Zurich, June 12, 2019

Overview on Blockchain-based Academic Certificate Handling

Bruno Rodrigues, Muriel Franco, Eder Scheid, Christian Killer, Burkhard Stiller

Communication Systems Group CSG
Department of Informatics IfI
University of Zürich UZH, Switzerland

[rodrigues¦franco¦scheid¦killer¦stiller]@ifi.uzh.ch

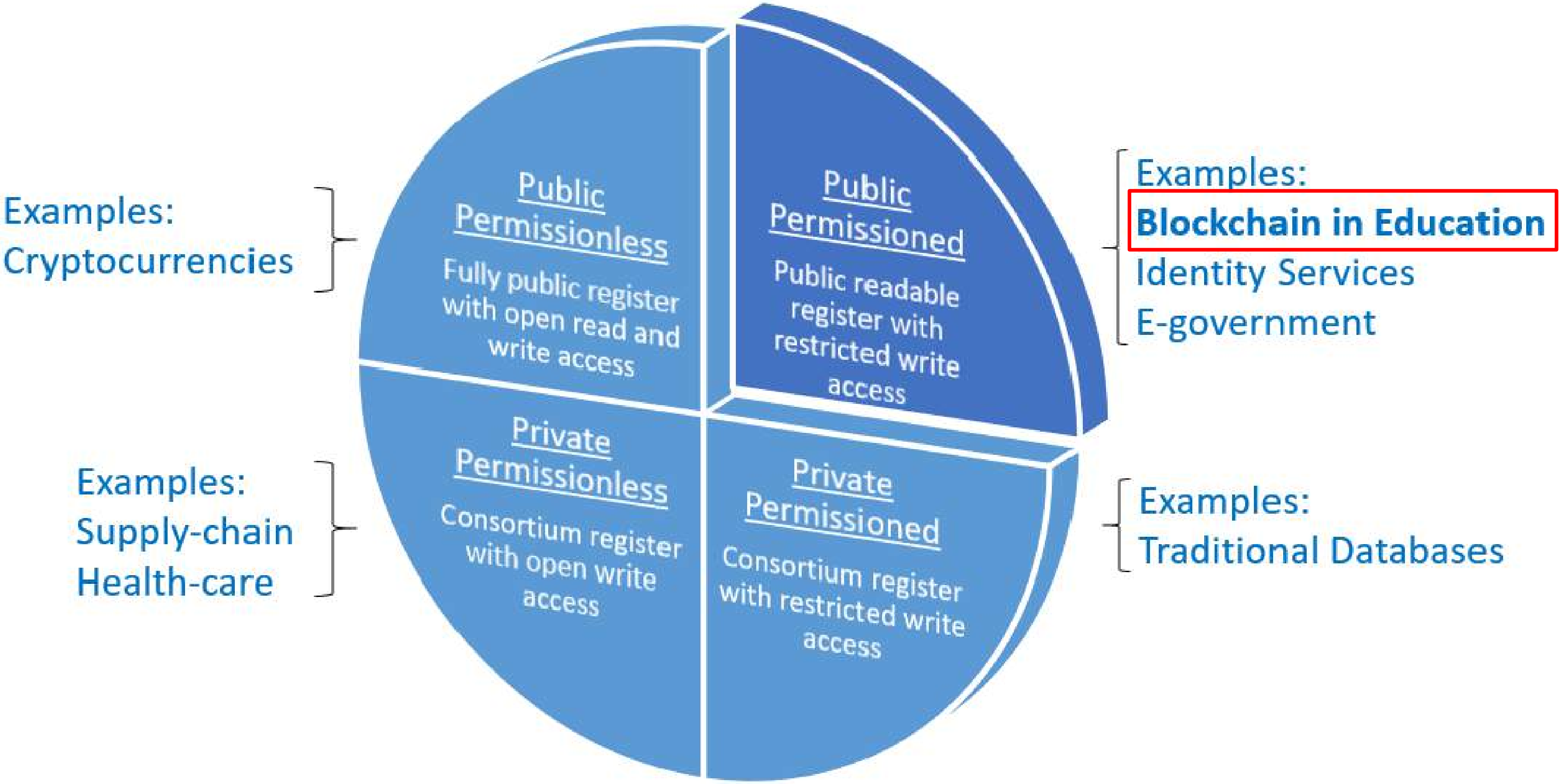
University of Zurich UZH

CSG
Communication Systems Group

Blockchains in Education

- ❑ Academic certificate handling
  - – Creation (issuance), revocation, and verification
- ❑ Interesting blockchain (BC) features
  - – Data immutability, *i.e.*, data cannot be changed
  - – Data replication, *i.e.*, availability, no single point-of-failure
  - – Data trust, *i.e.*, no need for a Trusted Third Party (TTP)
- ❑ BC can act as a public and distributed ledger of academic certificates
  - – Still necessary to trust the institutions that are issuing certificates are accredited
- ❑ BC-based Smart Contracts (SC)
  - – Automated and immutable code execution

