EBSI from the perspective of self-sovereign identity (SSI)

Roman Vitenberg

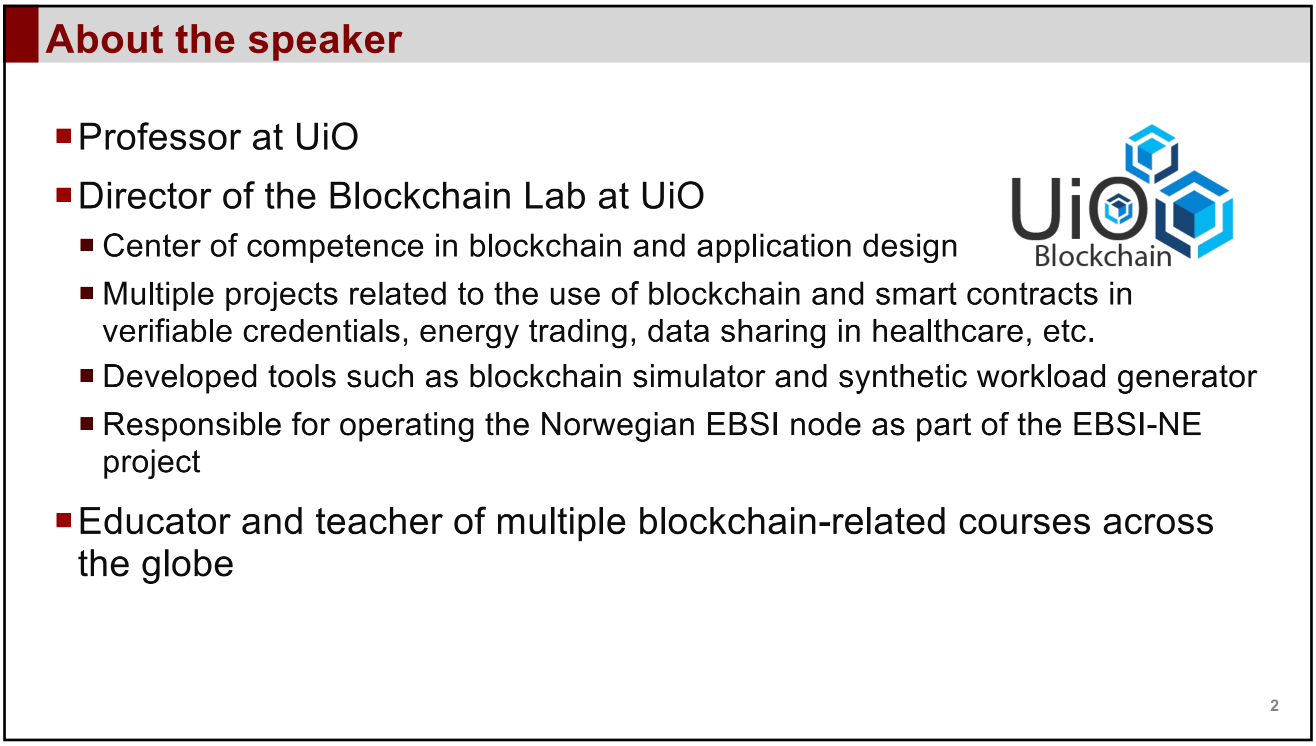
UiO Blockchain

EBSI-NE

ebsi European Blockchain

UiO : University of Oslo

1

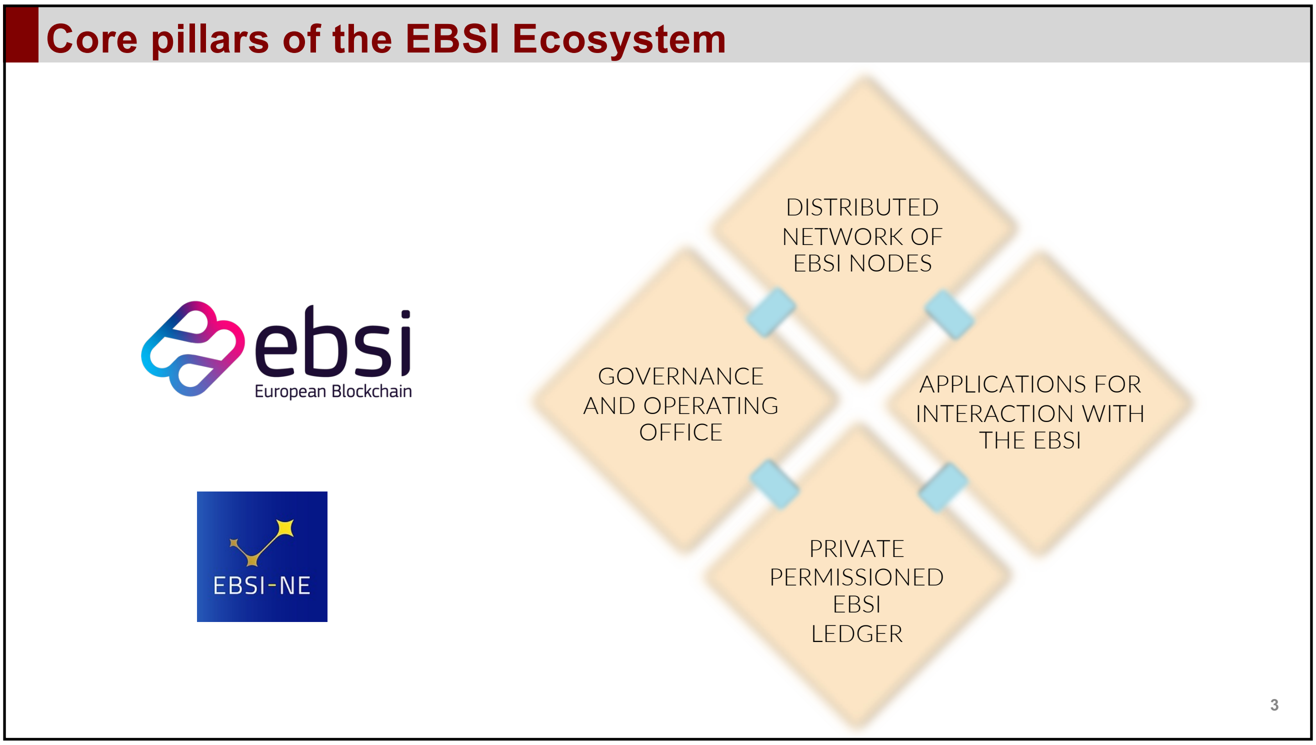


About the speaker

- Professor at UiO
- Director of the Blockchain Lab at UiO
  - Center of competence in blockchain and application design
  - Multiple projects related to the use of blockchain and smart contracts in verifiable credentials, energy trading, data sharing in healthcare, etc.
  - Developed tools such as blockchain simulator and synthetic workload generator
  - Responsible for operating the Norwegian EBSI node as part of the EBSI-NE project
- Educator and teacher of multiple blockchain-related courses across the globe

