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.
A known issue of blockchain architectures is the so-called "double spend attack" in which untrusted nodes try to modify an already confirmed block in the overall blockchain by removing the block and mining new blocks on top of the chain. If the alternative blockchain finally contains more "work" as the trusted one, the network will accept the new one and the attack is considered successful.
The resistance of a blockchain architecture against double spend attacks (in the following denoted RADS) may depend on several factors. Some potential factors are listed in the following:

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, no empirical evidence is available on how the above factors influence a blockchains RADS. Indeed, it is not even clear, whether these parameters do indeed have an impact on the RADS, at all. However, knowing more about this relationship would allow an architect to make better predictions about a blockchain architectures RADS, given a certain configuration.

Objectives

The following theses should aim towards a better understanding of how the above mentioned factors impact a blockchain architectures RADS. 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 some simulations to investigate whether the above factors do indeed have a statistical significant impact on RADS.
3) Optional: Based on the insights from the simulation an empirical model should be proposed.
4) Optional: Based on the insights of the simulation, hypotheses about further factors influencing an architectures RADS should be made.

Prerequisites

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

Supervisor

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

Advisor

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