Final Dissertation

Simulating large-scale network attacks against Bitcoin

Advisor
Alberto Montresor

Student
Davide Pedranz

University of Trento
Department of Information Engineering and Computer Science

10 October 2018

Outline

Outline

1. Bitcoin
   - Blockchain
   - Forks
   - Mining
2. Attacks
   - Double Spending
   - Balance Attack

Outline

1. Bitcoin
   - Blockchain
   - Forks
   - Mining
2. Attacks
   - Double Spending
   - Balance Attack
3. Experiments
   - Delay
   - Drop
   - Partition

Outline

Outline

Bitcoin

- Most used and valuable cryptocurrency:
  - Price = $\sim$ 8000 \$/BTC
  - Market cap = $\sim$ 141 billion \$

Bitcoin

- Most used and valuable cryptocurrency:
  - Price $= \sim$ 8000 \$/BTC
  - Market cap $= \sim$ 141 billion \$
- Usages:
  - in-shop payments
  - online purchases
  - low-cost money transfer

Blockchain

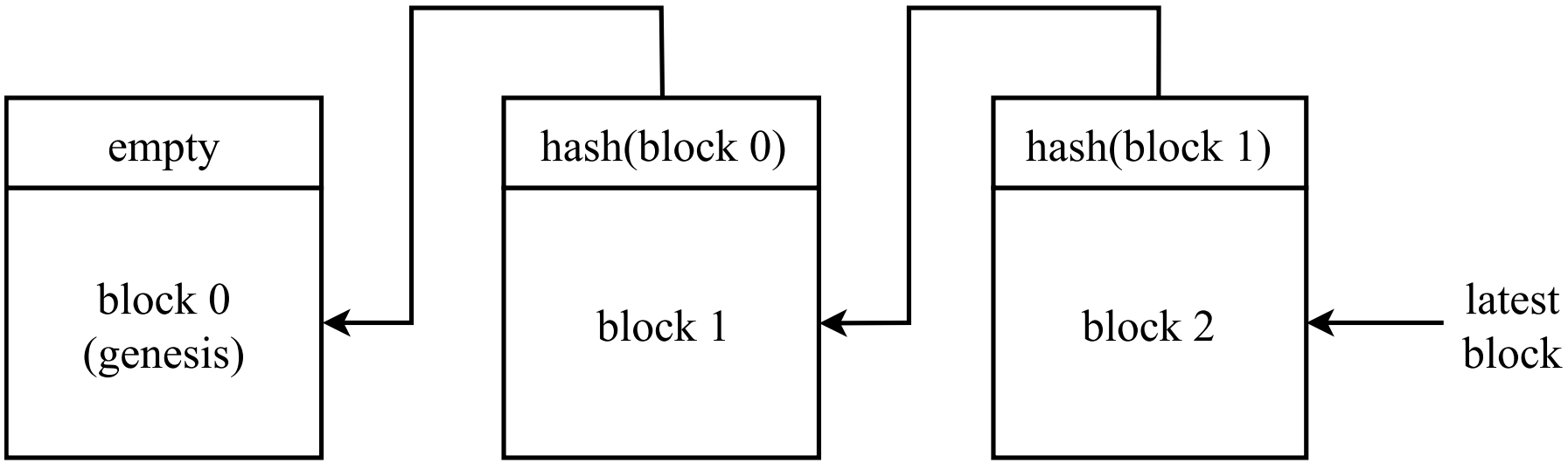


Figure: Schematic representation of a blockchain. A blockchain is a list of blocks, connected to each other with an hash pointer. Each block contains a set of transactions.

Forks

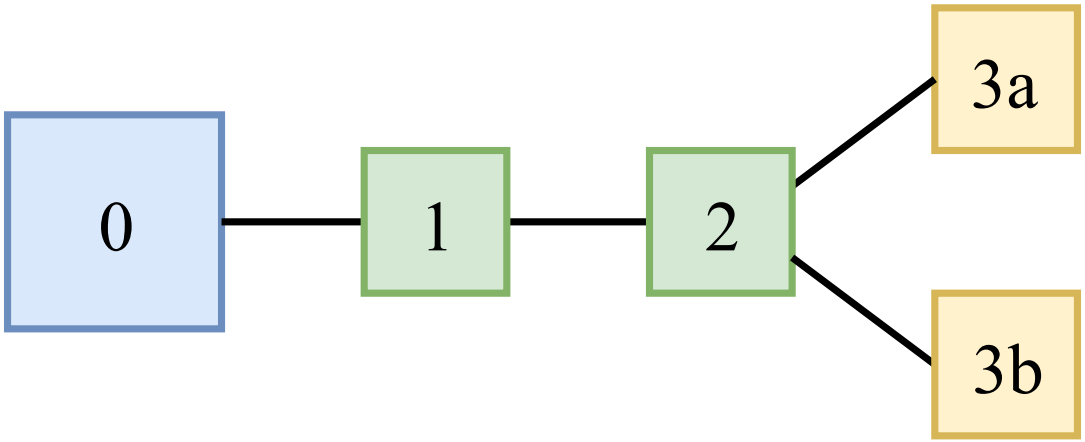


Figure: Schematic representation of a blockchain with 2 branches. The yellow blocks 3a and 3b are in conflict. The network will pick only one of them.

