A Privacy Evaluation of Blockchain-Based SSI

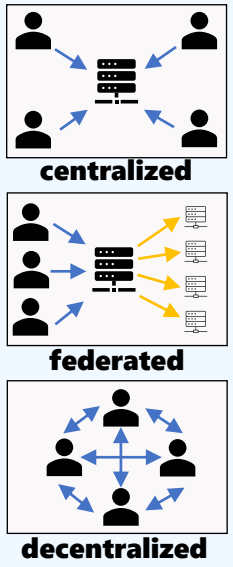
Remy Duijsens – Supervisor: Martijn De Vos – Professor: Johan Pouwelse

TU Delft Blockchain Lab

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

1 Privacy Problem

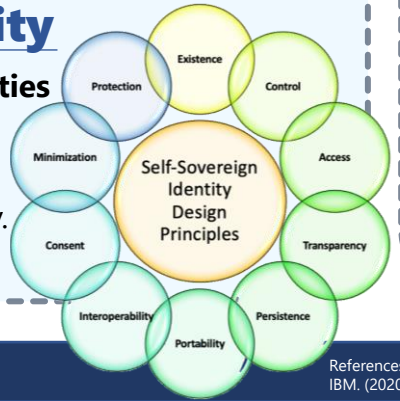
- Decay of **privacy** in the 21st century.
- Missing **identity layer** in the design of the Internet.
- Current **Centralized** and **Federated** solutions do not preserve **privacy rights**.
- Reported desire to be in **more control** of own identity.
- Christopher Allen proposes **10 principles**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



Self-Sovereign Identity

Authority over own digital identities

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



2 Privacy Criteria

1. Data Minimization	6. Usability Privacy
2. Interoperable Privacy	7. Open Source
3. Quantum Resistance	8. Privacy Plan
4. Erasable Data	9. Backdoor Proof
5. Privacy-Aware Development	10. Secure Key Storage

3 Evaluation

sovrin, SELFKEY, uport, evernym, lifeID, TrustChain, ShoCard

Implementations	Data Minimization	Usability Privacy	Privacy-Aware Development	Interoperable Privacy	Open Source	Erasable Data	Secure Key Storage	Backdoor Proof	Quantum Resistance	Privacy Plan
LifeID	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
SelfKey	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
Sovrin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
uPort	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
Evernym Verity	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No
Vetri Global	Yes	Yes	No	No	No	Yes	Yes	No	No	Yes
Trustchain	Yes	No	Yes	No	Yes	Yes	Yes	No	No	No
Spidchain	No	No	No	Yes	Yes	Yes	Yes	Yes	No	No
Affinidi	No	Yes	Yes	Yes	No	Yes	Yes	No	No	No
ShoCard	No	Yes	No	No	No	No	Yes	Yes	No	Yes
Sora	No	Yes	X	Yes	X	Yes	Yes	No	No	No
Blockpass	No	Yes	No	Yes	No	Yes	Yes	No	No	No
Everest	No	Yes	No	No	No	Yes	Yes	No	No	No
EverID	No	Yes	No	No	No	Yes	Yes	No	No	No
ID.ee	No	Yes	Yes	No	No	X	Yes	No	No	No
myIDsafe	No	X	Yes	Yes	X	Yes	X	X	X	No
DomiNode	X	X	X	X	No	X	X	No	X	No

Table 1: Evaluation results of selected blockchain-based SSI implementations based on defined criteria.

4 Conclusions

- **All criteria** can be **satisfied** with currently existing **privacy-preserving methods** for blockchain-based applications.
- **Privacy protection** in evaluated solutions often good when a **Privacy Plan** is present.
- Many SSI solutions **fail** to satisfy **most criteria**. The ones that are commonly satisfied are mostly due to **legislative requirements**.

References: [1] Image "SSI Design Principles" IBM. (2020). https://doc.ibmsecurity.verify-creds.com/learn/ssi-concepts/

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