ABC Research GmbH
Favoritenstraße 111
1100 Wien

Research Concept: Formal Verification Tool

Smart contracts on a blockchain are highly susceptible to attacks. There are often strong incentives for manipulation (e.g., transfer of valuable assets), their code is visible for any potential attacker and security vulnerabilities can hardly be fixed after deployment due to the immutability property of the blockchain. Security analysis of smart contracts is therefore of utmost importance. Formal verification methods can prove their correctness, but such analyses are technically challenging and require specialized expertise. Tools that can automate this process and make it accessible for ordinary smart contract developers would vastly improve security in distributed blockchain applications.

Although some tools can already detect common smart contract bugs, a suitable formal verification tool that can reliably detect any security vulnerability has not been available until now. Therefore, Prof. Maffei and his team at TU Wien have developed eThor[1], the first sound and automated static analyzer for EVM bytecode, the smart contract platform of the Ethereum blockchain. It is able to detect reentrancy vulnerabilities, check user-defined assertions, and verify contract-specific pre- and post-conditions.

Project Goals

The main goal of the envisioned research project is to extend and adapt the current academic prototype of the described static analysis tool for usage in real-world practical scenarios. This comprises two major objectives:

- ***Usability for smart contract developers:*** Developer-friendly mechanisms for the definition of application-specific security constraints and the display of verification results in a comprehensible way (e.g., by marking vulnerable parts in the Solidity source code and describing the possible attack scenarios) shall be researched.
- ***Applicability in complex DApps:*** The effectiveness and practical feasibility of the formal verification approach shall be tested in the context of real-world decentralized applications that feature complex data structures and multiple interrelated smart contracts. A decentralized voting application with sophisticated access management and highest privacy constraints shall be used as an initial example. This part may target optimizations regarding the precision and performance of the tool as well as extensions that consider cross-contract relations in the static analysis.

Our long-term vision is to develop a widely-adopted open source tool for smart contract verification (as part of a larger development toolchain) that helps to increase security in blockchain environments. Other future research topics include the development of similar tools for additional smart contract platforms (e.g., Hyperledger Fabric chaincode) on top of the generic static analysis framework[2] that serves as eThor's foundation.

[1] see https://informatics.tuwien.ac.at/news/1883 and https://secpriv.wien/ethor/
[2] see https://secpriv.wien/horst/