Optimization of Solidity Smart Contracts

Master thesis

1 Motivation

In the TAST project, we are researching various questions within blockchains and smart contracts. We have developed two protocols for transferring tokens between blockchains, a task which is so far unexplored in other research.

We have built a reference implementation using Solidity, in order to showcase how these transfers can be implemented using Ethereum. We have successfully performed transfers between private Ethereum blockchains. However, while the current reference implementation proves the functionality of the proposed protocol and demonstrates its performance with regards to cost and time, we seek to optimize this implementation.

This thesis aims at investigating the current Solidity implementation of DeXTT with regards to performance, and optimizing this performance to minimize the required gas cost. The student is expected to provide an analysis of the current implementation with a focus on gas cost, to devise a plan of possible reductions of gas cost, and to implement these optimizations. To this end, suitable tests must ensure that no functionality is lost throughout the optimization process.

2 Work Description

- Analysis of the current reference implementation.
- Identification of possible means of optimizing the implementation with regards to gas cost.
- Implementation of these optimization means.
- Cost evaluation and functional verification using tests.

3 Further Information

Start: Immediately (might also be later)

Basic Requirements: Knowledge in the blockchain field is required; experience with smart contracts is very helpful; eagerness to gain knowledge in new technologies

TAST Website: http://www.infosys.tuwien.ac.at/tast/

Distributed Systems Group
Faculty of Informatics
Privatdozent Dr.-Ing. Stefan Schulte, s.schulte@infosys.tuwien.ac.at
www.infosys.tuwien.ac.at