UiO Blockchain

2



Core pillars of the EBSI Ecosystem

ebsi European Blockchain

EBSI-NE

DISTRIBUTED NETWORK OF EBSI NODES

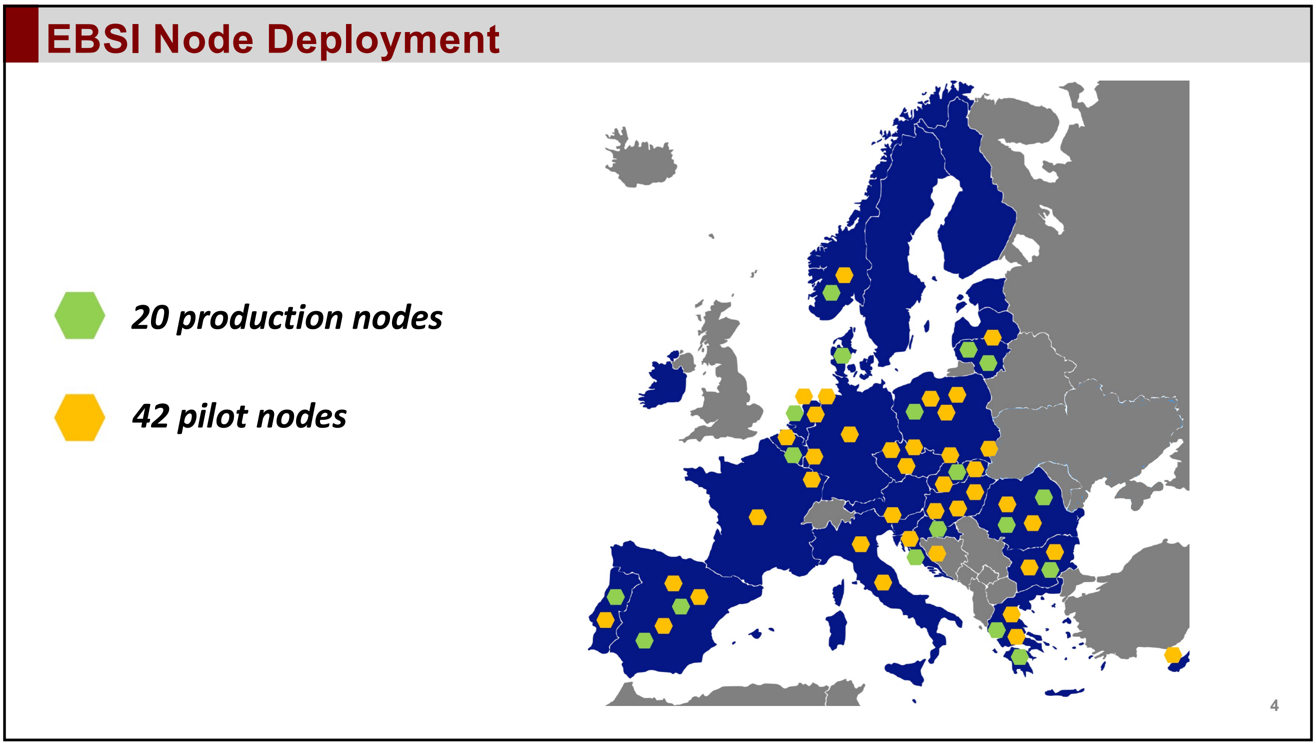
GOVERNANCE AND OPERATING OFFICE

APPLICATIONS FOR INTERACTION WITH THE EBSI

PRIVATE PERMISSIONED EBSI LEDGER

3

3



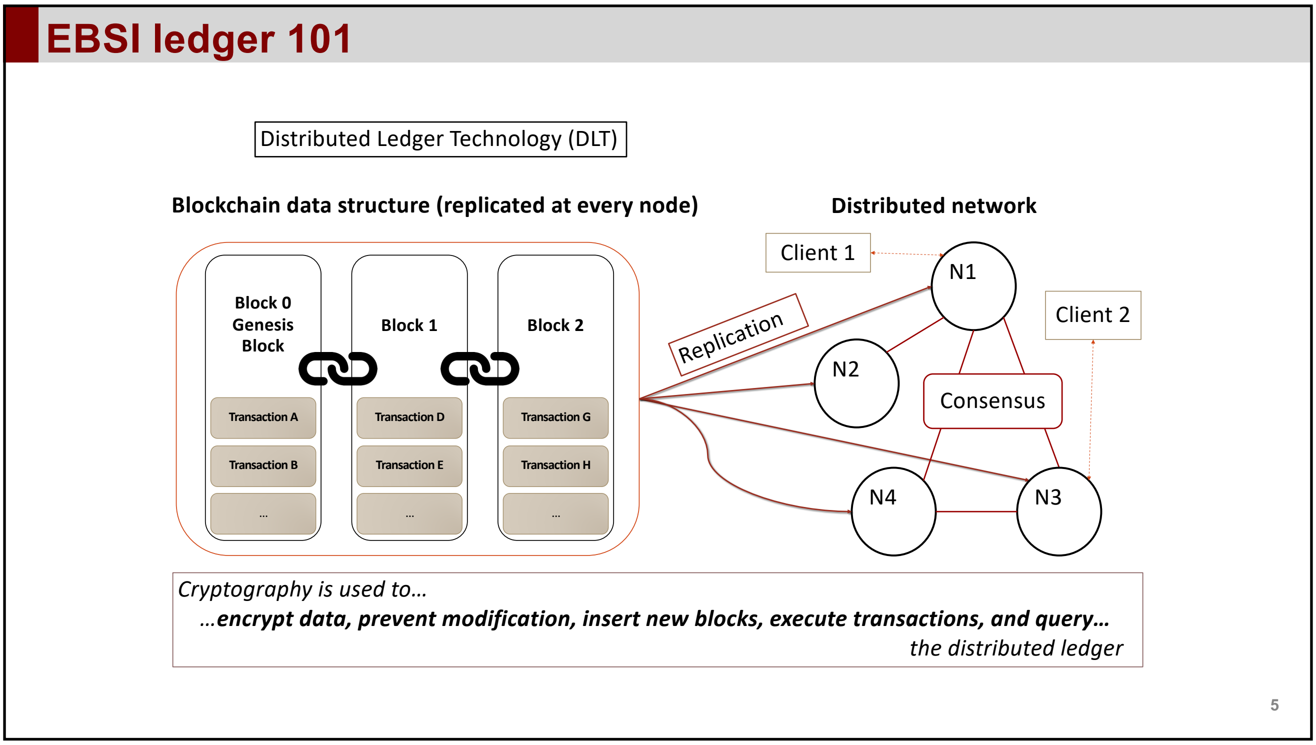
EBSI Node Deployment

🟩 ***20 production nodes***

🟨 ***42 pilot nodes***

4

4



EBSI ledger 101

Distributed Ledger Technology (DLT)

