EduChain – Proposal of Requirements and Architecture

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]

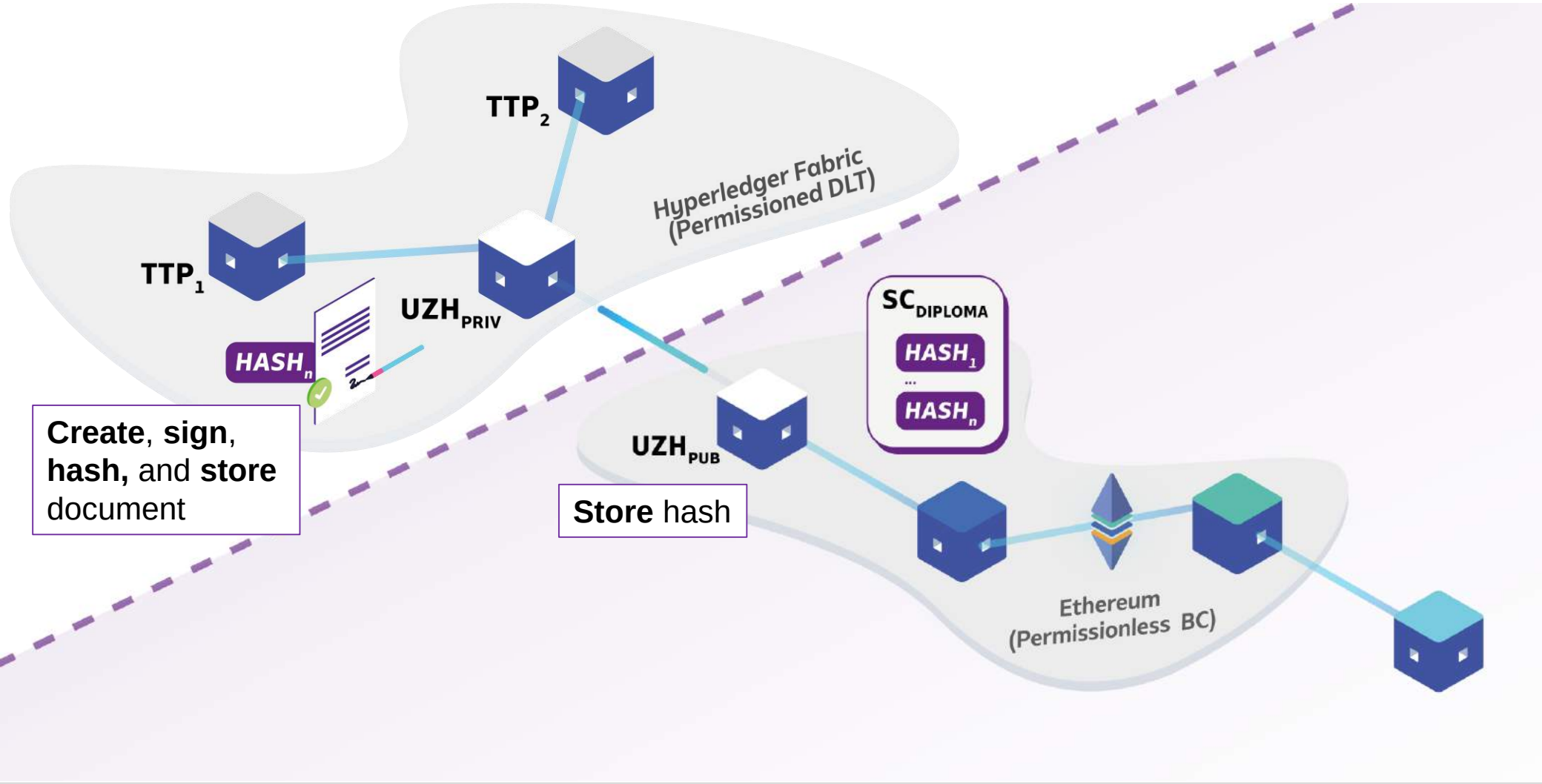
CSG
Communication Systems Group

Requirements

- Private Environment
  - Issuers are responsible → Permissioned DLT
  - Certificate and individual data must be kept private
  - Certificate revocation process
  - Operation with legacy systems