Forks

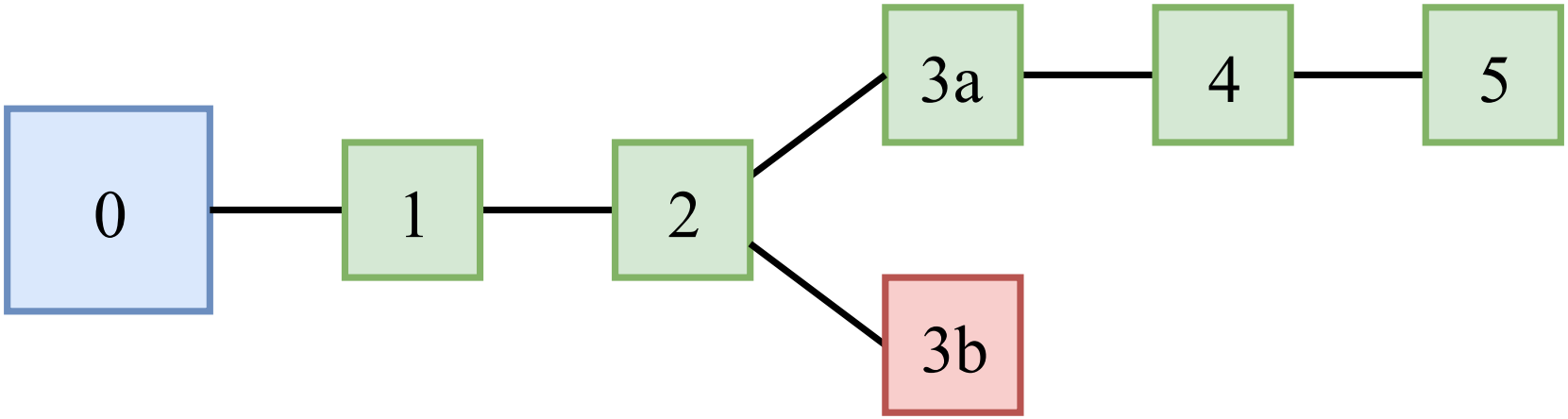


Figure: Schematic representation of a blockchain with one fork. The green block are on the longest chain. The red block 3b is in conflict with 3a.

Mining

Mining is the process of creating new blocks:

- each valid block contains the solution of a computational puzzle
- the only known way to solve the puzzle is the brute-force approach
- the puzzle's solution proves that some work has been done
- the miner receives a reward for each completed valid block on the longest chain

Proof-of-Work prevents attackers to generate too many valid blocks.

