FAKULTÄT FÜR !NFORMATIK
Faculty of Informatics

Diplomarbeitspräsentation

Simulation of different selfish mining strategies in Bitcoin

Masterstudium:

Software Engineering & Internet Computing

Simon Mulser

Technische Universität Wien
Institut für Information Systems Engineering
Arbeitsbereich: Information & Software Engineering
Betreuer: Privatdoz. Mag.rer.soc.oec. Dipl.-Ing. Dr.techn. Edgar Weippl

Context

Selfish mining is an attack on the Bitcoin mining process. In the attack, the selfish miner can increase the relative gain on mining rewards compared to the rest of the network. The miner achieves this by withholding his own blocks, which he later uses to match or overwrite blocks found by the honest network. The attack comprises the idea that the miner lets the rest of the network waste their computational power on mining blocks which do not end up in the longest chain.

Goals

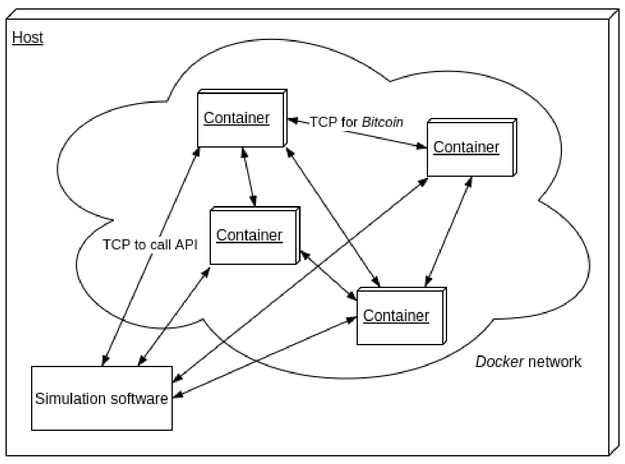
Development of a novel, *near-deterministic* simulation framework which:

- naturally respects the peer-to-peer network and its latency
- directly reuses the reference implementation to capture all protocol details and to avoid time-consuming and error-prone adaptation or abstraction of the protocol

Afterwards:

- Implement selfish mining strategies in a proxy which eclipses a normal node
- Simulate different selfish mining strategies under a realistic scenario
- Determine best performing strategies and compare them with honest mining
- Contrast and validate the obtained results with simulations of previous research

Simulation Framework



Virtual peer-to-peer network with *Docker*

Network:

- *Docker* is used to virtualise the whole peer-to-peer network
- Latency is applied to the TCP-connections between the nodes by using *Unix tc*
- The *Docker* containers execute the actual Bitcoin reference implementation
- Bitcoin nodes are not mining but are creating blocks on RPC-calls from the framework

Simulation:

- Network is set-up by framework based on pre-defined scenario
- Nodes generate blocks based on samples drawn from an exponential distribution
- Safety checks if simulation is executed to fast by splitting real time into multiple spans
- After a simulation run, log-files of nodes are parsed and calculated statistics are summarised in report

Selfish Proxy

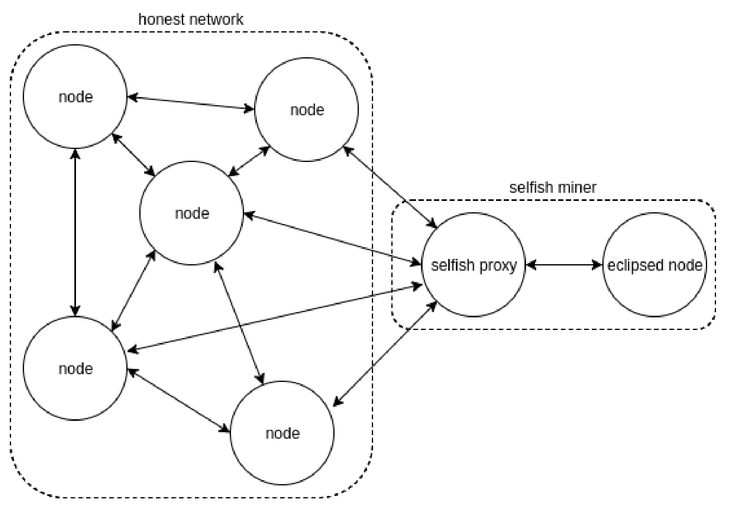
A node in the network which eclipses a normal Bitcoin node from the rest of the network. By withholding blocks from the eclipsed node to the honest network and vice versa, the selfish proxy is able to mimic different selfish mining strategies.

Advantages:

- No need to alter Bitcoin reference implementation
- Possibility to extend node for other attacks

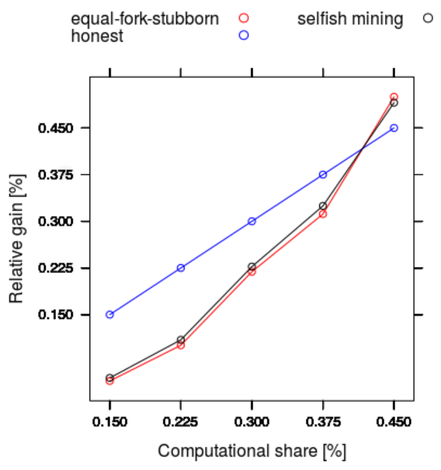
Disadvantage:

- Part of the Bitcoin protocol and the current state of the blockchain needs to be handled
- Introduces an extra hop and thus, impacts performance of selfish mining algorithms



Selfish proxy eclipsed node to perform selfish mining

Results



Relative gain of different mining methods

- The simulation confirmed that selfish mining increases the relative gain compared to honest mining
- With a computation power of 45%, the selfish miner can gather about 50% of the mining rewards
- Best performing strategies were equal-fork-stubborn and selfish mining

Further research

Performance selfish proxy:

- Use compact block relay mechanism to process blocks faster
- Remove extra hop by implementing strategies directly in a Bitcoin node scenarios

Scenario:

- Investigate in combining selfish mining with other known attacks
- Use transactions in scenario and thus, bigger blocks

Kontakt: simonmulser@gmail.com