Karlsruher Institut für Technologie

Institut für Theoretische Informatik (ITI)
Anwendungsorientierte Formale Verifikation
Prof. Dr. Bernhard Beckert

Praxis der Forschung

Scheduling Attacks on Smart Contracts

Background.
Smart contracts are programs that work on a blockchain or a distributed ledger (e.g, Ethereum or Hyperledger Fabric). They take control over assets in that ledger and manage them autonomously, according to their program logic. Since smart contracts are hard to change after deployment, programming errors usually have very serious consequences. Furthermore, smart contract source code is often open for all to see, so that exploits can and will be found by adversaries. Therefore, it is necessary that smart contracts are correct upon deployment, and formal methods are needed to ensure this.

Problem Description.
On smart contract platforms, nodes collaborate to establish a single view of a shared state. However, the power to determine the order of transactions, at least within one block, always lies with a single actor. This power can be used to achieve an unfair advantage for an attacker.

Goals.
The goal of this project is to analyse the vulnerability of smart contracts to scheduling attacks. This includes examining different smart contract platforms as to their scheduling architecture, using formal methods to reason about scheduling vulnerabilities, and finding ways to avoid these vulnerabilities in smart contracts.

Kontakt
Jonas Schiffl jonas.schiffl@kit.edu Office: 50.34, R226