

Bitcoin-NG and the Blockchain Test bed

Ittay Eyal
Cornell

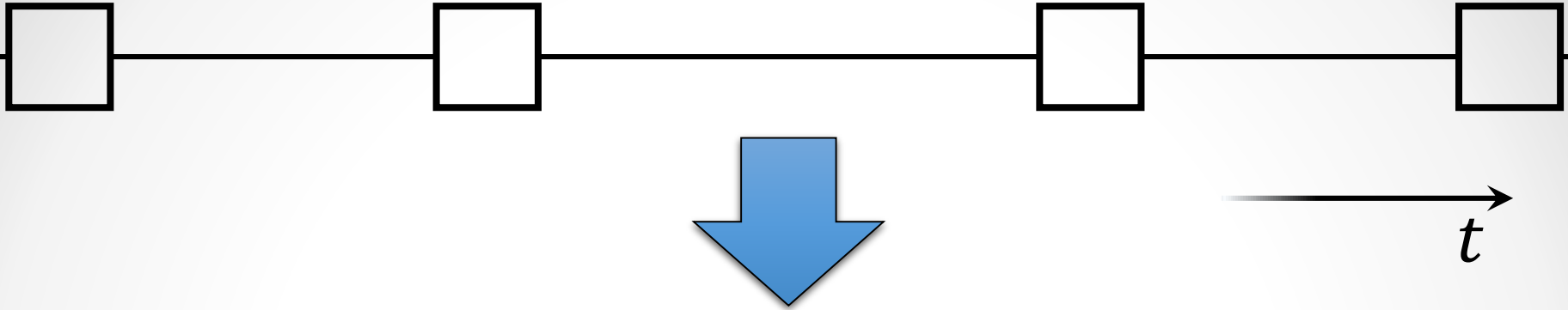
With **Adem Efe Gencer, Emin Gün Sirer**
and **Robbert Van Renesse**

Scaling Bitcoin Workshop, Montréal, August 2015

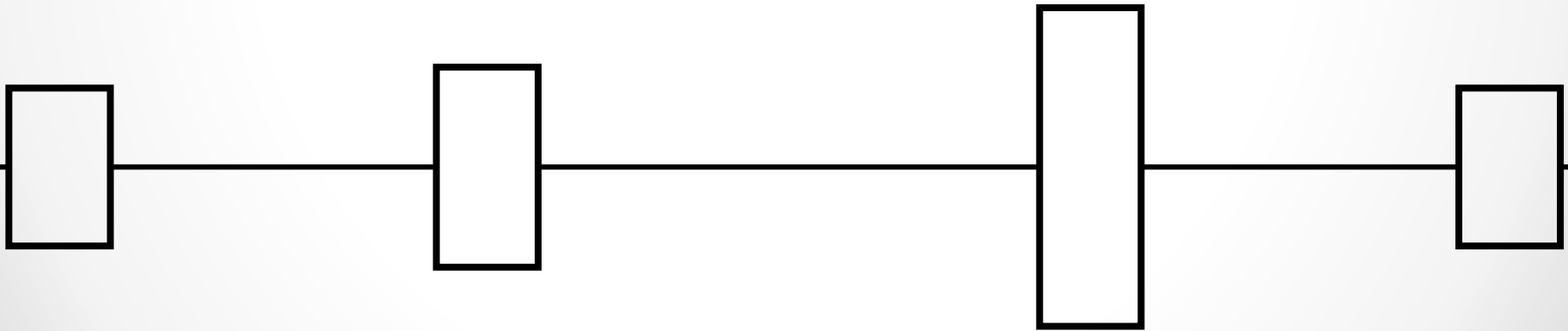
Goals

- Lower latency
- Higher throughput
- Security

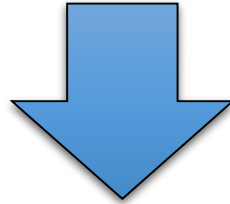
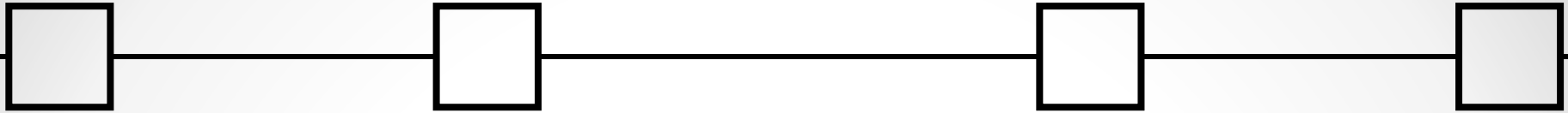
Parameter Tuning



