RIPE 83

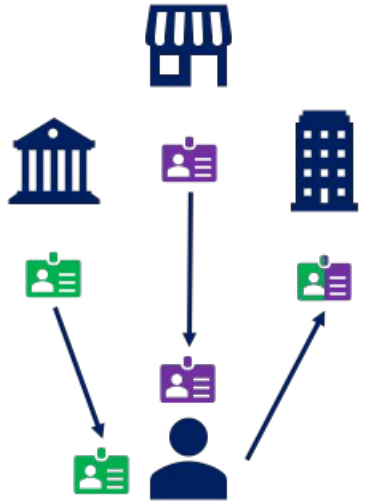
Blockchain Redaction in Self-Sovereign Identity

Šeila Bećirović
Faculty of Electrical Engineering University of Sarajevo

Self-Sovereign Identity (SSI)

"The Internet was built without an identity layer."

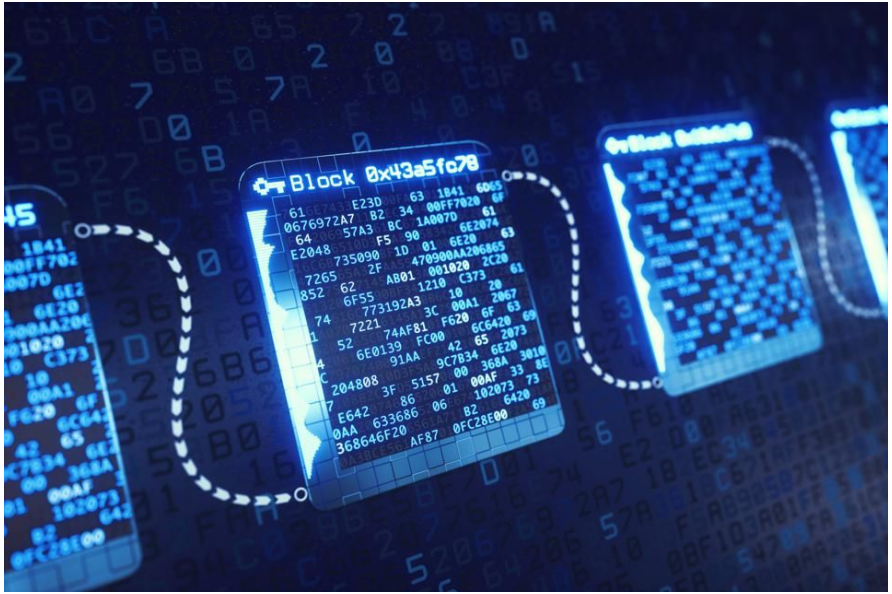
Kim Cameron, Chief Architecture of Identity, Microsoft



Self-Sovereign identity

- Identity management model
- Digital identity is controlled, and managed by the entity to which the identity and related data belongs
- Identity management infrastructure is somewhat **decentralized**

