

Self-Sovereign Identity with Blockchain technology

The innovation of Blockchain technology is found in its successful combination of already existing approaches: such as decentralised networks, cryptography, and consensus models. This innovative concept makes it possible to exchange values in a decentralised system. At the same time, there is no requirement for trust between its nodes.

The Blockchain can enable a new approach to identity management too. Currently identities in the Internet are contained in silos, controlled by large identity providers such as Facebook or Google. Through the use of distributed ledger technology, individuals are able to retain control over their data while at the same time staying verifiable for relying parties through the public recording of verified claims. This Self-Sovereign Identity (SSI) could be considered the next step in identity managements.

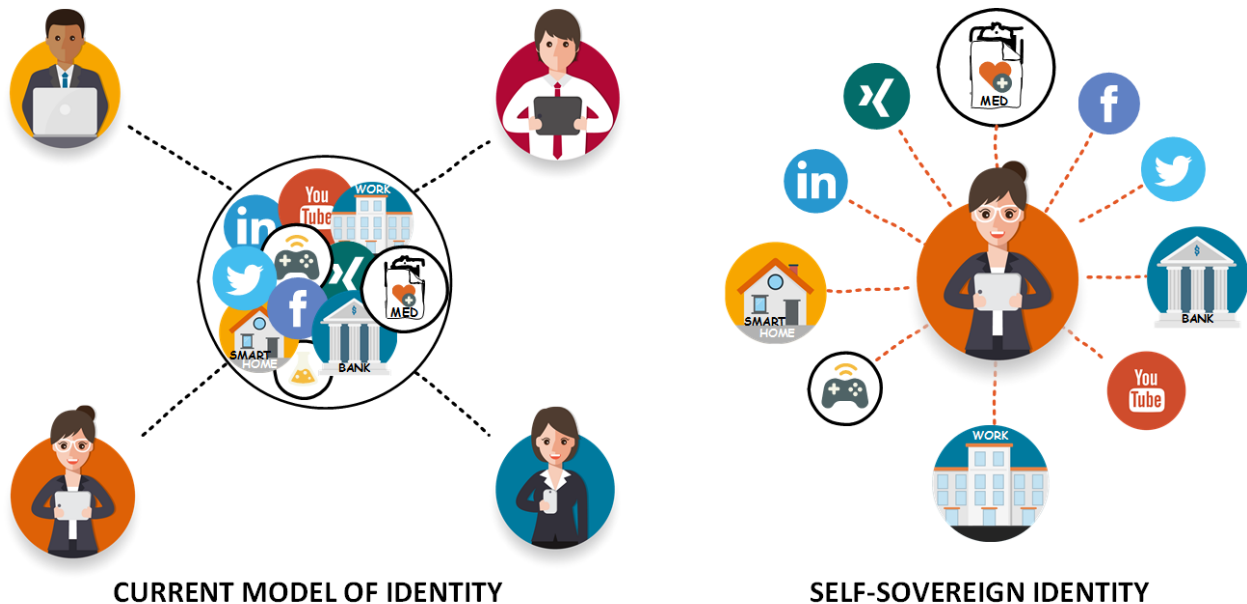


Figure 1: Comparison of current and self-sovereign identity models

In this project, we will further examine the concept of SSI.

Project tasks:

- Source analysis of current projects and approaches
- Conception of a self-sovereign identity system for a certain use case
- Prototypical implementation of the developed concept
- Comparison to current approaches and development of best practices

Students should investigate following topics:

- Blockchain network properties (permissioned/unpermissioned, consensus algorithms)
- Authentication method (asymmetric key, one-time password, biometrics)
- Data storage method (on-chain, decentralised (IPFS), distributed (cloudRaid), local (user device))

Contact

Research Group Secure Identity

- Prof. Dr. Christoph Meinel (office-meinel@hpi.de)
- Alexander Mühle (alexander.muehle@hpi.de)
- Tatiana Gayvoronskaya (tatiana.gayvoronskaya@hpi.de)