6th Workshop on Trusted Smart Contracts

In Association with Financial Cryptography 2022

May 6, 2022

Title: Not All Code are Create2 Equal

Authors: Michael Fröwis and Rainer Böhme.

Abstract

We describe the impact and measure the adoption of the CREATE2 instruction introduced to the Ethereum Virtual Machine in the Constantinople upgrade. This change to Ethereum's execution environment is fundamental because it enables to modify the program stored on a given address after deployment, making it much harder to reason about the immutability of smart contracts. We enumerate six use cases and novel attack vectors, and present empirical evidence from all 32 million code accounts created between March 2019 and July 2021. The data shows that the main beneficiaries of the upgrade are wallet contracts, which can now use predictable addresses. But they do not require the more risky feature of mutable smart contracts. So far, the only applications that use the latter are front-running bots and gas tokens.