An Educational Blockchain for the University of Zurich (UZHBC)

Jerinas Gresch,
Bruno Rodrigues, Burkhard Stiller
Communication Systems Group CSG
Department of Informatics IfI
University of Zürich UZH
jerinas.gresch@uzh.ch, [rodrigues¦stiller]@ifi.uzh.ch

Universität Zürich[UZH]

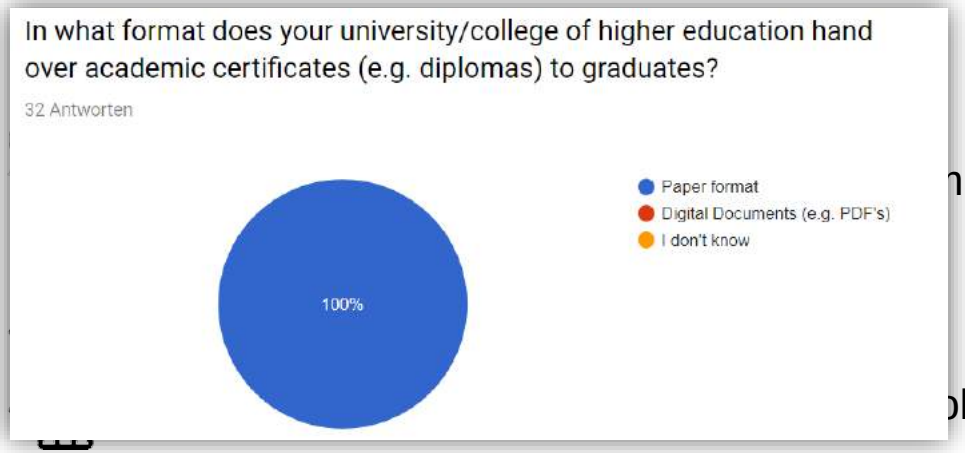
CSG
Communication Systems Group

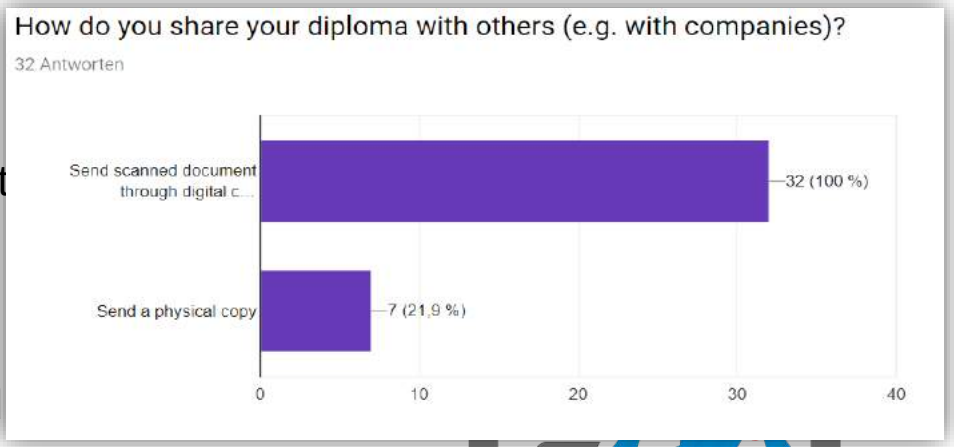
ifi

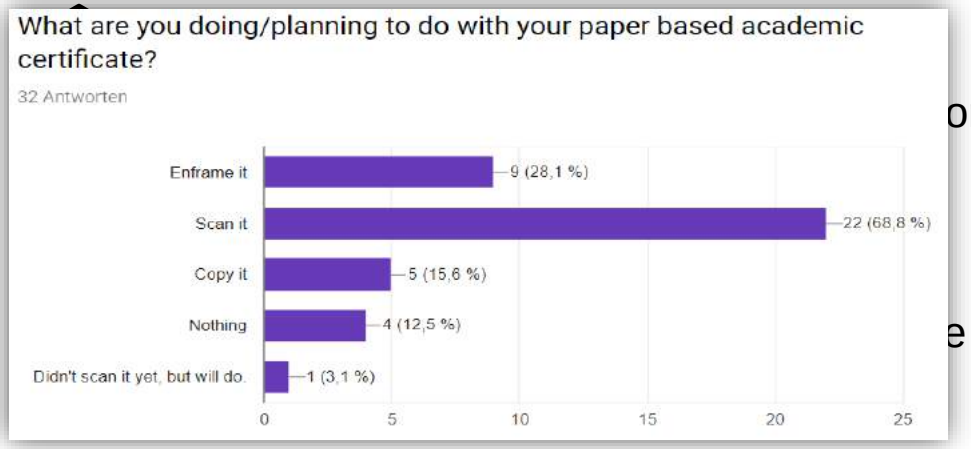
Agenda

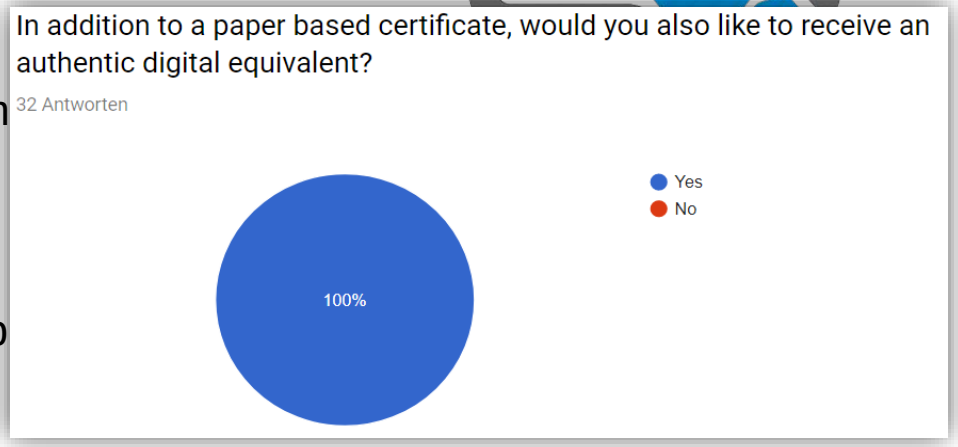
- UZH Basics
- Design
- Demo
- Summary

Introduction









Authenticity of digital copies must be guaranteed!

Goal and Methodology

- Integration of a digital verification system for academic certificates at the UZH
  - Requirement Elicitation
  - Prototype

- Why Blockchain?
  - Immutable
  - No need to maintain a database
  - Different independent issuers

- Methodology

UZH Facts and Stakeholders

- 25.672 Students
- 5.777 Graduations
- 7 faculties
  - Law, theology, economy, natural scientific, philosophy, medicine & veterinary
  - Independent issuance proceedings
- 1-2 verification requests per day

