Lehrstuhl für Sicherheit in der Informatik
Prof. Dr. Claudia Eckert

In cooperation with Fraunhofer AISEC

Verifiying Correctness of Smart Contracts

Motivation and Topic

Blockchains guarantee non-repudiation of decentralized information stored in the *ledger*, a distributed network of peers. Apart from merely storing information, most blockchains have the capability of executing *smart contracts* – small programs which may manipulate information stored in the blockchain and are executed in consensus by the peers. Depending on the expressivity of programming languages and execution environments of smart contracts, these programs can be limited to specific purposes – such as simple transactions in the case of Bitcoin – or be turing-complete programming languages with powerful APIs in case of Ethereum.

Correctness of smart contracts is of utter importance, as once deployed, a smart contract usually cannot be changed anymore and many applications put extremely high stakes into the correct execution of a smart contract, as shown by the hack of the DAO where an incorrect smart contract resulted in a $60m loss which could only be resolved by a hard fork of the Ethereum blockchain.

At the same time, smart contracts are small programs which operate against a limited and clearly defined API interface, which makes them perfect targets for automated verification.

The goal of this thesis is to first research the current state of the art in smart contracts and methods for formal verification of such. The scope will be further limited to a specific target platform, such as the mining-less Hyperledger blockchain and its Java-based smart contract implementation. In a second step, an approach for verification of smart contracts will be derived and implemented as a prototype.

Requirements

- Programming skills (mainly Java, some understanding of Go might help but is no prerequisite)
- A preliminary basic understanding of Blockchain technology
- Interest in program verification
- Ability to work self-directed and systematically

The thesis can be written in English or German.

Contact

Fraunhofer Institute for Applied and Integrated Security (AISEC)
Dr. Julian Schütte, Christof Ferreira Torres
E-Mail: julian.schuette@aisec.fraunhofer.de
Phone: +49 89 322-9986-173