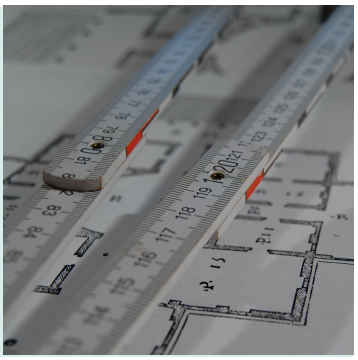
Karlsruhe Institute of Technology

Institut für Programmstrukturen und Datenorganisation (IPD)
Lehrstuhl für Software-Entwurf und -Qualität, Prof. Reussner

Software Design and Quality

Bachelorarbeit/Masterarbeit

Generation of Formal Specifications for Smart Contracts from Architectural Specifications



Motivation

Smart contracts are programs that run on a blockchain infrastructure. They take control over assets on that infrastructure and perform automated, deterministic execution of an agreement between network participants.
Smart contracts are a prime target for security attacks, because they manage resources representing valuable assets. Due to their distributed nature, bugs are hard to fix which makes them susceptible to attacks exploiting programming errors. This makes rigorous formal analysis of smart contracts highly desirable. Security risks in smart contracts can also arise due to their distributed interaction and deployment. Capturing such characteristics on code-level is difficult. Therefore architecture description languages like the Palladio Component Model (PCM) can be used to provide a more complete model of the system. To benefit from the architecture as well as the code, our goal is the usage of the PCM to create a precise model of a smart contract's functionality and interaction to enable the generation of formal specifications on the source-code level.

Tasks

Your research is located on the connection between the architectural domain and the source-code and verification domain for blockchain and smart contracts including

- Research about smart contract properties that can be described on architectural level
- Extension of the Palladio Component Model for a selection of these properties
- Automatic generation of formal specification

We provide

- Work on current technologies and topics like blockchain and smart contracts
- Research in the important field of software security in the context of the „Kompetenzzentrum für angewandte Sicherheitstechnologien“ (KASTEL)
- Intensive supervision of your thesis and a good working climate

Wenden Sie sich bei Interesse oder Fragen bitte an: **Frederik Reiche (IPD)**
E-Mail: frederik.reiche@kit.edu Tel: +49 721/608-45992
WWW: http://sdq.ipd.kit.edu/