Dean's offices

Student administration office

Diploma office

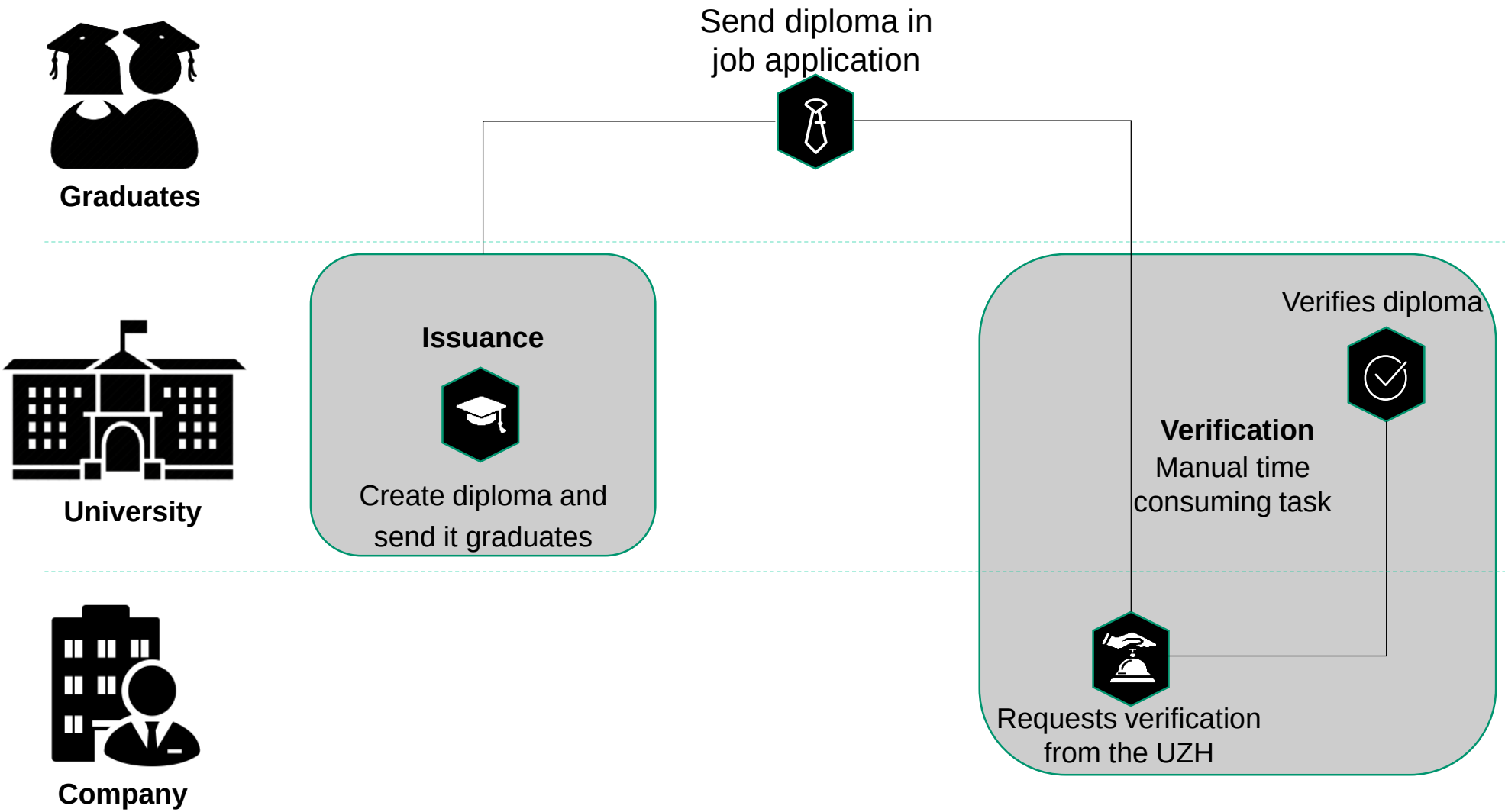
Data security department

