We implement our protocol with Blockchain systems establish a cryptographically secure data structure for Shamir’s secret sharing scheme can be used to obscure a secret and reveal it in this project we introduce, discuss and simulate a consensus-based secret sharing protocol on smart contracts with the goal of depositing a secret with the blockchain and ensuring data availability to the client nodes.

- Secure: Information-theoretic security.
- Minimal: The size of each secret share does not exceed the size of the original data.
- Extensible: When number of secret holders is kept fixed, new parties can be dynamically added or deleted without affecting the other parties.
- Dynamic: Security can be easily enhanced without changing the secret, but by only constructing new secret shares.

Flexible: In hierarchical organizations, we can supply each participant with different numbers of shares according to their importance. This weighting scheme allows constructing new secret shares.

Properties of DeSO

Future Work, References, and Acknowledgments

Ethereum has demonstrated itself to be secure in practice but at the expense of poor performance.

- We have decided to implement and design a smart contract into Ethereum in order to have a high-performance blockchain without sacrificing security.
- We propose an intermediate “data availability oracle” layer that interfaces between the side blockchains and the trusted blockchain. This oracle layer accepts blocks form side blockchains and pushes verifiable commitments to the trusted blockchain.

- Ethereum test-net Kovan.
- Second in throughput and 6,000x up to 10,000 transactions per implementation demonstrating high-performance into Ethereum via a functionality as a smart contract Rust code, integrate the full functionality in 7,500 lines of

- We have shown how Shamir’s secret sharing scheme can be used to obscure a secret when the majority of the parties in the contract are present.
- We have successfully deposit a secret with the blockchain and have the blockchain keep the secret and use it only in the specified manner (only when a specified number of members “vote” to reveal the secret).
- We have shown that our service can be used in disaster management, where medical records may be considered secret and these secrets needs to be released at the disaster time only to the appropriate authorities so that medicines can be availed in time.

We propose an intermediate “data availability oracle” layer that interfaces between the client nodes and the trusted blockchain. DeSO uses SSS in order to create secret shares and distribute it between client nodes. The oracle layer accepts secret share blocks from clients, pushes verifiable commitments to the trusted blockchain and ensures data availability to the client nodes.

- We have shown that our service can be used in disaster management, where medical records may be considered secret and these secrets needs to be released at the disaster time only to the appropriate authorities so that medicines can be availed in time.

We have proposed and developed DeOS as a solution to allow a public blockchain to act as a trusted long-term repository of secrets.

- We have shown how Shamir’s secret sharing scheme can be used to obscure a secret when the majority of the parties in the contract are presented.

- We have Successfuly deposit a secret with the blockchain and have the blockchain keep the secret and use it only in the specified manner (only when a specified number of members “vote” to reveal the secret).

- We have shown that our service can be used in disaster management, where medical records may be considered secret and these secrets needs to be released at the disaster time only to the appropriate authorities so that medicines can be availed in time.

• Blockchain systems establish a cryptographically secure data structure for storing data in the form of a hash chain.

• Smart contracts on a blockchain permit the performance of credible transactions without the involvement or oversight of a third party. However, in a smart contract, information needs to be known and independently verified.

• Shamir’s secret sharing scheme can be used to obscure a secret and reveal it only when the majority of the parties in the contract are present.

• In this project we introduce, discuss and simulate a consensus-based secret sharing protocol on smart contracts with the goal of depositing a secret with the blockchain, having the blockchain keep the secret and use it only in the specified manner (only when a specified number of members “vote” to reveal the secret).

• We implement our protocol with DeSO: Decentralized Secret Oracle for Blockchain

STUDENTS: Milad Fotouhi
SPONSORS: National Science Foundation
ADVISORS: Sreeram Kannan, Payman Arabshahi, Wei Cheng