6th Workshop on Trusted Smart Contracts

In Association with Financial Cryptography 2022

May 6, 2022

Title: Hours of Horus: Keyless Cryptocurrency Wallets

Authors: Dionysis Zindros.

Abstract

We put forth a *keyless wallet*, a cryptocurrency wallet where money can be spent using a password alone, and no private keys are required. It requires a smart contract blockchain. We propose a scheme in which the user uses an OTP authenticator seed to generate a long series of time-based OTP passwords for the foreseeable future. These are encrypted and organized in a Merkle tree whose root is stored in a smart contract. The user can spend funds at any time by simply visually providing the current OTP password from an air gapped device. These OTPs can be relatively short: Just 6 alphanumeric characters suffice. Our OTP scheme can work in proof-of-stake as well as static and variable difficulty proof-of-work blockchains. The low-entropy passwords and OTPs in our scheme are protected from brute force attacks by requiring that an adversary accompany any attempt by a transaction on the chain. This quickly incurs enormous economic costs for the adversary. Thus, we develop the first decentralized *rate limiting* scheme. We use *Witness Encryption* (WE) to construct a timelock encryption scheme in which passwords are encrypted from past into future blocks by leveraging the NP-language having proof-of-work or proof-of-stake performed as the witness. Witness Encryption is a currently impractical cryptographic primitive, but our scheme may become practical as these primitives are further developed.