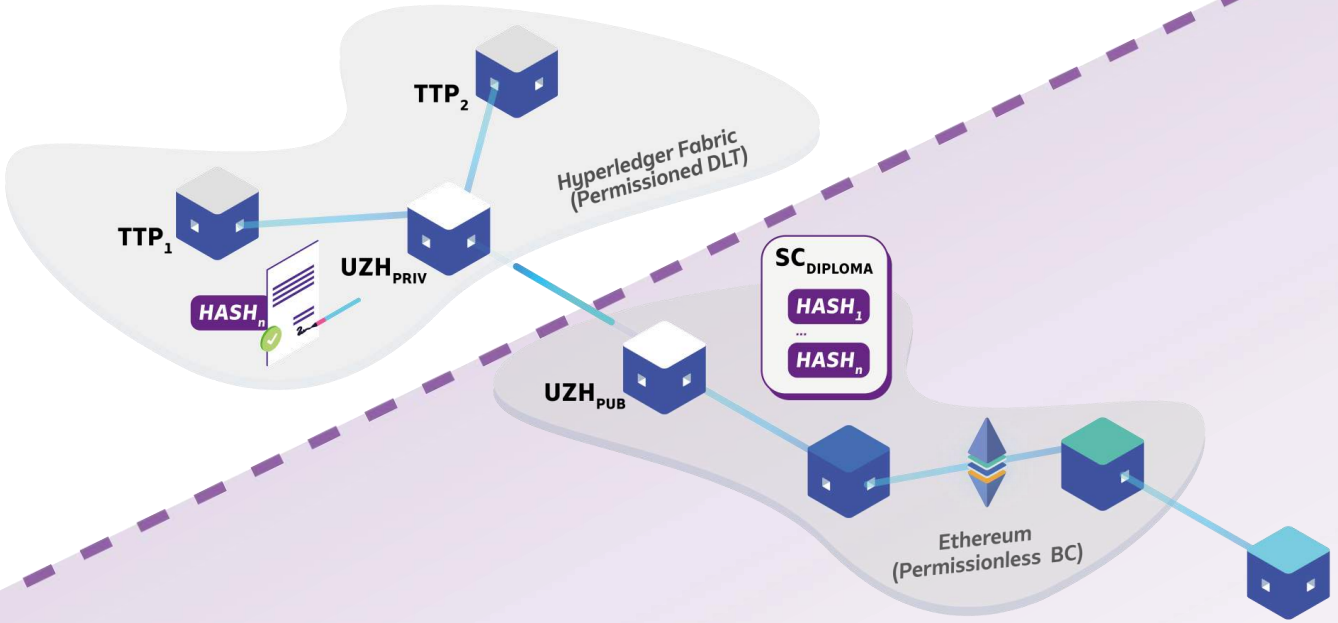
- Public Environment
  - Verifiers and recipients
  - Straightforward verification process
  - Availability of identifiers, *i.e.,* certiticate hash
    - Data must be decentralized → Permissionless BC

Example EduChain Architecture (1)