Outline

Double Spending

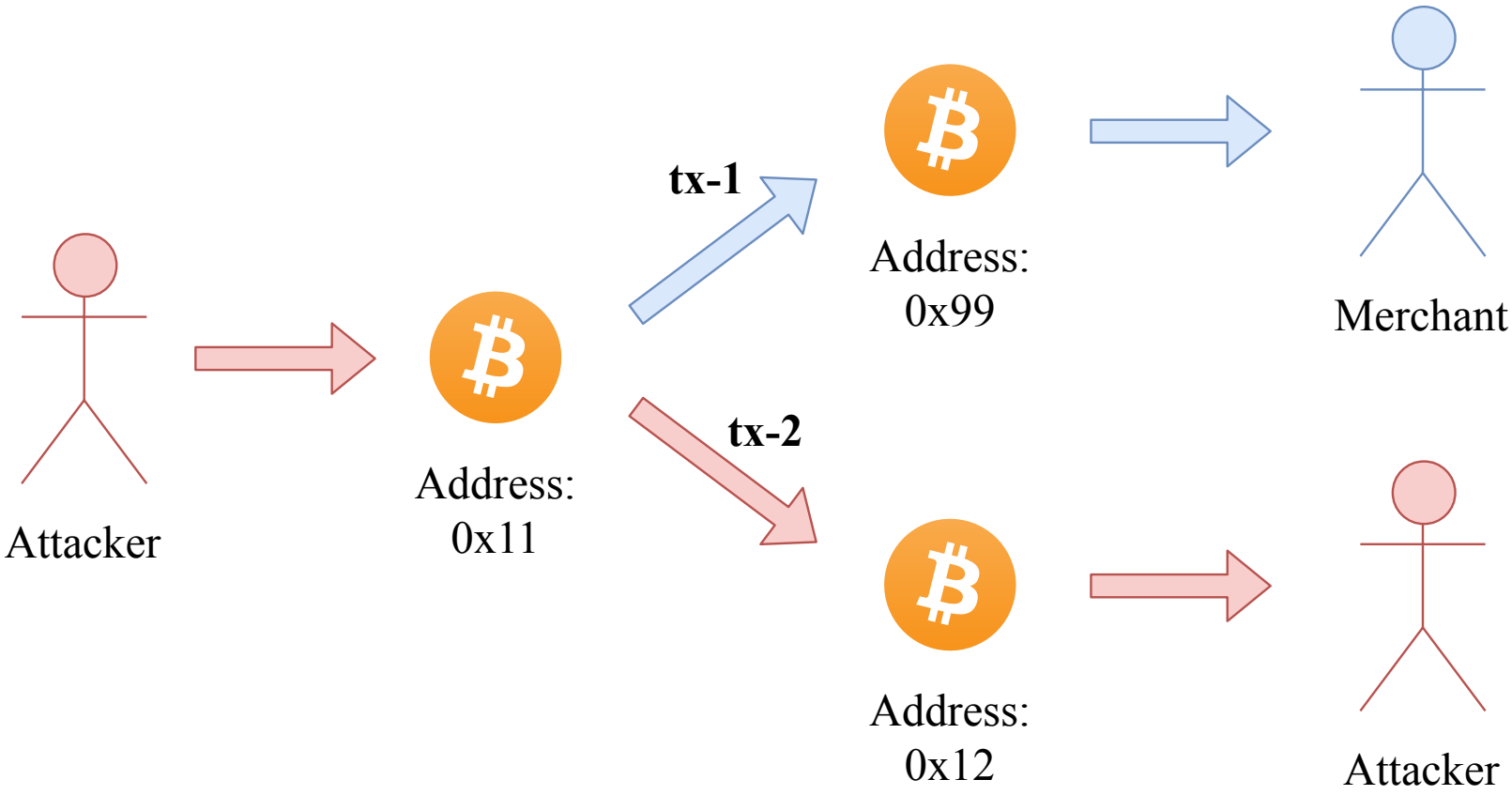


Figure: The attacker submits the transaction `tx-1` to pay the merchant. At the same time, it submits the conflicting transaction `tx-2`.