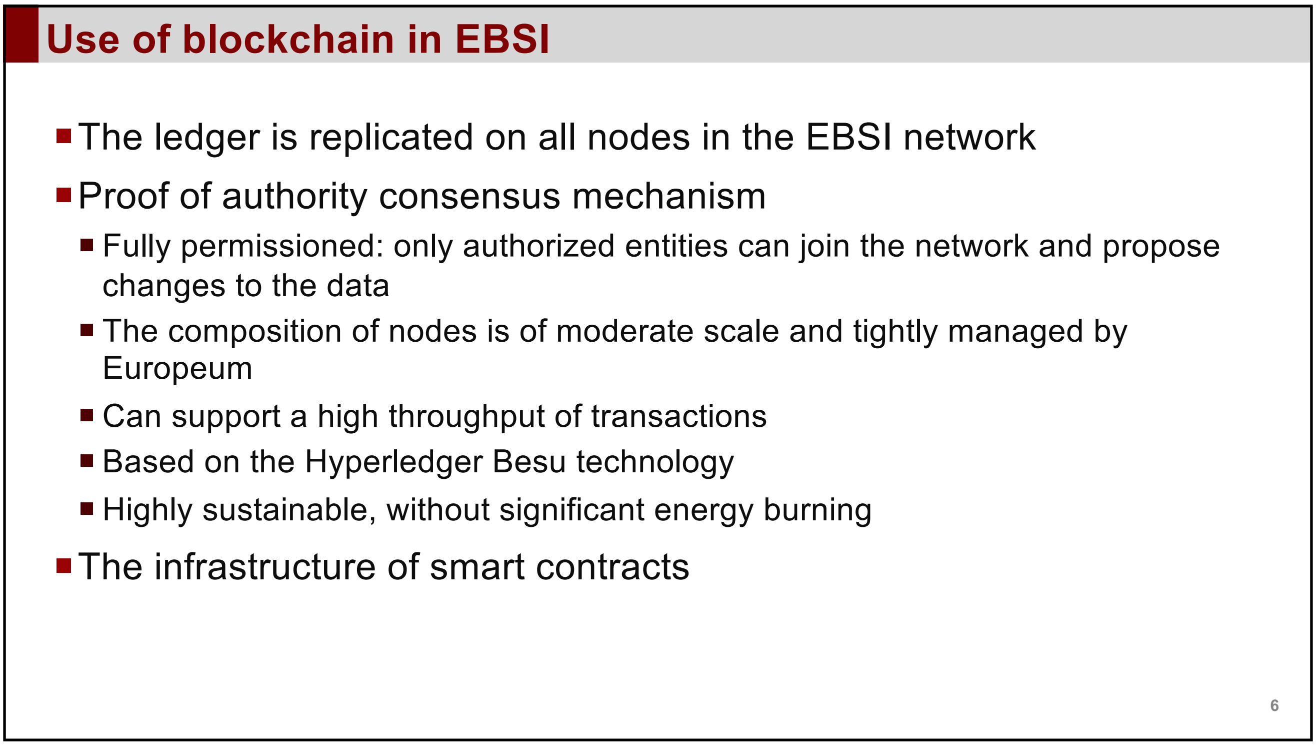
Blockchain data structure (replicated at every node)

Distributed network

Cryptography is used to…

…encrypt data, prevent modification, insert new blocks, execute transactions, and query…

the distributed ledger



Use of blockchain in EBSI

- The ledger is replicated on all nodes in the EBSI network
- Proof of authority consensus mechanism
  - Fully permissioned: only authorized entities can join the network and propose changes to the data
  - The composition of nodes is of moderate scale and tightly managed by Europeum
  - Can support a high throughput of transactions
  - Based on the Hyperledger Besu technology
  - Highly sustainable, without significant energy burning
- The infrastructure of smart contracts

