Privacy Protection in a Blockchain-Based Healthcare System

Supervisor: Chhagan Lal Responsible Professor: Mauro Conti

CSE3000 – Research Project – July 1st, 2021

Ivor Zagorac
i.zagorac@student.tudelft.nl

1. Contributions

- Present **privacy requirements** for blockchain
- Discuss benefits and limitations of **privacy protection techniques** for blockchain and provide a general design
- **Evaluation** of the design based on privacy requirements for healthcare found in research

2. Research Question

How can data confidentiality be achieved in a blockchain-based healthcare system?

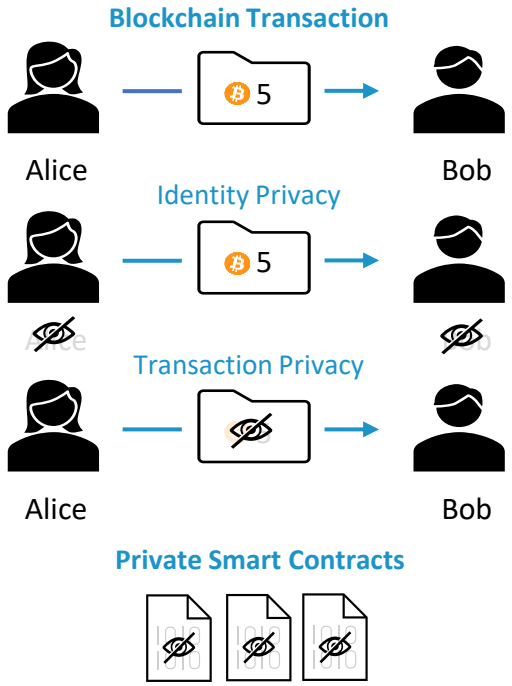
3. Background

1. Blockchain and Smart Contracts
2. Hyperledger Fabric
3. Healthcare Requirements
   - → Device Anonymity
   - → Data Anonymity
   - → Communication Anonymity
   - → Unlinkability

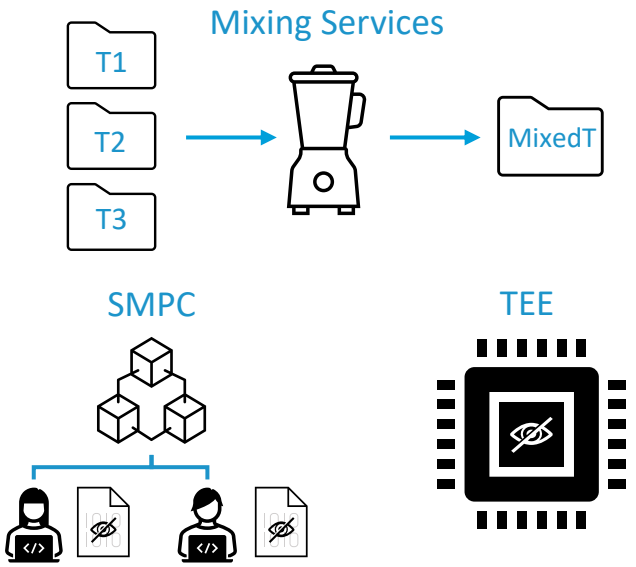
4. Related Work

- Emphasis on security instead of privacy
- Unlinkability requirement was often lacking

5. Privacy requirements



6. Privacy Protection Techniques



7. Evaluation

Healthcare requirements are satisfied when using multiple techniques

8. Conclusion

Combination of mixing services and SMPC are needed to achieve full data confidentiality

9. Future Work

- More research necessary to get rid of TEE limitations
- Implementation details of proposed design

TU Delft