1. Larger blocks →
 - Higher throughput

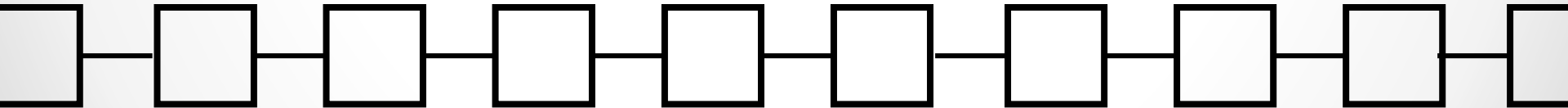


Parameter Tuning

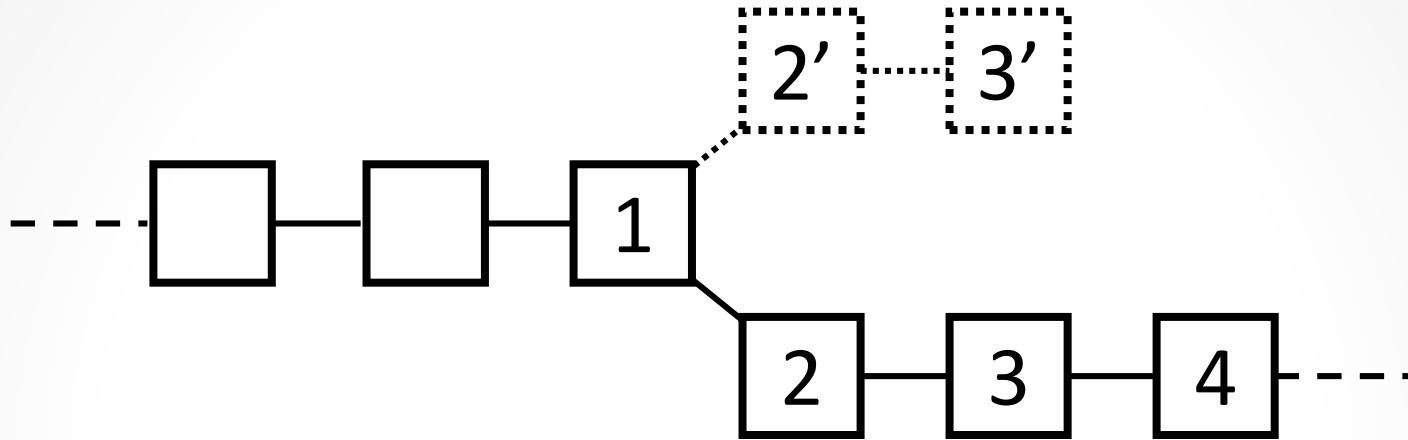


2. Shorter block intervals →

- Higher throughput
- Lower latency



Scaling by Tuning Causes Forks



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

Evaluation

Test Bed

```
sudo ip link add vlo04 type veth peer name vlo04b
sudo ip link add vlo05 type veth peer name vlo05b
sudo ip link add vlo06 type veth peer name vlo06b
sudo ip link add vlo07 type veth peer name vlo07b
# Assign one side of the virtual ethernet link to a namespace
sudo ip link set vlo01 netns node-020-01
sudo ip link set vlo02 netns node-020-02
sudo ip link set vlo03 netns node-020-03
sudo ip link set vlo04 netns node-020-04
sudo ip link set vlo05 netns node-020-05
sudo ip link set vlo06 netns node-020-06
sudo ip link set vlo07 netns node-020-07
# Bring links up: (10.2.1.100+i at namespaces; 10.2.1.0+i here)
sudo ifconfig vlo01 1.1/24 up
sudo ifconfig vlo02 2.1/24 up
sudo ifconfig vlo03 3.1/24 up
sudo ifconfig vlo04 4.1/24 up
sudo ifconfig vlo05 5.1/24 up
sudo ifconfig vlo06 6.1/24 up
sudo ifconfig vlo07 7.1/24 up
# Node node-020-01
sudo ip netns exec ns-020-01 ifconfig vlo01b 10.2.1.100/24 up
# Node node-020-02
sudo ip netns exec ns-020-02 ifconfig vlo02b 10.2.2.100/24 up
# Node node-020-03
sudo ip netns exec ns-020-03 ifconfig vlo03b 10.2.3.100/24 up
# Node node-020-04
sudo ip netns exec ns-020-04 ifconfig vlo04b 10.2.4.100/24 up