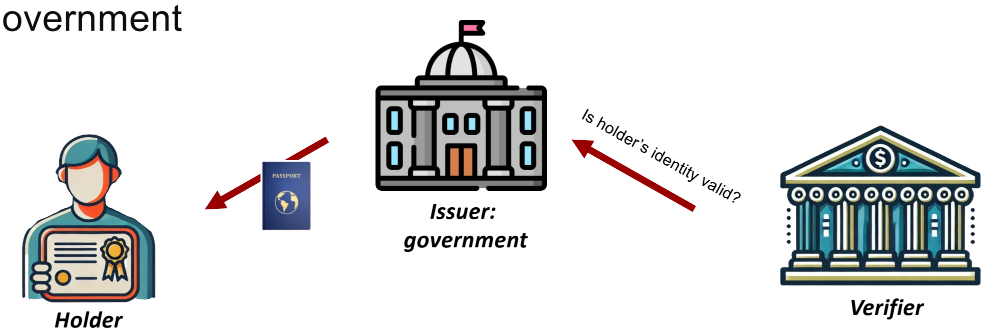
Digital Identity management

Holder
Issuer
Verifier

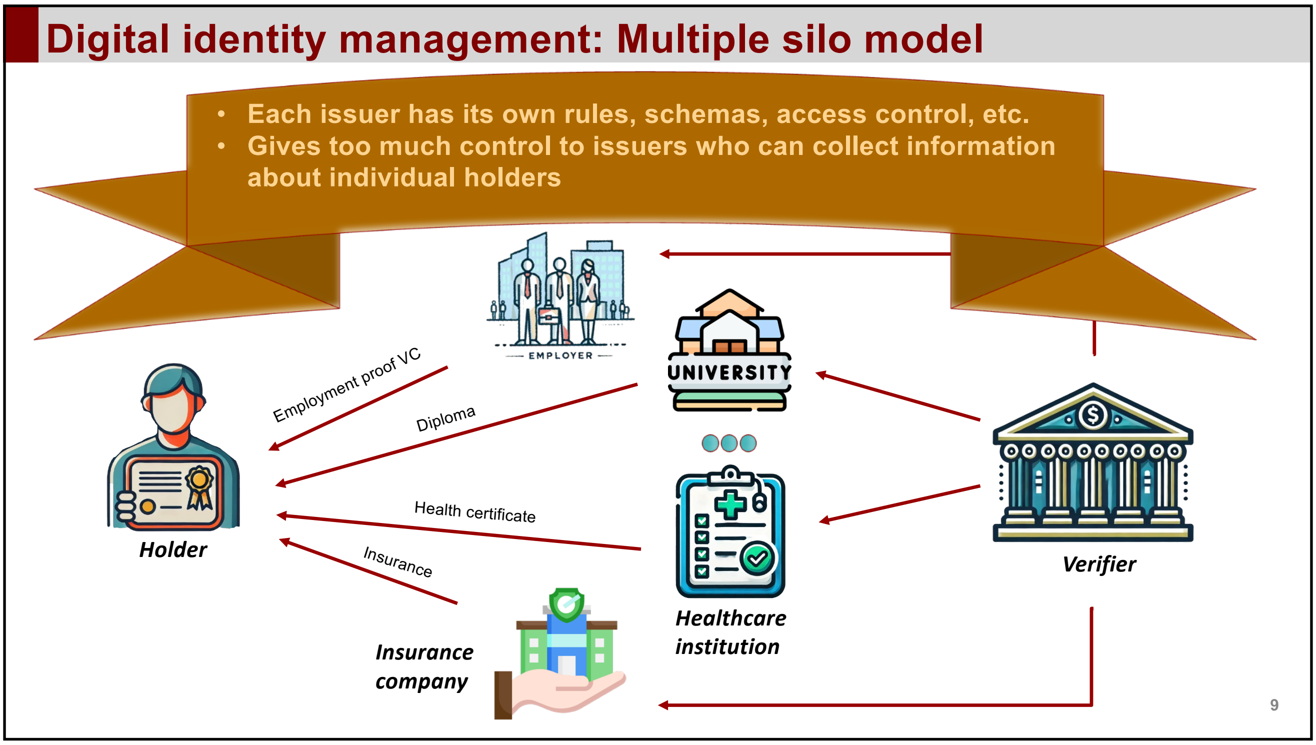
- All entities must be authenticated and authorized
- Issuers must be credible
  - First tier of credibility: approval by the government
  - Second tier of credibility: discretion of the verifier
- Verifiable Credentials (VCs) must be valid (not expired or revoked)
- The system manages all but the second tier of credibility

Digital identity management: from centralized to federated to self-sovereign

- Classic centralized model: A few verifiable credentials (VCs) issued by the government

