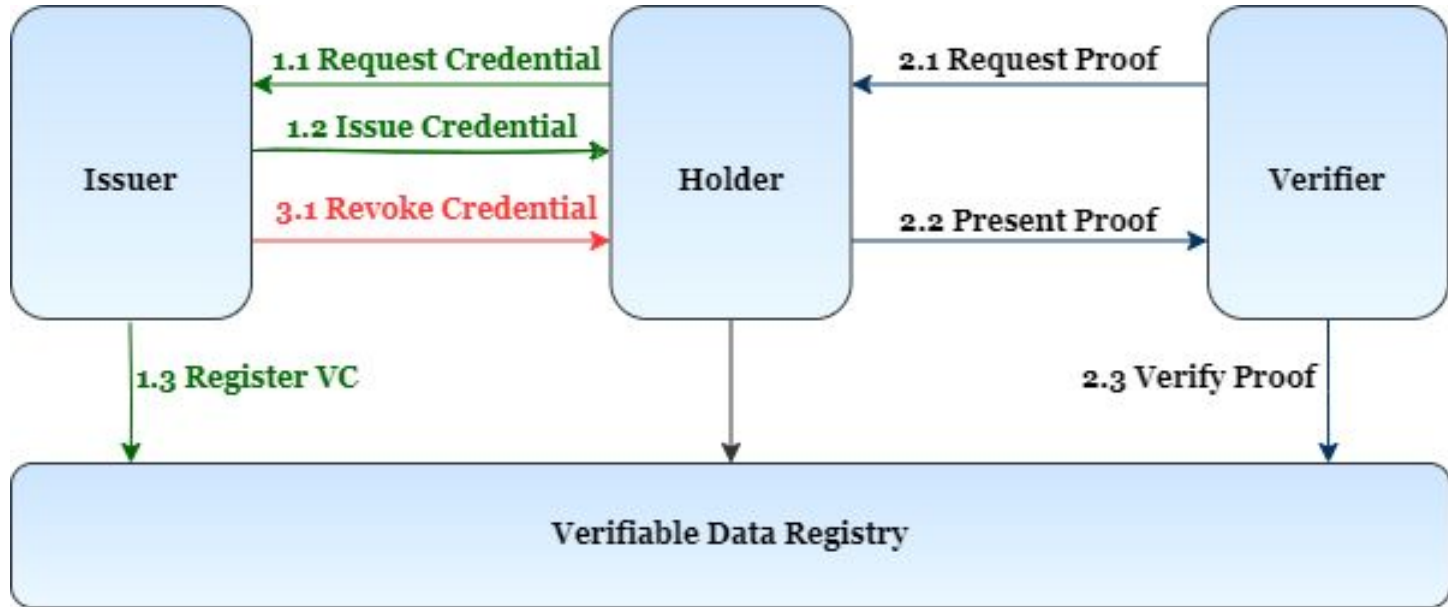
Identity management systems manage digital identities and their interconnection, permitting to identify people in digital activities. However:

- Centralized systems -> security **vulnerabilities**
- Need to rely on a **trusted third party**
- Lack of adequate **data ownership** and **control**



Self Sovereign Identity is a decentralised identity model that provides **individuals control over their personal data** and allows them to share this data securely without having to rely on a single central authority

SSI Concepts



Main Objective

PROBLEM

Complexity in the development of self-sovereign identity system represents a barrier to its adoption¹



