Motivation

Smart contracts are blockchain-powered computer protocols that are intended to facilitate, verify, or enforce a digital agreement between mutually untrusted parties (users) automatically and without the use of any trusted authorities (such as notary services and law enforcement agencies).

A smart contract is able to automatically manage financial transactions between its users, based on the rules that were encoded by the smart contract developer using a Turing complete programming language such as Solidity. Once a smart contract is deployed to the blockchain, its code cannot be modified and its successful transactions cannot be reverted. This gives a new meaning to the phrase “code is law”, because any unintentional behavior (or bug) encoded by the developer in the smart contract can be used by malicious actors to drain funds from that contract. Smart contract bugs have lead to 100s of millions of USD in losses for both users and developers. Therefore, nowadays all responsible smart contract developers seek the help of security experts.

In collaboration with US-based blockchain startup

This Master thesis will be co-supervised by Quantstamp – a blockchain startup located in San Francisco, USA. Quantstamp provides security services to smart contract developers and helps to secure smart contracts at scale using computer-aided reasoning tools. Its mission is to help boost adoption of exponentially growing blockchain technology. Quantstamp’s team boasts decades of combined experience in formal verification, static analysis, and software verification. In its mission to proliferate development and adoption of blockchain applications, Quantstamp is developing a new protocol for smart contract security assurance. Security policies that can correctly specify what are the conditions under which an attack or vulnerability is detected are at the core of the Quanstamp Security Assurance Protocol and the core focus of this thesis.

Goals of the thesis

The goal of this thesis is to develop a methodology for engineering smart contract security policies for a wide range of smart contracts written in Solidity, for the Ethereum Virtual Machine. The key aspect of the result is its usability by non-technical users. This methodology must be implemented and integrated with the existing Quantstamp Security Assurance Protocol and evaluated using a scientific control experiment.

We offer

- Co-supervision by rockstar research engineers from Quantstamp
- An opportunity to work on exciting research problems relevant for real world systems
- The potential to evaluate the implementation in the Quantstamp community (> 10K users)

Contact

Prof. Dr. Alexandra Dmityrienko alexandra.dmitrienko@uni-wuerzburg.de
Informatikgebäude M2, 1.OG, office A115

Dr. Sebastian Banescu sebi@quantstamp.com

Julius-Maximilians-Universität, Würzburg