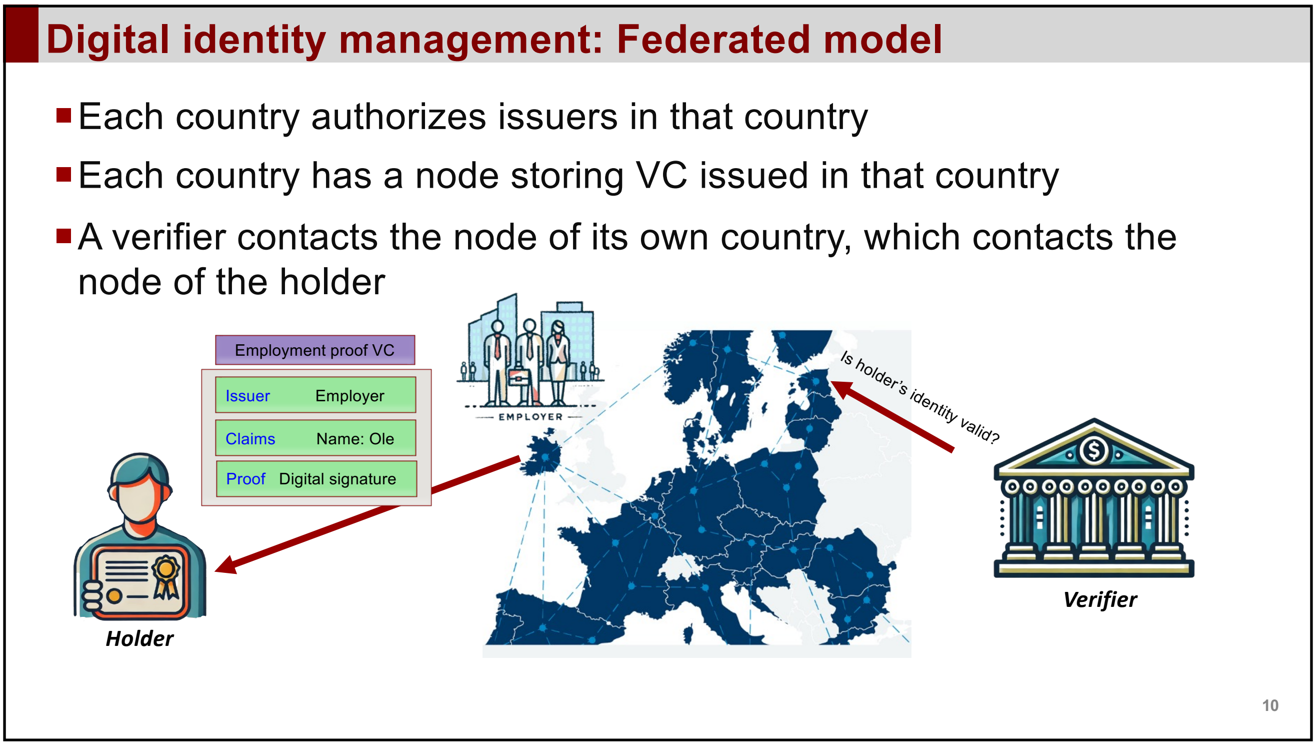


Problem: issuers are numerous, inherently decentralized, and multifaceted



Digital identity management: Multiple silo model

- Each issuer has its own rules, schemas, access control, etc.
- Gives too much control to issuers who can collect information about individual holders



Digital identity management: Federated model

- Each country authorizes issuers in that country
- Each country has a node storing VC issued in that country
- A verifier contacts the node of its own country, which contacts the node of the holder

Employment proof VC

Issuer	Employer
Claims	Name: Ole
Proof	Digital signature

Digital identity management: Analysis of the federated model

Advantages

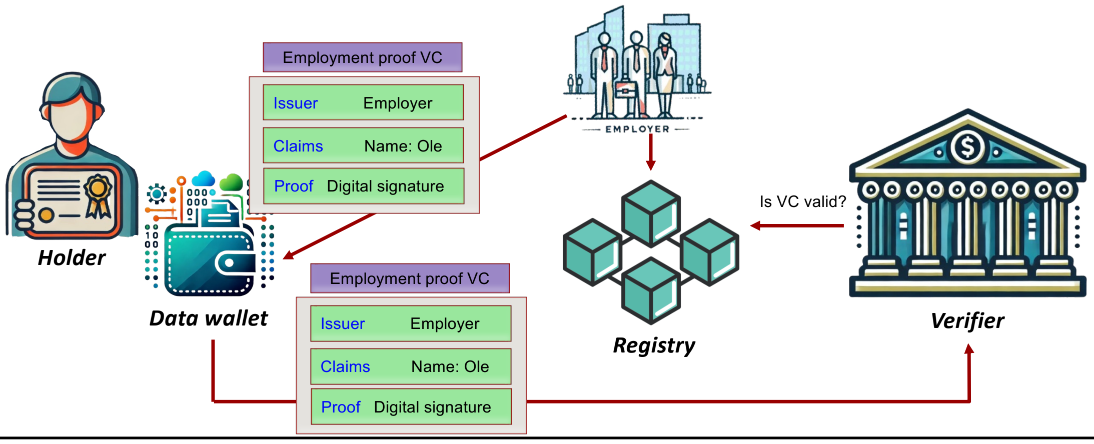
- Enforces homogeneity
- Issuers do not participate in the verification

Shortcomings

- Government still needs to be in control of issuers
- Holders do not participate in the verification
  - No control about the sharing
  - Not informed about a verification attempt

Digital identity management: SSI model

- Each holder has a data wallet to keep his/her VCs
- A holder may decide to share the VC with individual verifiers
- A verification process involves global public registry accessible to all

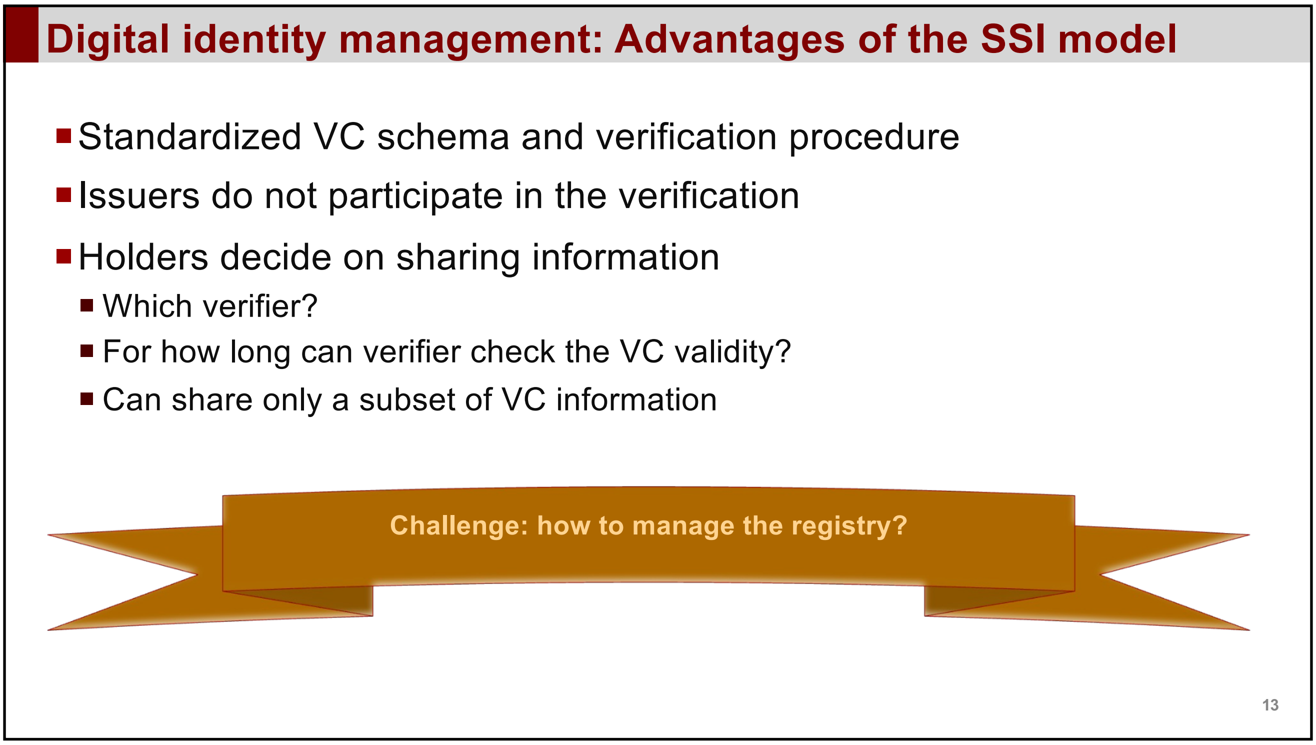


Employment proof VC

Issuer	Employer
Claims	Name: Ole
Proof	Digital signature

Employment proof VC

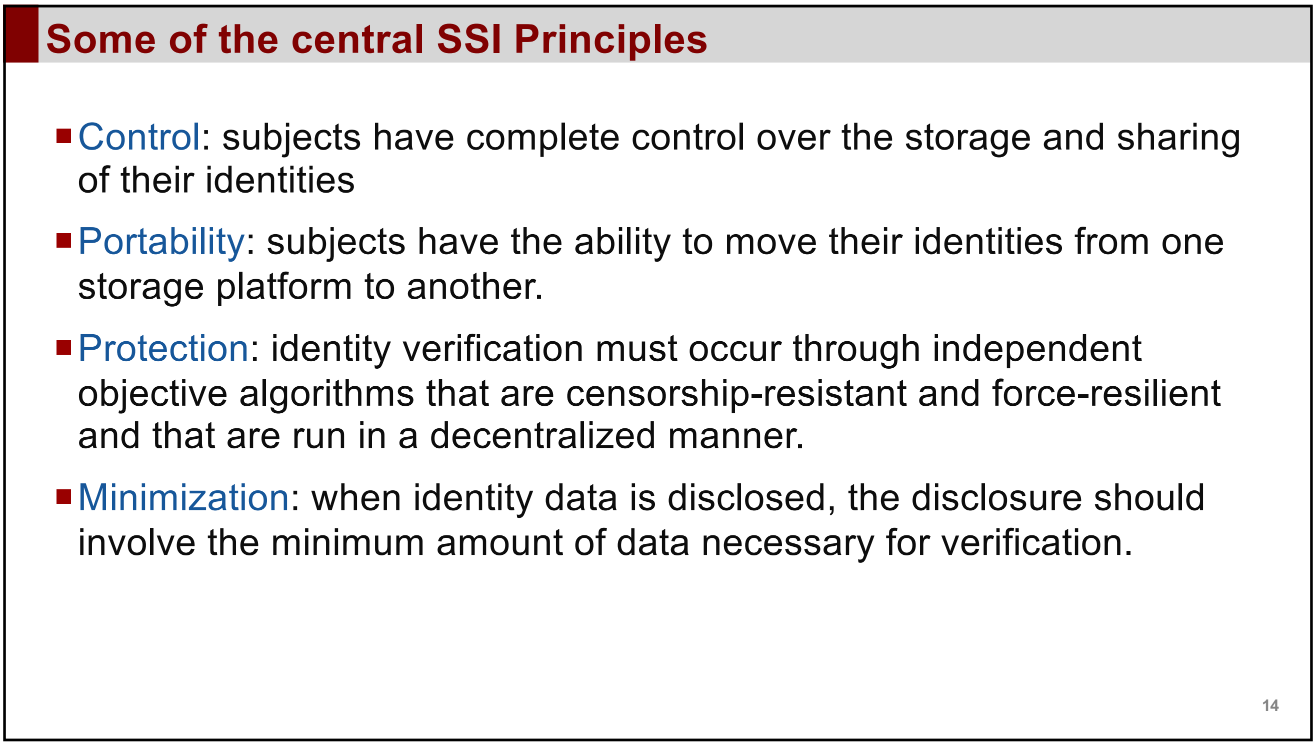
Issuer	Employer
Claims	Name: Ole
Proof	Digital signature



Digital identity management: Advantages of the SSI model

- Standardized VC schema and verification procedure
- Issuers do not participate in the verification
- Holders decide on sharing information
  - Which verifier?
  - For how long can verifier check the VC validity?
  - Can share only a subset of VC information

Challenge: how to manage the registry?



