Attack and Vulnerability Simulation Framework for Bitcoin-like Blockchain Technologies

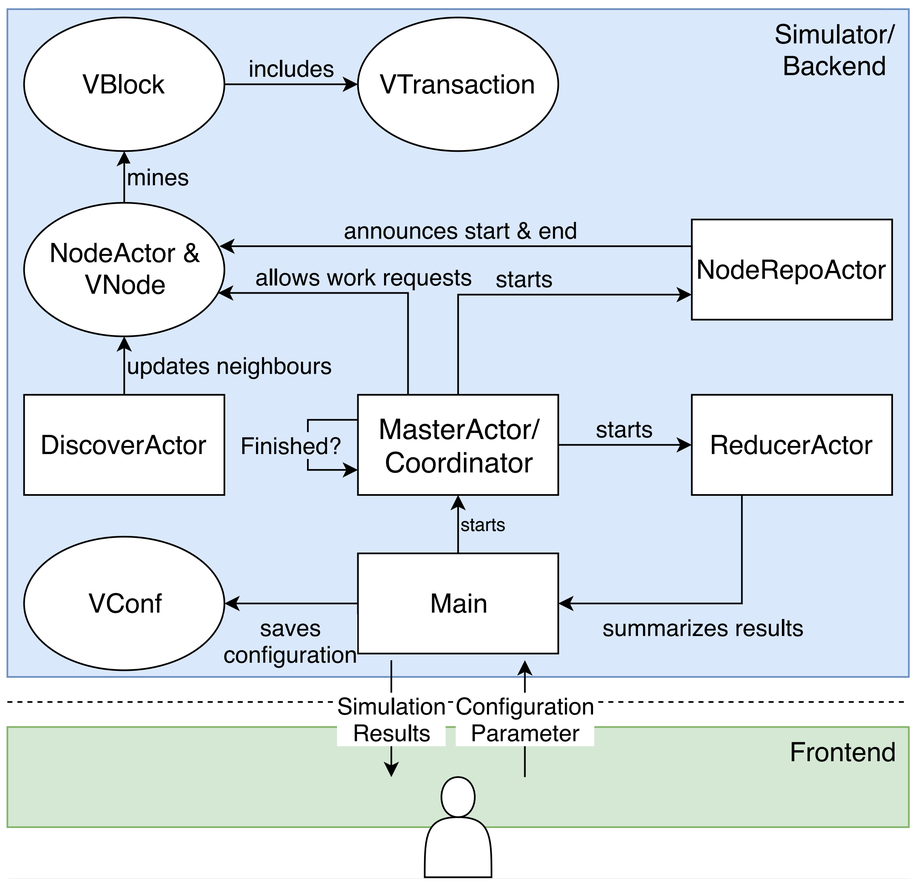
Fabian Schüssler, Pezhman Nasirifard and Hans-Arno Jacobsen
Technical University of Munich

Attack and Vulnerability Simulation Framework

- **Bitcoin** is a cryptocurrency with a solution for the double-spending problem.
- **VIBES configurable blockchain simulator** is capable of conducting distributed large-scale network simulations of PoW based cryptos.
- VIBES enables researchers with studying the network under various attacks, such as **double-spending attacks and flood attacks**.
- The primary goal is a derivation of empirical insights on the behavior of the system under attack and intuitively comparing different scenarios.

VIBES Architecture

- The MasterActor coordinates and controls the nodes and the execution of the simulation.



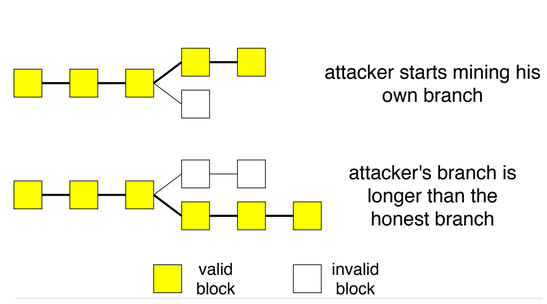
Simulation Configuration

- A total of **17 configuration parameters** (including strategy) are supported.

Bitcoin Attacks

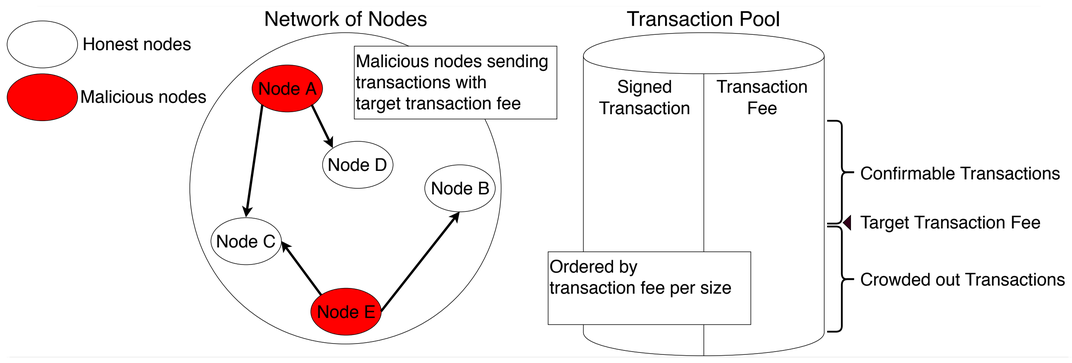
Double-Spending Attack

- A double-spending attack attempts to spend the same Bitcoin twice.
- The attacker succeeds when the invalid transaction is included and remains in the **longest mined blockchain**.
- The success probability depends on the **malicious miner's hashrate** and the **number of confirmations** required by potential victims.



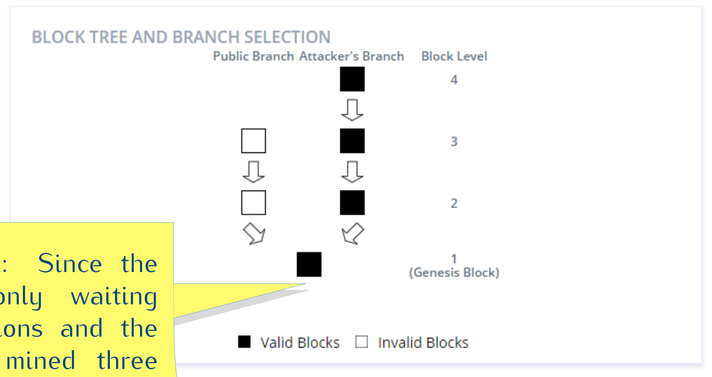
Flood Attack

- Transaction spam or flood attack attempts to make everyone in the network pay at least a certain transaction fee by spamming the network with valid transactions.
- Blockchains with low scalability can be rendered unusable by a malicious actor.



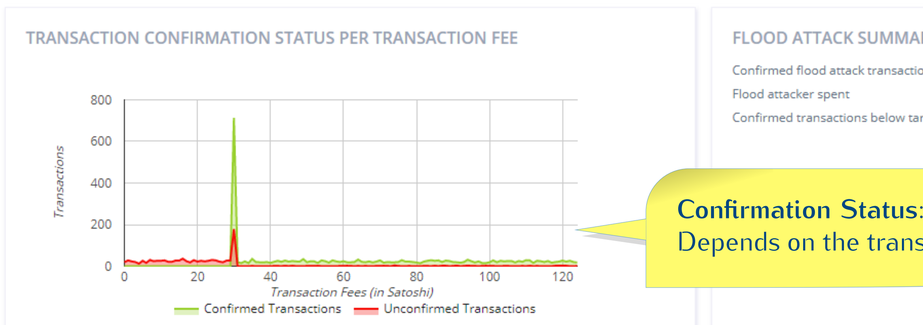
Simulation Results

Double-Spending Attack

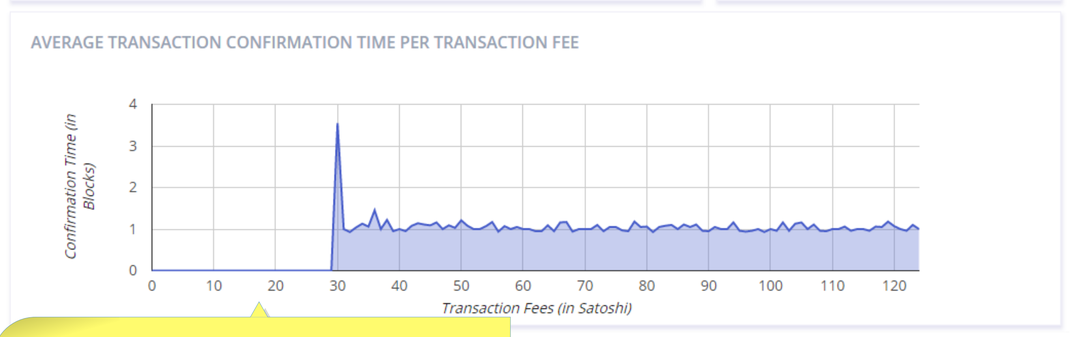


Successful Attack: Since the merchants are only waiting for two confirmations and the attacker already mined three blocks.

Flood Attack



Confirmation Status: Depends on the transaction fee.



Minimum fee: No transactions with fees below the attacker's target transaction fee were confirmed.