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
BetreuerIn: Privatdoz. Mag.rer.soc.oec. Dipl.-Ing. Dr.techn. Edgar Weippl

Context

Selfish mining is an attack on the Bitcoin mining process. Recent research showed that the selfish miner can increase the relative gain on mining rewards compared to the rest of the network. The miner achieves this by withholding found blocks, which it then later uses to match or overwrite blocks found by the honest miners. 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

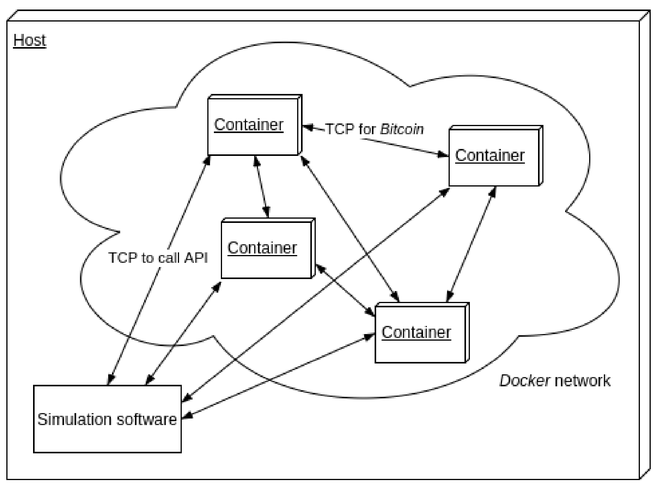
Development of a novel, more accurate simulation framework which:

- naturally respects the 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 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*
- In the *Docker* container the actual Bitcoin reference implementation is executed
- Bitcoin nodes are not mining but are creating blocks on RPC-call from framework

Simulation:

- Network is set-up by framework based on pre-defined scenario
- Framework let 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

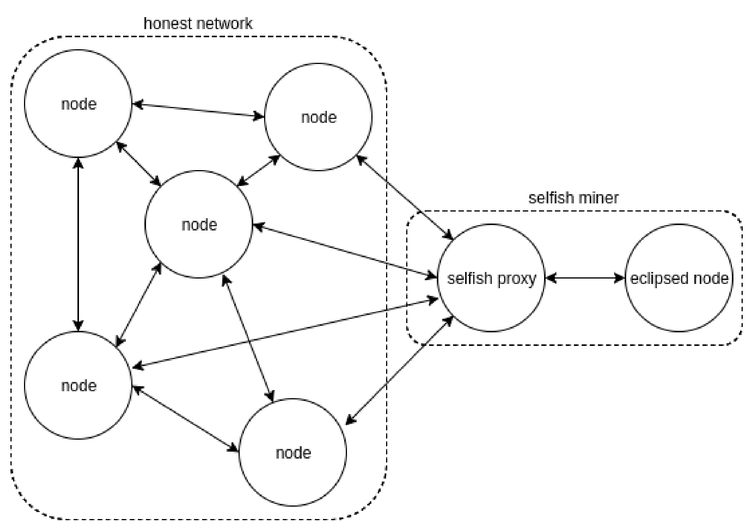
Node in the network which eclipses a normal Bitcoin node from the rest of the network. By withholding blocks from the eclipsed node to the honest network and vice versa, the selfish proxy is able to mimic different selfish mining strategies.

Advantages:

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

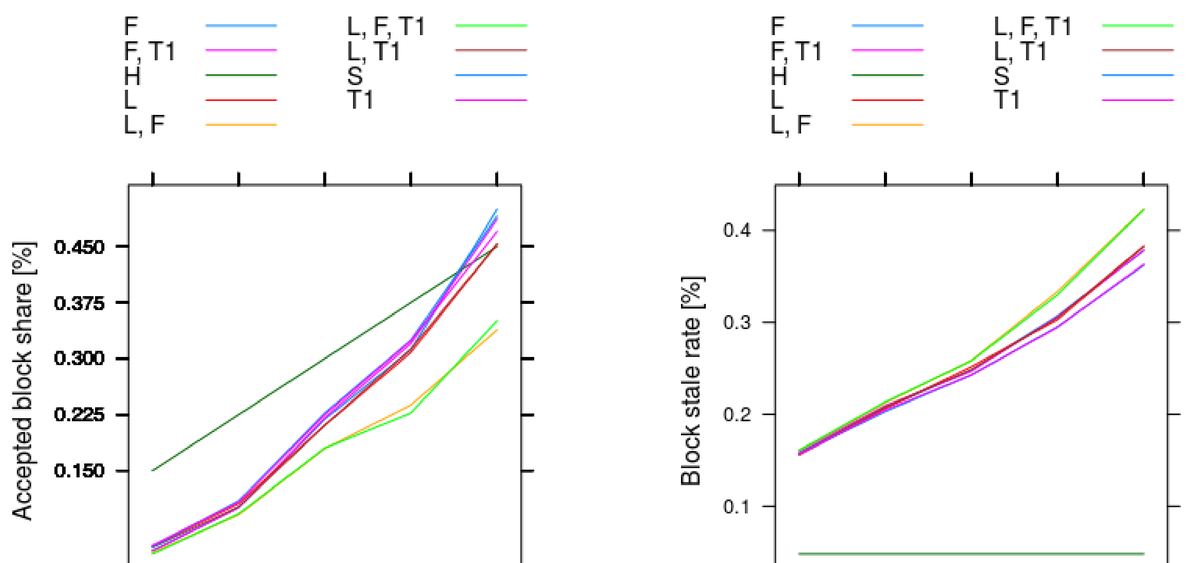
Disadvantage:

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



Selfish proxy eclipsed node to perform selfish mining

Results



Additional Outcome

- RQ1: Do the simulations of selfish mining with the proposed software solutions show an increase of the total and relative gain for the selfish miner compared to the normal, honest mining behaviour?
- RQ2: How do the obtained results of the simulation match the outcome of previous research in the area of selfish mining?

Kontakt: simon.mulser@gmail.com