6th Workshop on Trusted Smart Contracts

In Association with Financial Cryptography 2022

May 6, 2022

Title: Not so immutable: Upgradeability of Smart Contracts on Ethereum

Authors: Mehdi Salehi, Jeremy Clark, and Mohammad Mannan.

Abstract

A smart contract that is deployed to a blockchain system like Ethereum is, under reasonable circumstances, expected to be immutable and tamper-proof. This is both a feature (promoting integrity and transparency) and a bug (preventing security patches and feature updates). Modern smart contracts use software tricks to enable upgradeability, raising the research questions of how upgradeability is achieved and who is authorized to make changes. In this paper, we summarize and evaluate six upgradeability patterns. We develop a measurement framework for finding how many upgradeable contracts are on Ethereum that use certain prominent upgrade patters. We find 1.4 million proxy contracts which 8,225 of them are unique upgradeable proxy contracts. We also measure how they implement access control over their upgradeability: about 50% are are controlled by a single Externally Owned Address (EOA), and about 20% are controlled by multi-signature wallets in which a limited number of persons can change the whole logic of the contract.