IT Services / Infrastructure provider

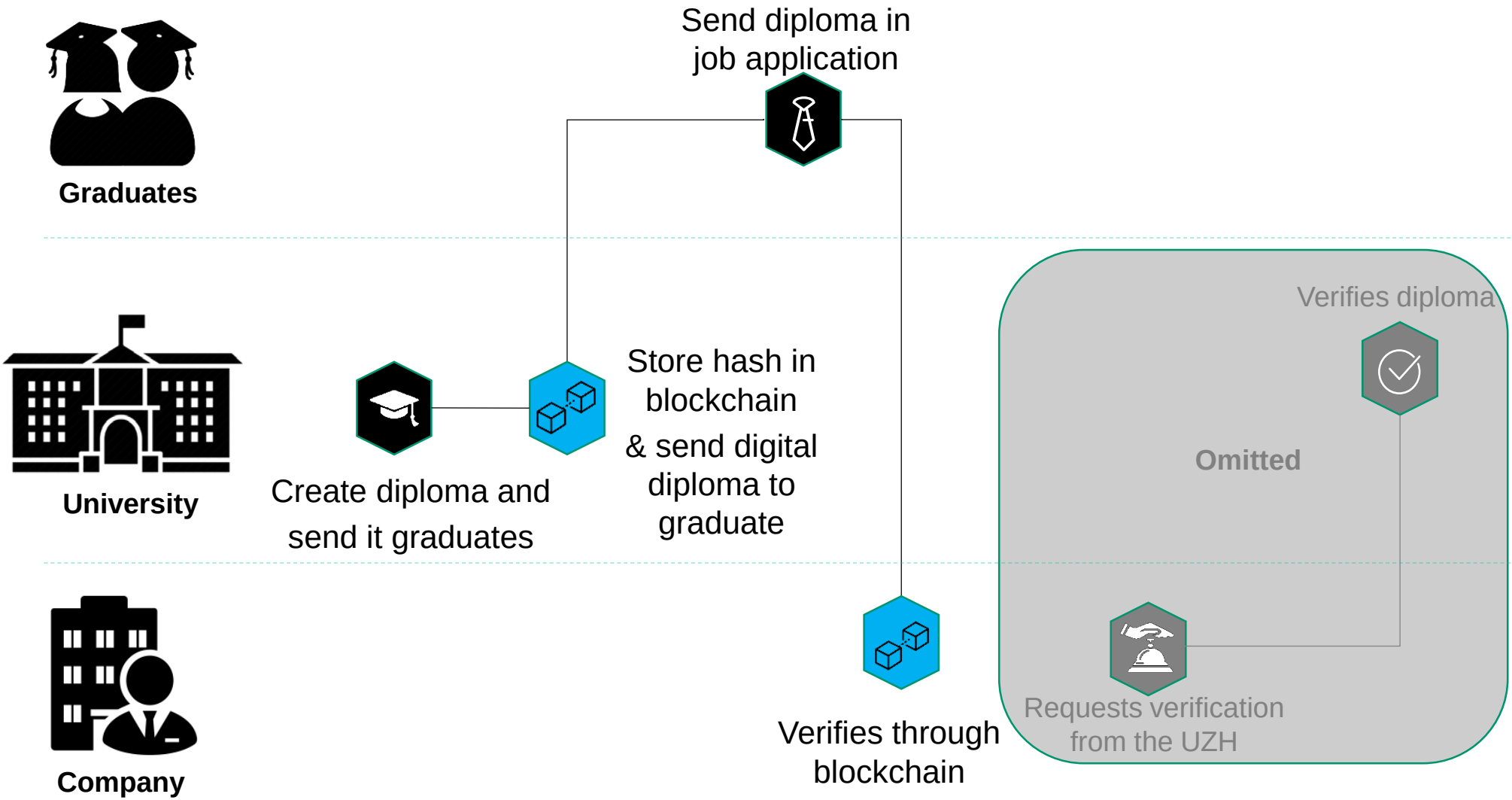
Consolidated UZH Requirements

RQ1	Only authorized UZH