# Is Formal Verification Practical?

**Wolfgang Grieskamp**
Aptos Labs, Palo Alto, CA, USA

## Abstract

There is arguably no other domain in which the prospect of formal verification is as promising as in the area of smart contracts. Smart contracts are small- to medium-sized programs which are strongly isolated from external components. They handle high-value digital assets, and correctness is of utmost importance. Many large-impact bugs and exploits have been documented over the years. Bug bounty programs for contracts are common in the industry, offering awards in the millions of dollars, making the cost of bugs exorbitant, and the motivation for better solutions high. *Move* is a newer smart contract language used by multiple blockchains and has been designed at Meta from the ground up with formal verification in mind, featuring an integrated specification language and semantics well suited for formal reasoning. This opportunity resulted in the *Move Prover* [1], a tool that has been successfully used in the exhaustive formal verification of Diem at Meta, as well as for the frameworks of the Aptos protocol [2]. However, even though extensive work has been invested in the Move Prover to make it feasible for regular developers, most applications of the prover required specifically skilled engineers and tedious detail work to succeed, preventing it from going mainstream. In this talk, we explore the state-of-the-art of formal verification for Move. We identify the challenges that users face when trying to apply formal verification and point out future research directions to improve the expressiveness and usability of the Move Prover.

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

**Keywords and phrases** Formal verification, smart contracts, Move

**Digital Object Identifier** 10.4230/OASIcs.FMBC.2025.1

**Category** Invited Talk

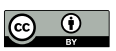
## Bio

Dr. Wolfgang Grieskamp is the head of the Move platform team at Aptos Labs, a startup incubated out of the previous work on blockchain technology at Meta between 2018 and 2021. At Aptos, Wolfgang helps operate the Aptos blockchain, a high-tps, low-latency layer 1 blockchain, which went to mainnet in 2022. He leads the work on the Move language, compiler, virtual machine, developer tooling, and formal verification. Before joining Aptos, Wolfgang was part of the Diem team (formerly Libra) at Meta, where he developed the Move Prover together with a team of fellow researchers. Before joining Meta, Wolfgang worked for a decade at Google on multiple projects in cloud computing and AI. Before Google, Wolfgang spent most of the 2000s at Microsoft Research, where he developed specification languages and related tools. Wolfgang obtained a PhD in 1999 from the Technical University of Berlin in the area of programming languages and systems. His publication record includes over 40 peer-reviewed articles at conferences and in journals.

## References

1 David Dill, Wolfgang Grieskamp, Junkil Park, Shaz Qadeer, Meng Xu, and Emma Zhong. Fast and reliable formal verification of smart contracts with the move prover. In Dana Fisman and Grigore Rosu, editors, *Tools and Algorithms for the Construction and Analysis of Systems*, pages 183–200, Cham, 2022. Springer International Publishing.

2 Junkil Park, Teng Zhang, Wolfgang Grieskamp, Meng Xu, Gerardo Di Giacomo, Kundu Chen, Yi Lu, and Robert Chen. Securing Aptos Framework with Formal Verification. In Bruno


© Wolfgang Grieskamp;
licensed under Creative Commons License CC-BY 4.0

Bernardo and Diego Marmsoler, editors, *5th International Workshop on Formal Methods for Blockchains (FMBC 2024)*, volume 118 of *Open Access Series in Informatics (OASIcs)*, pages 9:1–9:16, Dagstuhl, Germany, 2024. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. doi:10.4230/OASIcs.FMBC.2024.9.