Double Spending

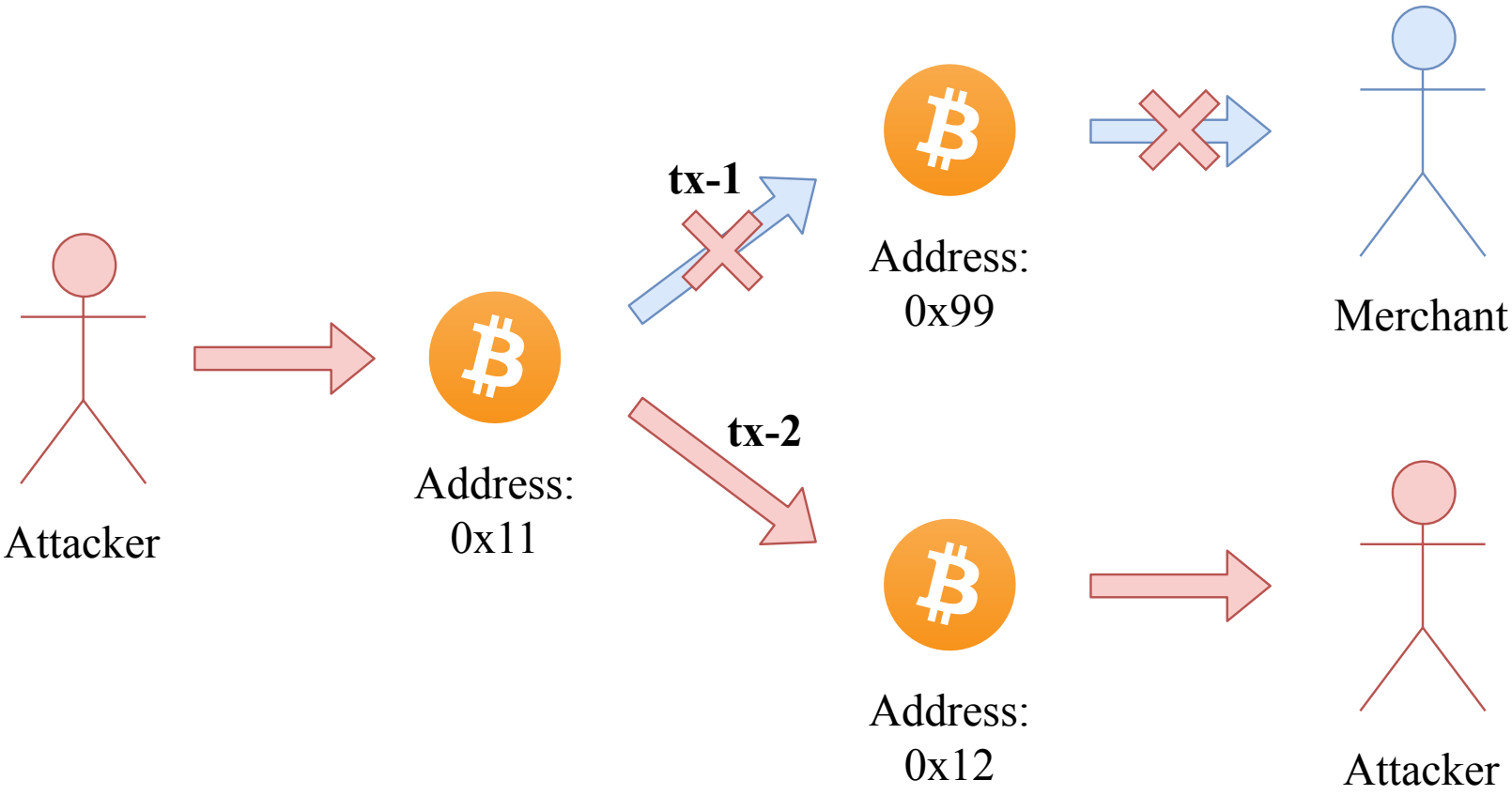
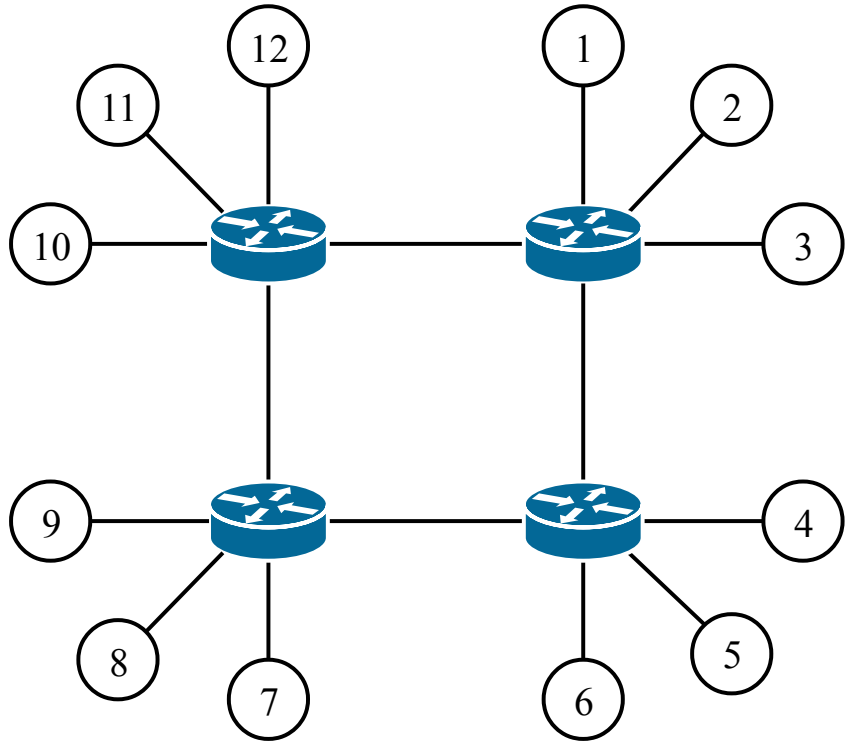


Figure: The transaction `tx-2` is accepted, `tx-1` is rejected. The attacker gets its money back, while the merchant does not get anything.

