Privacy-Aware Blockchain-Based SSI

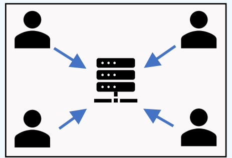
Remy Duijsens – Supervisor: Martijn De Vos – Professor: Johan Pouwelse

TU Delft

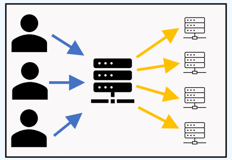
‘What are the technical limitations for privacy protection in current blockchain-based SSI implementations?’

1 Privacy Problem

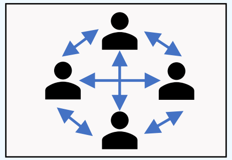
- Decay of **privacy** in the 21st century.
- Missing **identity layer** in the design of the Internet.
- Current **Centralized** and **Federated** solutions do not preserve **privacy rights**.
- Reported desire to be in **more control** of own identity.
- Christopher Allen proposes **10 principles** for a **self-sovereign identity**.



centralized



federated

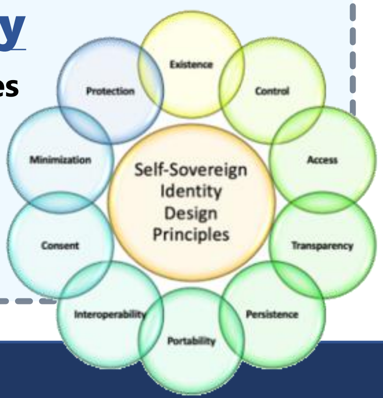


decentralized

Self-Sovereign Identity

Authority over own digital identities

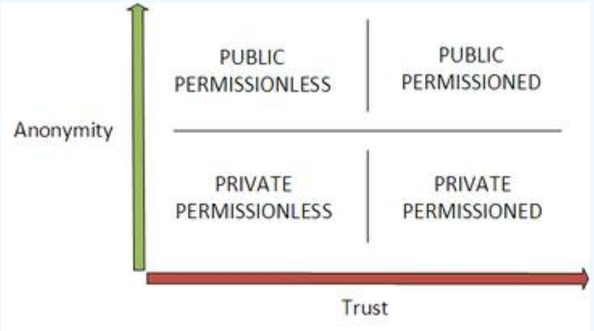
Goal Critical review on current blockchain-based SSI implementations regarding privacy



2 Blockchain & SSI

- Blockchain is a **decentralized ledger** on which users can store data, in this case identities.
- **Decentralized Identifiers** (DID’s) on-chain, to allow off-chain data.
- Several existing blockchain-based SSI implementations.

Public Permissioned blockchains the dominant kind.



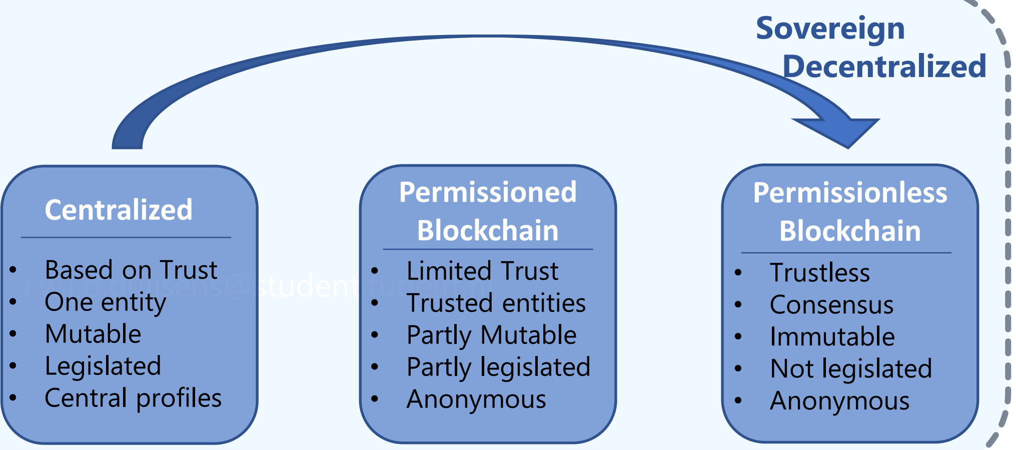
sovrin TrustChain HYPERLEDGER uport

3 Evaluation

Privacy is a concept that is **inherently different** in specific settings: e.g. politically, culturally, socially.

Local permissioned blockchains.

Legislation & **Technology** not ready to adopt fully decentralized self-sovereign identity.



Sovereign Decentralized

Centralized
- Based on Trust
- One entity
- Mutable
- Legislated
- Central profiles

Permissioned Blockchain
- Limited Trust
- Trusted entities
- Partly Mutable
- Partly legislated
- Anonymous

Permissionless Blockchain
- Trustless
- Consensus
- Immutable
- Not legislated
- Anonymous

CSE3000 – Research Project - Q4 2021

Email: r.w.j.p.duijsens@student.tudelft.nl