Formal Methods for the Security Analysis of Smart Contracts

Mattei Maffei
TU Wien
Vienna, Austria
matteo.maffei@tuwien.ac.at

***Abstract*—Smart contracts consist of distributed programs built over a blockchain and they are emerging as a disruptive paradigm to perform distributed computations in a secure and efficient way. Given their nature, however, program flaws may lead to dramatic financial losses and can be hard to fix. This motivates the need for formal methods that can provide smart contract developers with correctness and security guarantees, ideally automating the verification task.**

This tutorial introduces the semantic foundations of smart contracts and reviews the state-of-the-art in the field, focusing in particular on the automated, sound, static analysis of Ethereum smart contracts. We will highlight the strengths and drawbacks of different methods, suggesting open challenges that can stimulate new research strands. Finally, we will overview eThor, an automated static analysis tool that we recently developed based on rigorous semantic foundations.

https://doi.org/10.34727/2021/isbn.978-3-85448-046-4_3