Towards Data Resilience for Fully Distributed Self-Sovereign Identity Managers

Research Question

A group of identity managers uses either local consensus or no consensus at all for resolving transaction history. These implementations generally satisfy real-world requirements for throughput and latency. Such systems are also fully distributed, thus allowing offline transactions. However, they have no data resilience. And in the case that an identity owner loses access to his identity manager, the identity gets lost irrevocably.

There is a need for a solution to the data resilience problem of fully distributed SSI management systems. The following research question is at the center of this work:

How to make fully distributed Self-Sovereign Identity management systems data resilient?

Requirements for Data Resilience

CONTROL. Users need to have direct control over their identities.

ACCESS. Identity backups need high availability.

TRANSPARENCY. Backup protocols need to be open source.

PERSISTANCE. Identity backups should never be lost.

PORTABILITY. Identity backups need to be transportable between different backup systems.

INTEROPERABILITY. Backup systems need to be able to store identity backups from different identity managers.

USABILITY. Backup system need to be accessible to all kinds of users.

LEGALITY. Transactions need to be synced with backup before considering them legal.

ACCESS REVOCATION. Only the real identity owner need to have access to identity backups.

Three Solution Proposals

- Third-Party Storage Providers
- Peer-to-Peer Backup
- Identity Owner as Storage Provider

Engineering Effort

- IPv8 and Trustchain Superapp
- Access Revocation Mechanism
- Transaction Synchronisation Algorithm
- Identity Recovery Mechanism

AUTHOR: **KALIN KOSTADINOV** SUPERVISOR: **MARTIJN DE VOS**
RESPONSIBLE PROFESSOR: **JOHAN POUWELSE**
CSE3000 RESEARCH PROJECT **19 MAY 2021**

DELFT BLOCKCHAIN LAB