netidee Call12 | Stipendium-ID 2235

Abstract

The Cryptocurrency Bitcoin was started in 2008 with the creation of the first block, the Genesis Block. Since then, the computing power of the network, which secures the blockchain of the digital currency, has multiplied considerably. Today, around twenty professional mining pools share over 95% of the hash rate, and are constantly extending the blockchain, always building on the latest block known to them. The miners are incentivised to do so, as they create with each found block new Bitcoins for themselves. In 2014, Eyal and Gün Sirer showed for the first time that apart from this desired, honest behaviour, there are deviating mining methods that increase the relative gain of a miner compared to the rest of the network. This so-called selfish mining attack and all its modifications are examined in this thesis in a defined scenario with twenty miners and are compared with previous research results. In contrast to previous investigations, a novel, near-deterministic simulation framework based on *Docker* was developed for this purpose. This simulation framework makes it possible to naturally include the network latency and to directly reuse the reference implementation of Bitcoin. The latter has the advantage that no time-consuming and error-prone adaptation or abstraction of the reference implementation is necessary, and all properties of the implemented Bitcoin protocol are automatically included in the simulation. To simulate the various selfish mining strategies, additionally, a proxy was implemented that eclipsed a node in the network and misuses the node to perform the various selfish mining attacks.

The simulations of the various selfish mining strategies show that a dishonest miner can increase its relative gain over the rest of the network, thus reinforcing the current state of research and the relevance of the selfish mining attack. In accordance with previous results, the most efficient selfish mining strategies under the simulation scenario with twenty miners, selfish mining and equal-fork-stubbornness were identified.

Keywords

selfish mining, selfish mining attack, Bitcoin, blockchain, simulation, simulation framework, network latency, reference implementation, Docker