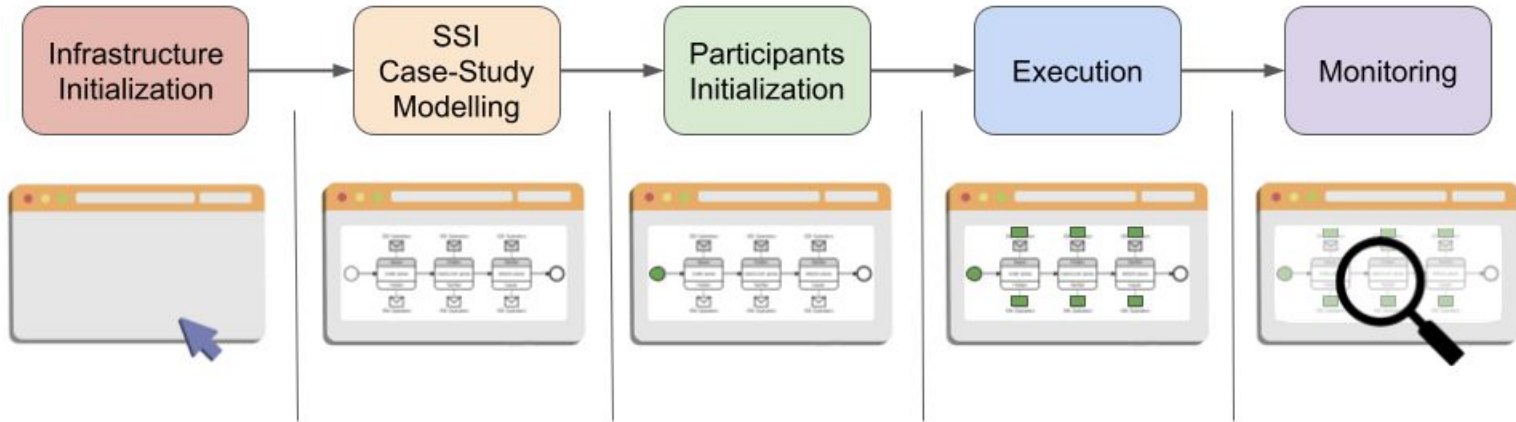
PROPOSED SOLUTION

Create **support** for technological development

Model-driven approach for automatic software development

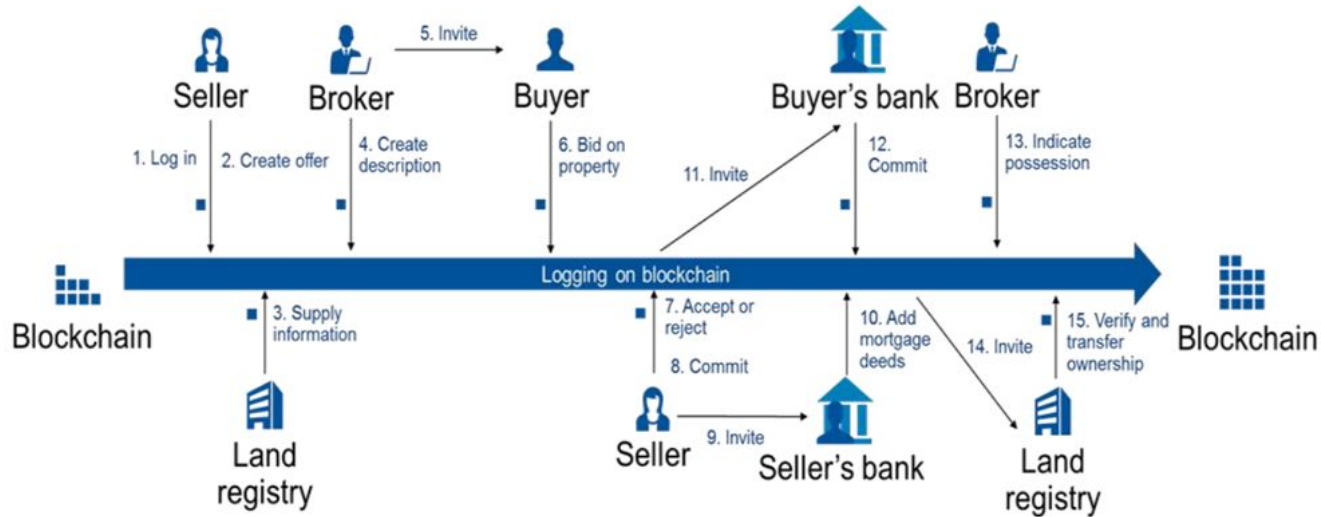
1. Sarah Manski. "Distributed ledger technologies, value accounting, and the self sovereign identity", 2020.