Blockchain Deployment Types



Examples:
Cryptocurrencies

Public Permissionless

Fully public register with open read and write access

Public Permissioned

Public readable register with restricted write access

Examples:
Blockchain in Education
Identity Services
E-government

Examples:
Supply-chain
Health-care

Private Permissionless

Consortium register with open write access

Private Permissioned

Consortium register with restricted write access

Examples:
Traditional Databases

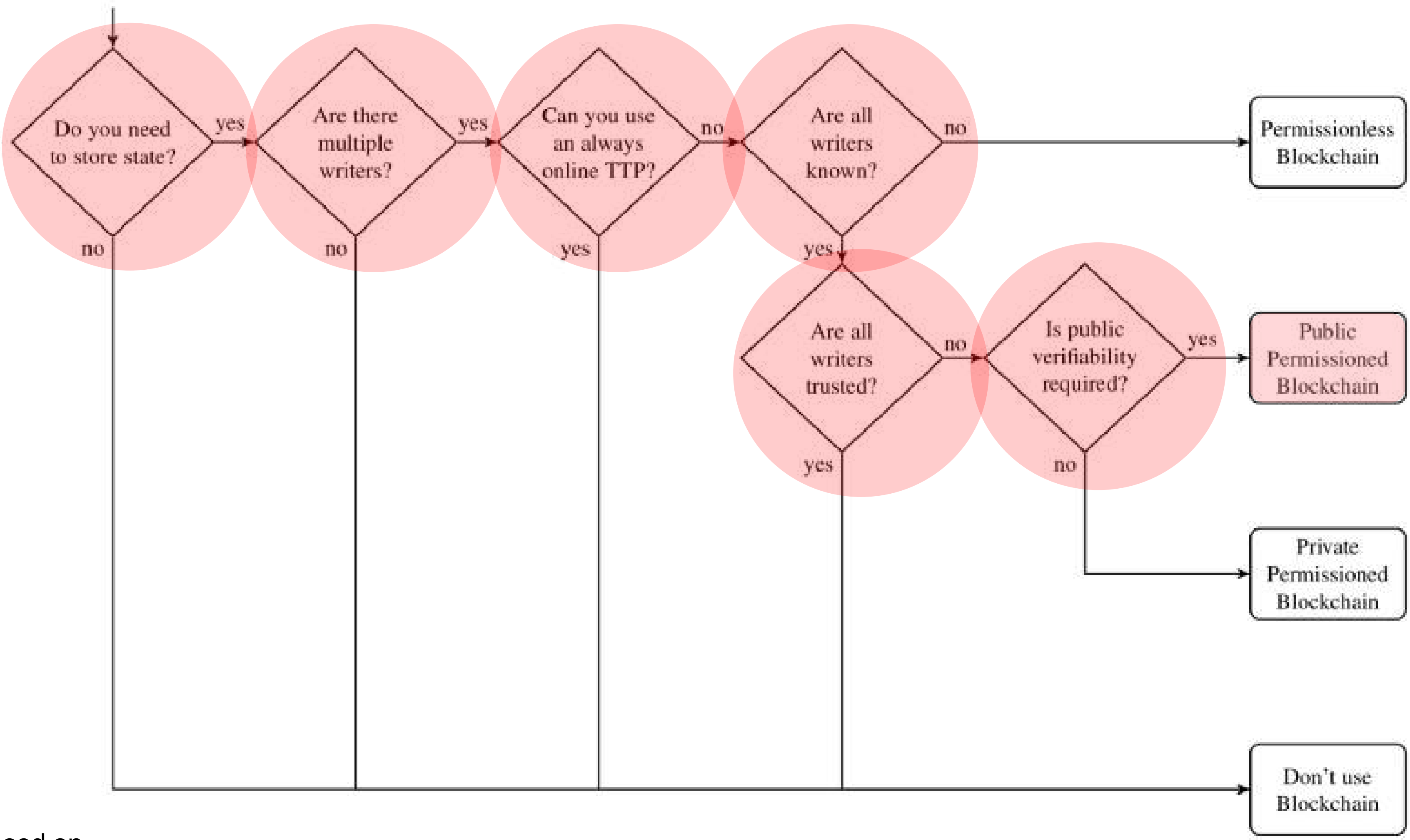
Stakeholders and Roles

- Issuers
  - Accredited education institutions, *e.g.*, UZH or ETH
  - BC permissions: write and read

- Recipients
  - Certificate owners, *e.g.*, students
  - BC permissions: read

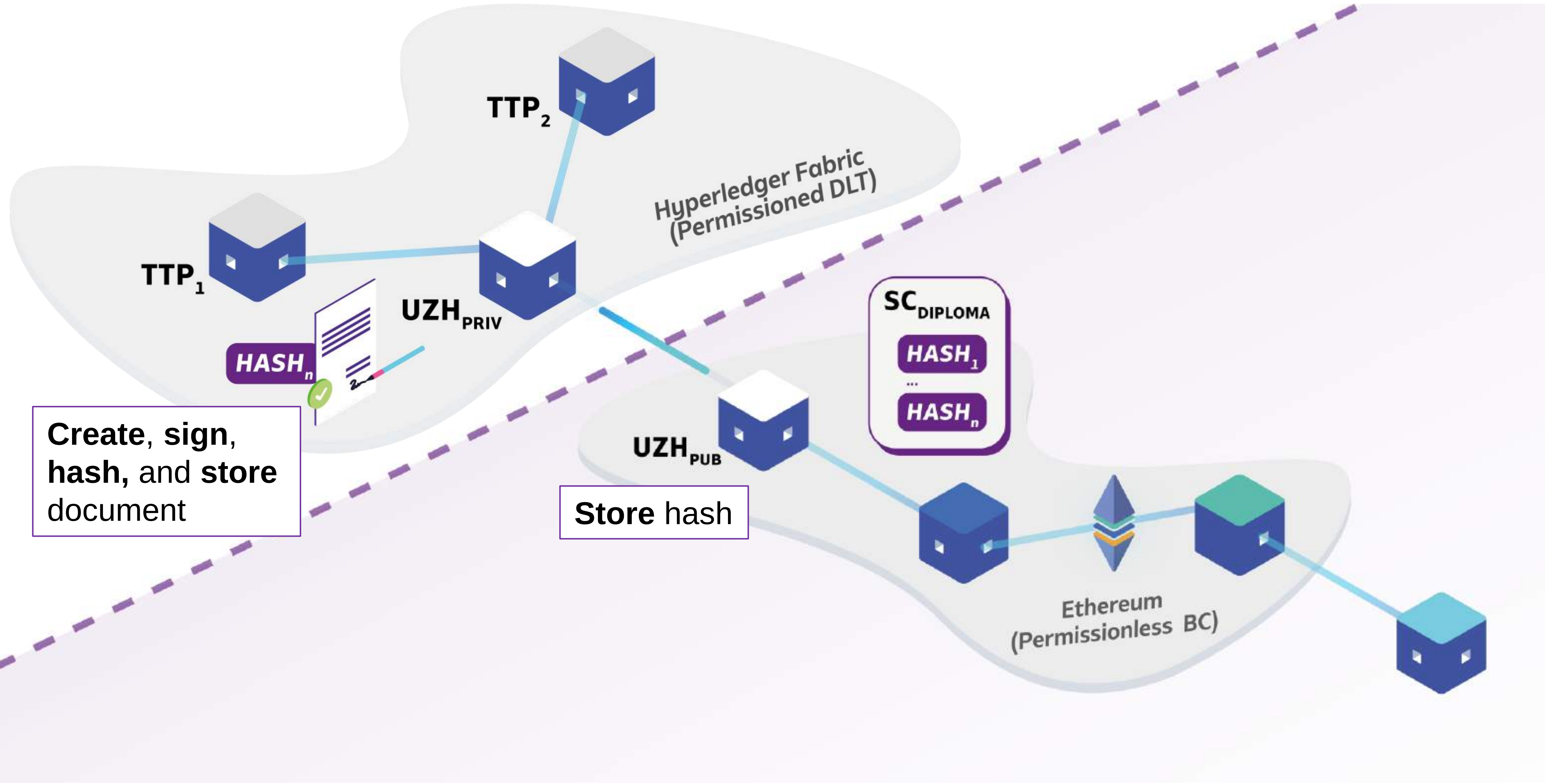
- Verifiers
  - Interested parties, *e.g.*, companies, universities
  - BC permissions: read