# Node node-020-05
sudo ip netns exec ns-020-05 ifconfig vlo05b 10.2.5.100/24 up
# Node node-020-06
sudo ip netns exec ns-020-06 ifconfig vlo06b 10.2.6.100/24 up
# Node node-020-07
sudo ip netns exec ns-020-07 ifconfig vlo07b 10.2.7.100/24 up
# Node node-020-01
sudo iptables -A FORWARD -i ethTPECCA j- DETALER,DEHSILBATSE,WEN etats-- e
sudo iptables -t nat -A PREROUTING -p tcp -d ot-- TAND j- DETALER,DEHSILBA
10.2.4.100:20040
sudo iptables -A FORWARD -i ethTPECCA j- DETALER,DEHSILBATSE,WEN etats-- e
sudo iptables -t nat -A PREROUTING -p tcp -d ot-- TAND j- DETALER,DEHSILBA
10.2.4.100:20041
# Node node-020-05
sudo iptables -A FORWARD -i ethTPECCA j- DETALER,DEHSILBATSE,WEN etats-- e
sudo iptables -t nat -A PREROUTING -p tcp -d ot-- TAND j- DETALER,DEHSILBA
10.2.5.100:20050
sudo iptables -A FORWARD -i ethTPECCA j- DETALER,DEHSILBATSE,WEN etats-- e
sudo iptables -t nat -A PREROUTING -p tcp -d ot-- TAND j- DETALER,DEHSILBA
10.2.5.100:20051
# Node node-020-06
sudo iptables -A FORWARD -i ethTPECCA j- DETALER,DEHSILBATSE,WEN etats-- e
sudo iptables -t nat -A PREROUTING -p tcp -d ot-- TAND j- DETALER,DEHSILBA
10.2.6.100:20060
```

**Infrastructure: ~150 machines x 8 cores
1Gb network**

Client: 0.10.0

Network: emulated

P2P topology: manual

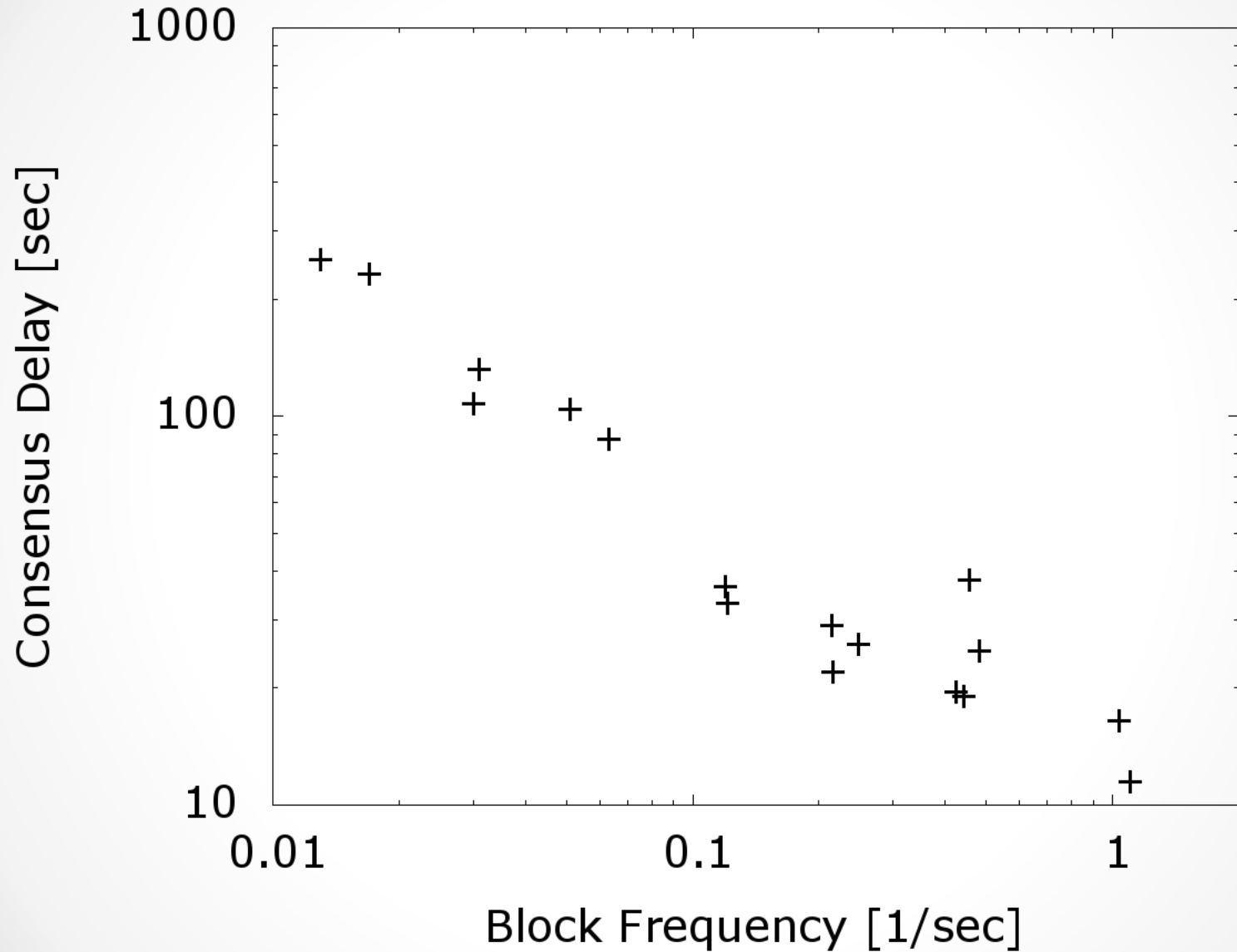
Blockchain content and mempool bootstrap

Consensus Delay

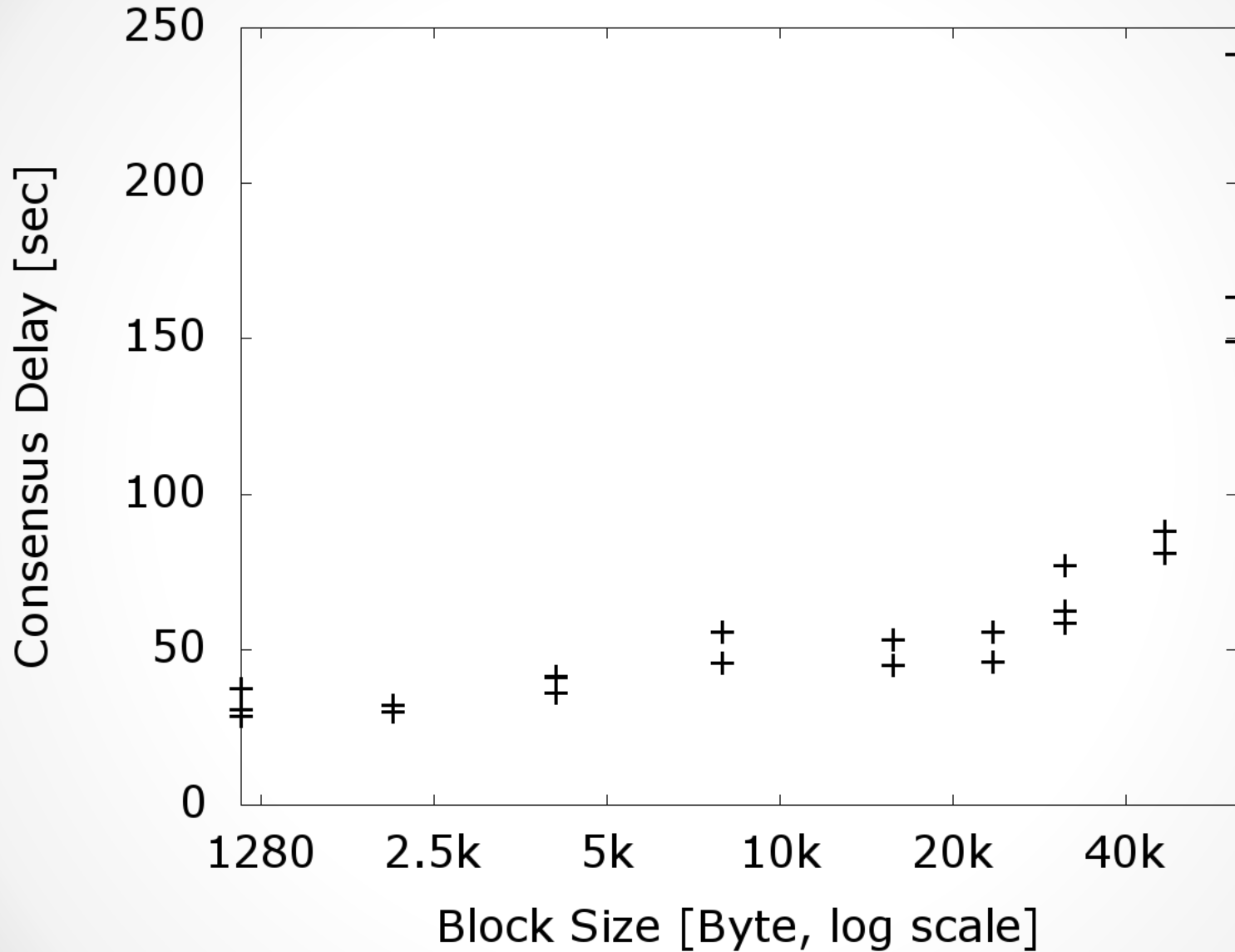
By example:

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.

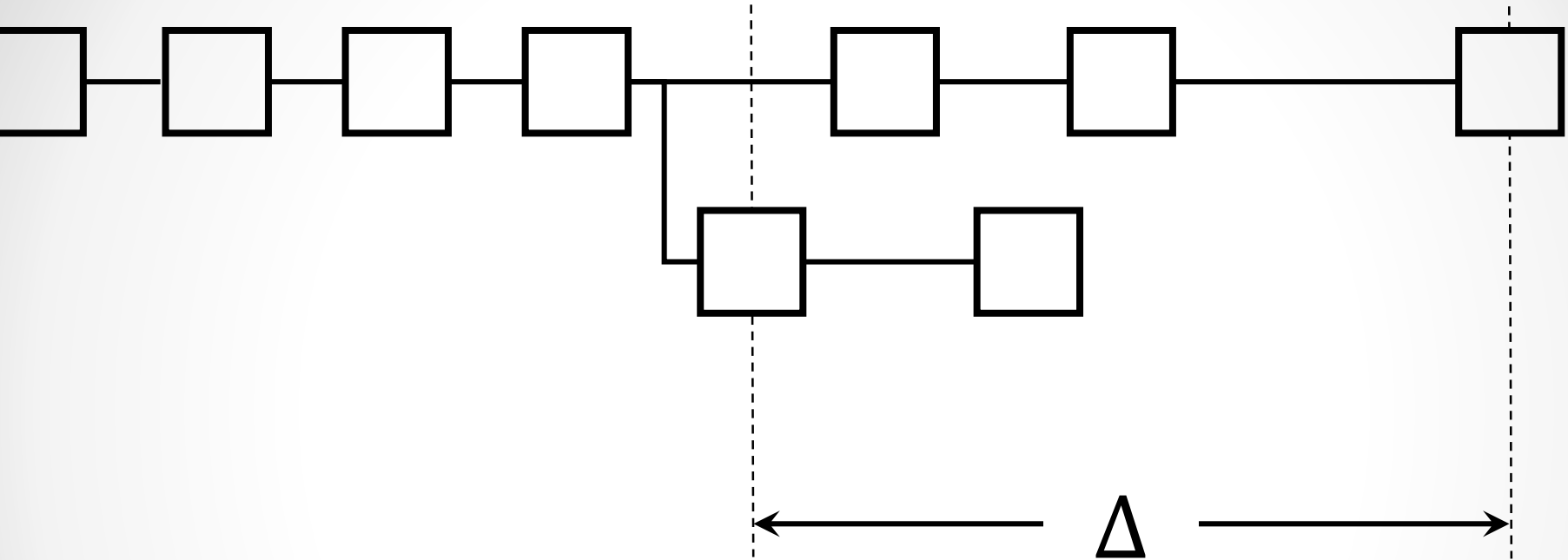
Consensus Delay



Consensus Delay

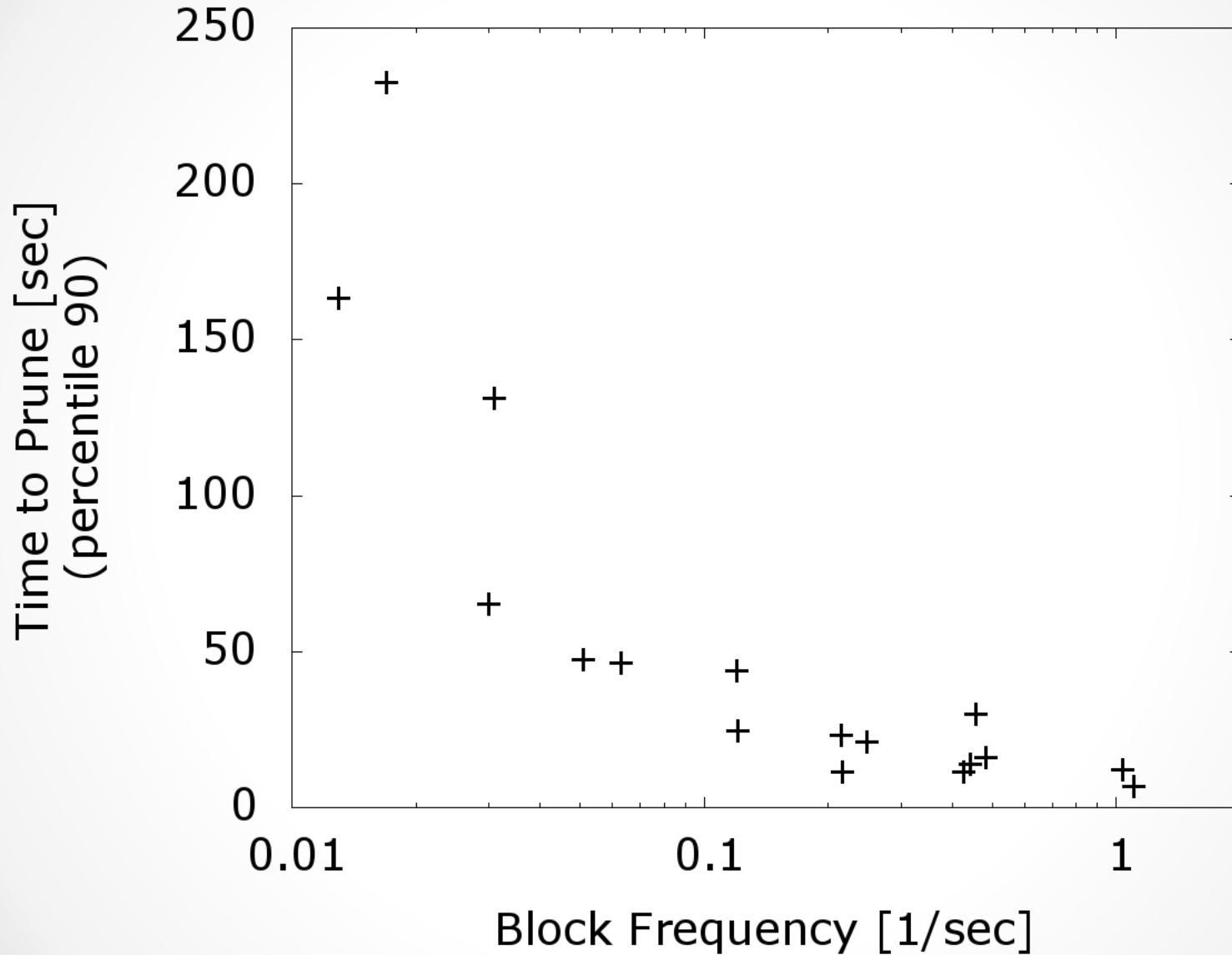


Subjective Time to Prune

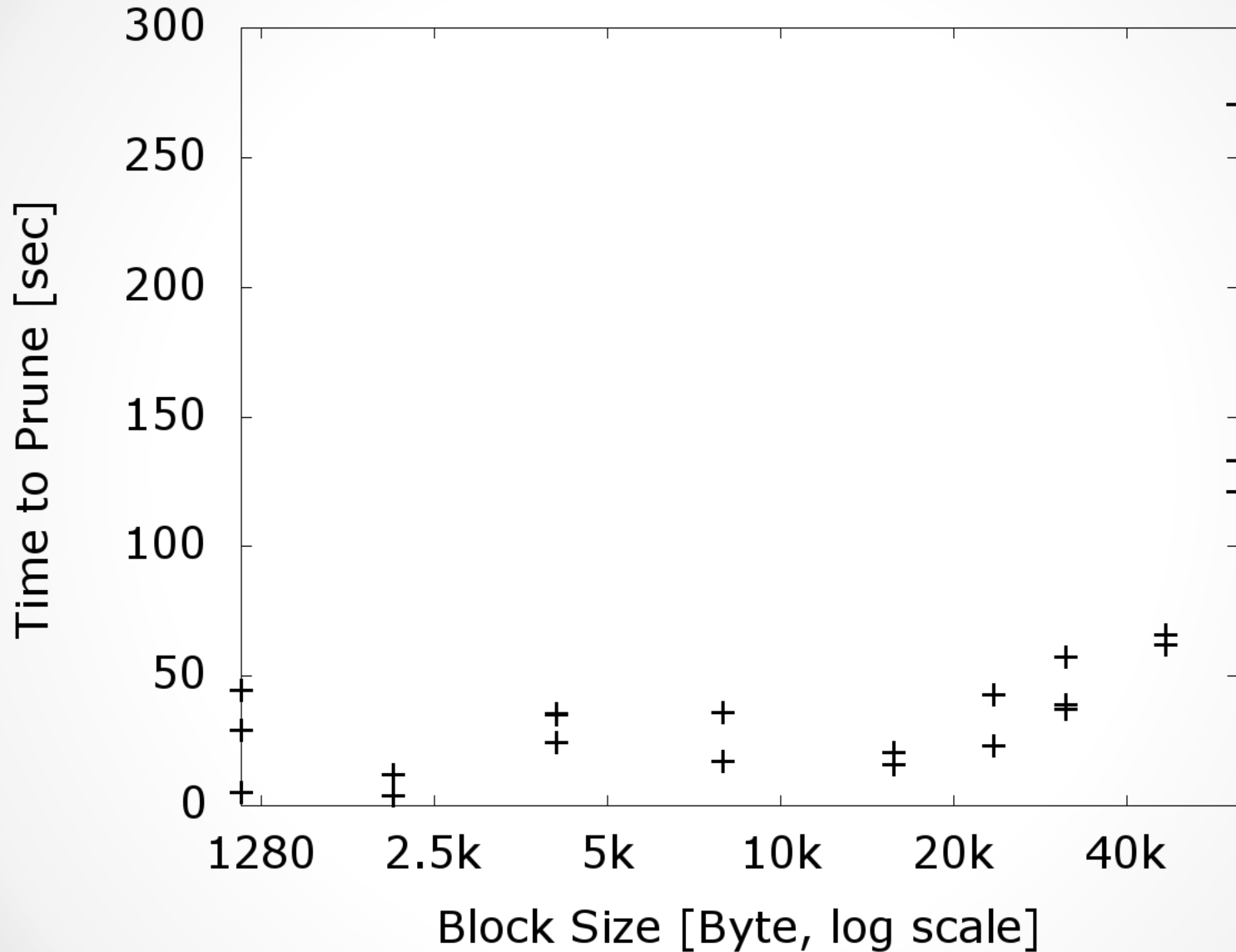


Time to prune: Until branch is pruned

Subjective Time to Prune



Subjective Time to Prune