dean’s offices are allowed to issue diplomas

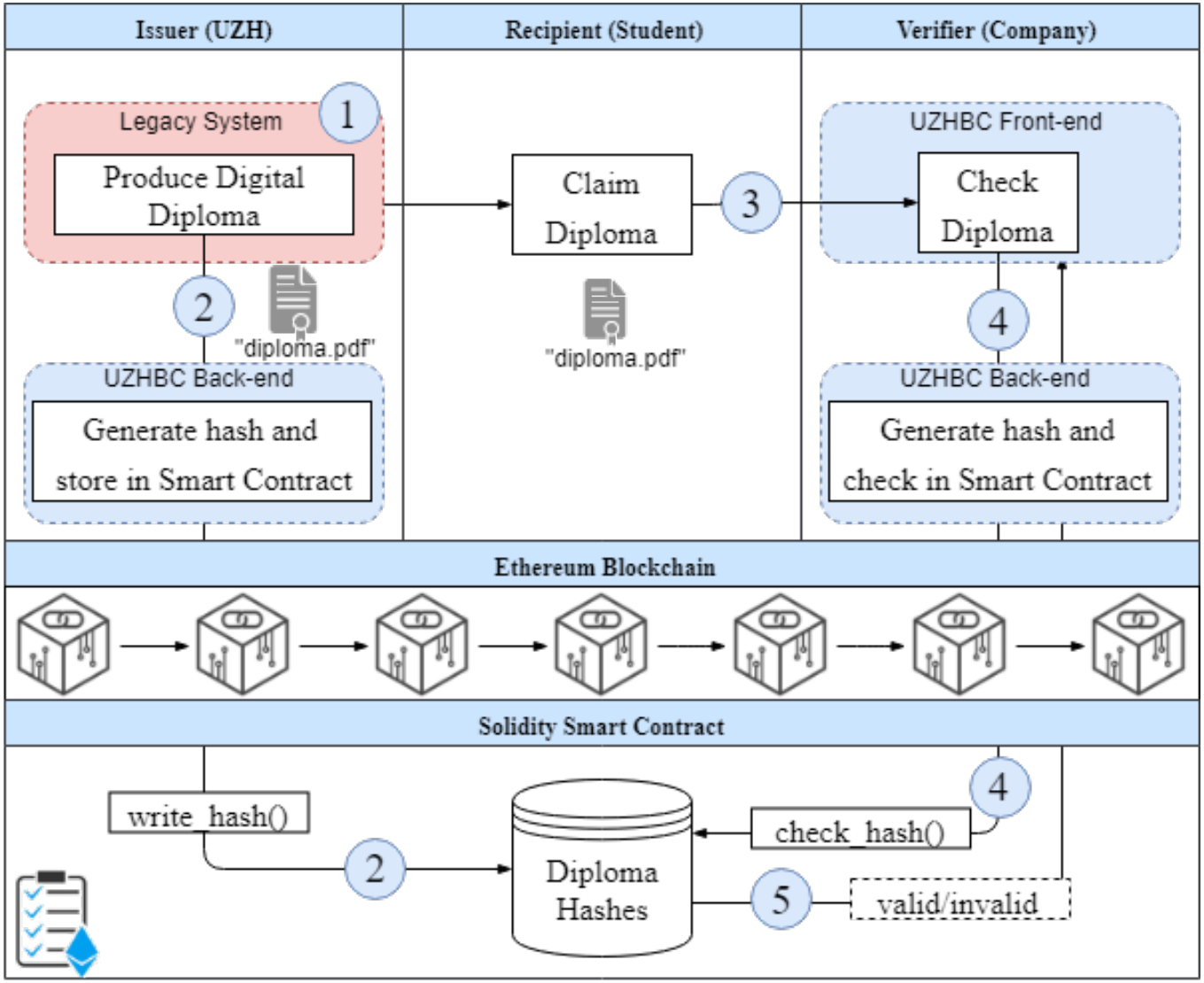
Current UZH Issuance and Verification Process



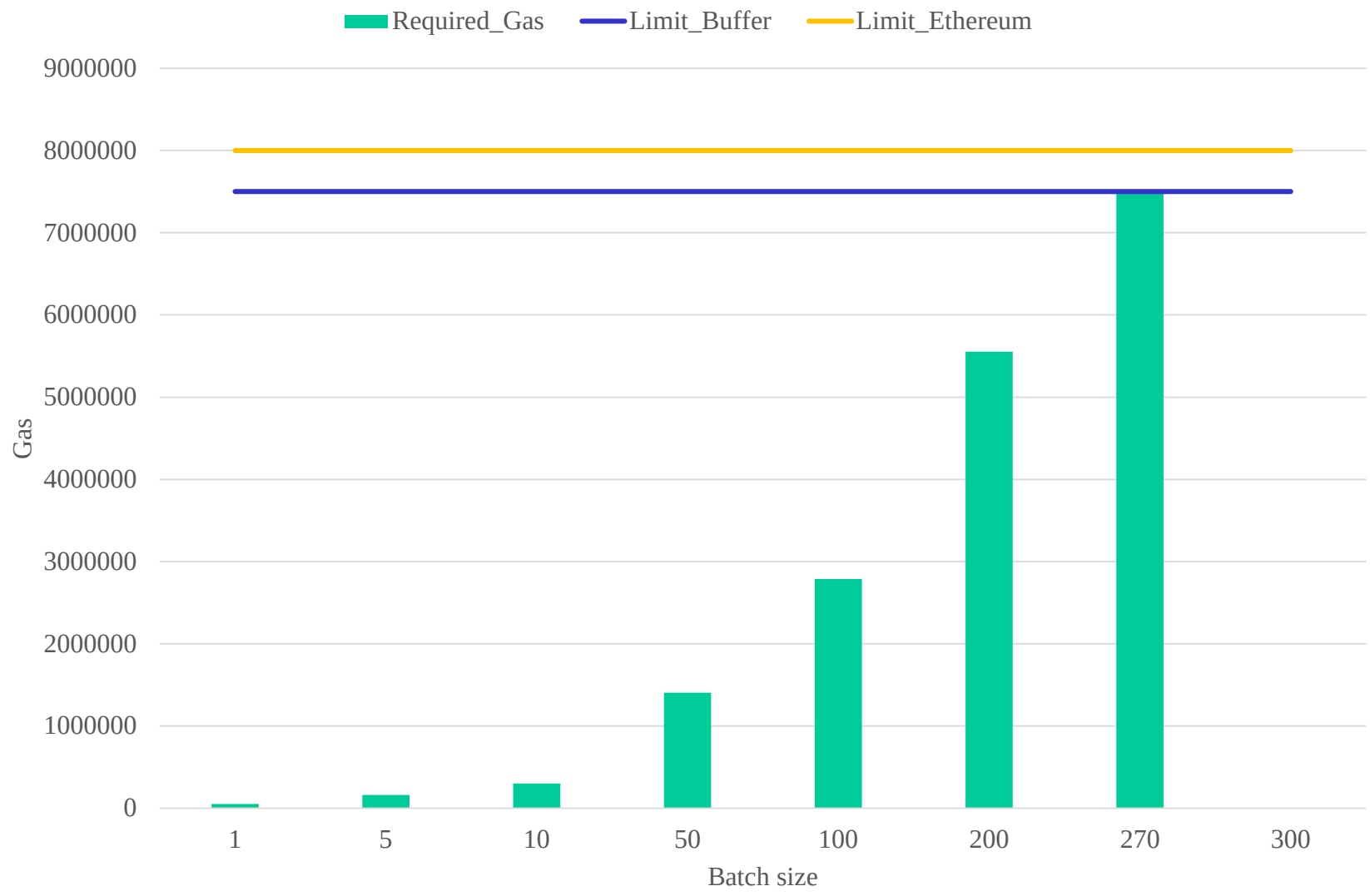
Desired UZH Process



Proposed UZHBC Architecture



Single Transaction vs. Batch

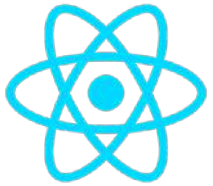


Implementation Details

Algorithm 1: Mechanism to issue files as hashes to a Smart Contract

Input: diploma_Files⟵PDF files that are created by the UZH
Output: Success message from the Smart Contract

```
1  begin
2      hash_List ← filesToSHA3(diploma_Files)
3      batch_Size ← calculateBatchSize(hash_List)
4      num_Of_Batch ← hash_List.size() / batch_Size
5      for each batch ∈ num_Of_Batch:
6          tmp_Batch ←
             slizeToBatch(hash_List, batch · batch_Size, (batch + 1) · batch_Size)
7          unlock_Account(password)
8          if account.status == unlocked:
9              transaction_msg ←
                 web3.UZH_Contract.sendTransaction(owner, tmpBatch)
10             if transaction_msg == success:
11                 msg = transaction_completed
12             else:
13                 msg = transaction_rejected
```



Demo

Related Work

- Many approaches – Not reinventing the wheel