Mapping Stakeholder Permissions to BC


Do you need to store state?
yes
no
Are there multiple writers?
yes
no
Can you use an always online TTP?
no
yes
Are all writers known?
no
yes
Permissionless Blockchain
Are all writers trusted?
no
yes
Is public verifiability required?
yes
no
Public Permissioned Blockchain
Private Permissioned Blockchain
Don't use Blockchain

Based on
K. Wüst, A. Gervais

Foreseen EduChain Architecture



Create, **sign**, **hash,** and **store** document

Store hash

© UZH 2019

Landscape of Blockchain in Education

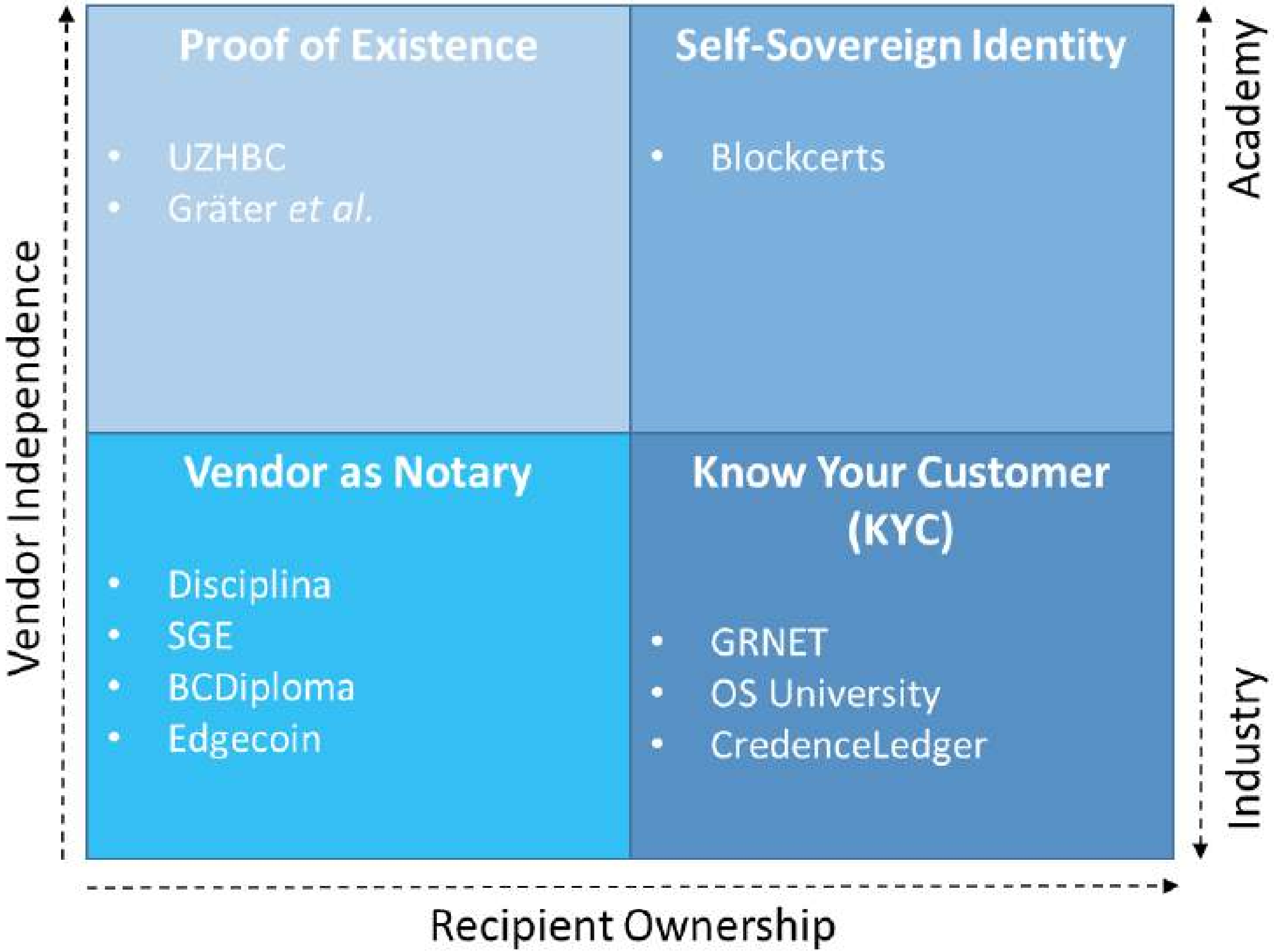
Work	BC Type	BC	Certificate Storage	Permissions to Issue Certificates
Blockcerts	Permissionless	Bitcoin, Ethereum	Traditional DB	Off-chain Overlay
Disciplina	Permissionless	Own Blockchain	Own Blockchain	Smart Contract
UZHBC	Permissionless	Ethereum	Traditional DB	Smart Contract
BCDiploma	Permissionless	Ethereum	Traditional DB	Smart Contract
Edgecoin	Permissionless	Ethereum	IPFS	Smart Contract
OS University	Permissionless	Ethereum	IPFS	Smart Contract
Gräter et al.	Permissionless	Ethereum	IPFS	Smart Contract
Sony Global Education	Permissioned	IBM HyperLedger	Traditional DB	Selected institutions
GRNET	Permissioned	Cardano	Traditional DB	Selected institutions
CredenceLedger	Permissioned	MultiChain	Traditional DB	Selected institutions