ChorSSI Methodology

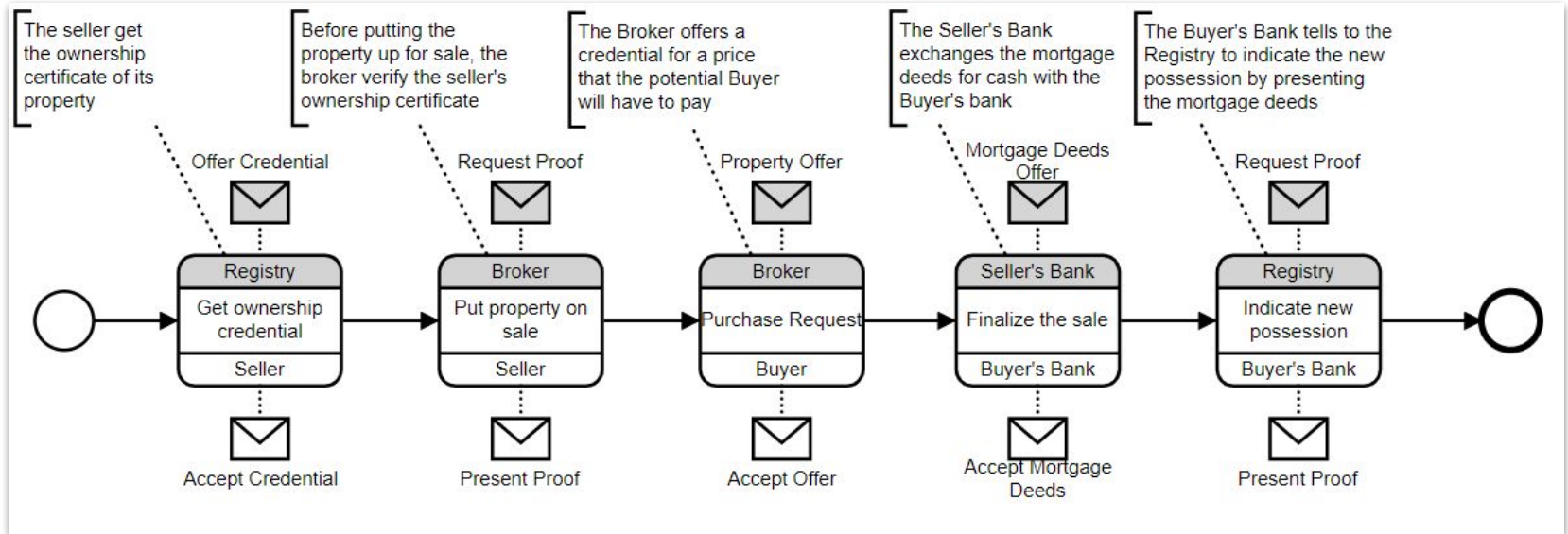


Use Case

Chromaway property transactions – Sweden

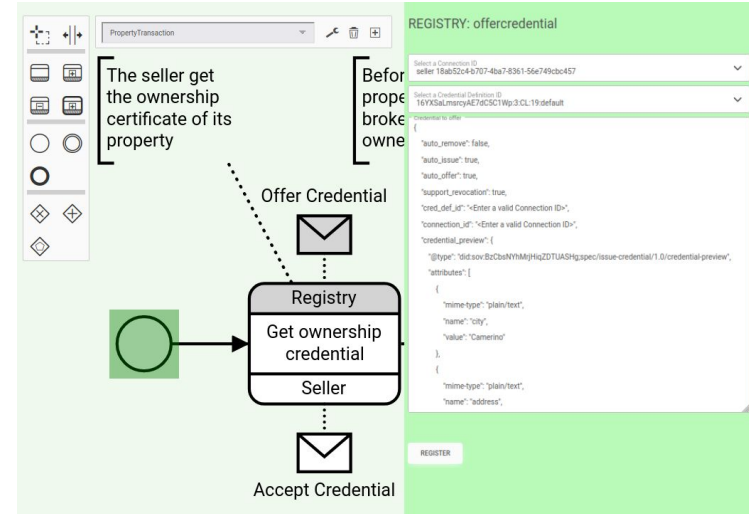
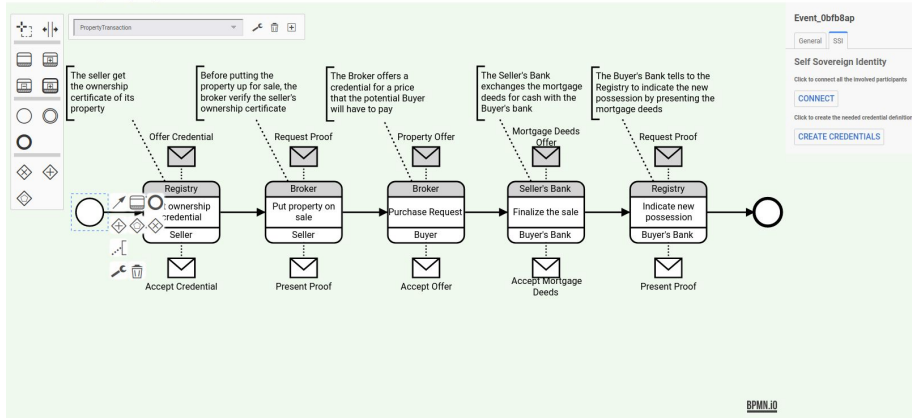