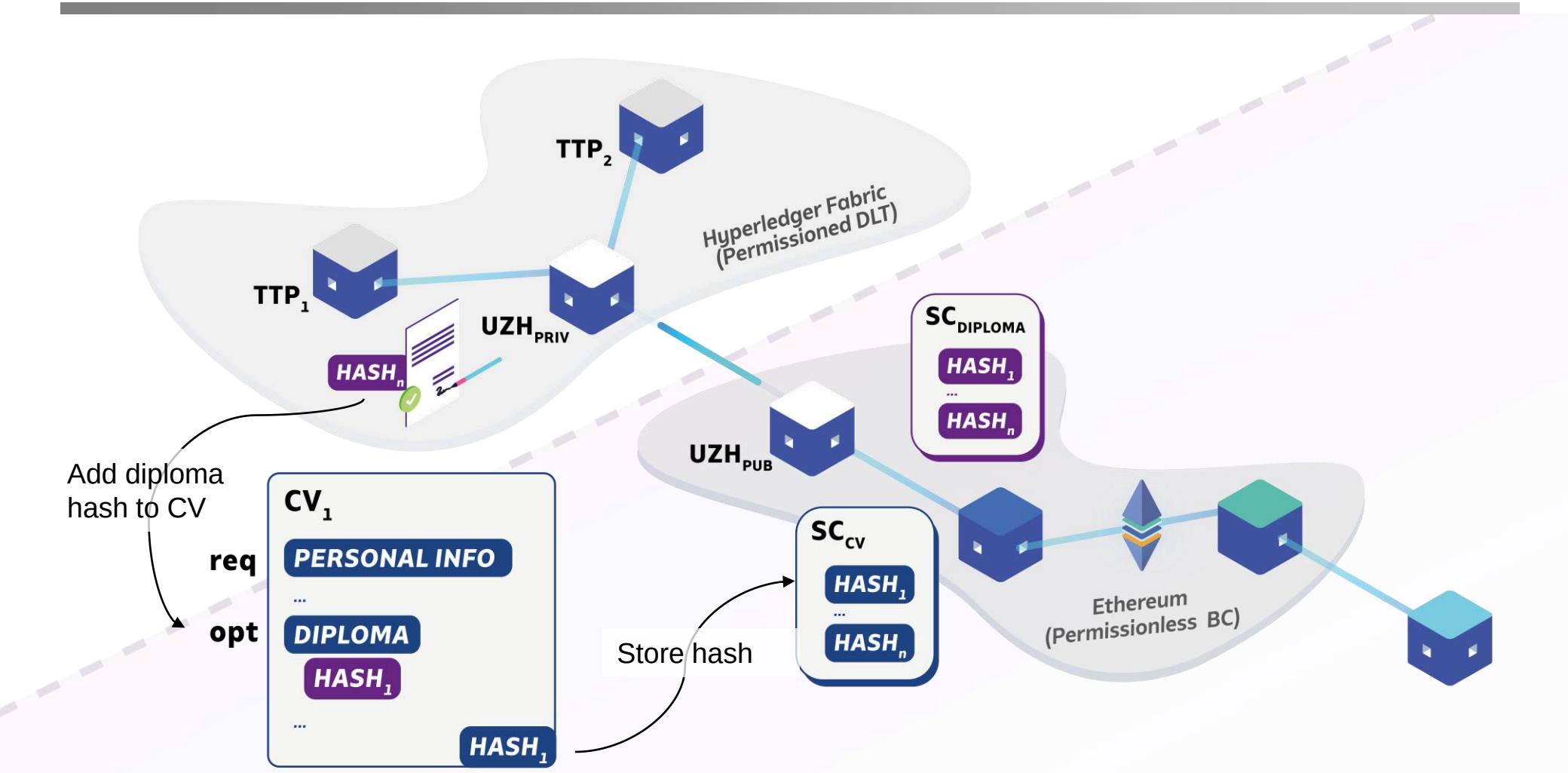
Example EduChain Architecture (2)

Development: (Front-End) Applications, “chaincode”
Infrastructure: Operations and deployment



Development: (Front-End) Applications, Solidity SC
Security: Node operations, key management