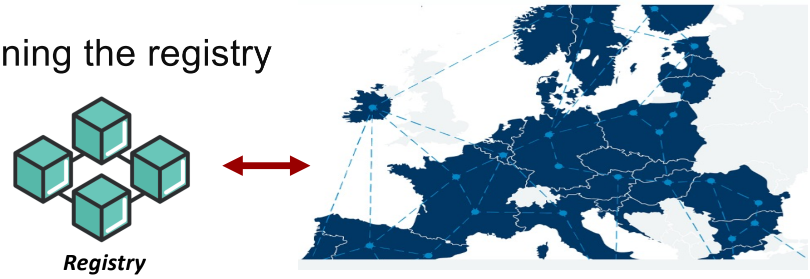
Some of the central SSI Principles

- Control: subjects have complete control over the storage and sharing of their identities
- Portability: subjects have the ability to move their identities from one storage platform to another.
- Protection: identity verification must occur through independent objective algorithms that are censorship-resistant and force-resilient and that are run in a decentralized manner.
- Minimization: when identity data is disclosed, the disclosure should involve the minimum amount of data necessary for verification.

How SSI principles are satisfied in EBSI

- EBSI is maintaining the registry

ebsi European Blockchain



- Individual holders own data wallets storing VCs
  - Decide upon sharing and storage, which gives control and portability
  - Can also provide minimization
- It is not fully decentralized, however:
  - The registry is tightly controlled and not publicly accessible
  - Every single issuer must be appointed by the governing body
  - May possibly be the most practical compromise