Balance Attack

The attacker:

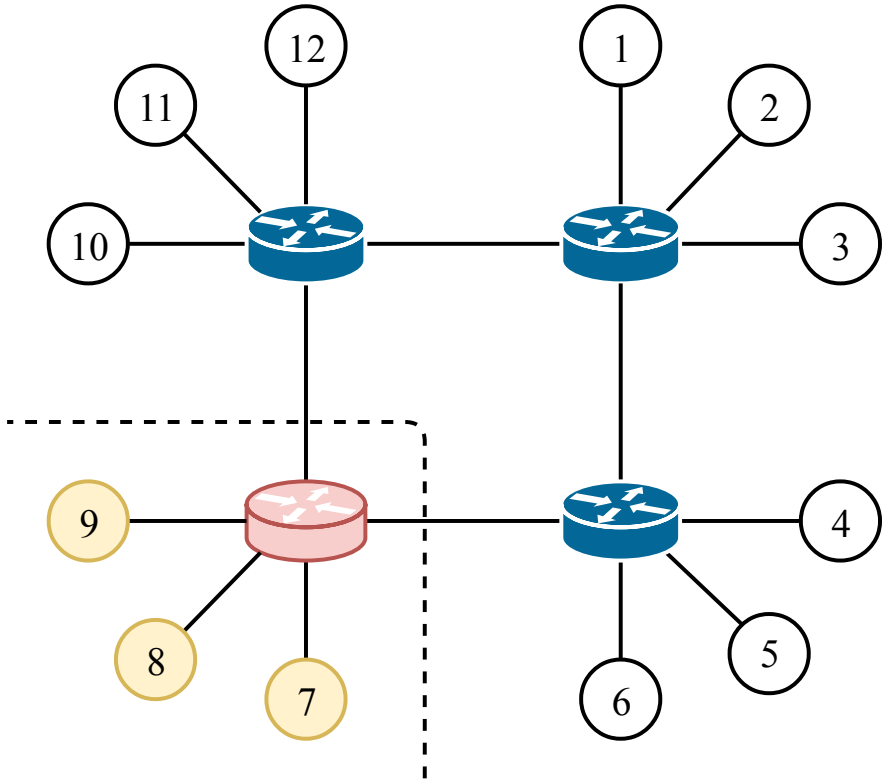
- partitions the nodes into groups with about the same computational power
- delays or drops messages between nodes in different groups



Balance Attack

The attacker:

- partitions the nodes into groups with about the same computational power
- delays or drops messages between nodes in different groups