Extended EduChain Functionality to CVs



Extended CV Functionality: Data Types

- Example Definition of required data structure

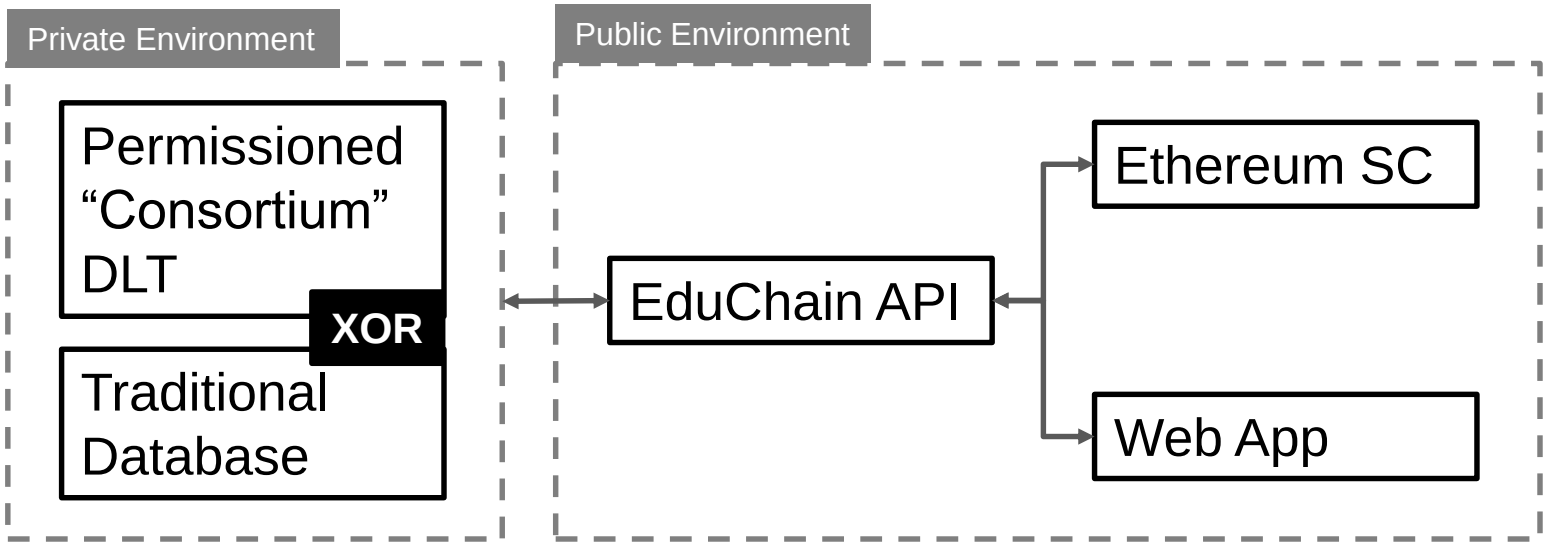

```
{
    "basics": {
        "first name": "John",
        "lastname":"Doe",
        "email": "john@gmail.com",
        "gender": "Male",
        "birthday": "01-01-1990",
        "location": {
            "address": "Binzmühlestrasse 14",
            "countryCode": "CH",
            "postalCode": "8050",
            "city": "Zurich",
            "canton": "Zurich"
            }
    },
    "work": [
        {
            "company": "Universitätsspital Zürich",
            "companyUID": "CHE-108.904.325",
            "position": "System Administrator",
            "startDate": "2013-01-01",
            "endDate": "2014-01-01",
            "hash": "c84f2e7767be14b872b77056d28a1d0c[...]",
            "evidenceURL": "https://educhain.uzh.ch/verify/[...]"}
            ],
    "education": [
            {
            "institution": "University of Zurich",
            "department": "Department of Informatics",
            "degree": "Bachelor's Degree",
            "startDate": "2011-01-01",
            "endDate": "2013-01-01",
            "finalGrade": "4.0",
            "hash": "c84f2e7767be14b872b77056d28a1d0c[...]",
            "evidenceURL": "https://educhain.uzh.ch/[...]"}
```


Personal information

Work experience

Academic degrees

Possible Implementation Paths



Technical Challenges and Decisions

- Storage of Data (Diplomas, CVs)
  - On-chain vs. off-chain?
    - Private permissioned DLT vs. traditional database
    - Cost, privacy
- Storage of certificate identifier (Hashes)
  - Public permissionless BC vs.
    - *E.g.,* Ethereum Smart Contracts
  - Public permissioned BC
    - *E.g.,* own instance of Proof-of-Authority (PoA) Ethereum
- Determination of roles, access policies, IDs

Thank you for your attention.