Enhancing Hyperledger Fabric Smart Contracts with Secret Sharing

1 Introduction & Motivation

Hyperledger Fabric: a joint distributed ledger technology blockchain platform for permissioned blockchains

Why?

A distributed ledger solutions supported by a modular architecture providing high degrees of confidentiality.

Scalable and fast while preserving privacy..

high ability of customizing the consensus and network protocols.

Preserving the privacy law of the Netherlands (and EU) and protecting the information of clients.

2 Research Hypothesis

Enhancing the security and privacy of Hyperledger Fabric's smart contracts using secret sharing methods

Are Hyperledger Fabric's smart contracts secure?

What is secret sharing, how does it work?

Combine secret sharing with a Hyperledger Fabric smart contract.

How does that combination affect the performance?

Author: Ali Kahwati
a.kahawati@student.tudelft.nl
Responsible professor
Prof. Dr. Kaitai Liang

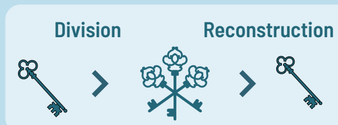
3 Method

Literature Research › Implement Prototype › Test & Analyse › Discussion & Future work

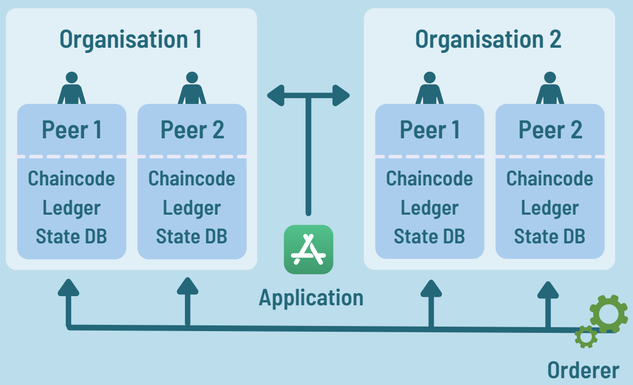
4 Background

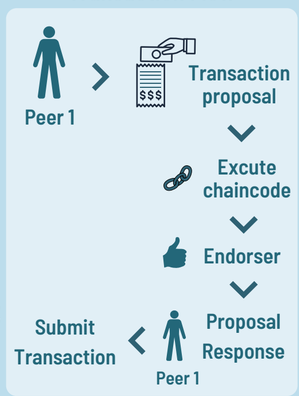
Shamir's Secret Sharing

Distribute key into N useless parts (keys) so that K parts can reconstruct the key.



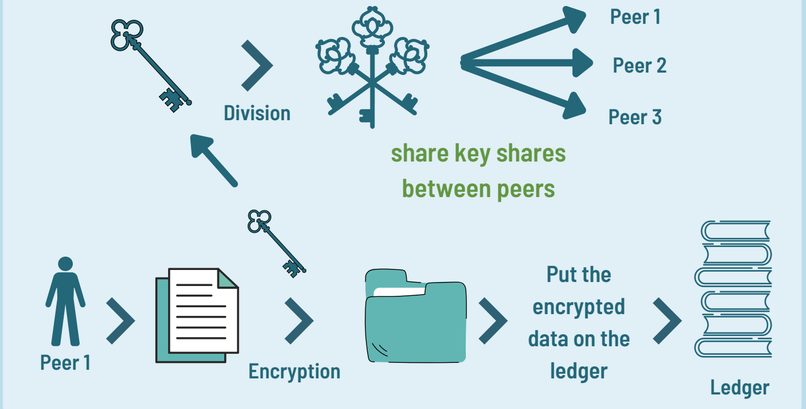
Hyperledger Fabric

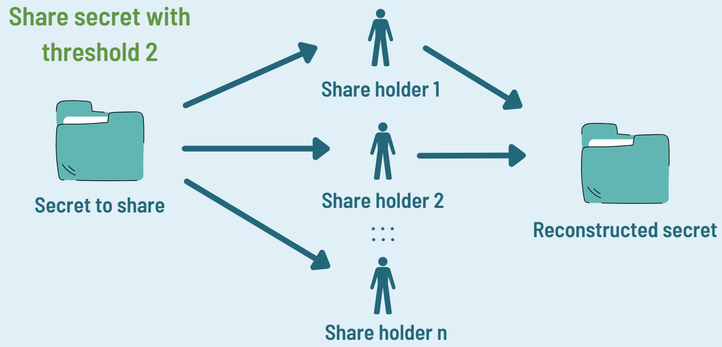




5 Results

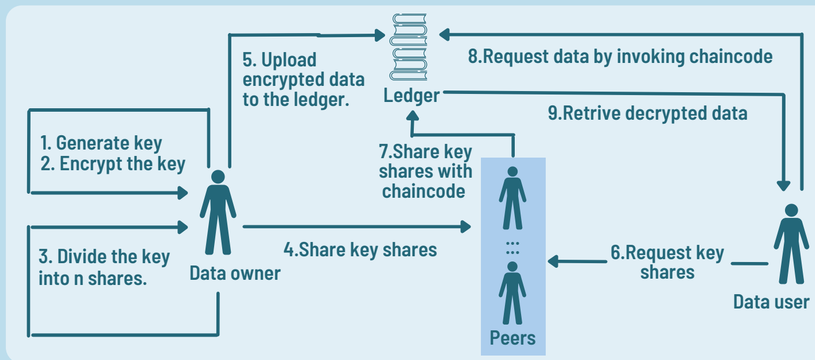
1- Decreasing the complexity of managing a secret key.
2- Increasing the security of the encrypted data
3- keys can be used multiple times.





6 Conclusion

A scheme for enhancing security of Hyperledger Fabric using Secret sharing.



7 Limitation

- Increase runtime complexity
- Multiple peers are needed to retrieve the data.
- Key managment may become underrated
- difficult for peers to have access to the data without having all other peers involved in the transaction.