Verifying zkEVMs: Making Large Scale Formal Verification Work

Alexander Hicks
Ethereum Foundation, London, UK

Abstract

The effort to formally verify core parts of zkVMs for their deployment on the Ethereum L1 has been ongoing for over a year now, with many teams involved and progress across several axes. This talk will focus on formally verifying such a large, complex, and unstable stack, the lessons learned, and the remaining challenges.

2012 ACM Subject Classification Software and its engineering → Formal software verification

Keywords and phrases Formal Verification, Zero-Knowledge Virtual Machines

Digital Object Identifier 10.4230/OASIcs.FMBC.2026.2

Category Invited Talk

Bio

Alexander Hicks is a researcher at the Ethereum Foundation where he leads the Protocol Snarkification team focusing on formal verification. As part of this he oversees the `verified-zkevm.org` project to formally verify critical components of zkVMs ahead of their deployment on the Ethereum L1.

7th International Workshop on Formal Methods for Blockchains (FMBC 2026).
Editors: Massimo Bartoletti and Diego Marmsoler; Article No. 2; pp. 2:1–2:1

OpenAccess Series in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany