DIPLOMA THESIS

# Simulation of different selfish mining strategies in Bitcoin respecting network topology and reference implementation

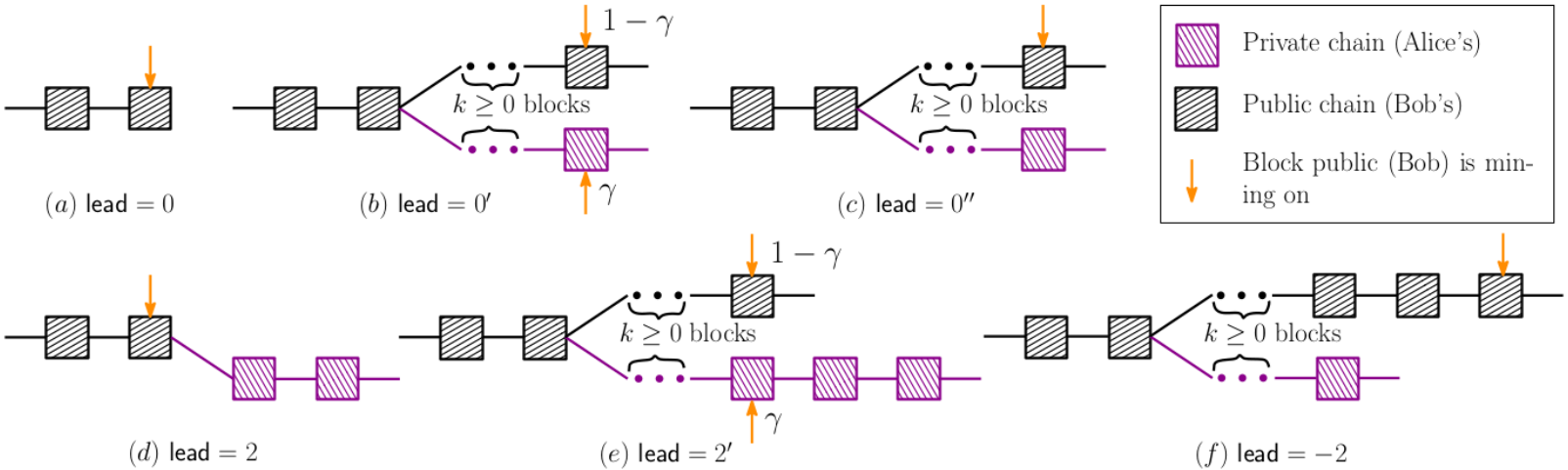
Simon Mulser, BSc

Advisor: Edgar Weippl, Privatdoz. Mag.rer.soc.oec. Dipl.-Ing. Dr.techn.
Assistance: Aljosha Judmayer, Univ.Lektor Dipl.-Ing.

