Implementing an Ideal Ledger Functionality

Project Group "Praxis der Forschung" – Winter Term 2021/22

1 Motivation

Distributed Ledgers (e.g., Blockchains) are used to establish consensus in decentral networks (e.g., a Hyperledger Fabric network). They offer a set of functionalities to network participants, like reading from the ledger, and executing transactions to change the ledger's state.

Formal analysis of programs which work together with a distributed ledger - i.e., smart contracts - can be difficult because a suitable abstraction of the underlying ledger data structure is necessary.

How about simply implementing it in Java?

2 Project Description

The goal of this project is to implement the functionality of a distributed ledger in an imperative programming language (Java), with the goal of simplifying formal analysis of programs using the ledger (e.g., Hyperledger Fabric chaincode). This includes modelling the environment of the decentral network. Desirable properties range from functional correctness (e.g., method pre-/postconditions) to temporal correctness.

3 Requirements

Understanding of first order logic and program verification as taught, e.g., in the *Formale Systeme* lecture.

4 Contact / Supervision

Jonas Schiffl, jonas.schiffl@kit.edu, Room 226 (Geb. 50.34)