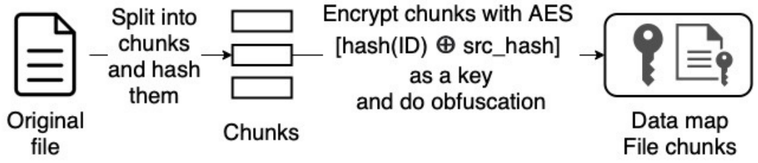
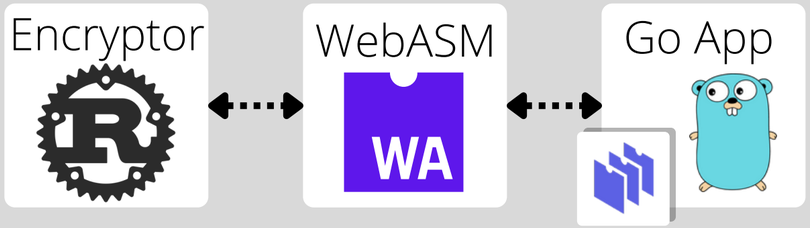
ID-based self-encryption via Hyperledger Fabric-based smart contract

Introduction

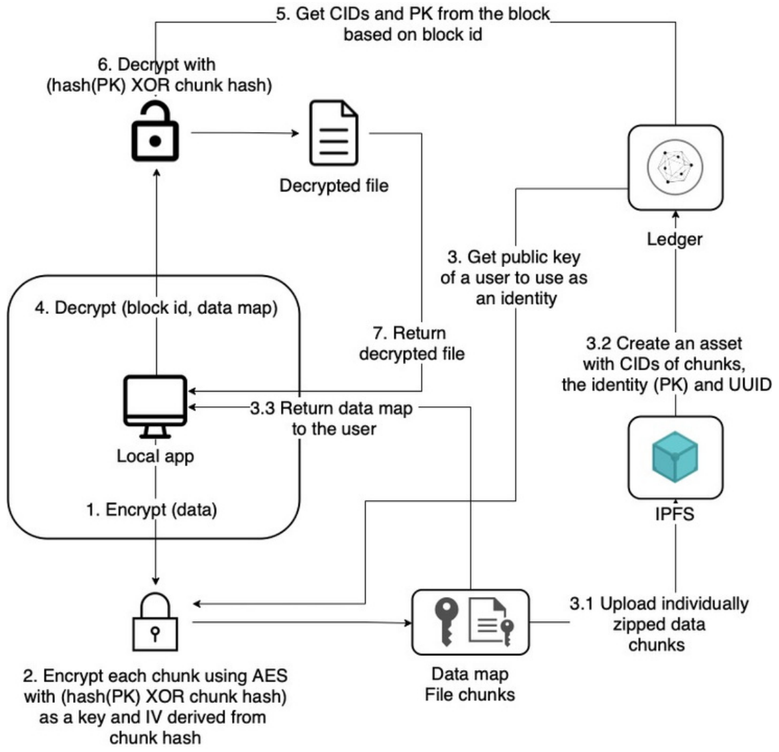
- **Hyperledger Fabric** is a privacy focused permissioned blockchain [1]
- **Self-encryption** allows to encrypt files without user intervention or password [2]

ID-based self-encryption



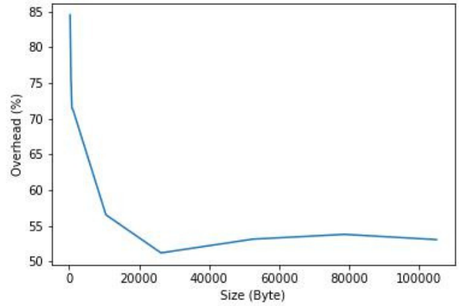


Methodology



Results

- **WASM** has ~50% overhead when the file that is being encrypted is larger than 25MB



Discussion & Conclusion

- The work can be expanded by **analyzing the CPU and memory load** of the WASM library in a standardized way [3]

- **ID-based self-encryption** improves security of file storage on the Hyperledger Fabric blockchain and overall trust in the system

[1] E. Androulaki κ.ά., 'Hyperledger fabric: a distributed operating system for permissioned blockchains', στο Proceedings of the thirteenth EuroSys conference, 2018, σσ. 1–15.
[2] D. Irvine, 'Self encrypting data', 2010.
[3] I. Gouy, "Toy benchmark programs." [Online]. Available: https://benchmarksgame-team.pages.debian.net/benchmarksgame/ why-measure-toy-benchmark-programs.html

Author: Ilya Grishkov (I.Grishkov-1@student.tudelft.nl)
Responsible professor : Kaitai Liang (Kaitai.Liang@tudelft.nl)
Supervisor: Roland Kromes (R.G.Kromes@tudelft.nl)