Based on: B. Rodrigues, M. Franco, E. Scheid, B. Stiller, S. Kanhere: A Technology-driven Overview on Blockchain-based Academic Certificate Handling.

Approaches for BC Certificate Handling

- ❑ Proof of Existence
  - – BC used as time-stamping solution, providing integrity
- ❑ Vendor as Notary
  - – Intermediator providing access to the information on the BC
- ❑ Know your customer (KYC)
  - – Allow recipients to demonstrate the ownership of their certificates
  - – Vendor-dependent validation
- ❑ Digital Self-Sovereign (Identity)
  - – Individuals control the sharing of certificates
  - – Vendor-independent

Classification of Work



Proof of Existence

- UZHBC
- Gräter *et al.*

Self-Sovereign Identity

- Blockcerts

Vendor as Notary

- Disciplina
- SGE
- BCDiploma
- Edgecoin

Know Your Customer (KYC)

- GRNET
- OS University
- CredenceLedger

Challenges

- ❑ Privacy
  - – Data in the BC (*e.g.*, certificate hash) is personal data?
  - – GDPR Compliance → cannot remove data from the BC
- ❑ Integrity
  - – Prevent certificates issued by recognized and accredited institutions from being modified
- ❑ Access Control / Organizational
  - – Prevent unrecognized and unaccredited institutions from issuing certificates
- ❑ Novelty
  - – Skepticism of BC adoption
  - – Price volatility

Opportunities

- BC conceived to promote disintermediation
- However, stakeholders operate in different BC networks that are closed in their own ecosystem
  - Standards → fundamental aspect to make these different isolated networks to communicate, *i.e.*, interoperability

- User-centric Data Control
  - Allow verifiable claims in Curriculum Vitae (CV) independently of a vendor or educational institution
  - Secure sharing of CV/certificate data (control of data access)

Thank you for your attention.