Blockchain

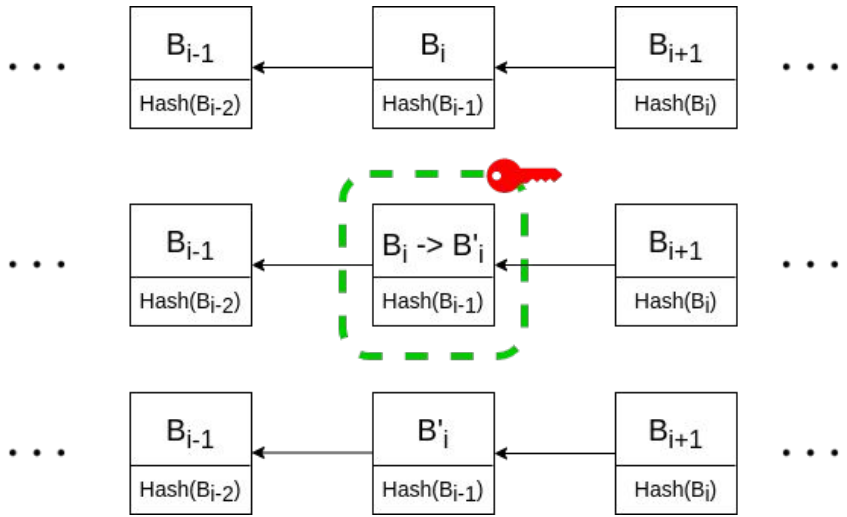


Public or private distributed ledger built on a peer-to-peer network

Append only transactional database

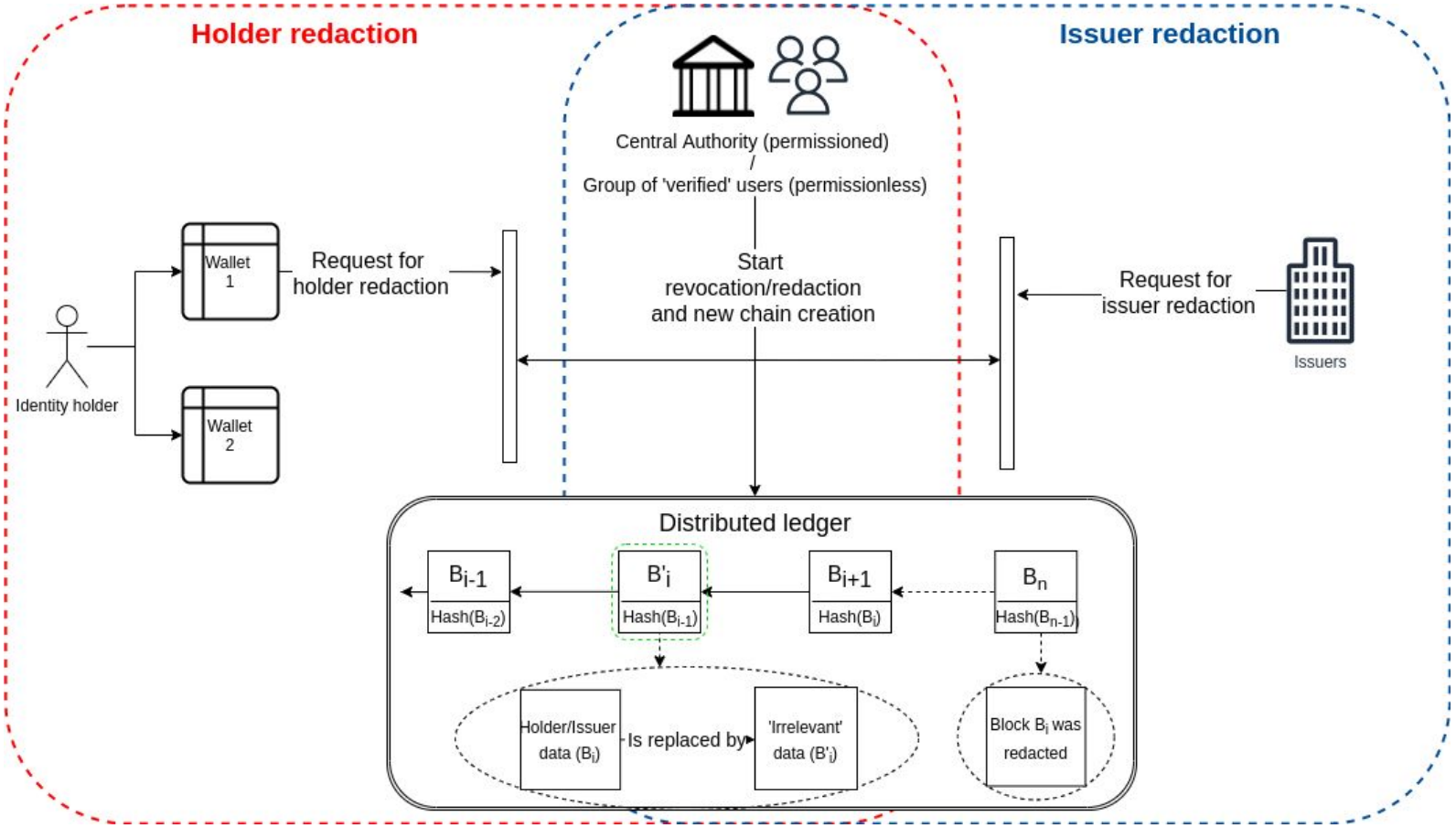
Immutable database

Redaction



- Re-writing one or more blocks
  - Chameleon hash function
  - Secret-sharing schemes
  - Multi Party Computation
- Under specific constraints

Holder redaction	Issuer redaction
'Right to be forgotten'	Registry/VC revocation
Agent revocation	Public keys revocation
User data revocation	Revocation of delegation, guardianship, controllership



An overview of the redaction process

Q&A