Chromaway BPMN model



ChorSSI implementation

Choreography SSI



ChorSSI implementation

SELLER: presentproof

Select a Presentation Exchange ID
98c1e874-8e31-46c2-b331-b6d2223660c

Request received

```
[
  {
    "presentation_exchange_id": "98c1e874-8e31-46c2-b331-b6d2223660c",
    "auto_verify": false,
    "updated_at": "2023-05-02T14:14:40.811877Z",
    "trace": false,
    "connection_id": "f915b9a1-353f-40c6-bb60-4151479f3f8f",
    "presentation_request_dict": {
```

Select a valid Credential
1fb273d9-1f4c-4401-ac46-5d97d890542d

Credential

```
[
  {
    "cred_info": {
      "referent": "1fb273d9-1f4c-4401-ac46-5d97d890542d",
      "attrs": {
        "city": "Camerino",
        "purchase_date": "2021/01/01",
        "number_of_rooms": "8",
```

REQUEST

Agents

SELLER	REGISTRY	BROKER	BUYER	SELLERBANK	BUYERBANK
✓	✓	✓	✓	✓	✓

Credential

16YXSaLmsrcyAE7dC5C1Wp:2.ownershipSchema:1.0

Schema Id: 16YXSaLmsrcyAE7dC5C1Wp:3.CL:19.default

amplitude: 200mq

purchase_date: 2021/01/01

address: Via Madonna delle Carceri

timestamp: 2022/01/01 15:40:30

city: Camerino

number_of_rooms: 8

Not Revoked

Issued Credential

b0847c47-6563-4dbb-a753-f6fa739b4485

Schema Id: 16YXSaLmsrcyAE7dC5C1Wp:2.ownershipSchema:1.0

Credential Id: 16YXSaLmsrcyAE7dC5C1Wp:3.CL:19.default

Issued to: 6c79693-3ea8-4674-8f2f-f8bb3a490421

[REVOKE](#)

Presentation

Proof of mortgage deeds

Id: fffe027e979f47aa-af3a-bfba6570430a

Created at 2023-05-02T15:06:47.694411Z

Verified

Created Schemas

ownershipSchema

16YXSaLmsrcyAE7dC5C1Wp:2.ownershipSchema:1.0

purchase_date

number_of_rooms

timestamp

amplitude

city

address

Credential Definition

16YXSaLmsrcyAE7dC5C1Wp:3.CL:19.default

Schema Id: 19

Tag: default

Version: 1.0

To resume

Conclusion

- We presented a model-driven **methodology** allowing to overcome the SSI complexity problem, making SSI accessible to a wider audience
- We proposed a model-driven **framework** that automatically perform SSI operations from models
- We developed a specific **use case** that demonstrates the functionality and usability of the framework

Future Works

- **ChorSSI access management**
- Introduce **multi-tenancy**
- **Enrich** expressiveness of the model



Thanks for the attention!
andrea.morichetta@unicam.it