# What is selfish mining?

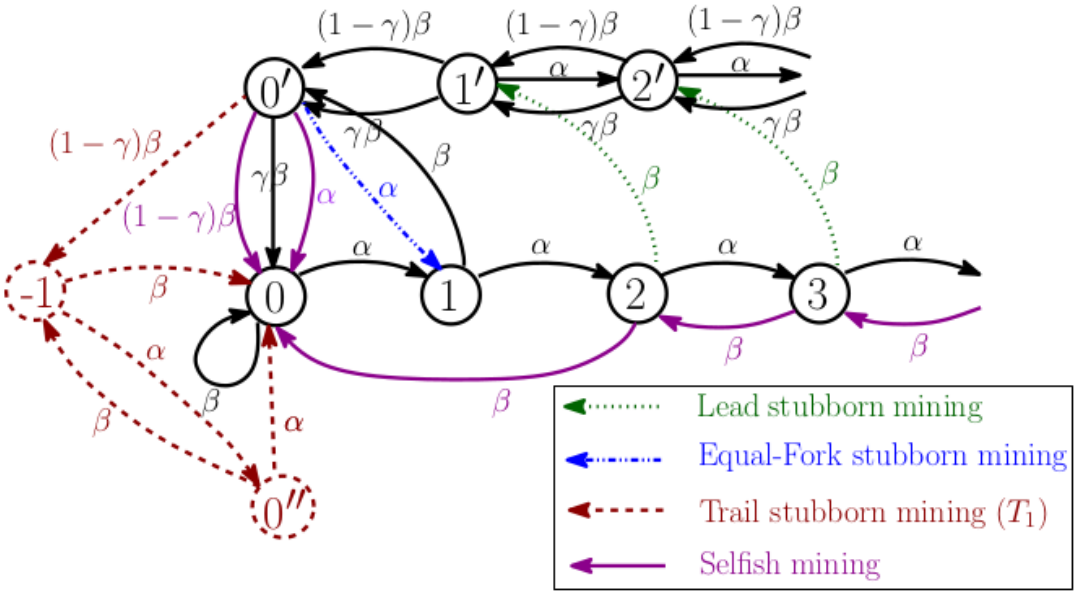
An attack on the Bitcoin mining process, where the attacker can increase its relative gain compared to other miners in the network. The attack compromises idea that the other miners waste their mining power for blocks, which will not end up in the longest chain.

# Selfish mining (1)




Nayak, K., Kumar, S., Miller, A., & Shi, E. (2016, March). Stubborn mining: Generalizing selfish mining and combining with an eclipse attack. In Security and Privacy (EuroS&P), 2016 IEEE European Symposium on (pp. 305-320). IEEE.

# Selfish mining (2)




Nayak, K., Kumar, S., Miller, A., & Shi, E. (2016, March). Stubborn mining: Generalizing selfish mining and combining with an eclipse attack. In Security and Privacy (EuroS&P), 2016 IEEE European Symposium on (pp. 305-320). IEEE.

# Goals (1)

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

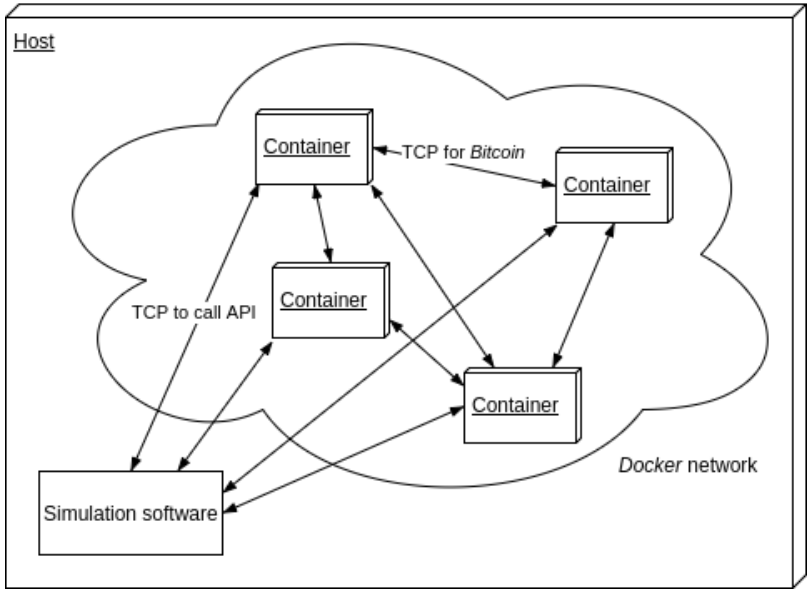
And, implement selfish mining strategies in a proxy which eclipses a normal node.

