Abstract

Today, there is an increasing need for an efficient threshold signatures that enforce the protection of identities and multi device-based authentication when interacting with a blockchain technology. This study presents a comprehensive analysis of threshold signatures, establishing FROST as the most efficient scheme in terms of performance. We uniquely demonstrate FROST's adaptability with empirical results, showcasing its feasibility on middle-range IoT devices and smartphones. In addition, we propose an implementation, with a primary goal to enable IoT devices interaction with Hyperledger Fabric v3.0 using FROST for transaction signing. An IoT network of 5 devices can perform a signature and commit to the blockchain ledger in 3.2 seconds, when network latency is optimal. Index Terms—IoT, FROST, Blockchain, Privacy