- Not all elements of the related work fit the requirements of the UZH

- i.e. TrueRec
  - Only SAP certificates
  - Certificates have special format
  - Forces all parties to use this app

UNIC

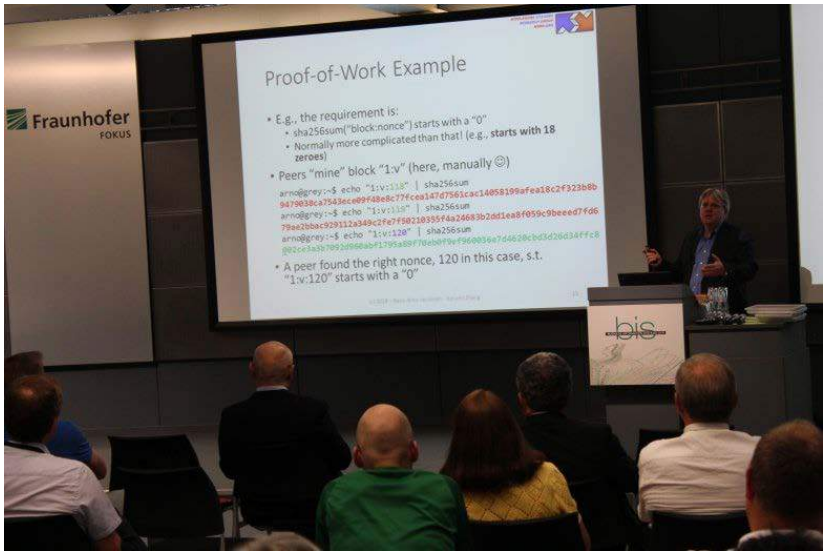
BCDiploma

EDU

grnet

Summary and Future Work

- Approach enable the verification of diplomas using a blockchain
  - Proof of existence
  - Automated verification process
  - Smart Contract can store up to 2^{261} bytes [3]
- Future work
  - More specific Requirements - involve management
  - Regulations
  - Include other institutions
- BIS Recap
  - Wide range of topics
  - Prototype made a good impression
  - Experts & business people



Questions & Discussion

References

1. Musee, Nicholas Mwaniki. "AN ACADEMIC CERTIFICATION VERIFICATION SYTEM BASED ON CLOUD COMPUTING ENVIRONMENT." PhD diss., University of Nairobi (2015).
2. Park, H., Craddock, A.: Diploma Mills: 9 Strategies for Tackling One of Higher Educations Most Wicked Problems (Dec 2017), https://bit.ly/2DoEeyu
3. Vitalik Buterin: Is there a (theoretical) limit for amount of data that a contract can store? (2016), https://bit.ly/2uAAEyd