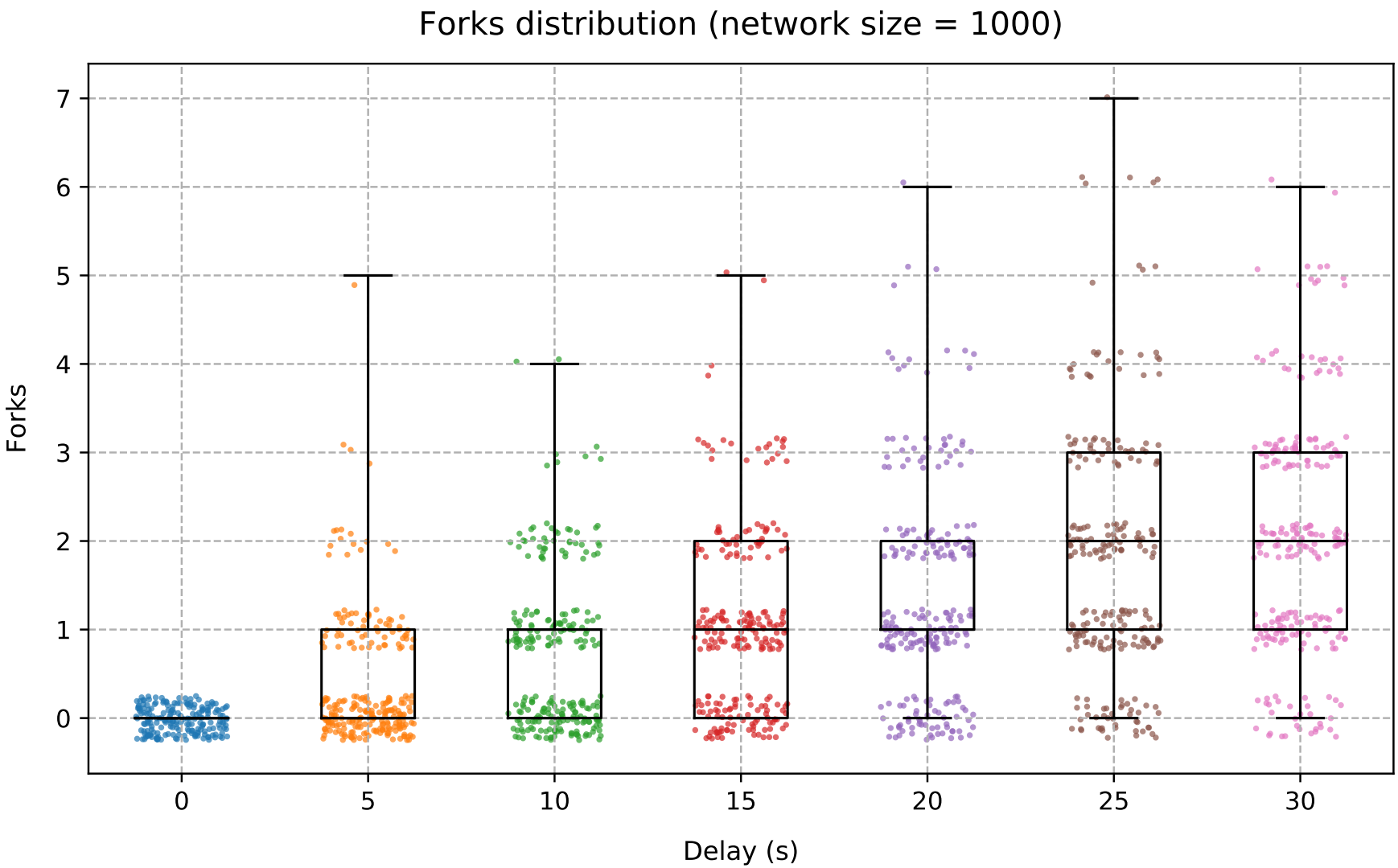


Outline

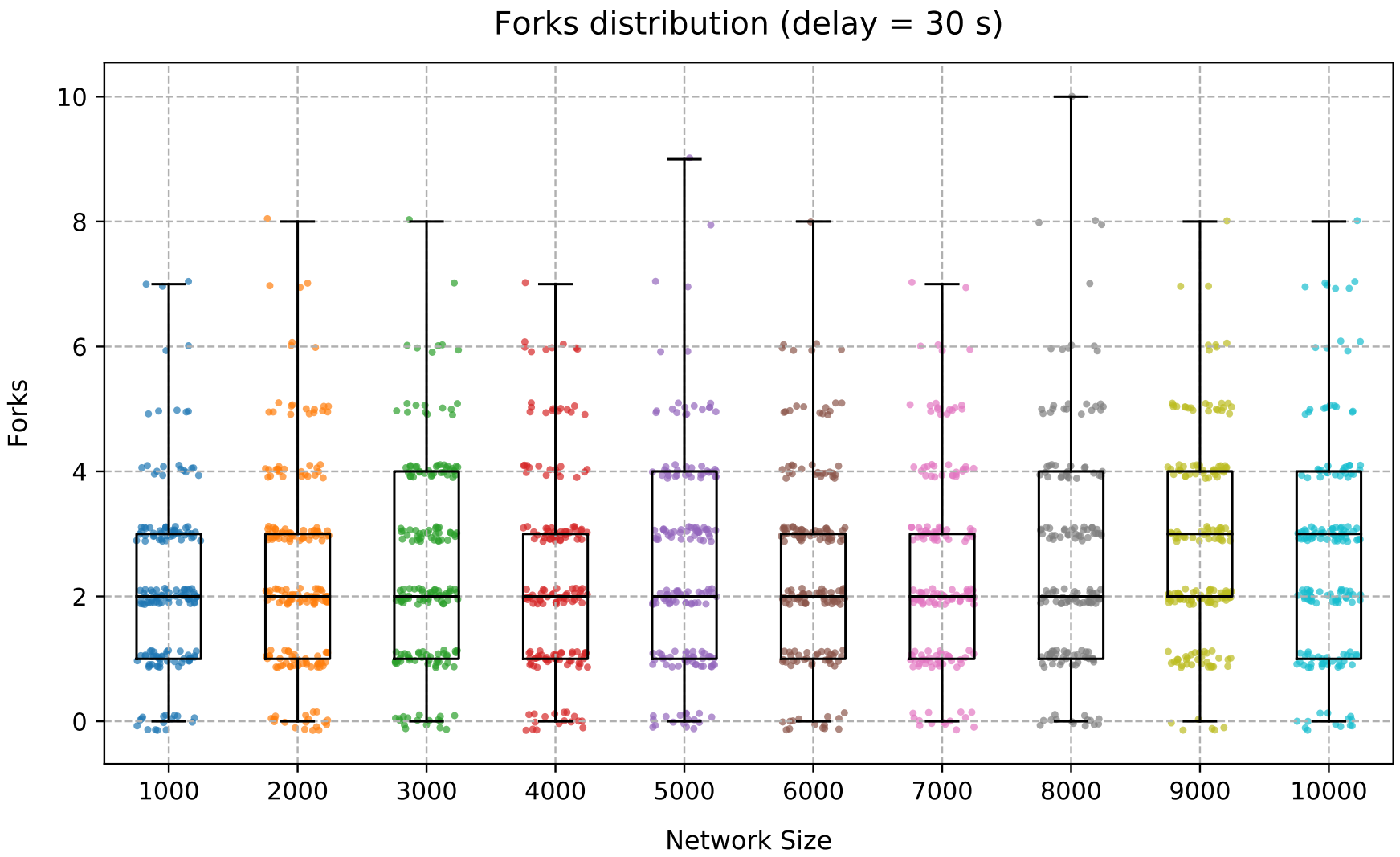
Simulator

- Bitcoin protocol:
  - network bootstrap
  - topology construction
  - blocks and transactions propagation
- Simulate the Balance Attack for different:
  - delays
  - drops
  - partitions
- Evaluation metric: number of forks

