Scaling Formal Verification Across DeFi Ecosystems

Pamina Georgiev
Certora, Seattle, WA, USA

Abstract

Formal verification is essential for ensuring the safety of smart contracts in decentralized finance (DeFi), but scaling these techniques across diverse blockchain ecosystems remains a challenge. In this talk, we present our experience making formal verification practical across multiple platforms, including the EVM, Solana, Stellar, and Sui. We discuss how automated reasoning techniques can be adapted to different execution models and programming paradigms while still providing strong correctness guarantees. We focus on what it takes to apply verification in real-world settings: handling complex DeFi primitives, integrating with development workflows, and maintaining usability for engineers. Drawing from verification projects with production protocols, we highlight key challenges and lessons learned in bringing formal methods from theory into practice.

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

Keywords and phrases Formal Verification, Smart Contracts

Digital Object Identifier 10.4230/OASIcs.FMBC.2026.1

Category Invited Talk

Bio

Pamina Georgiev is a Formal Verification Team Lead at Certora, where she focuses on ensuring the safety and correctness of smart contracts across the DeFi ecosystem. Her work centers on applying and scaling automated reasoning techniques to real-world DeFi systems, working closely with customers to verify complex protocols and deliver strong correctness guarantees. She received her PhD in Automated Reasoning from TU Wien under the supervision of Prof. Laura Kovács, where her research focused on program verification and logic-based methods. At Certora, she leads the team working on verification projects for major DeFi protocols across multiple blockchain platforms, including the EVM, Solana, Stellar, and Sui, helping bring formal verification into practical, high-stakes development workflows.

7th International Workshop on Formal Methods for Blockchains (FMBC 2026).
Editors: Massimo Bartoletti and Diego Marmsoler; Article No. 1; pp. 1:1–1:1
OpenAccess Series in Informatics
OASICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany