6th Workshop on Trusted Smart Contracts

In Association with Financial Cryptography 2022

May 6, 2022

Title: Towards Smart Contract-based Verification of Anonymous Credentials

Authors: Robert Muth, Tarek Galal, Jonathan Heiß, and Florian Tschorsch.

Abstract

Smart contracts often need to verify identity-related information of their users. However, such information is typically confidential, and its verification requires access to off-chain resources. Given the isolation and privacy limitations of blockchain technologies, this presents a problem for on-chain verification.

In this paper, we show how CL-signature-based anonymous credentials can be verified on smart contracts using the example of Hyperledger Indy, a decentralized credential management platform, and Ethereum, a smart contract-enabled blockchain. Therefore, we first outline how smart contract-based verification can be integrated in the Hyperledger Indy credential management routine and, second, provide a technical evaluation based on a proof-of-concept implementation of CL-signature verification on Ethereum. While our results demonstrate technical feasibility of smart contract-based verification of anonymous credentials, they also reveal technical barriers for its real-world usage.