Bitcoin-NG and the Blockchain Test bed

Ittay Eyal

Cornell

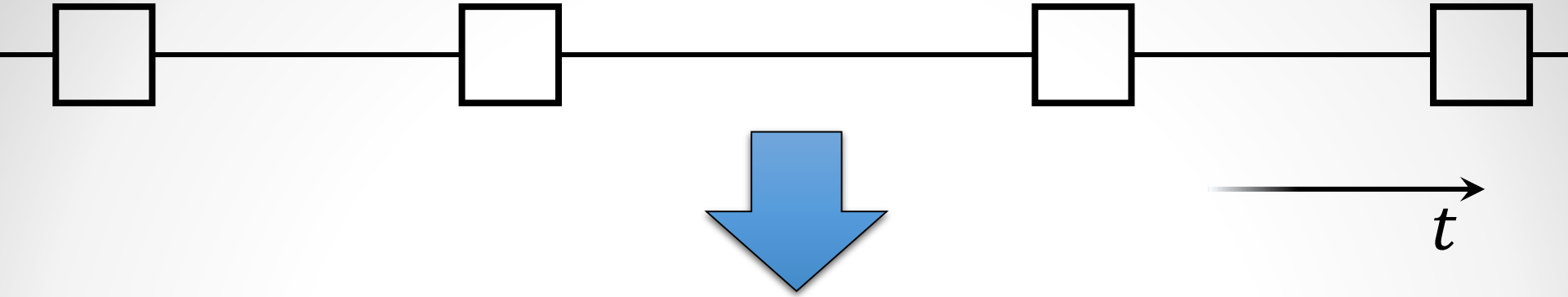
With **Adem Efe Gencer**, **Emin Gün Sirer**
and **Robbert Van Renesse**

Scaling Bitcoin Workshop, Montréal, August 2015

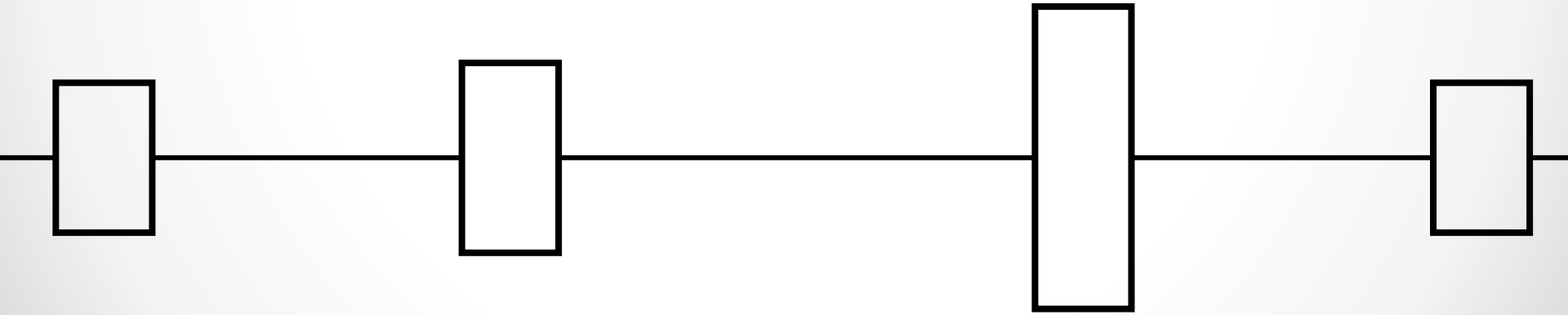
Goals

- Lower latency
- Higher throughput
- Security

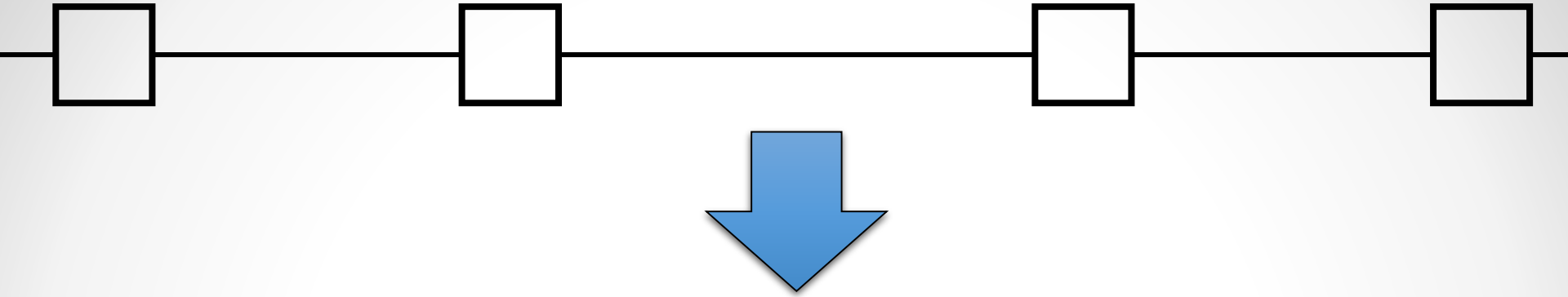
Parameter Tuning



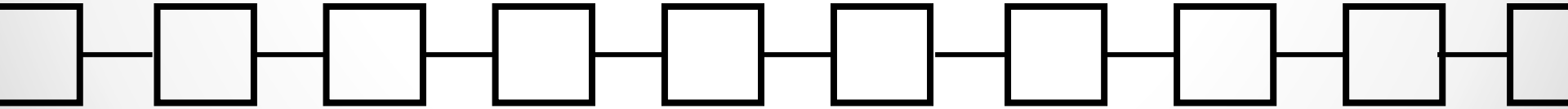
1. Larger blocks →
    - Higher throughput



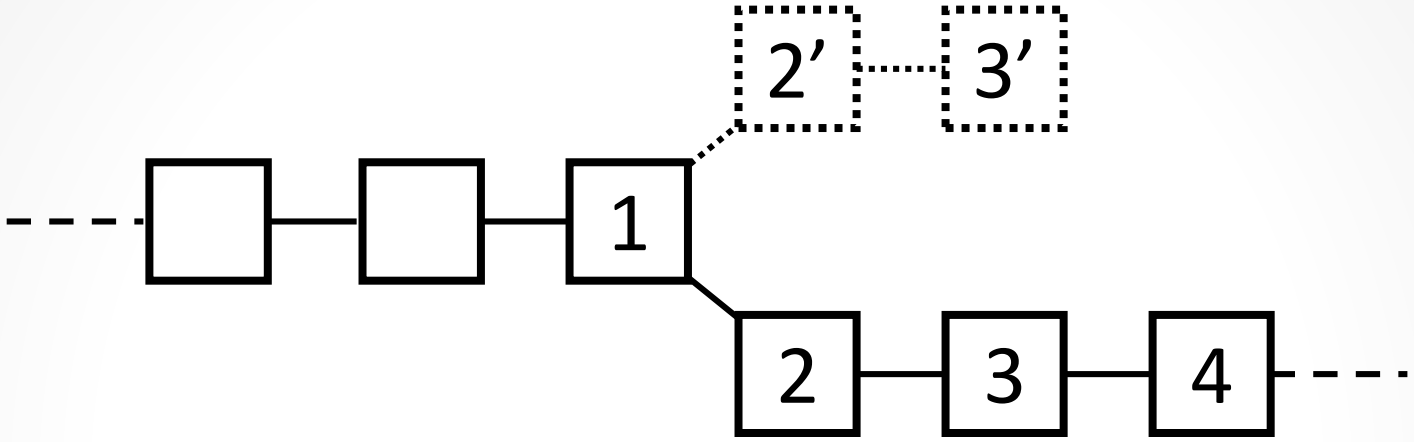
Parameter Tuning



2. Shorter block intervals →
    - Higher throughput
    - Lower latency



Scaling by Tuning Causes Forks



- Mining power loss
- Unfairness → centralization
- Longer time to convergence

Evaluation

Test Bed

Infrastructure: ~150 machines x 8 cores
1Gb network

Client: 0.10.0

Network: emulated

P2P topology: manual

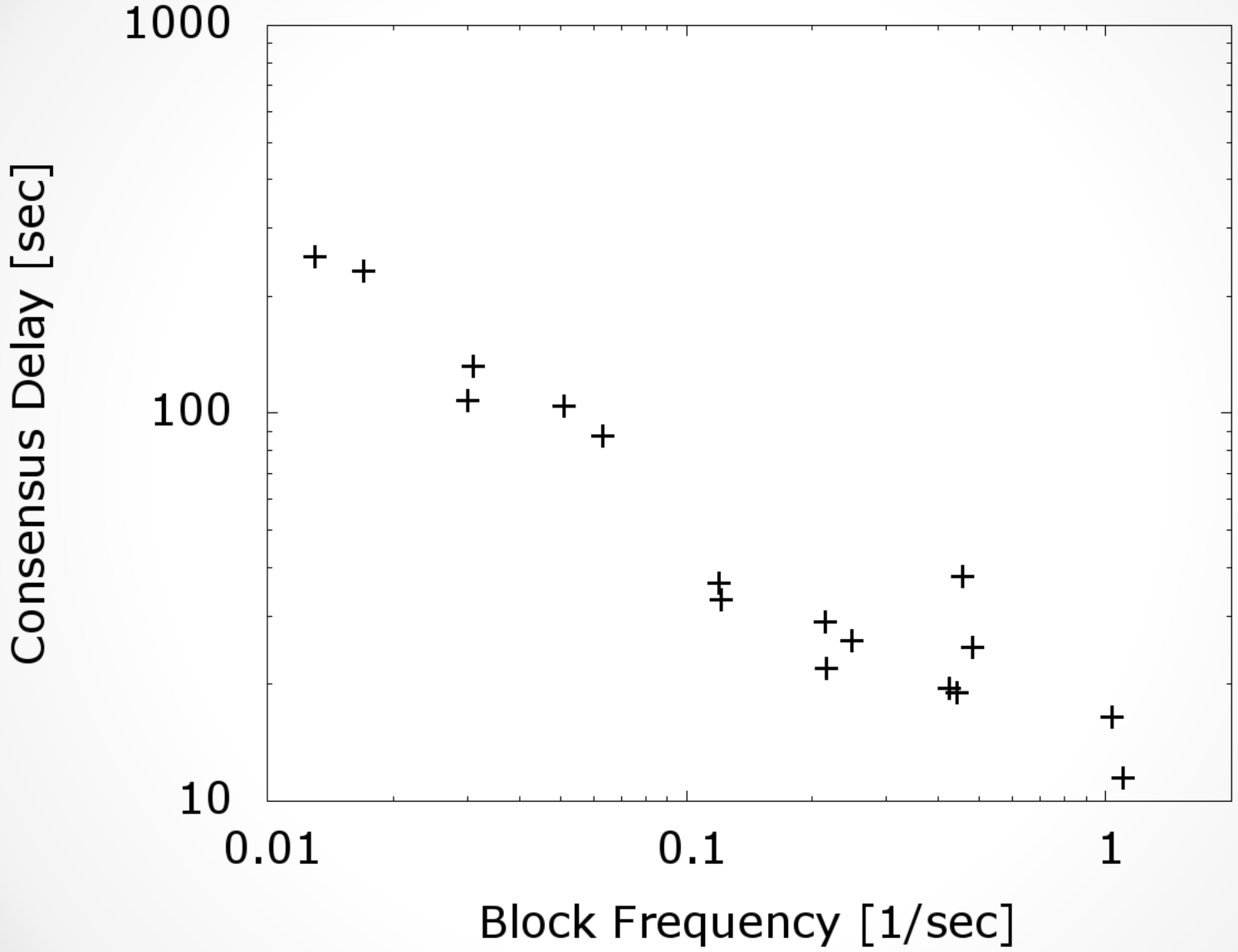
Blockchain content and mempool bootstrap

Consensus Delay

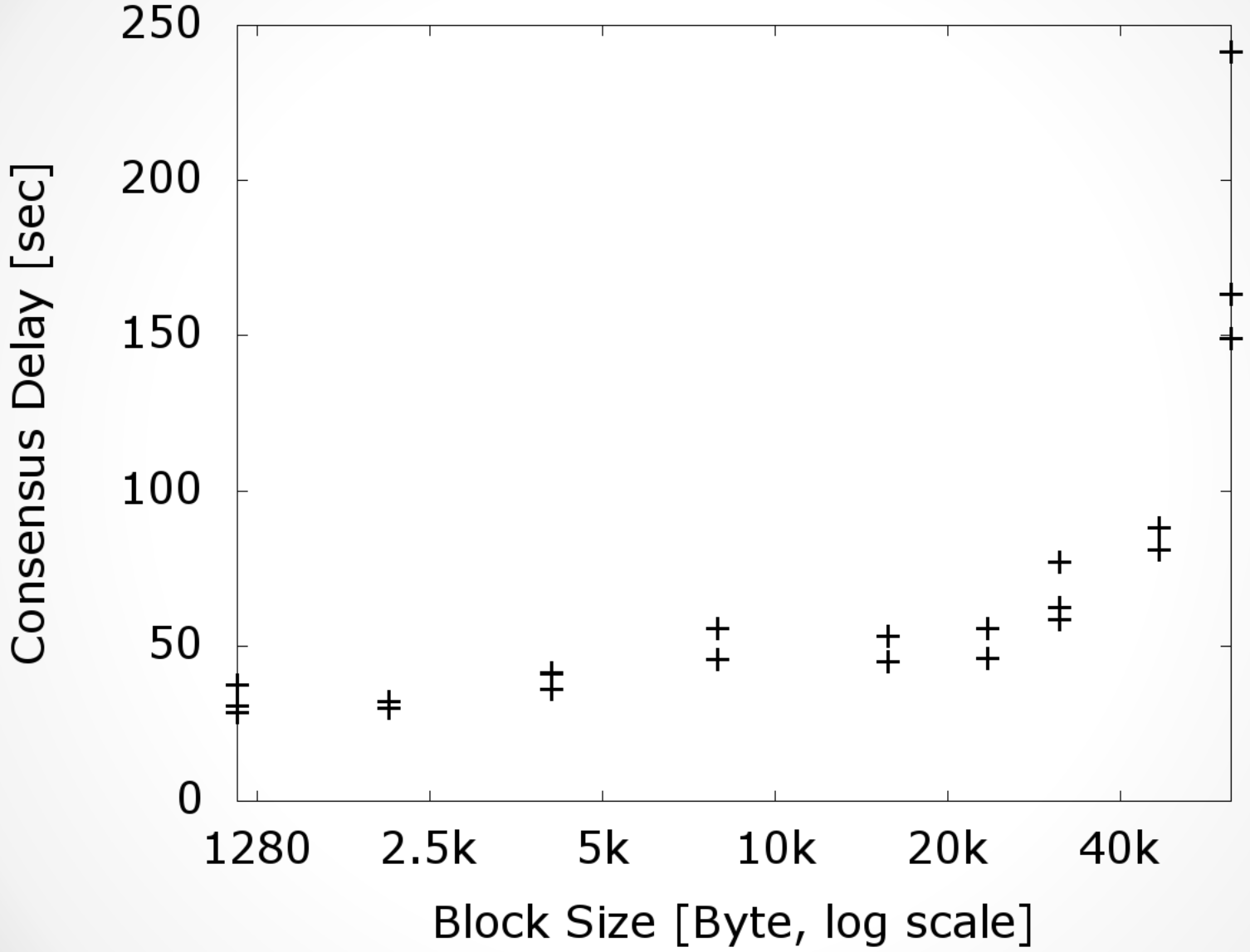
By example:

The (80%, 80%)-*consensus delay* is 10 seconds if 80% of the time, 80% of the nodes agree on the history until 10 seconds ago.

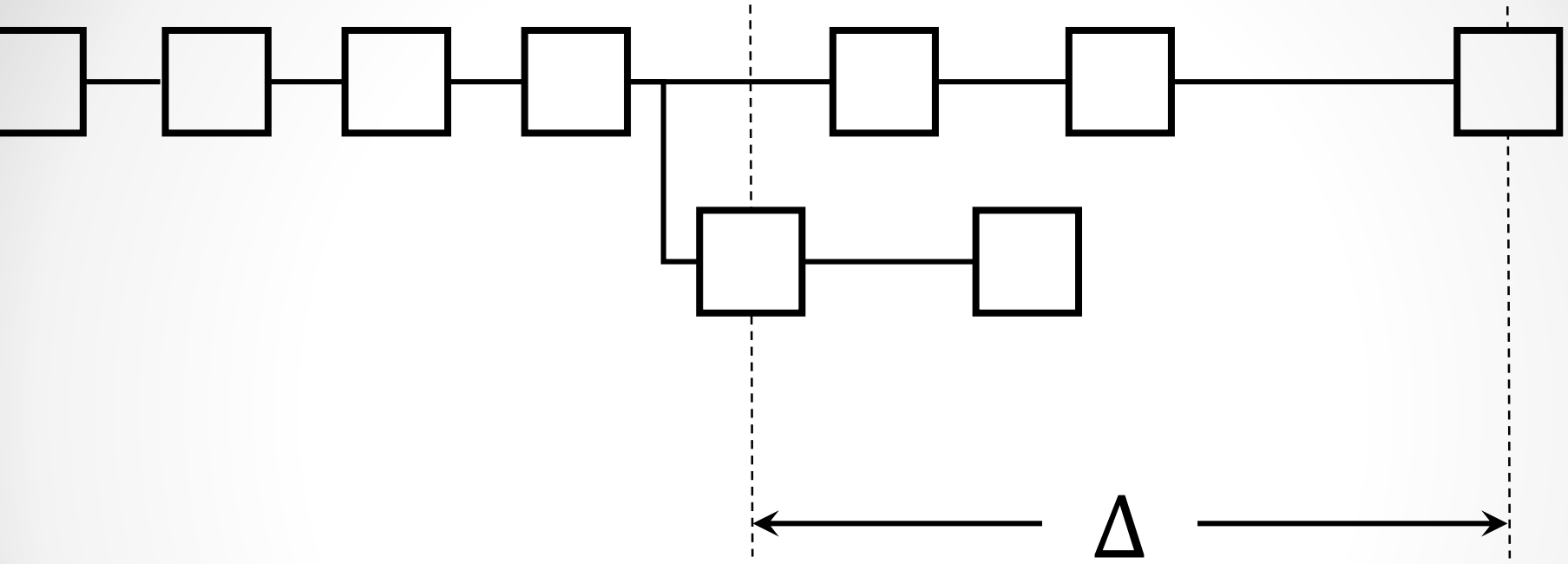
Consensus Delay



Consensus Delay

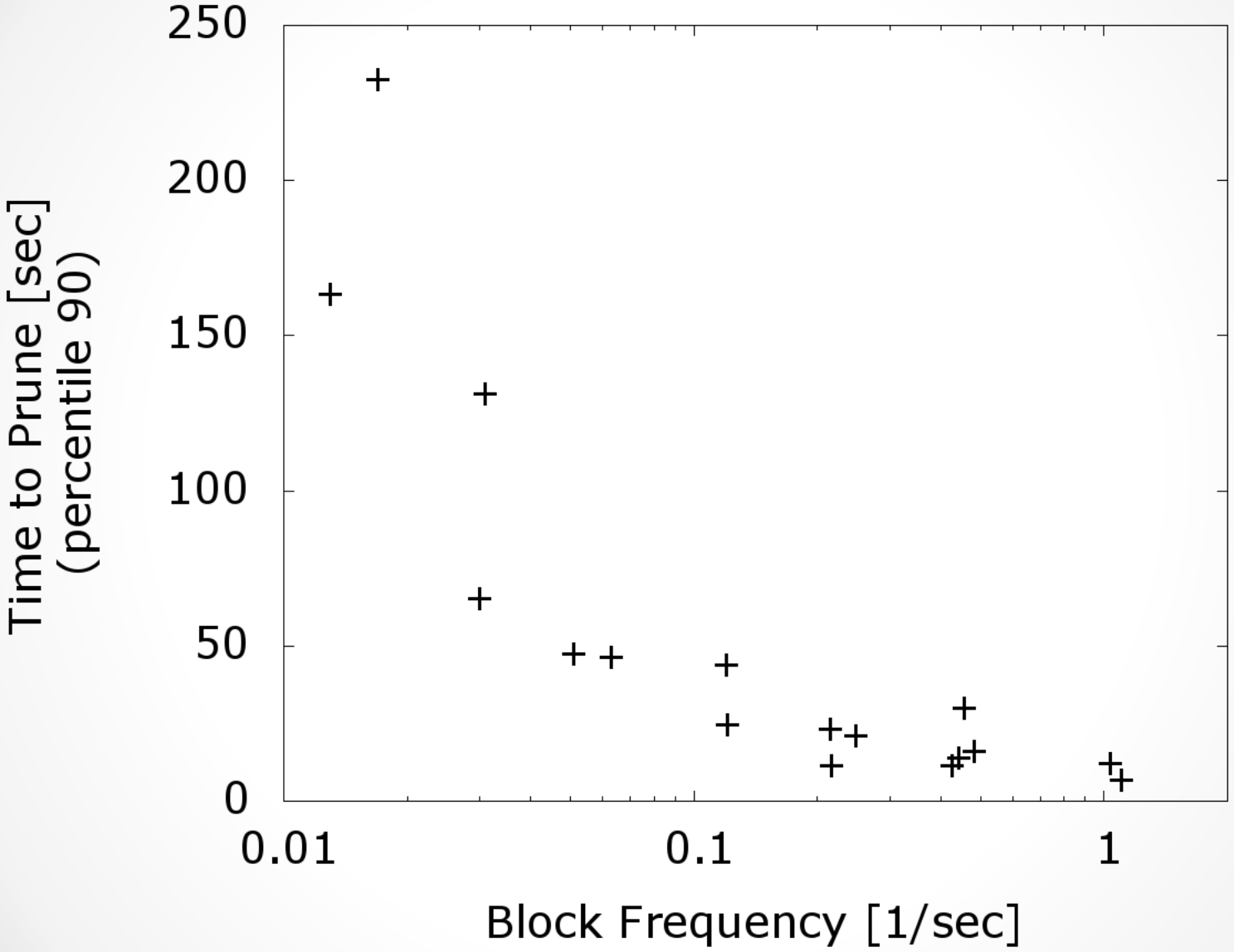


Subjective Time to Prune

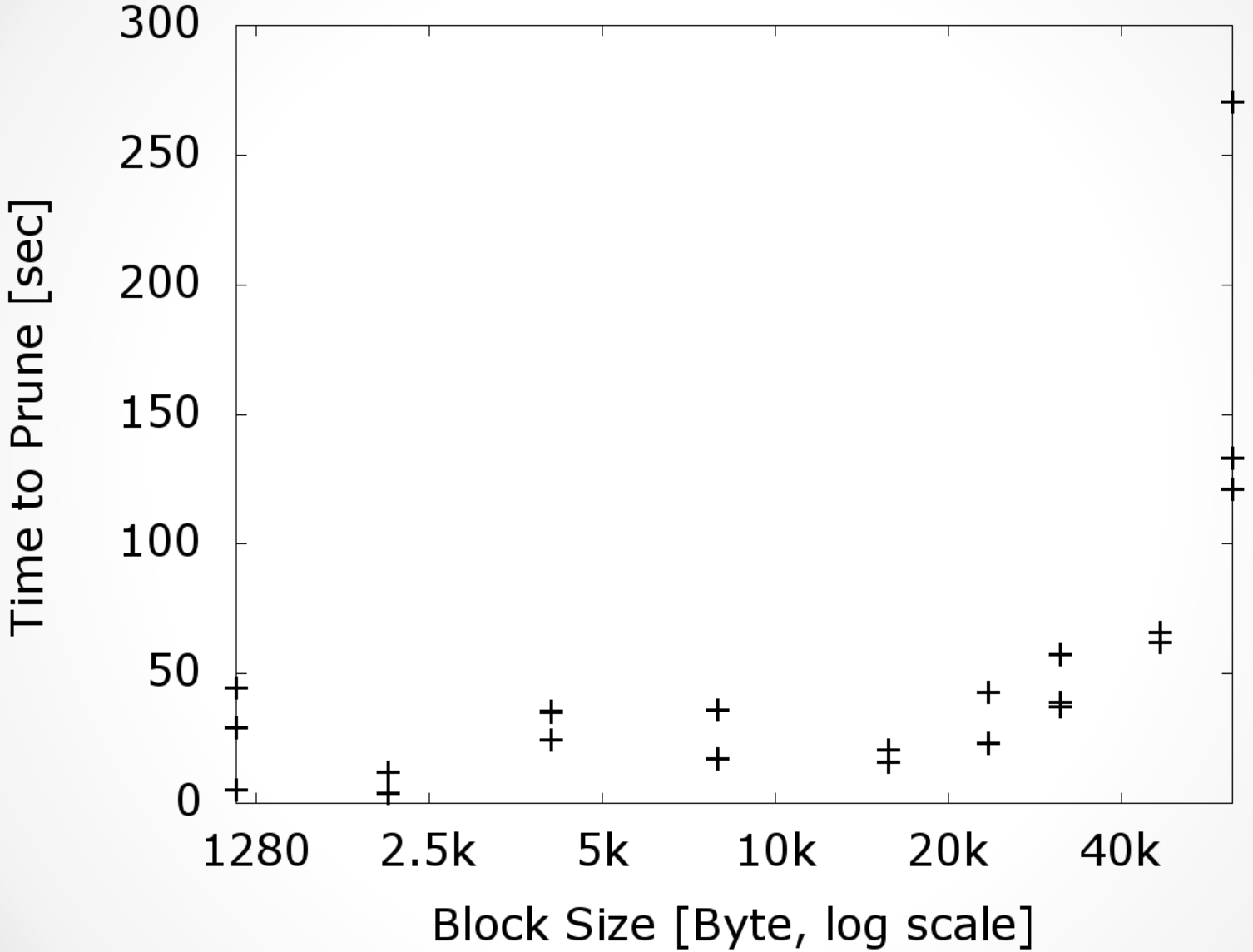


Time to prune: Until branch is pruned

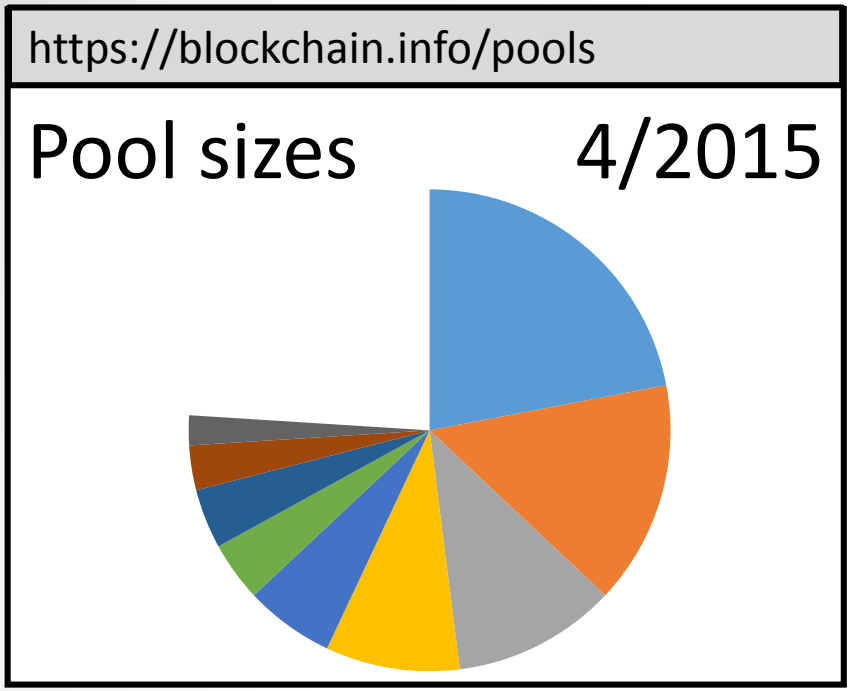
Subjective Time to Prune



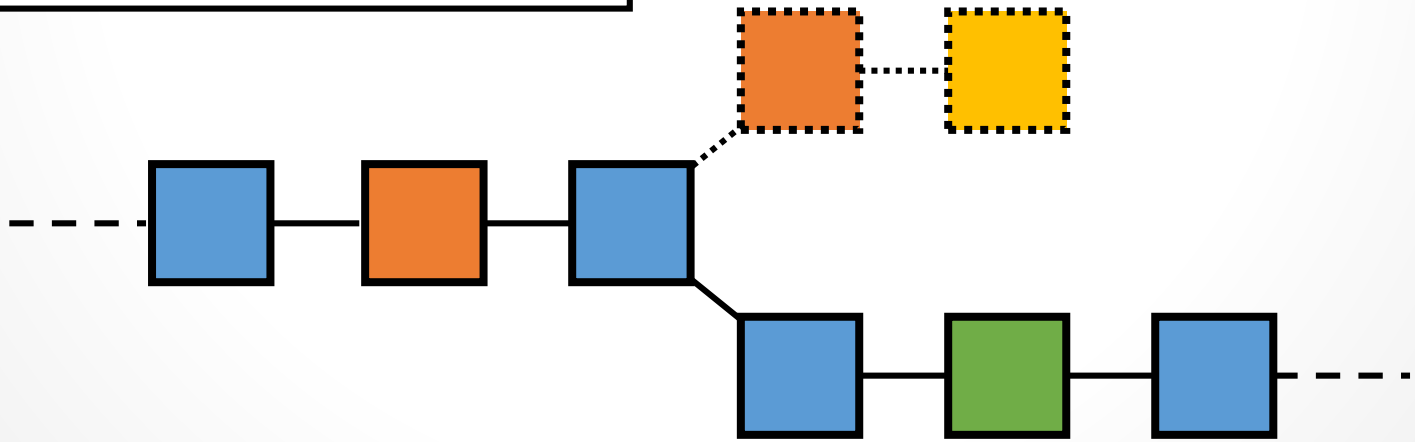
Subjective Time to Prune



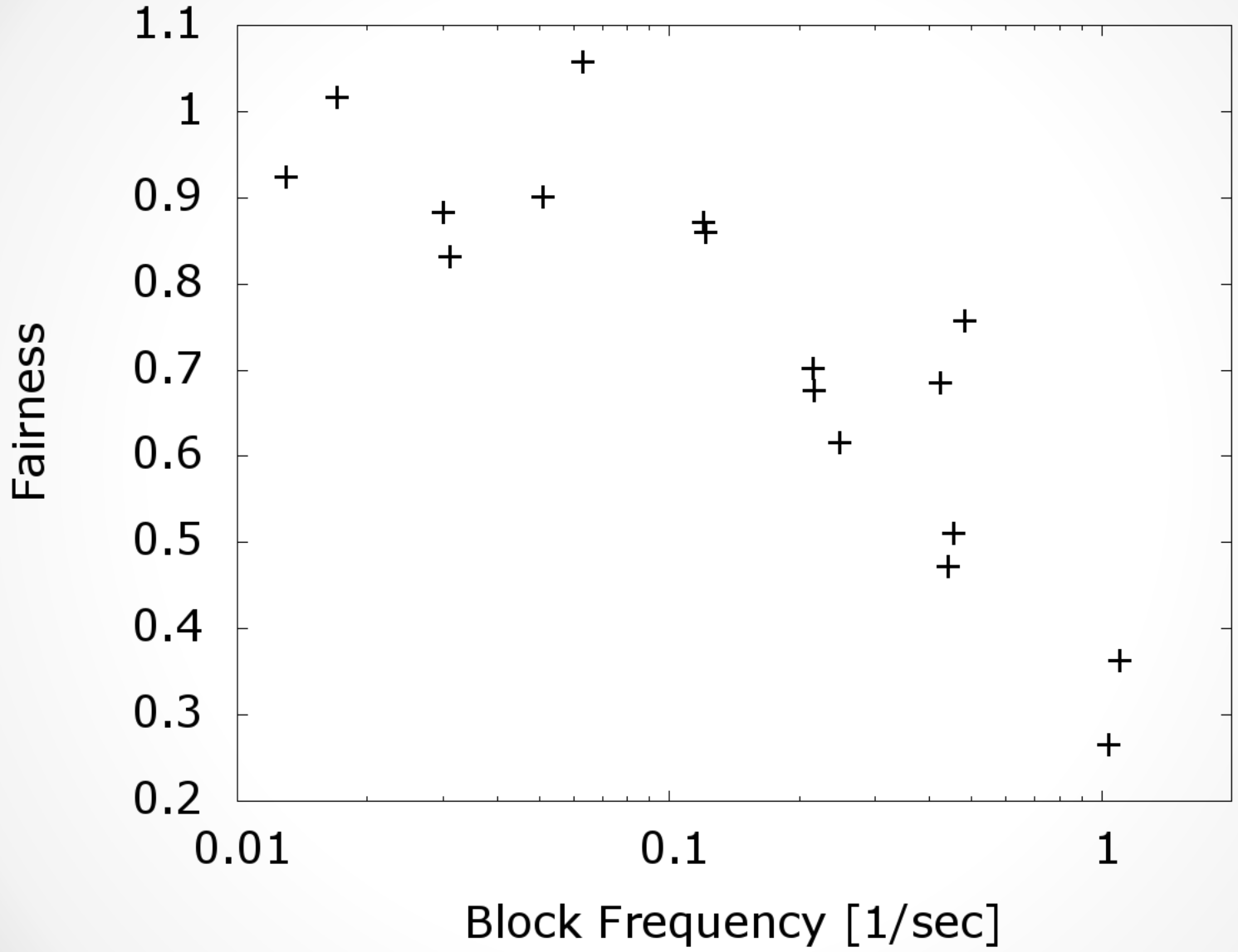
Fairness



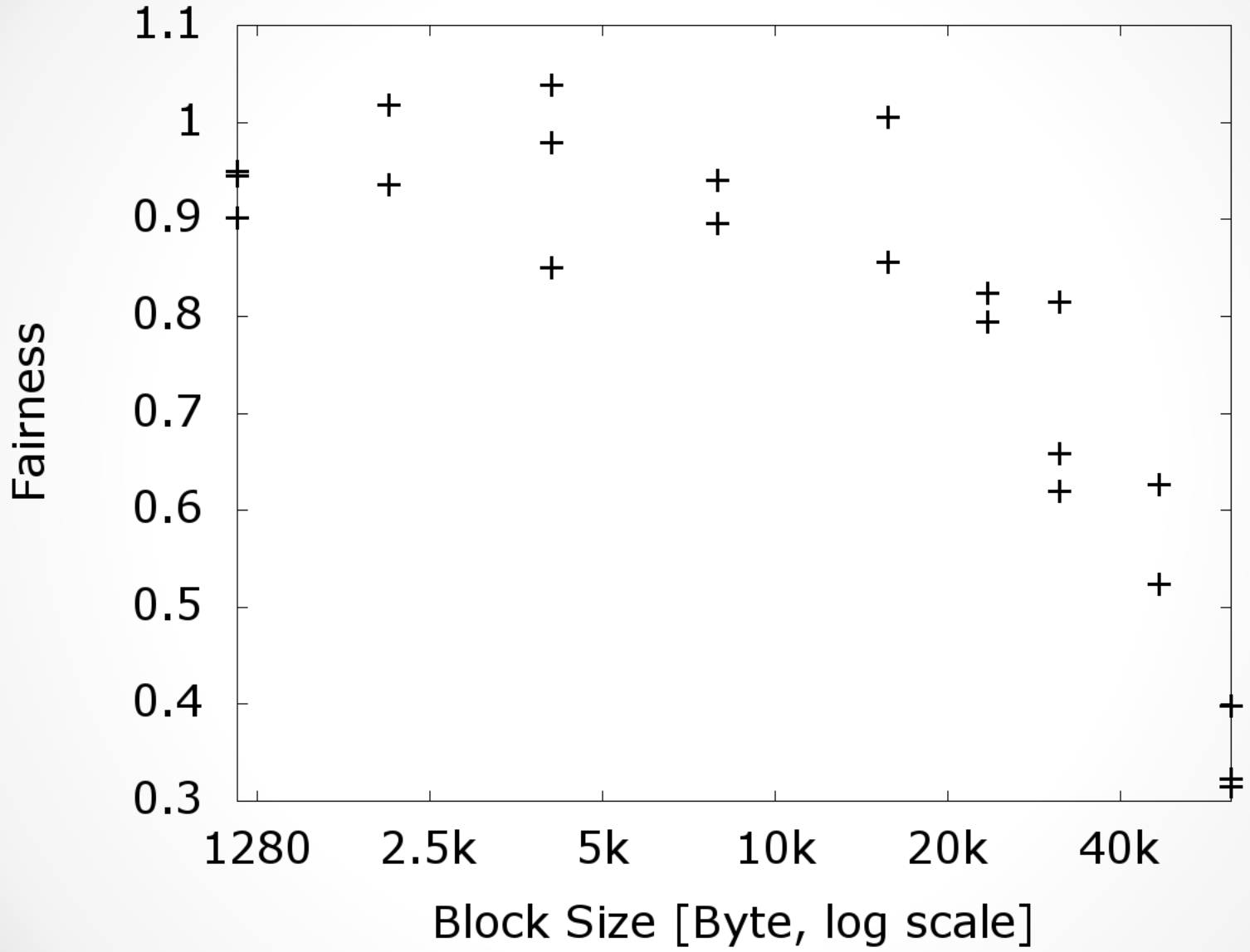
Fairness: Ratio of chain blocks **not** from largest pool (normalized)



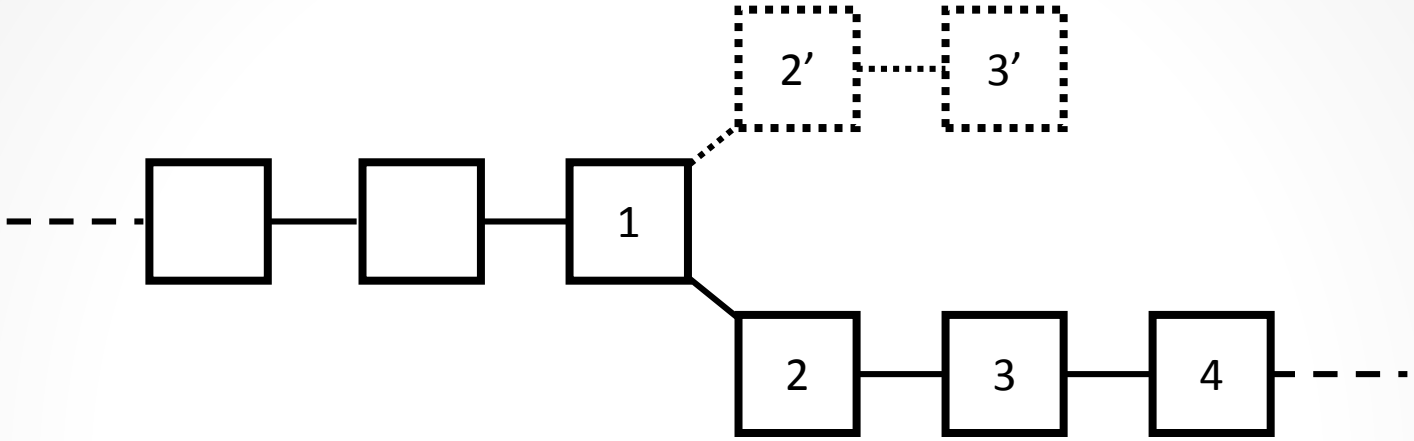
Fairness


1.1
1
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
Fairness
0.01
0.1
1
Block Frequency [1/sec]

Fairness

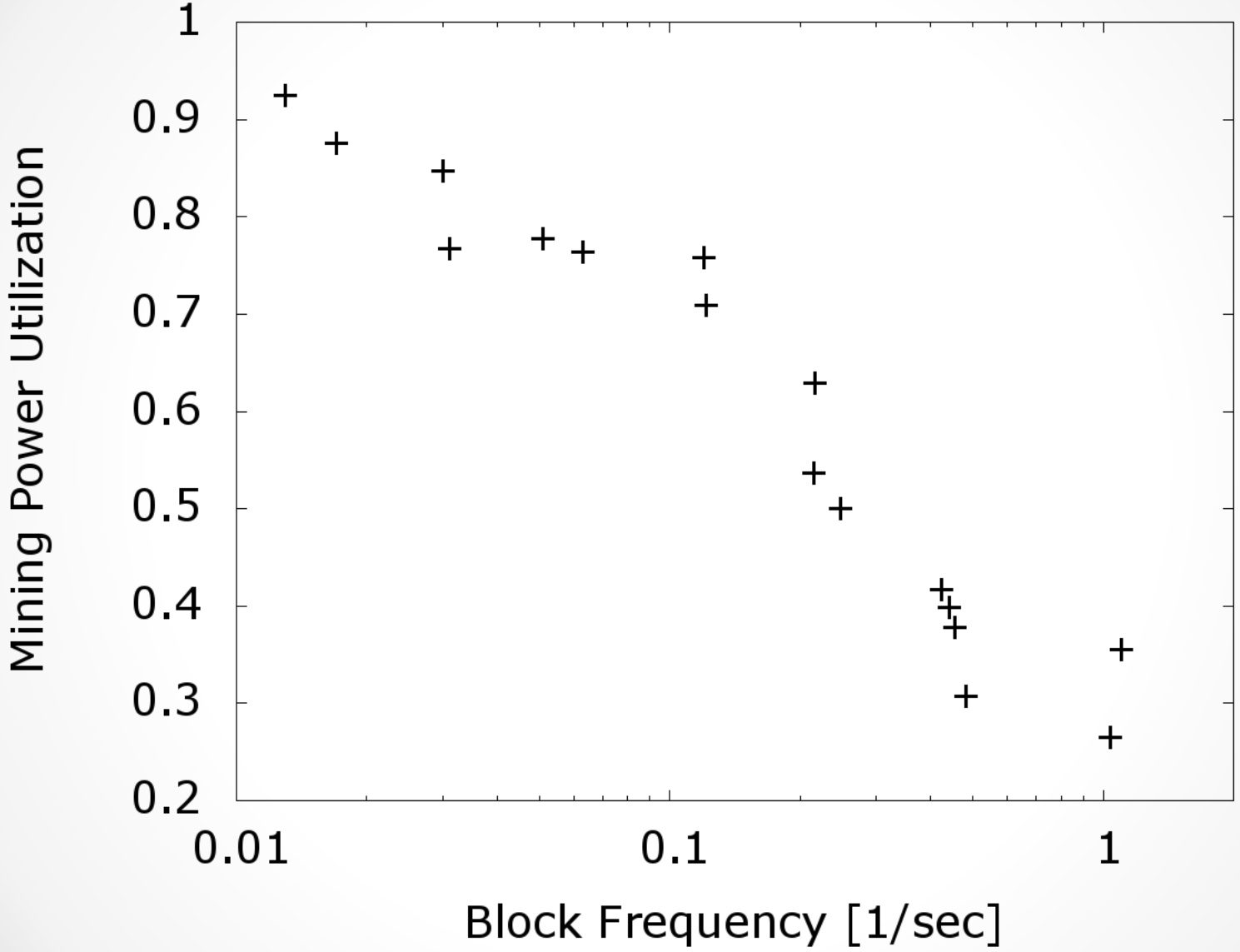

1.1
1
0.9
0.8
0.7
0.6
0.5
0.4
0.3
Fairness
1280
2.5k
5k
10k
20k
40k
Block Size [Byte, log scale]

Mining Power Utilization

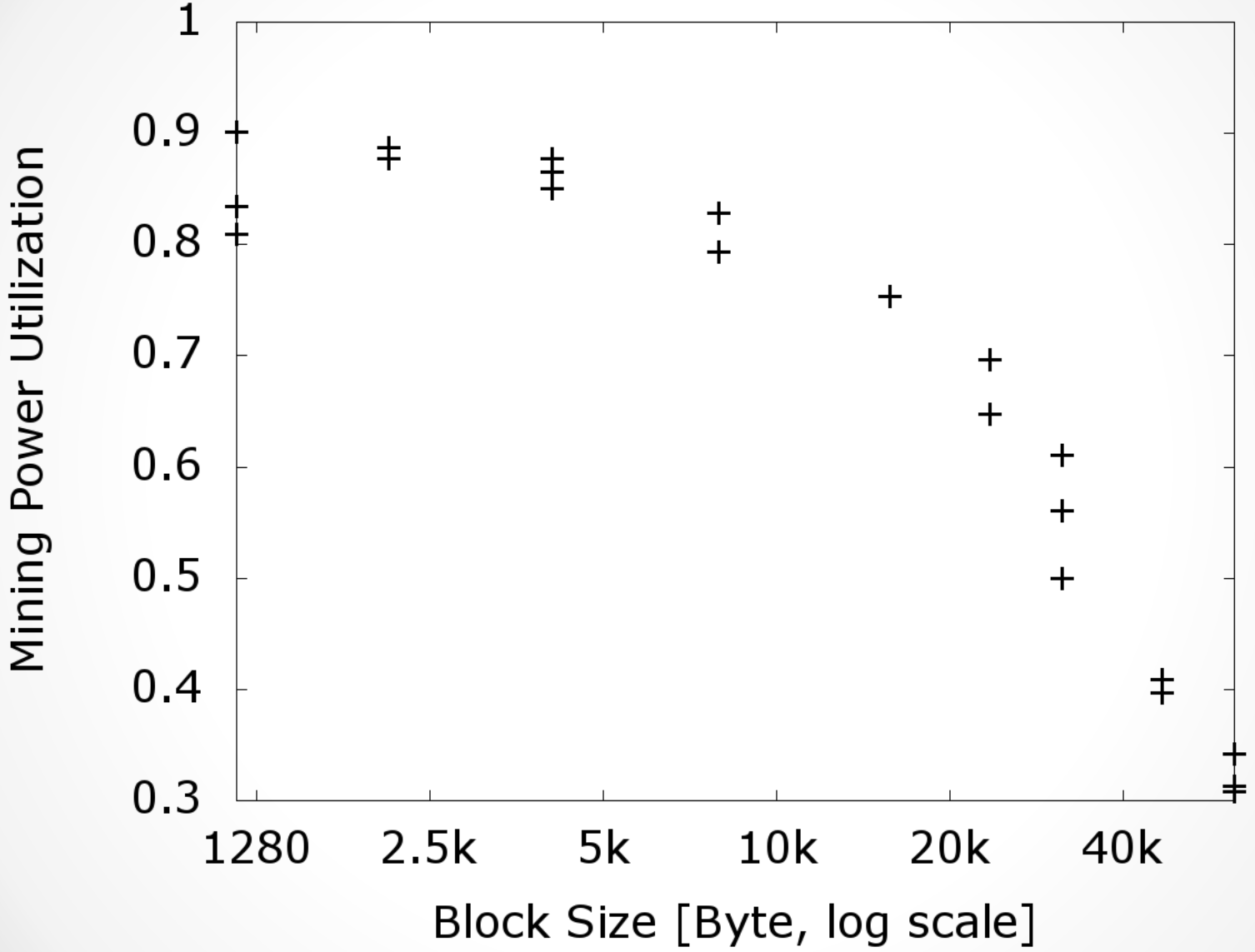


Mining power utilization: Ratio of generated blocks in the main chain

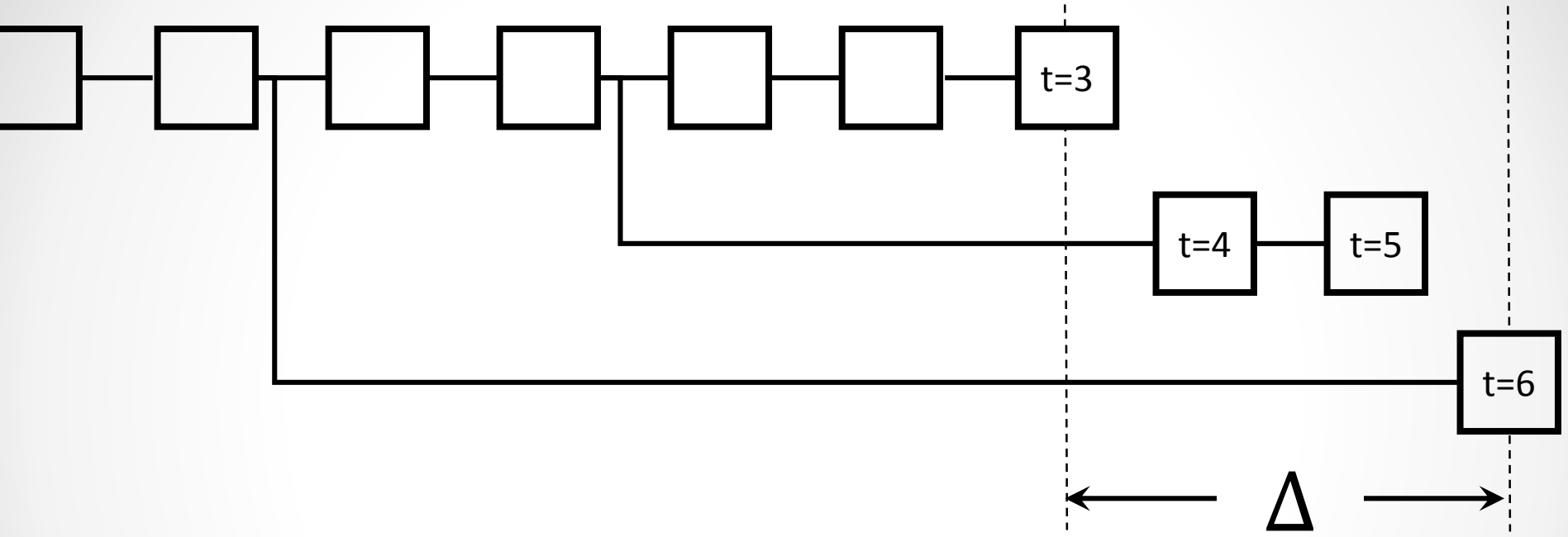
Mining Power Utilization



Mining Power Utilization

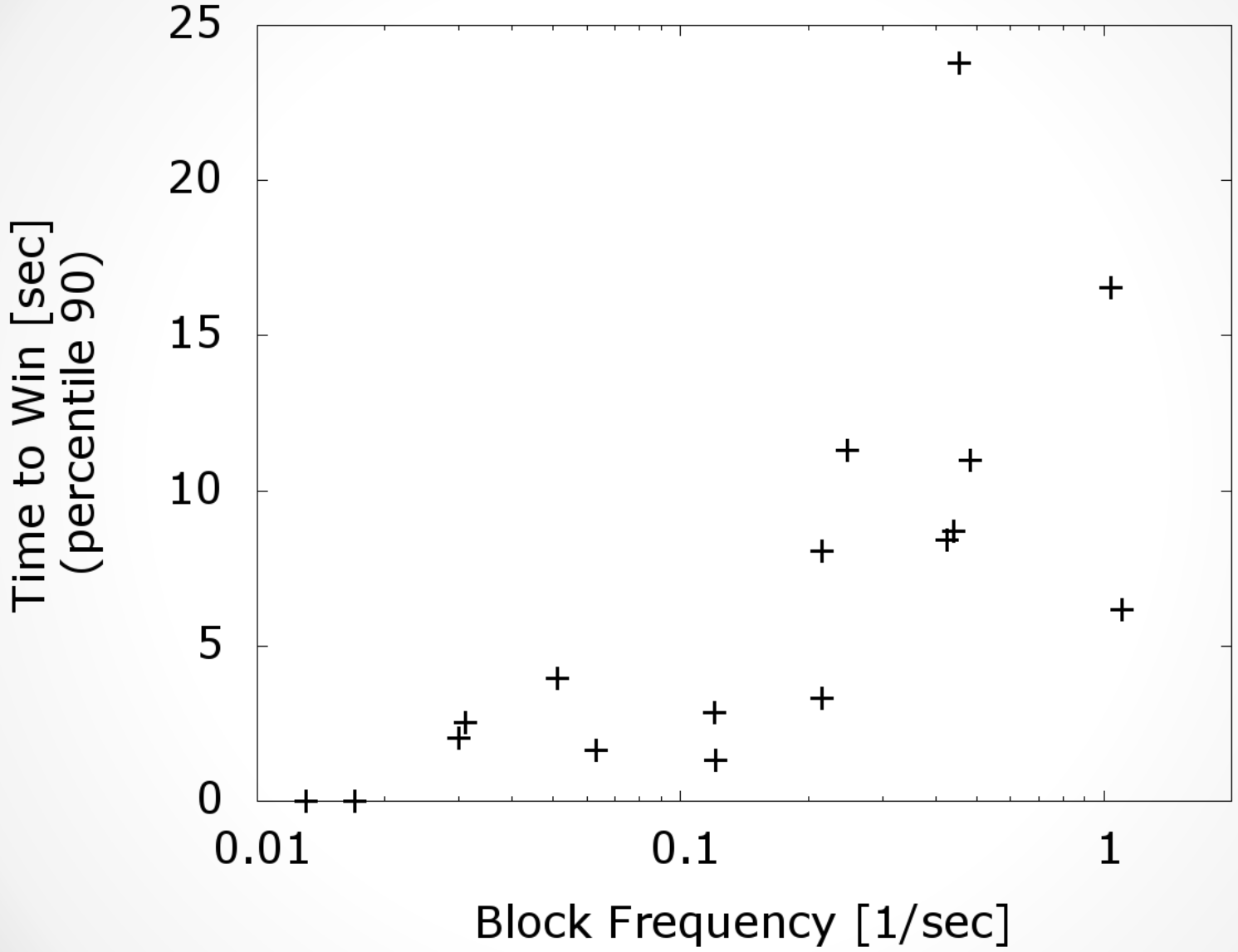


Time to Win

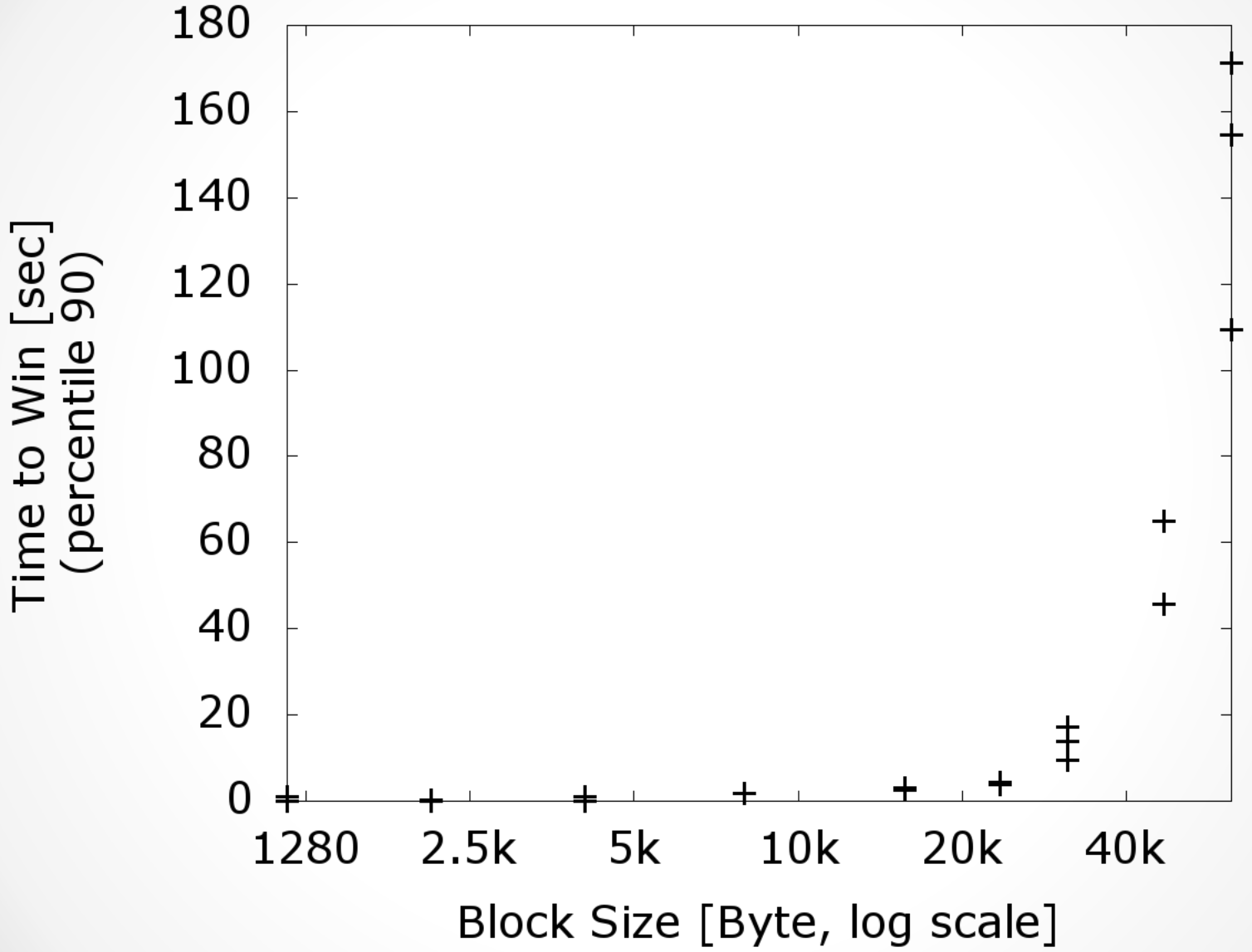


Time to win: Until latest block on any competing branch

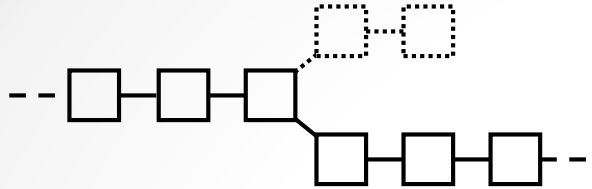
Time to Win


Time to Win [sec]
(percentile 90)
25
20
15
10
5
0
0.01
0.1
1
Block Frequency [1/sec]

Time to Win


Time to Win [sec]
(percentile 90)
180
160
140
120
100
80
60
40
20
0
1280
2.5k
5k
10k
20k
40k
Block Size [Byte, log scale]

Summary



Scaling the Blockchain

Metrics

- Consensus delay
- Fairness
- Power utilization
- Time to win
- Time to prune

The Blockchain test bed

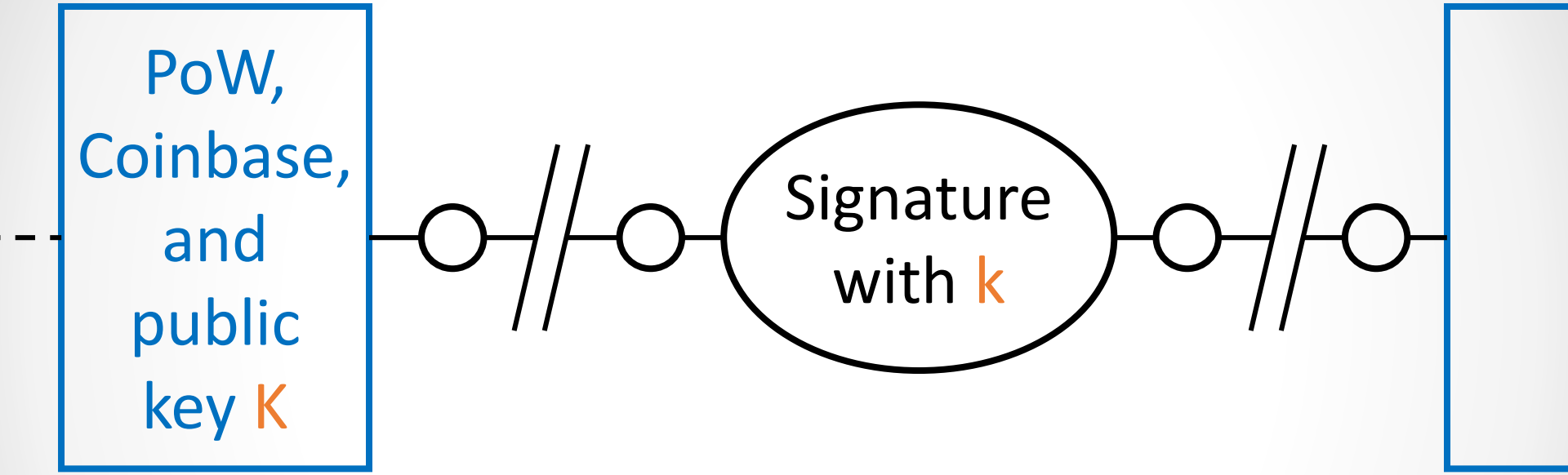
Bitcoin NG

Bitcoin-NG

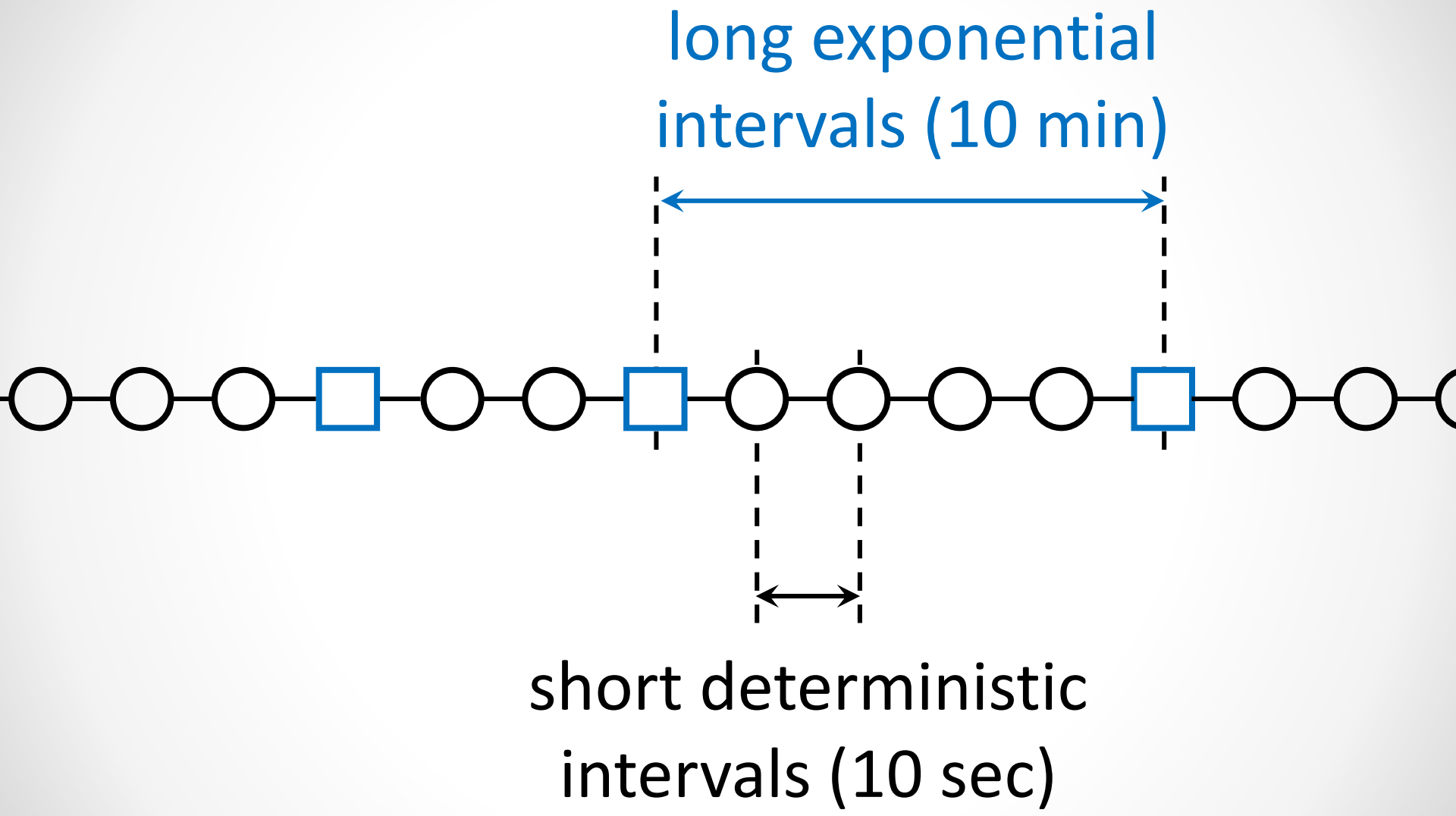
- Key blocks:
  - No content
  - Leader election

- Microblocks:
  - Only content
  - No contention

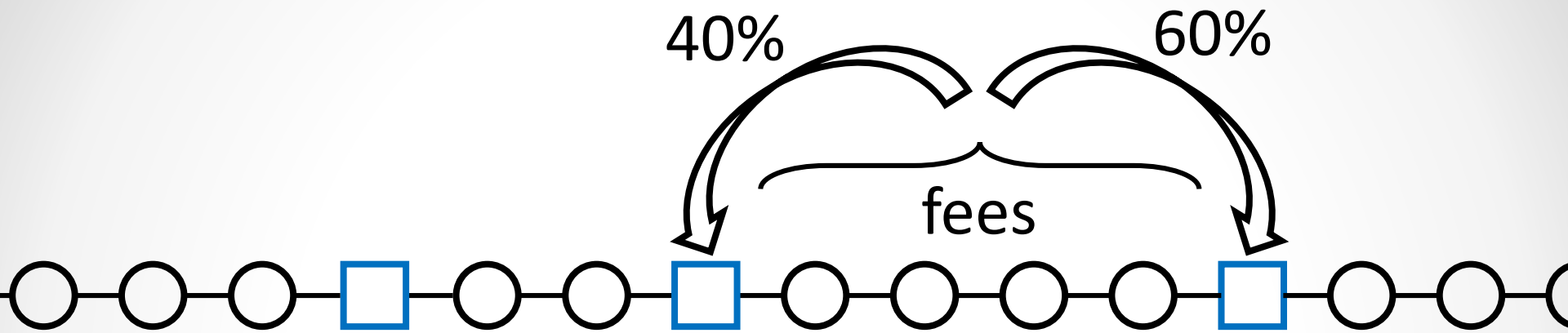
Bitcoin-NG



Bitcoin-NG


long exponential
intervals (10 min)
short deterministic
intervals (10 sec)

Transaction Fees



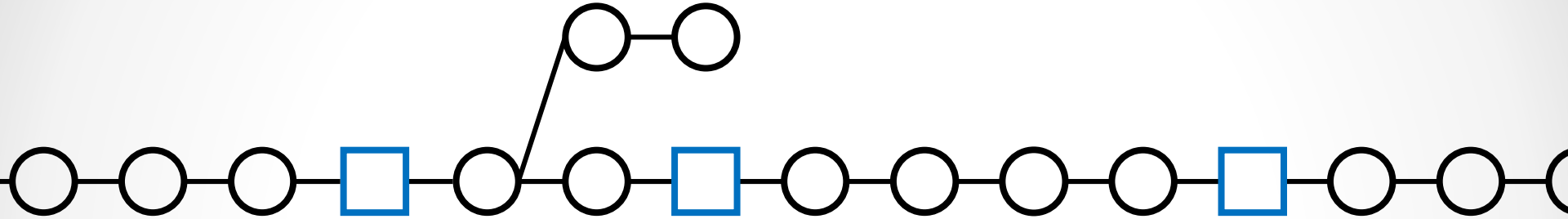
Incentives

Next miner: Include previous micro-blocks

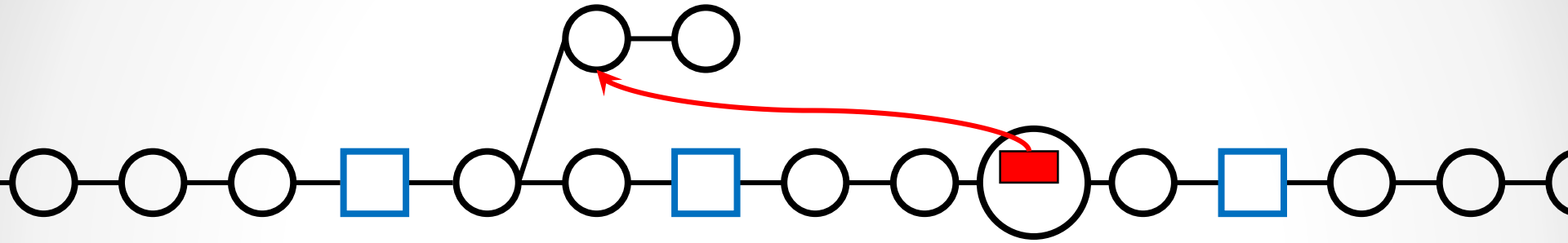
Leader: Place transactions in micro blocks;

Smaller chance to win after a microblock

Double Spending



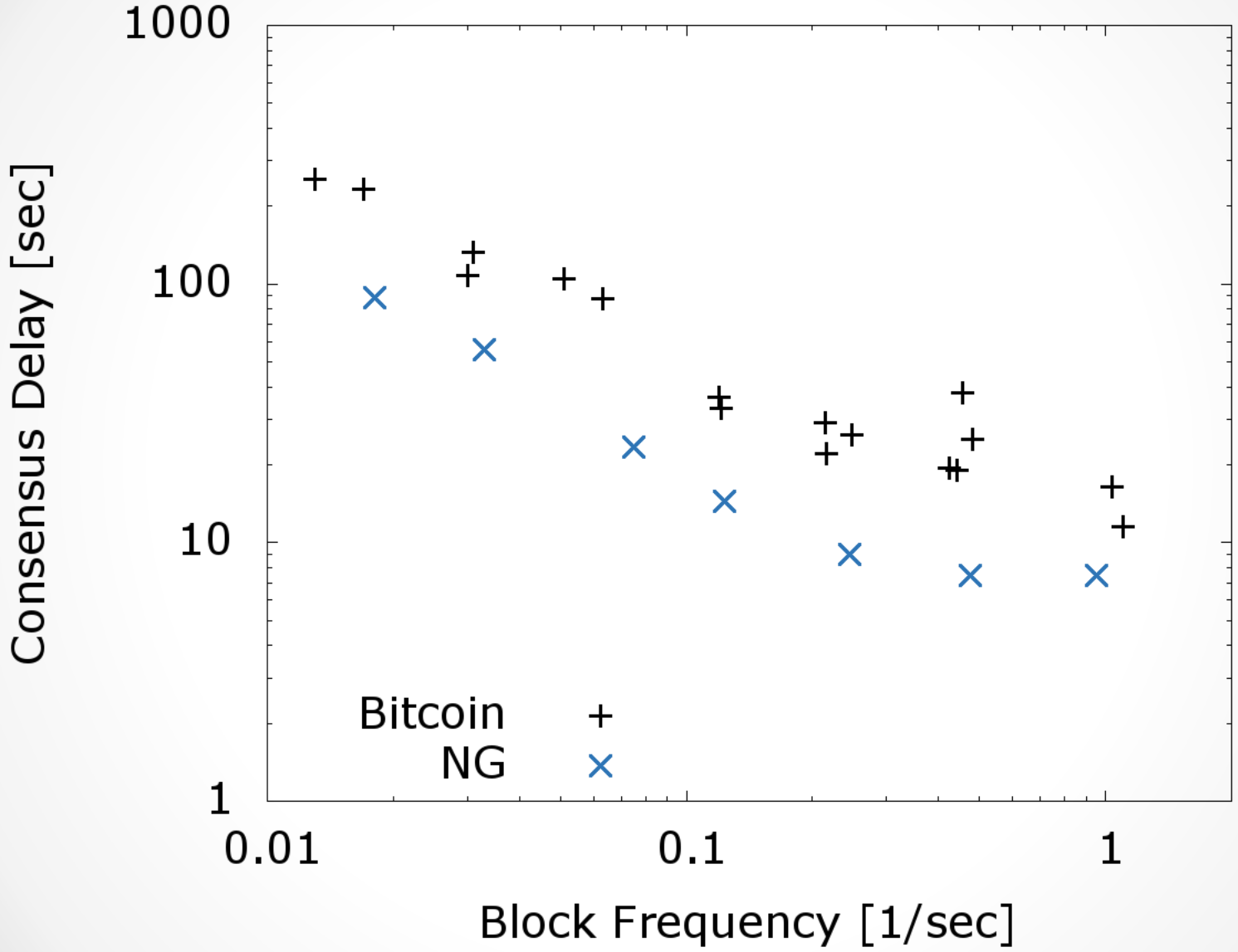
Double Spending



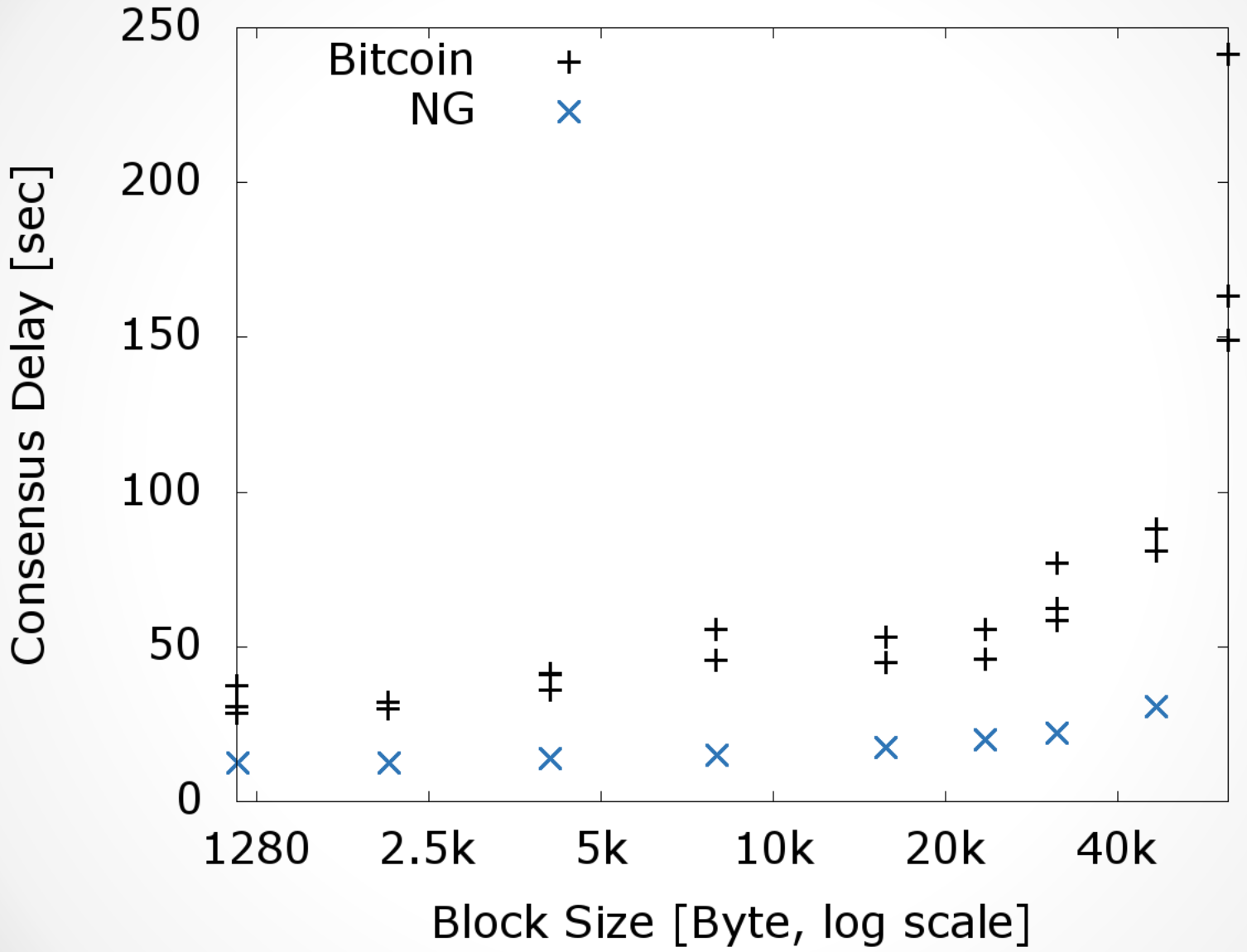
Poison transaction cancels cheater reward

Poisoner receives nominal prize

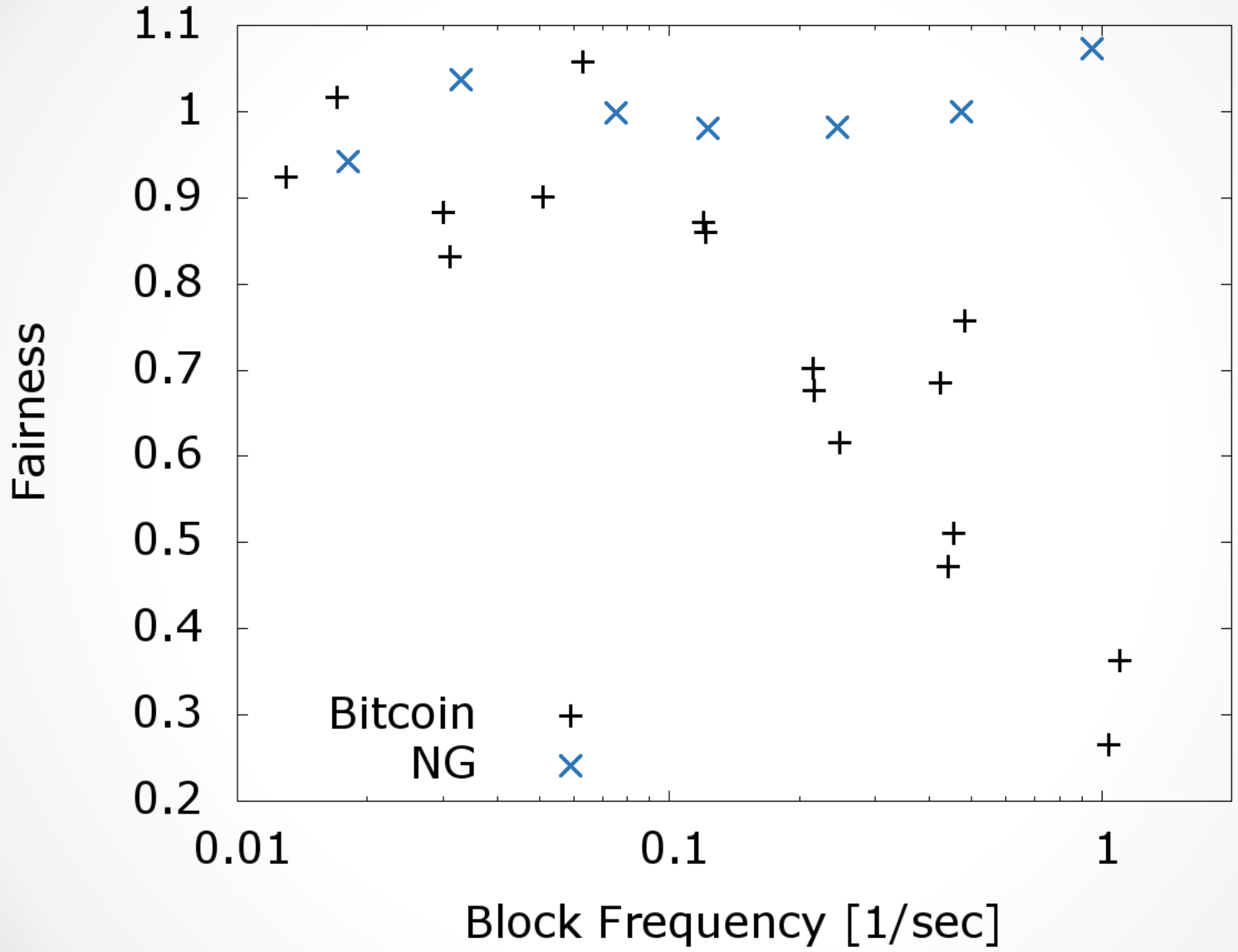
Consensus Delay



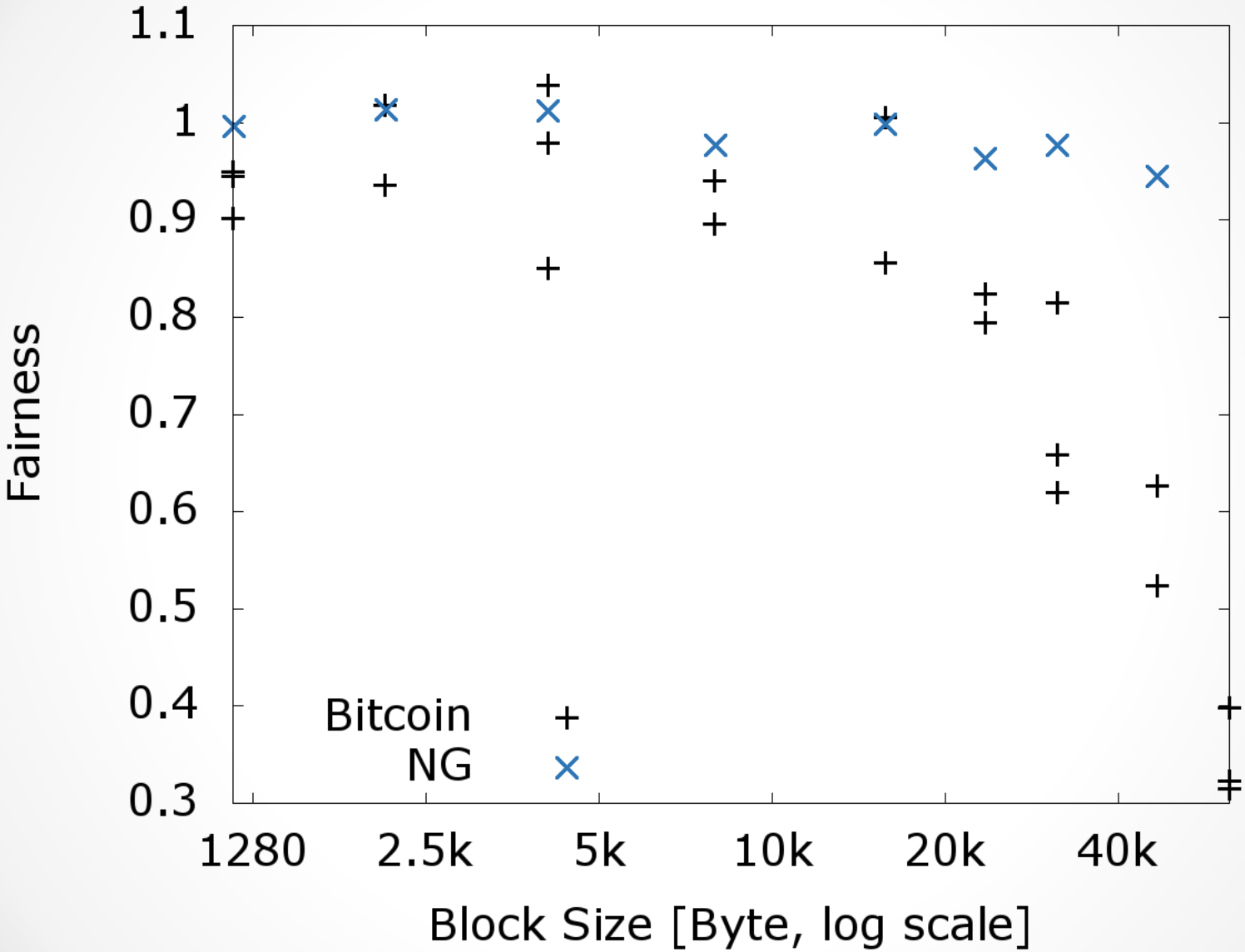
Consensus Delay



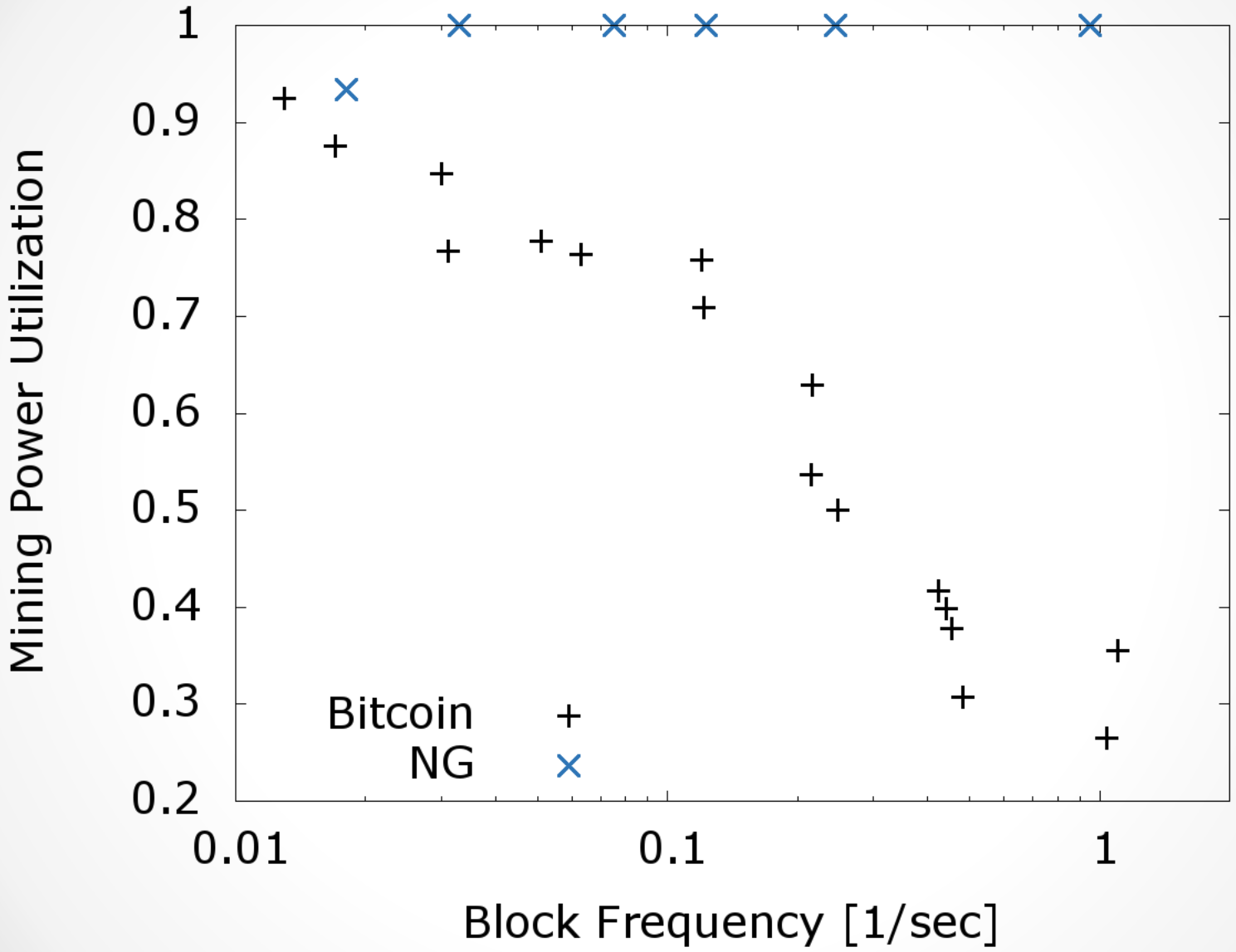
Fairness


1.1
1
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
Fairness
0.01
0.1
1
Block Frequency [1/sec]
Bitcoin
NG

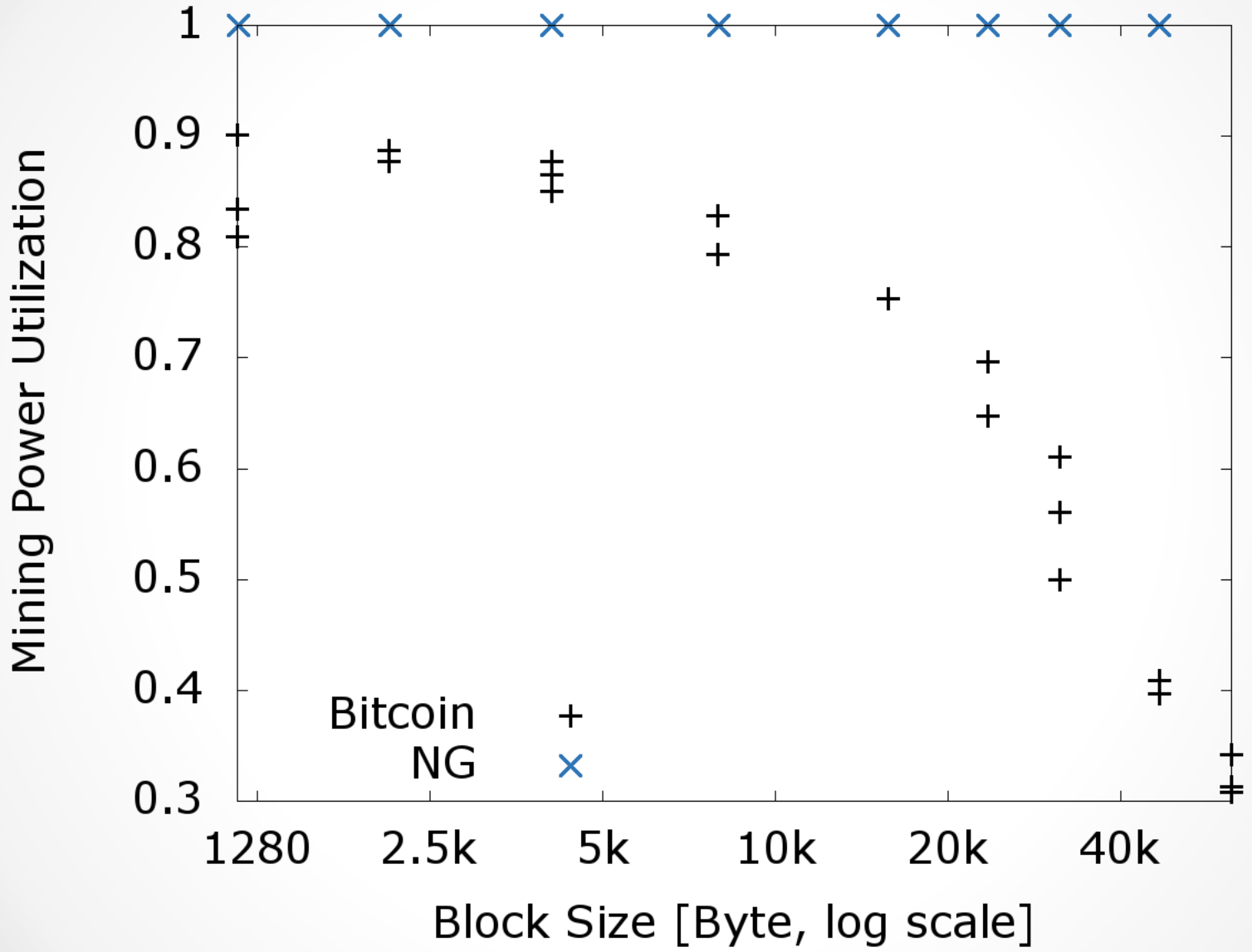
Fairness


1.1
1
0.9
0.8
0.7
0.6
0.5
0.4
0.3
Fairness
Bitcoin
NG
1280
2.5k
5k
10k
20k
40k
Block Size [Byte, log scale]

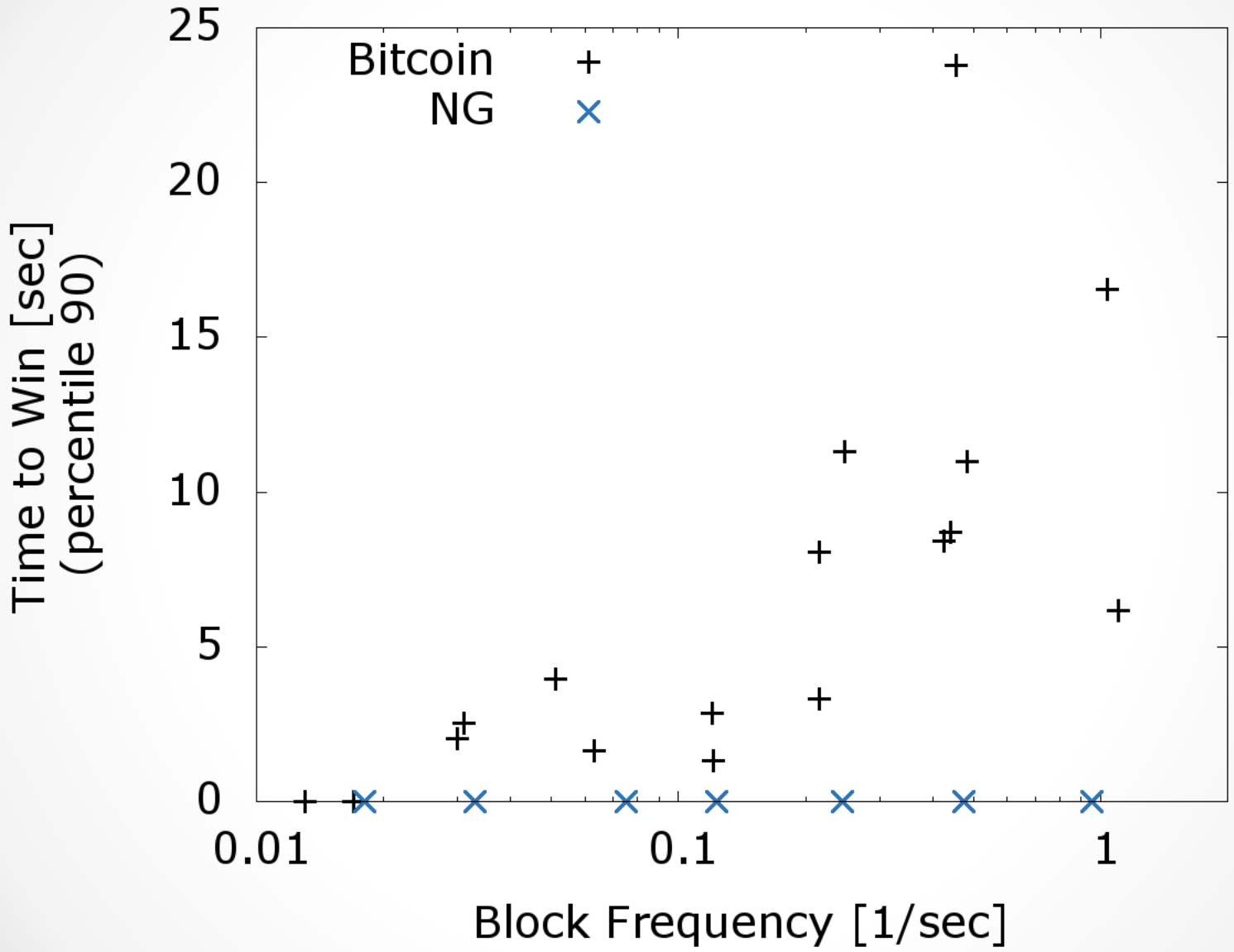
Mining Power Utilization



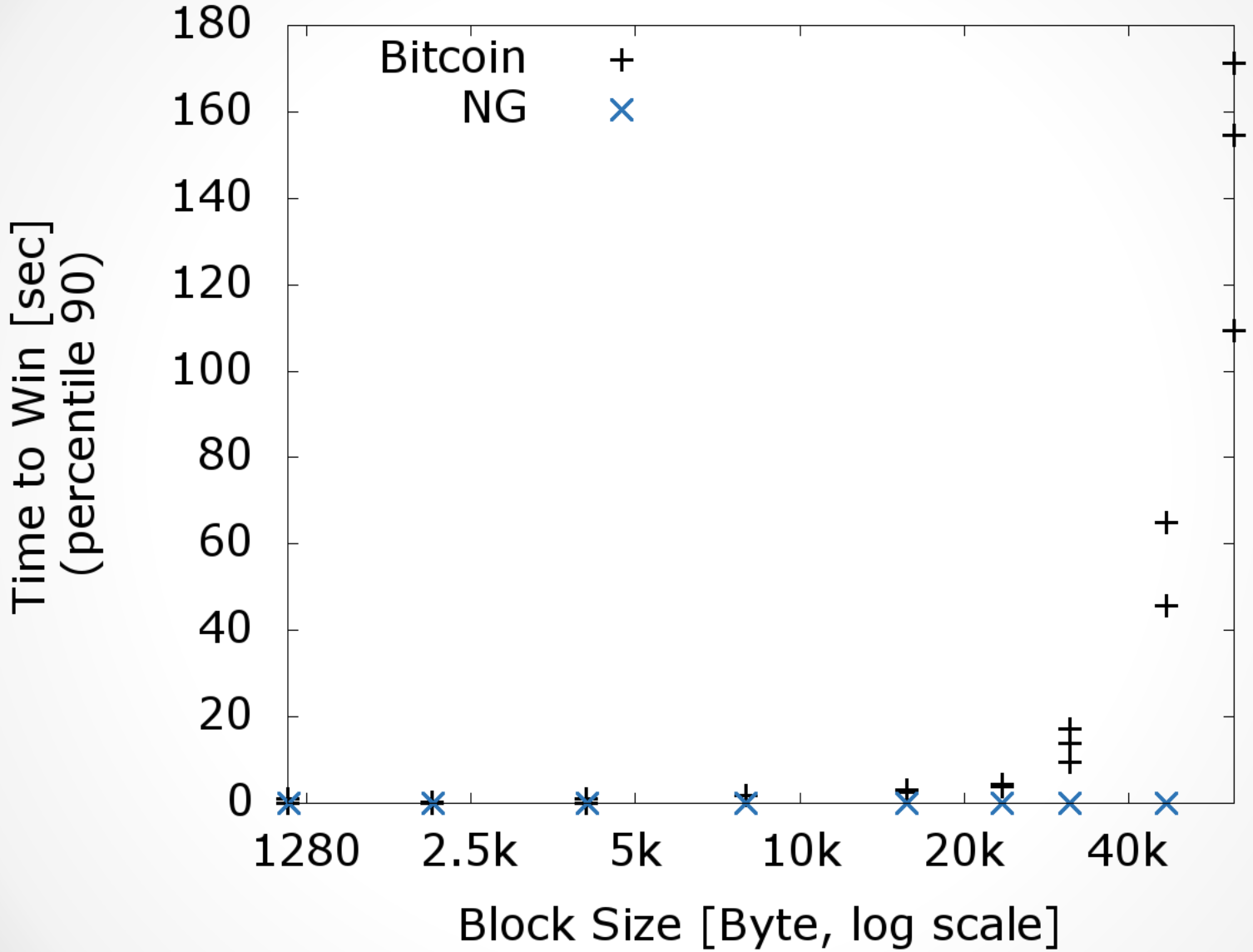
Mining Power Utilization



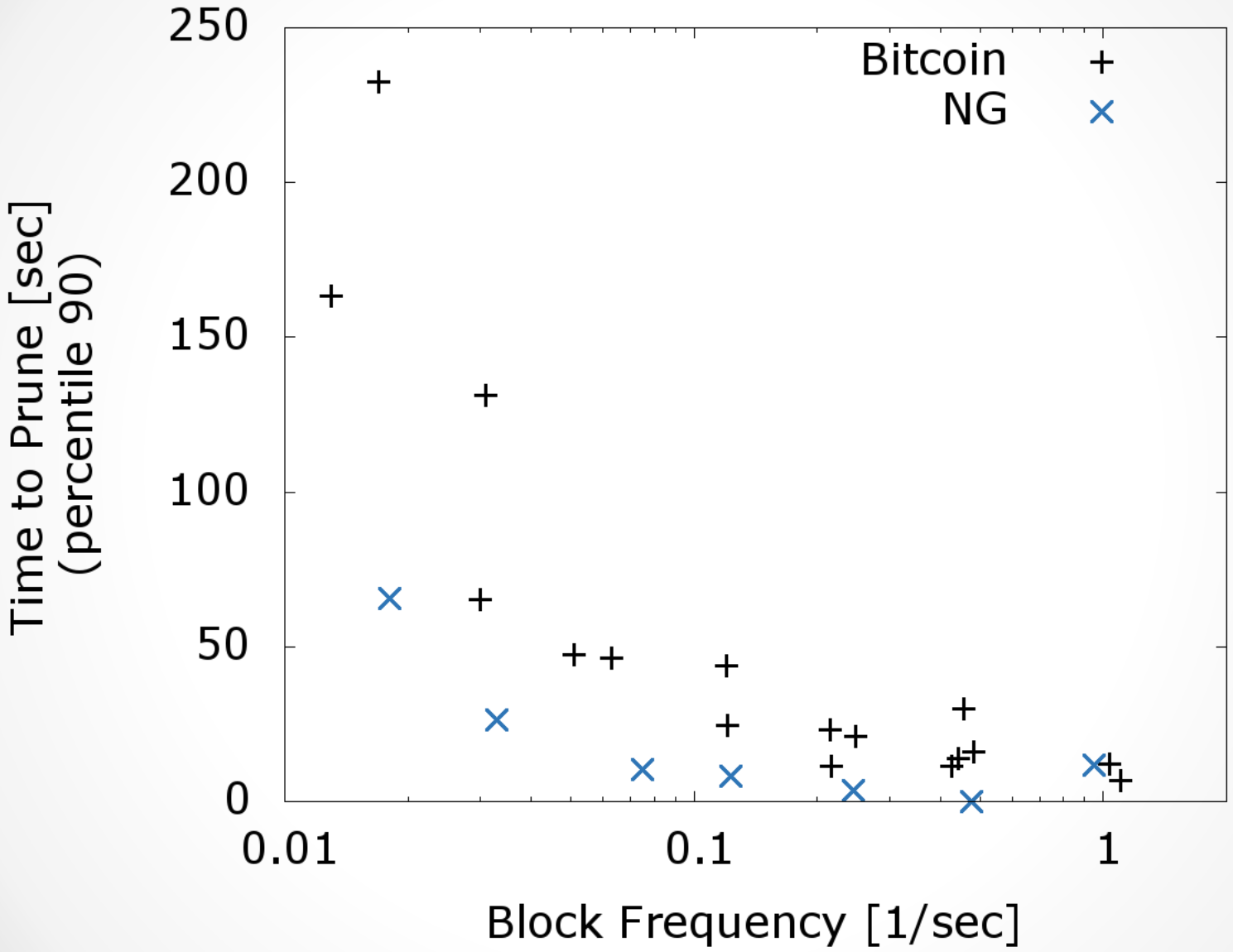
Time to Win


Bitcoin
NG
Time to Win [sec]
(percentile 90)
25
20
15
10
5
0
0.01
0.1
1
Block Frequency [1/sec]

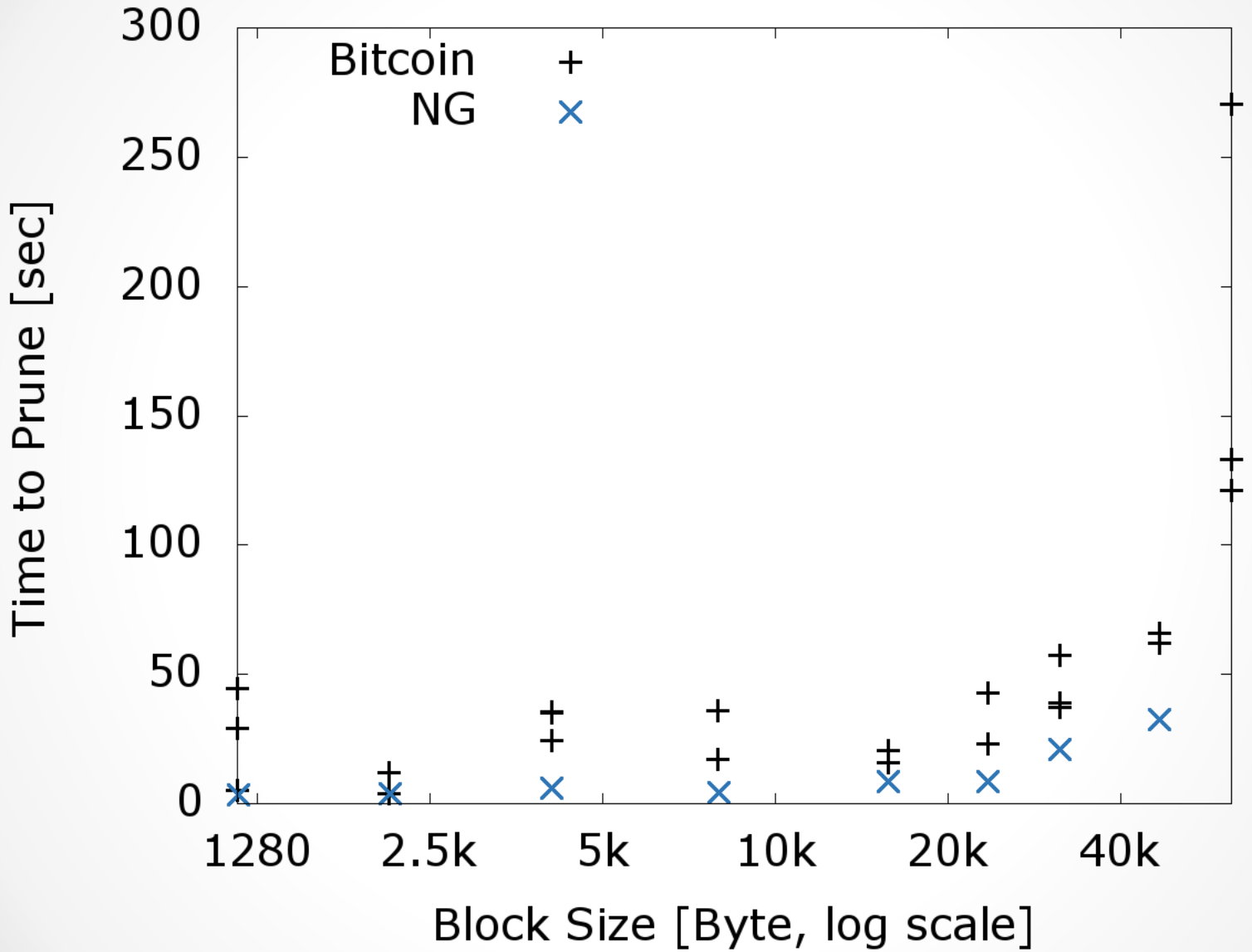
Time to Win


Bitcoin
NG
Time to Win [sec]
(percentile 90)
180
160
140
120
100
80
60
40
20
0
1280
2.5k
5k
10k
20k
40k
Block Size [Byte, log scale]

Subjective Time to Prune



Subjective Time to Prune



Conclusion

Test Bed

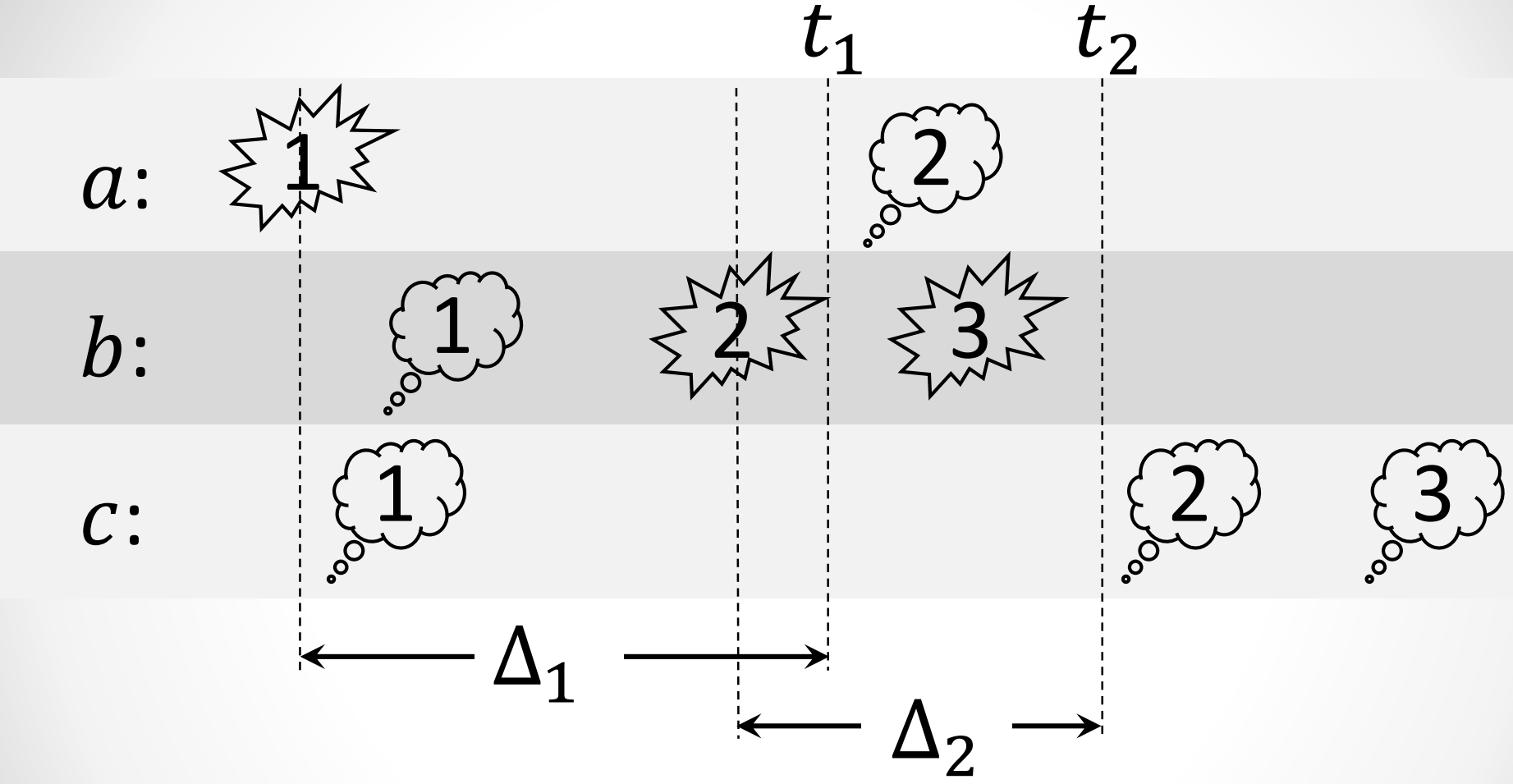
- Metrics
- P2P topology
- Properties to test

Bitcoin-NG

- Comments and concerns
- Adoption by Bitcoin

Ittay Eyal with **Adem Efe Gencer**, **Emin Gün Sirer** and **Robbert Van Renesse**

Consensus Latency



What is Δ such that at least δ of the time, ε of the nodes agree on the history up to $t - \Delta$