# Goals (2)

Afterwards:

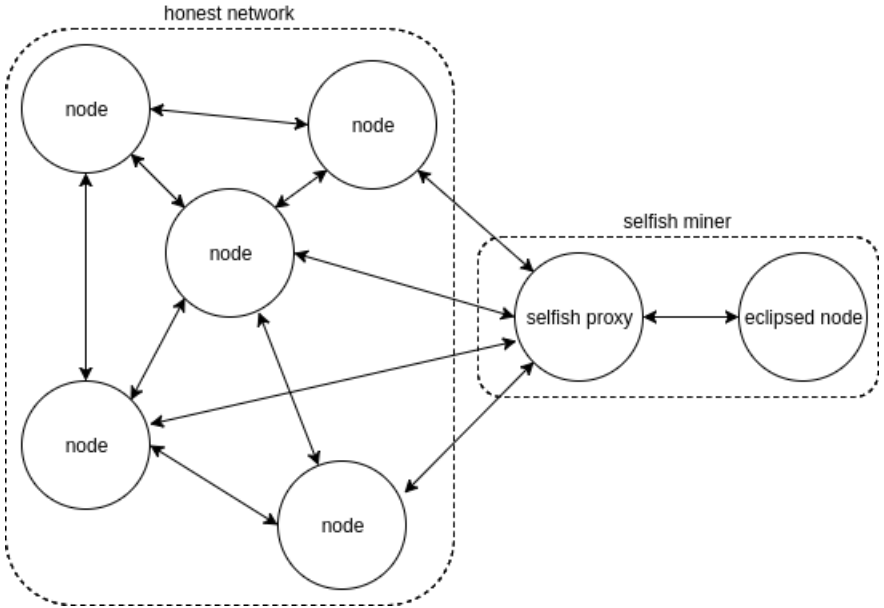
- Simulate different selfish mining strategies under a realistic scenario
- Investigate best performing strategies and compare them with honest mining
- Contrast and validate the obtained results with simulations of previous research

# Simulation framework




*Available under: github.com/sbaresearch/simcoin*

# Selfish proxy

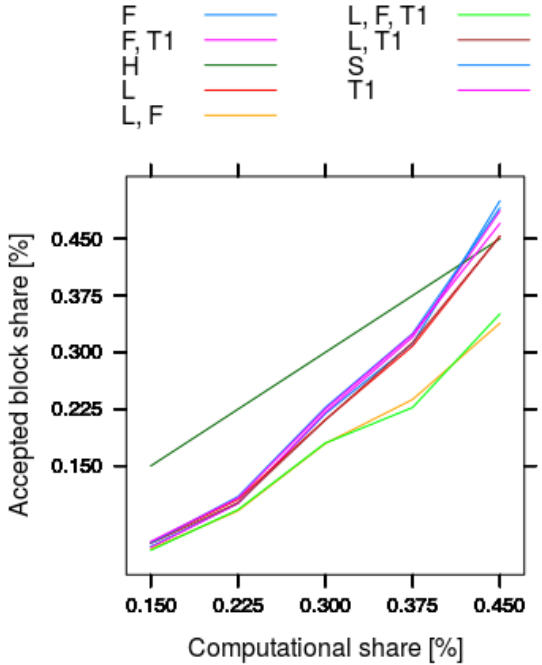


# Simulation scenario

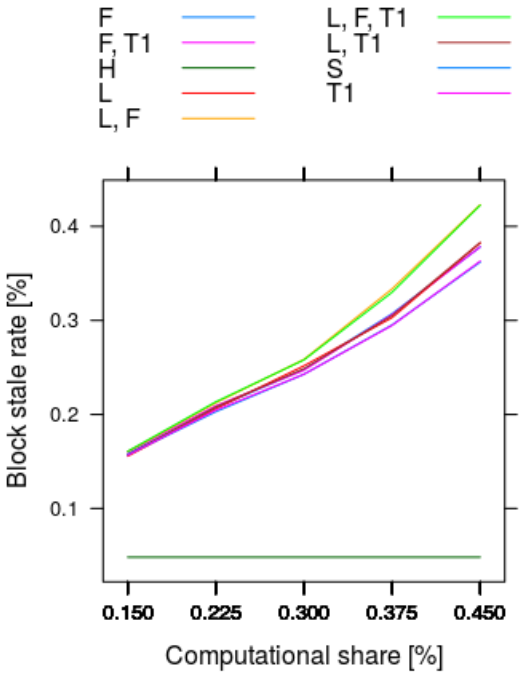
The simulation scenario is a simplification of the real world Bitcoin network:

- 20 miners
- All of them are connected with each other directly
- One miner is eclipsed by the selfish proxy
- Simulation of two weeks of Bitcoin in 100 minutes (200x faster)
- No transactions and hence, empty blocks

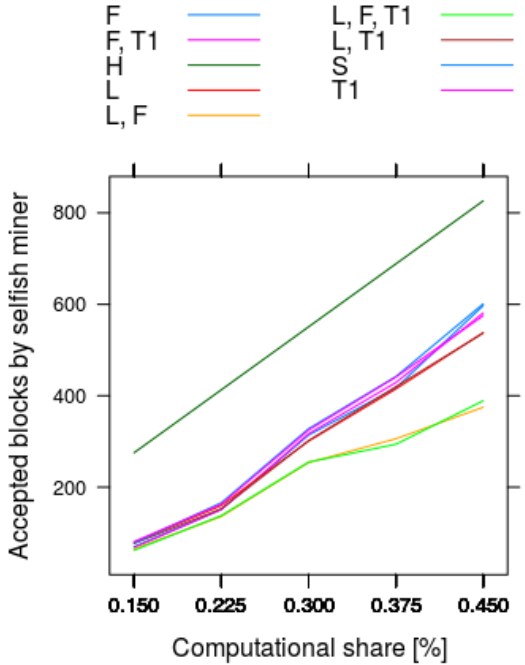
# Simulation: Relative gain of selfish miner



# Simulation: Stale rate



# Simulation: Accepted blocks by selfish miner



# Evaluation

The selfish miner can increase its relative gain by conducting selfish mining.

But:

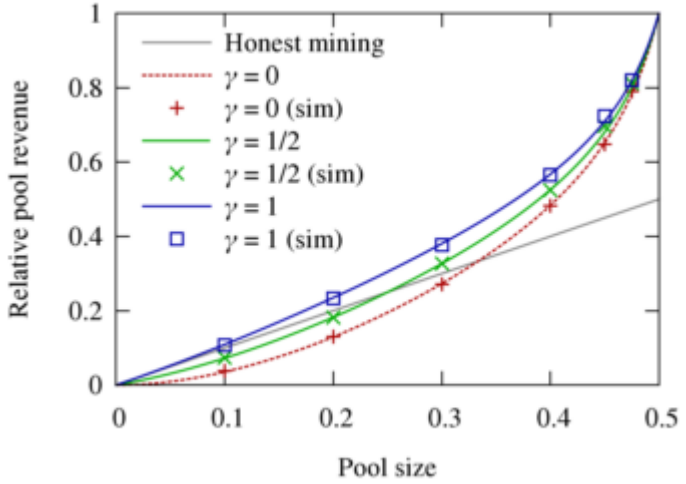
- Over 40% of the mining power of the network is needed
- And the strategies normal selfish mining (S) or equal-fork stubbornness (F) need to be used

Then, the miner is able to increase its relative gain 4.1% and 5% respectively.

# Compared to previous research

The simulation results are comparable with results from previous research where the miner does not win any block race.

In our simulation, the attacker is not able to win block races because of the realistic simulation scenario and the disadvantages of the selfish proxy.




Eyal, I., & Sirer, E. G. (2014, March). Majority is not enough: Bitcoin mining is vulnerable. In International conference on financial cryptography and data security (pp. 436-454). Springer, Berlin, Heidelberg.

# Further research

Performance selfish proxy:

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

Scenario:

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