Bachelor Thesis

Simulation-Based Analysis of Blockchain Architectures

Subject Area

- Software Architectures
- Blockchain
- Empirical Software Engineering

Context

With the emergence of cryptocurrencies, blockchain architectures have become more and more important. In such an architecture, components store data elements in a distributed data structure, the so-called blockchain. Thereby, each component contains a local copy of the blockchain and exchanges its version with other nodes. While new elements can be added to the overall blockchain, contained blocks should not be allowed to change in the future.

A blockchain architecture may be modelled in terms of a function from a set of parameters to a degree of blockchain security. Thereby, possible input parameters may be as follows:

1) Number of trusted participants.
2) Number of untrusted participants.
3) Difficulty of mining a new block.
4) Confirmation length, i.e., the number of blocks we wait until we consider a block as confirmed.

Problem

Until now, however, only little is known about the nature of this function. Indeed, it is not even known whether these parameters do have an impact on the security, at all. However, knowing more about the nature of this function would allow an architect to make better prediction about the security of a given blockchain architecture.

Objectives

The following theses should aim towards a better understanding of this function. Its main objective is to investigate factors which do indeed impact a blockchain's security. Thereby, the following steps need to be performed:

1) A simulation framework for blockchain architectures should be implemented. The framework should allow to fix certain values for the above mentioned parameters and simulate double spend attacks in such an environment.
2) The framework should be used to run several labor-experiments to investigate the impact of the above factors on blockchain security.
3) Finally, a hypothesis about the nature of the function should be made which can be used to generate falsifiable predictions for a blockchains security in a blockchain architecture.

Prerequisites

- Interest in software design and architectures.
- Programming experience in Java or related PL.

Supervisor

Prof. Dr. Dr. h.c. Manfred Broy

Advisor

Diego Marmsoler, TU München (diego.marmsoler@in.tum.de)