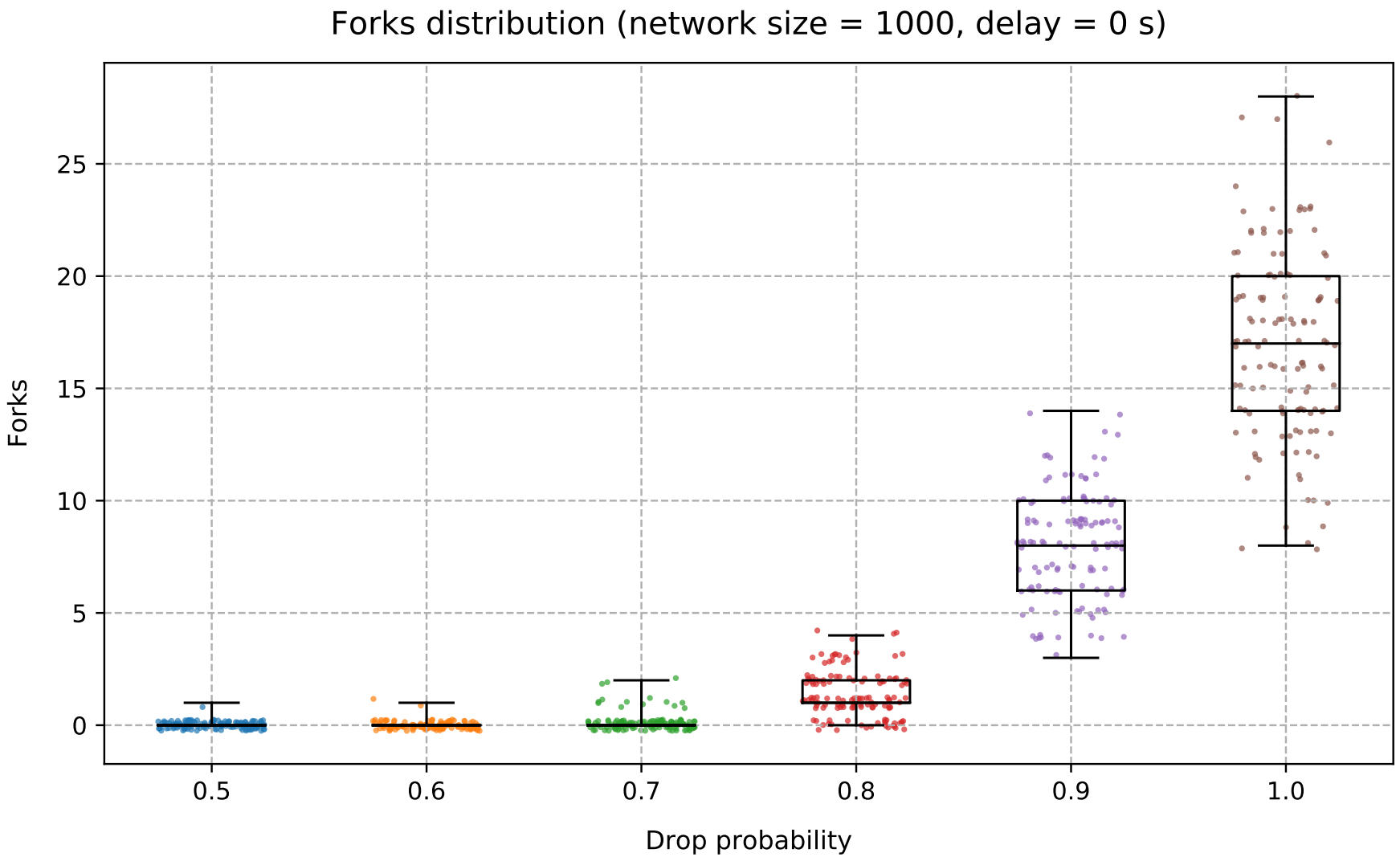
Balance Attack with Delays



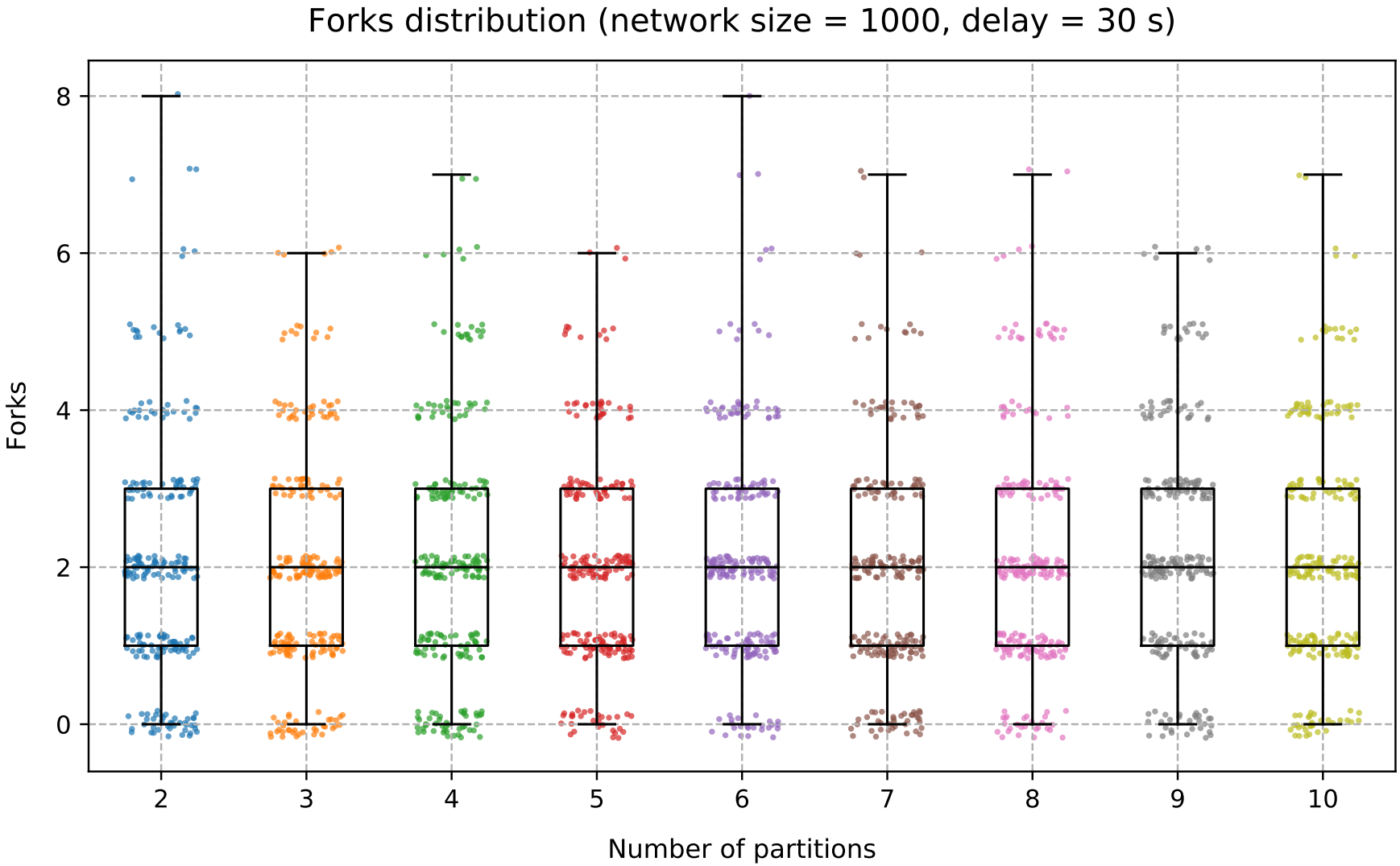
Balance Attack with Delays for Different Networks



Balance Attack with Random Message Drop



Balance Attack with Multiple Groups



Outline

Conclusions

- Bitcoin behaves well under normal network conditions

Conclusions

- Bitcoin behaves well under normal network conditions
- The Balance attack works and scales to different network sizes

Conclusions

- Bitcoin behaves well under normal network conditions
- The Balance attack works and scales to different network sizes
- The Bitcoin protocol handles well the loss of many messages

Conclusions

- Bitcoin behaves well under normal network conditions
- The Balance attack works and scales to different network sizes
- The Bitcoin protocol handles well the loss of many messages
- The number of groups does not affect the attack's performances

Thanks for the attention!