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

Tommaso Cippitelli, Alessandro Marcelletti, Andrea Morichetta
University of Camerino

5th Distributed Ledger Technology Workshop (DLT 2023)
Identity management systems manage digital identities and their interconnection, permitting to identity 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

Issuer → Holder

1.1 Request Credential
1.2 Issue Credential
3.1 Revoke Credential
1.3 Register VC

Holder ➔ Verifier

2.1 Request Proof
2.2 Present Proof
2.3 Verify Proof

Verifier ➔ Issuer

Verifiable Data Registry
**Main Objective**

**PROBLEM**

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

**PROPOSED SOLUTION**

- Create **support** for technological development
- **Model-driven** approach for automatic software development

---

ChorSSI Methodology
Use Case

Chromaway property transactions – Sweden
Chromaway BPMN model

1. The seller gets the ownership certificate of its property
2. Before putting the property up for sale, the broker verifies the seller's ownership certificate
3. The broker offers a credential for a price that the potential buyer will have to pay
4. The seller's bank exchanges the mortgage deeds for cash with the buyer's bank
5. The buyer's bank tells the registry to indicate the new possession by presenting the mortgage deeds

- Offer Credential
- Request Proof
- Property Offer
- Mortgage Deeds Offer
- Request Proof
ChorSSI implementation
ChorSSI implementation
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