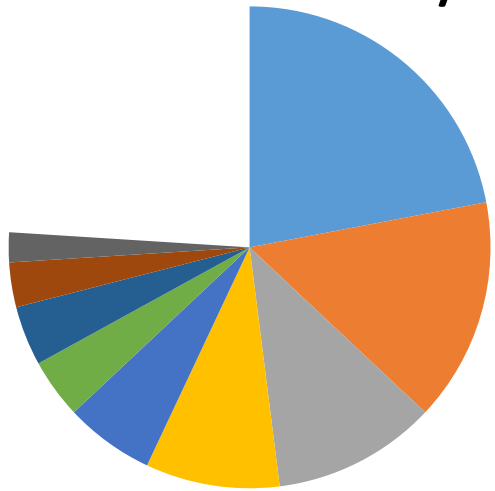


Fairness

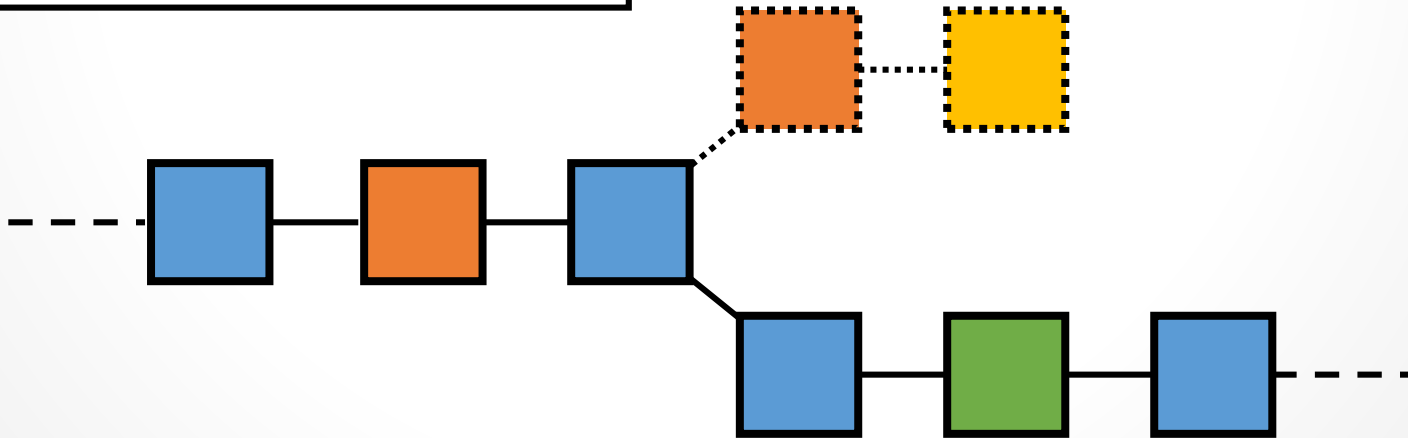
<https://blockchain.info/pools>

Pool sizes

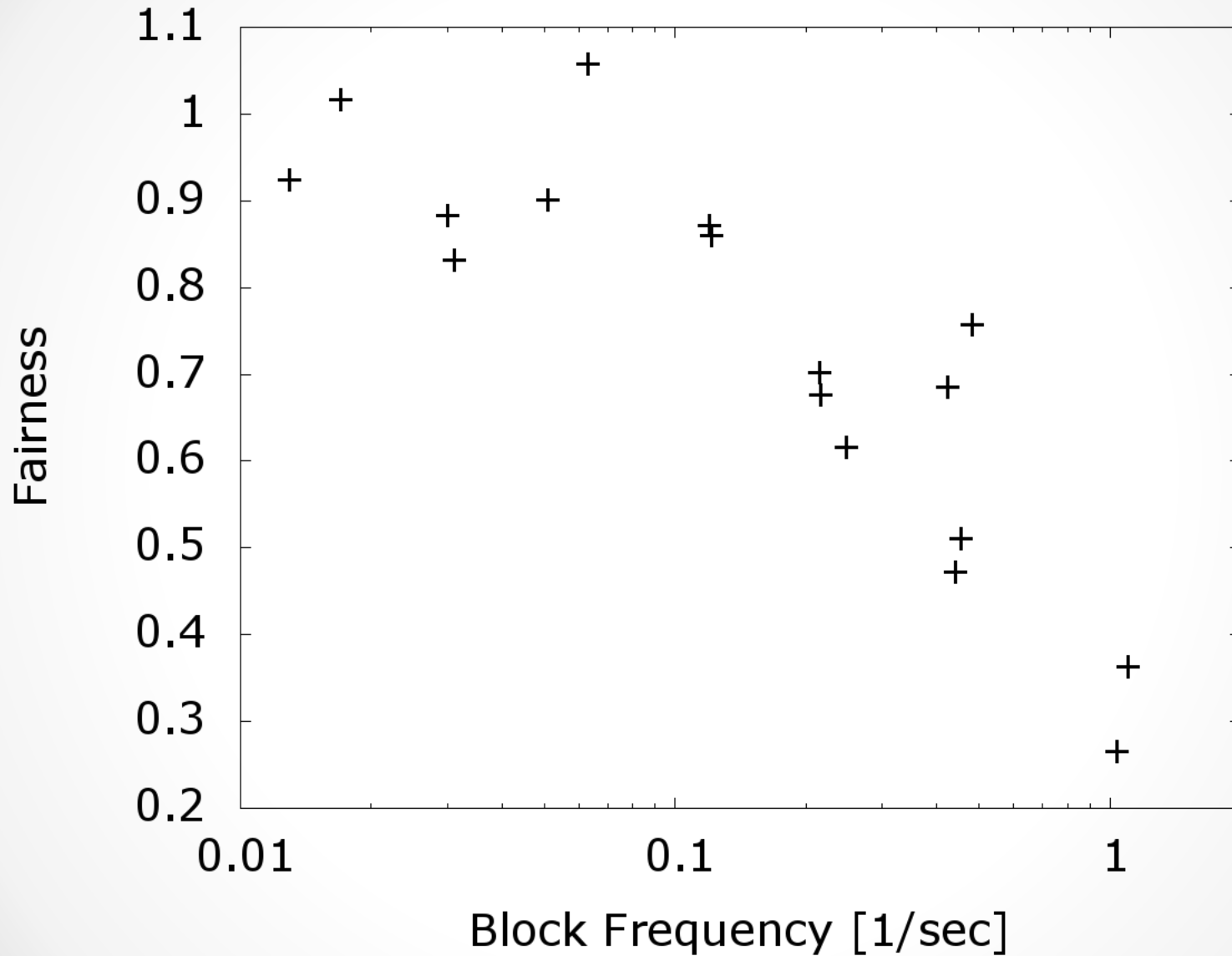
4/2015



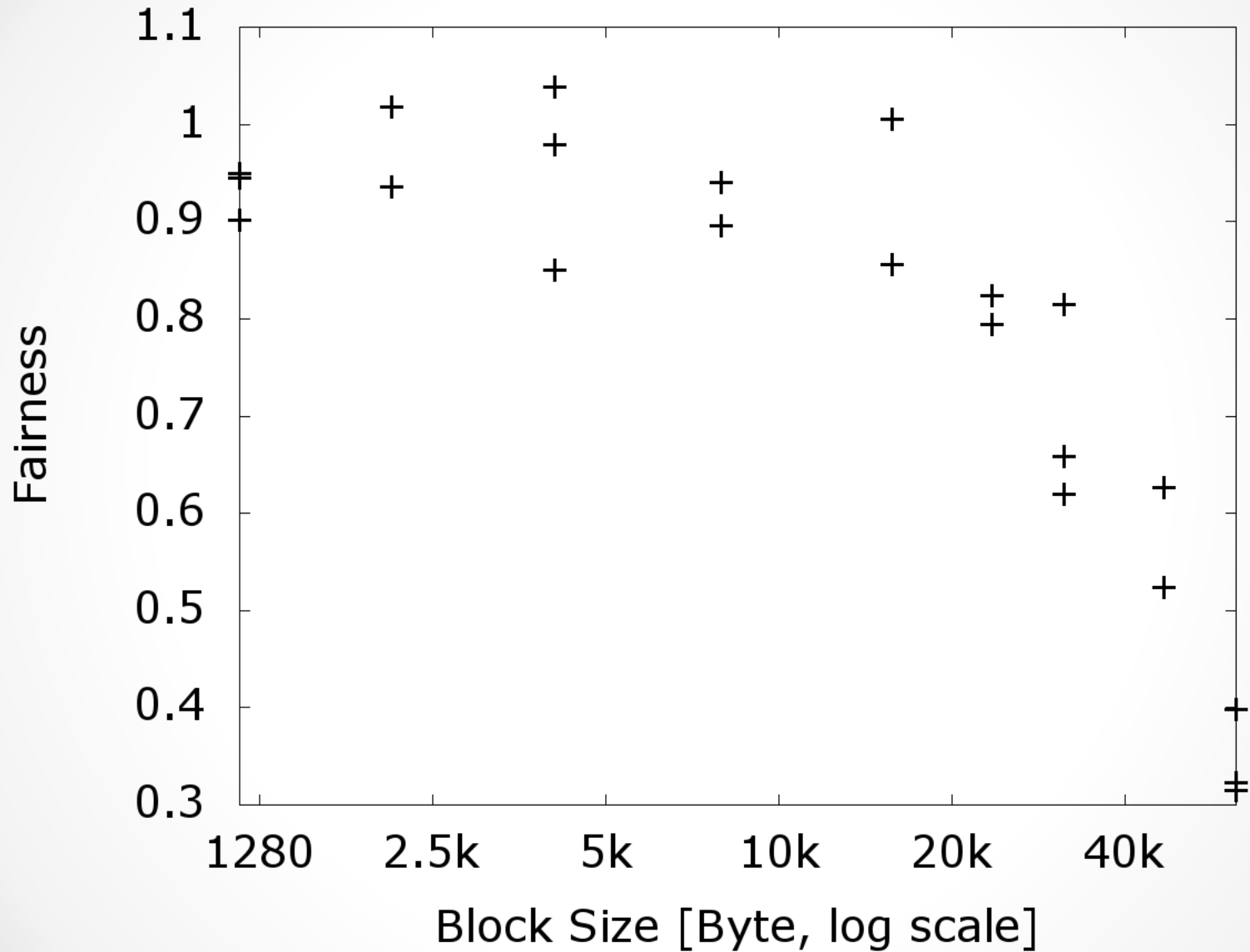
Fairness: Ratio of chain blocks **not** from largest pool (normalized)



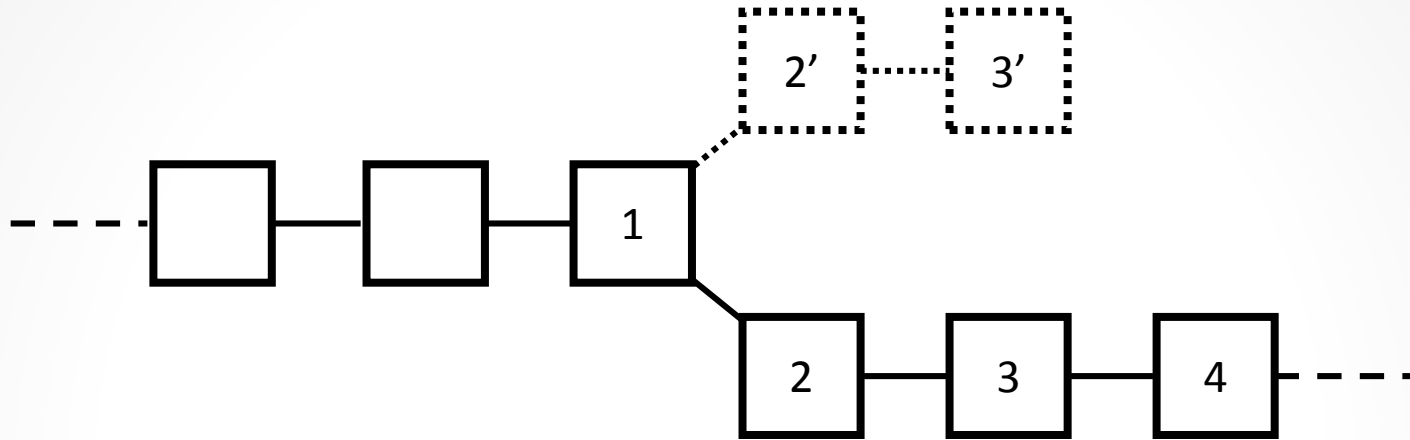
Fairness



Fairness

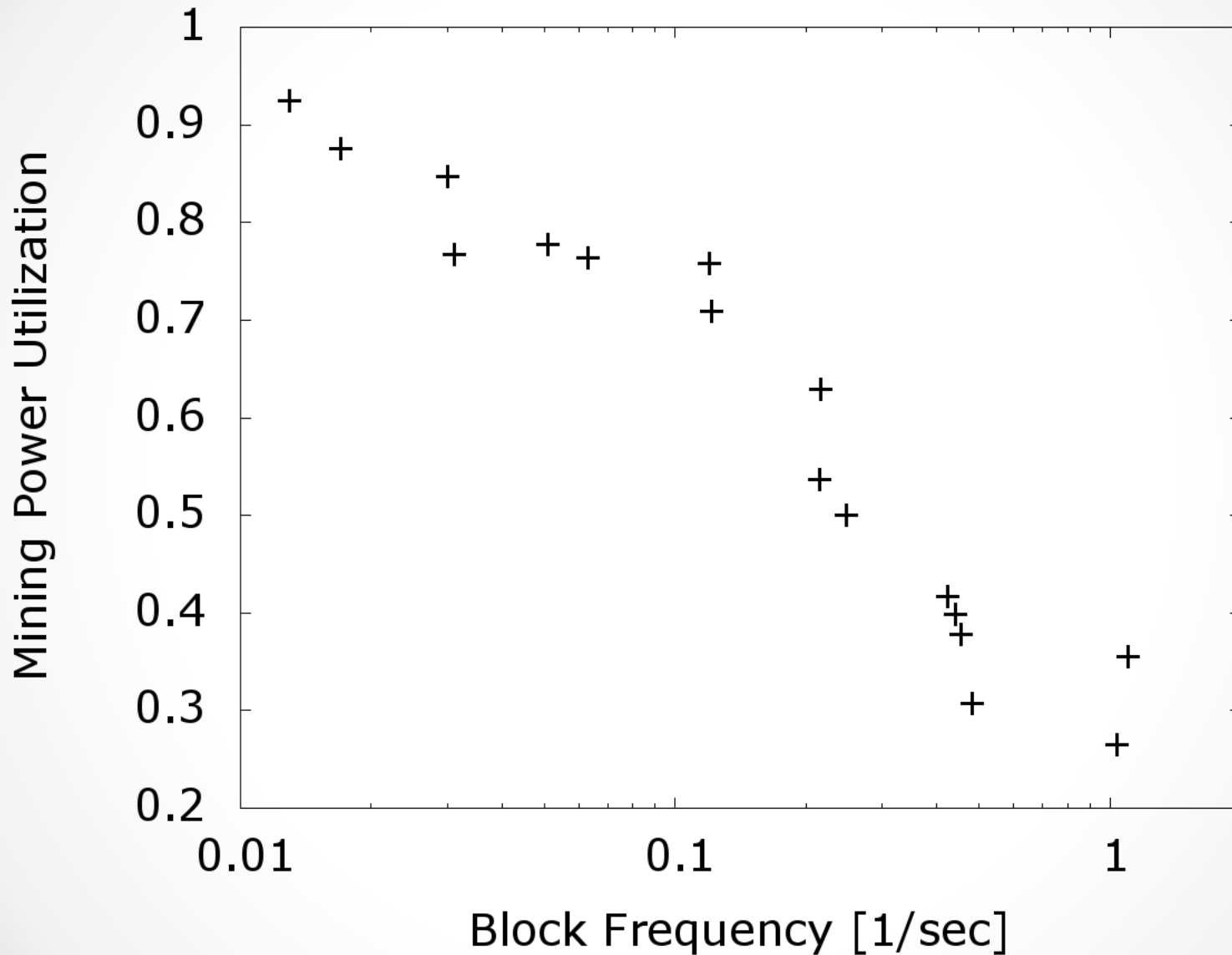


Mining Power Utilization

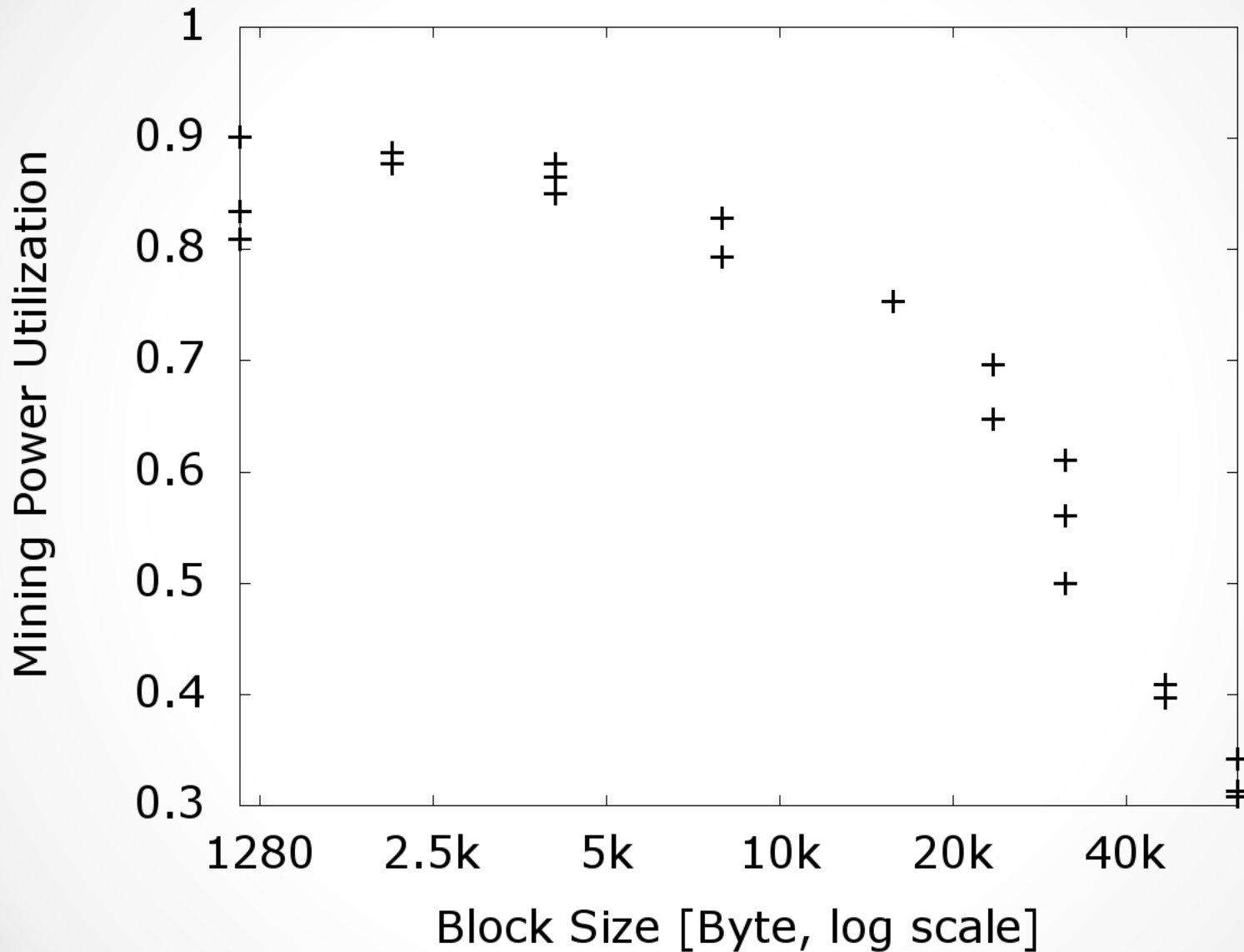


Mining power utilization: Ratio of generated blocks in the main chain

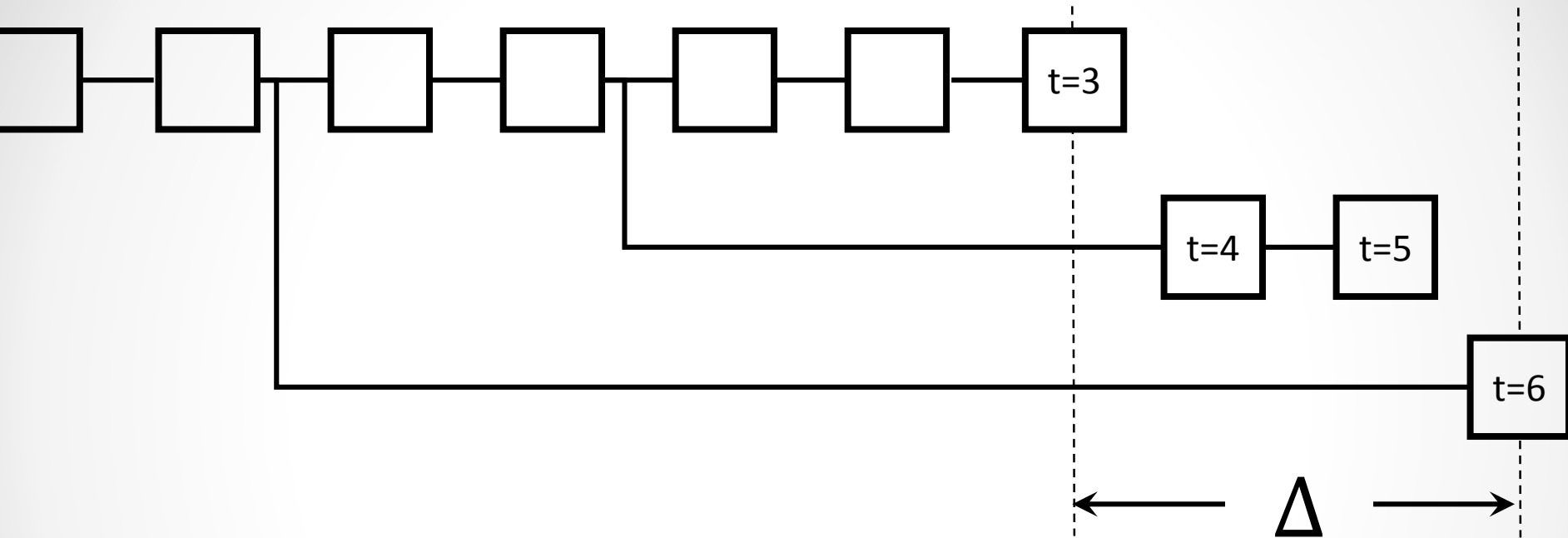
Mining Power Utilization



Mining Power Utilization

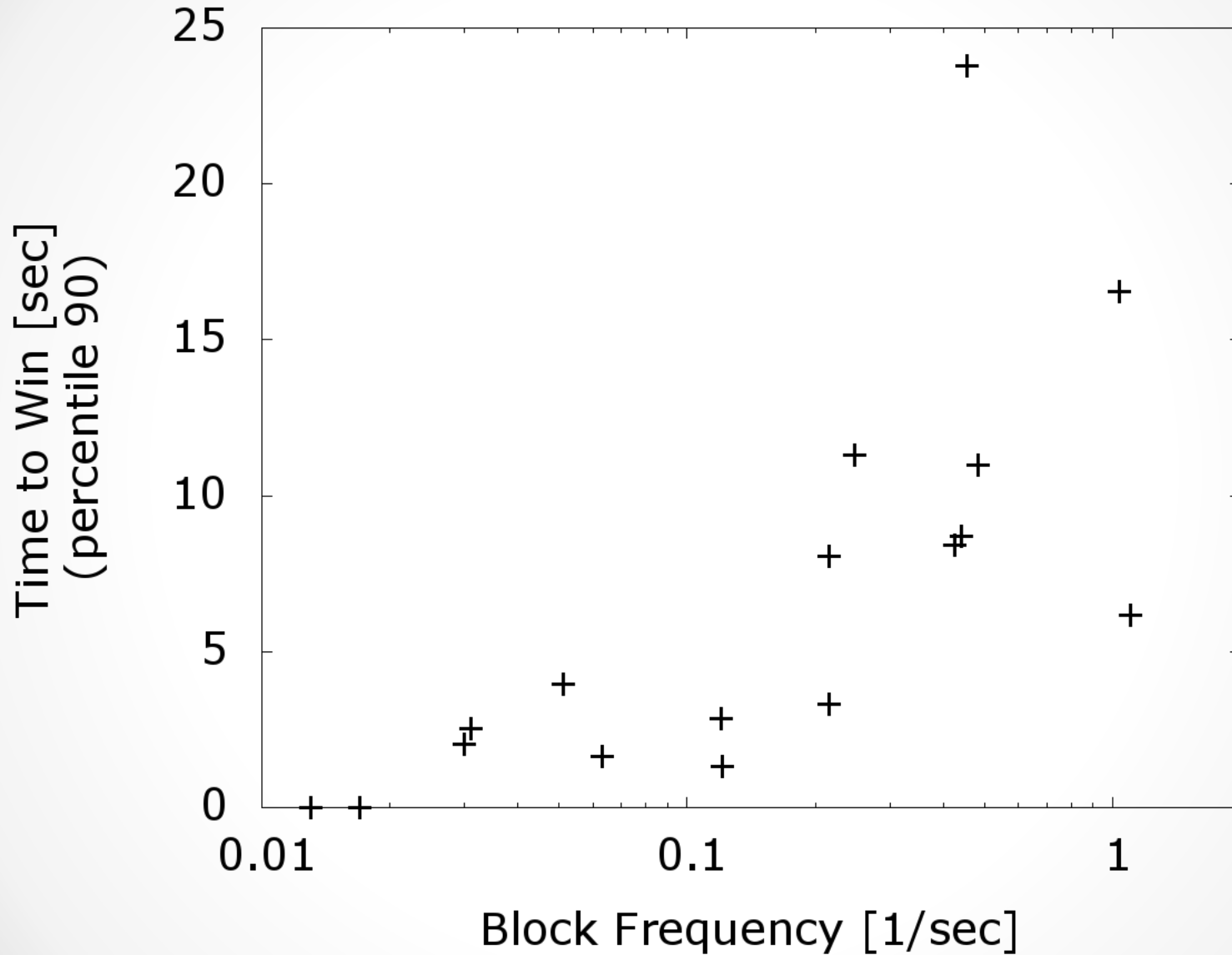


Time to Win

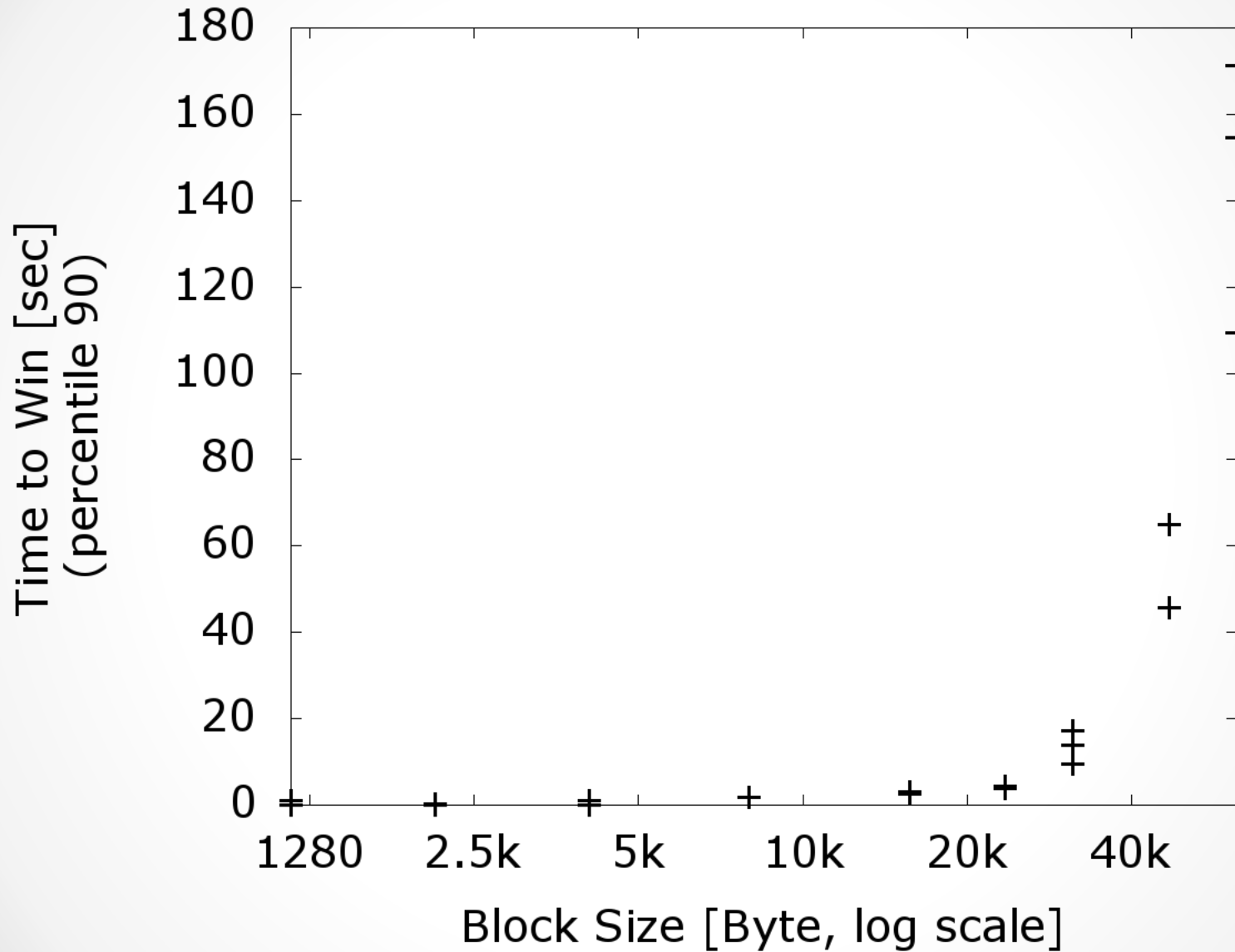


Time to win: Until latest block on any competing branch

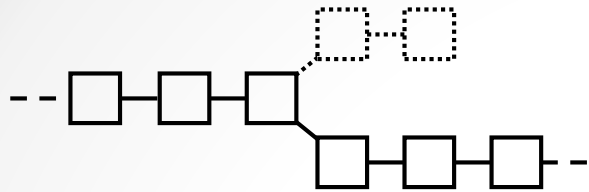
Time to Win



Time to Win



Summary



Scaling the Blockchain

Metrics

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

The Blockchain test bed



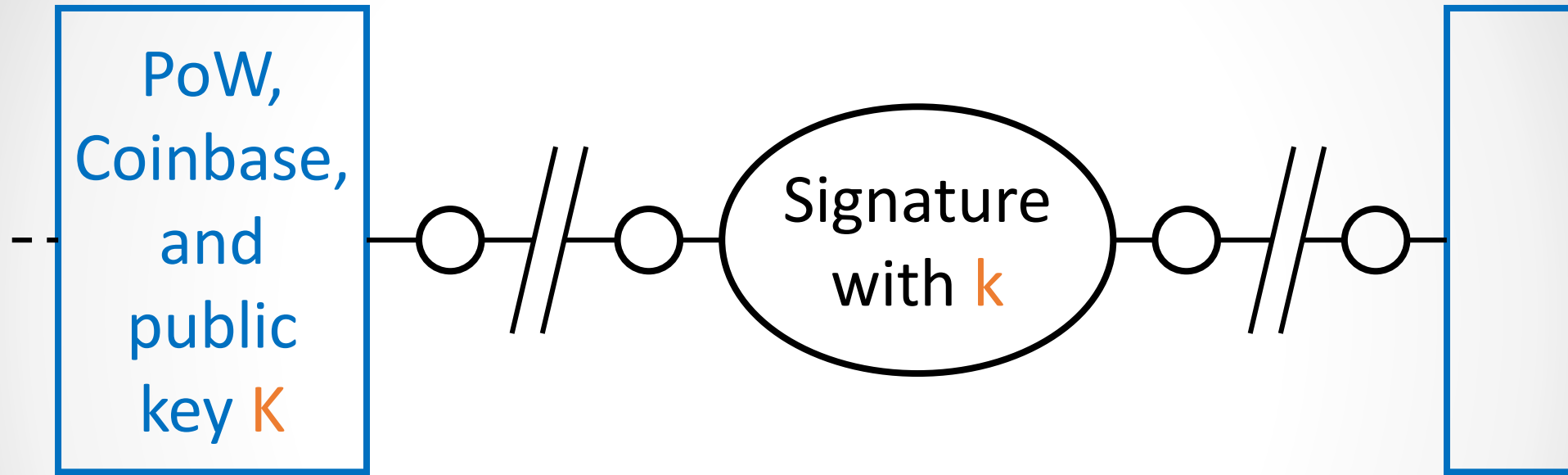
Bitcoin NG

Bitcoin-NG



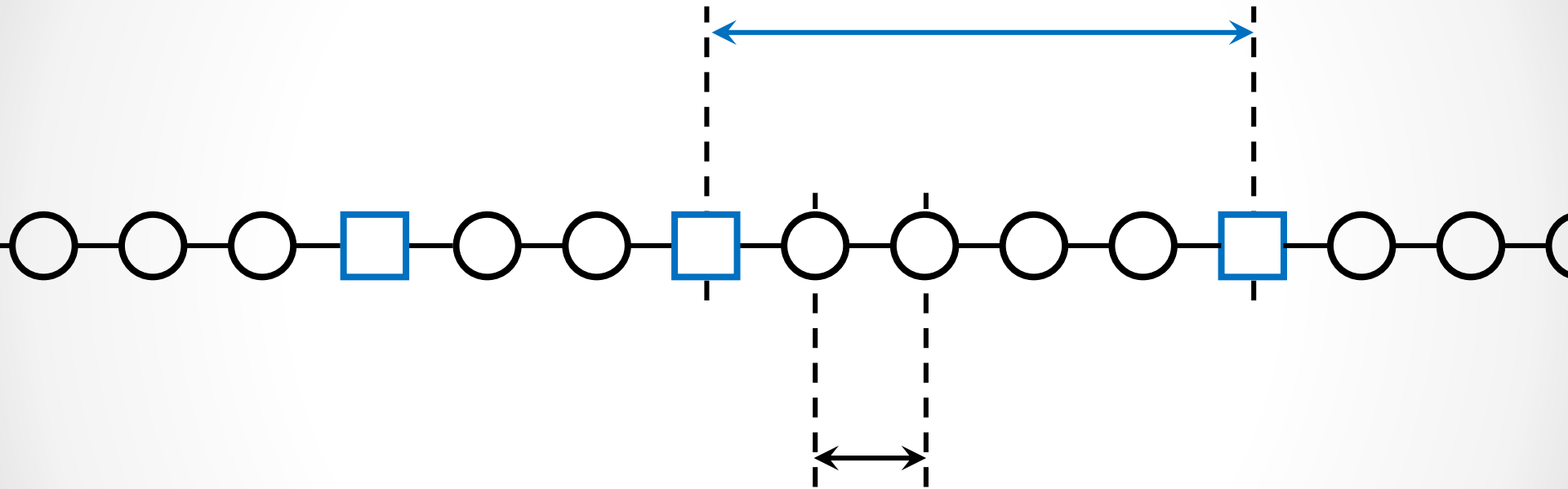
- Key blocks:
 - No content
 - Leader election
- Microblocks:
 - Only content
 - No contention

Bitcoin-NG



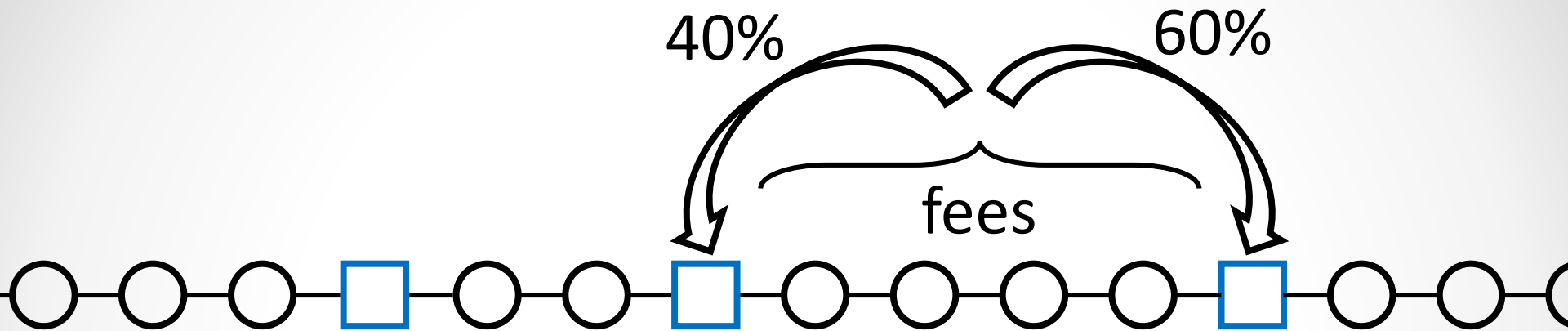
Bitcoin-NG

long exponential
intervals (10 min)



short deterministic
intervals (10 sec)

Transaction Fees

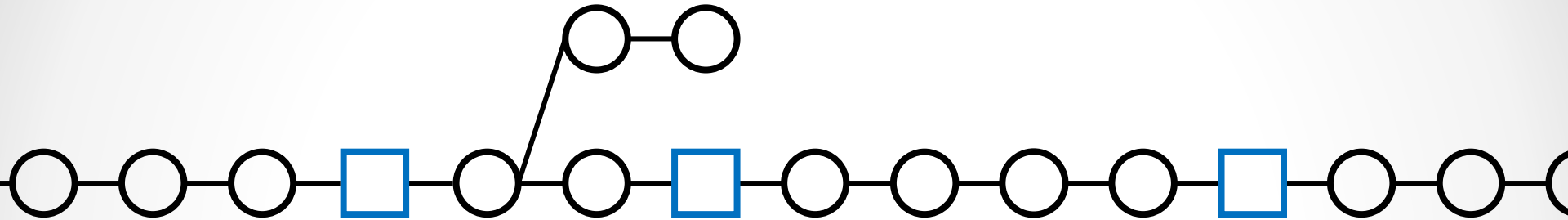


Incentives

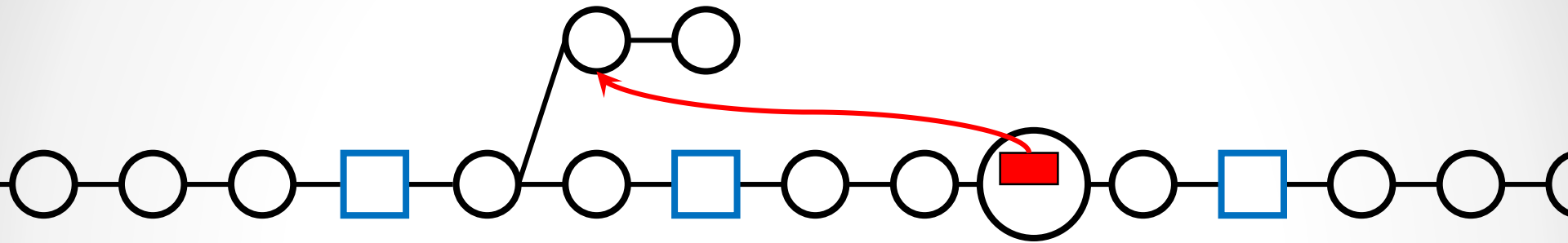
Next miner: Include previous micro-blocks

Leader: Place transactions in micro blocks;
Smaller chance to win after a microblock

Double Spending

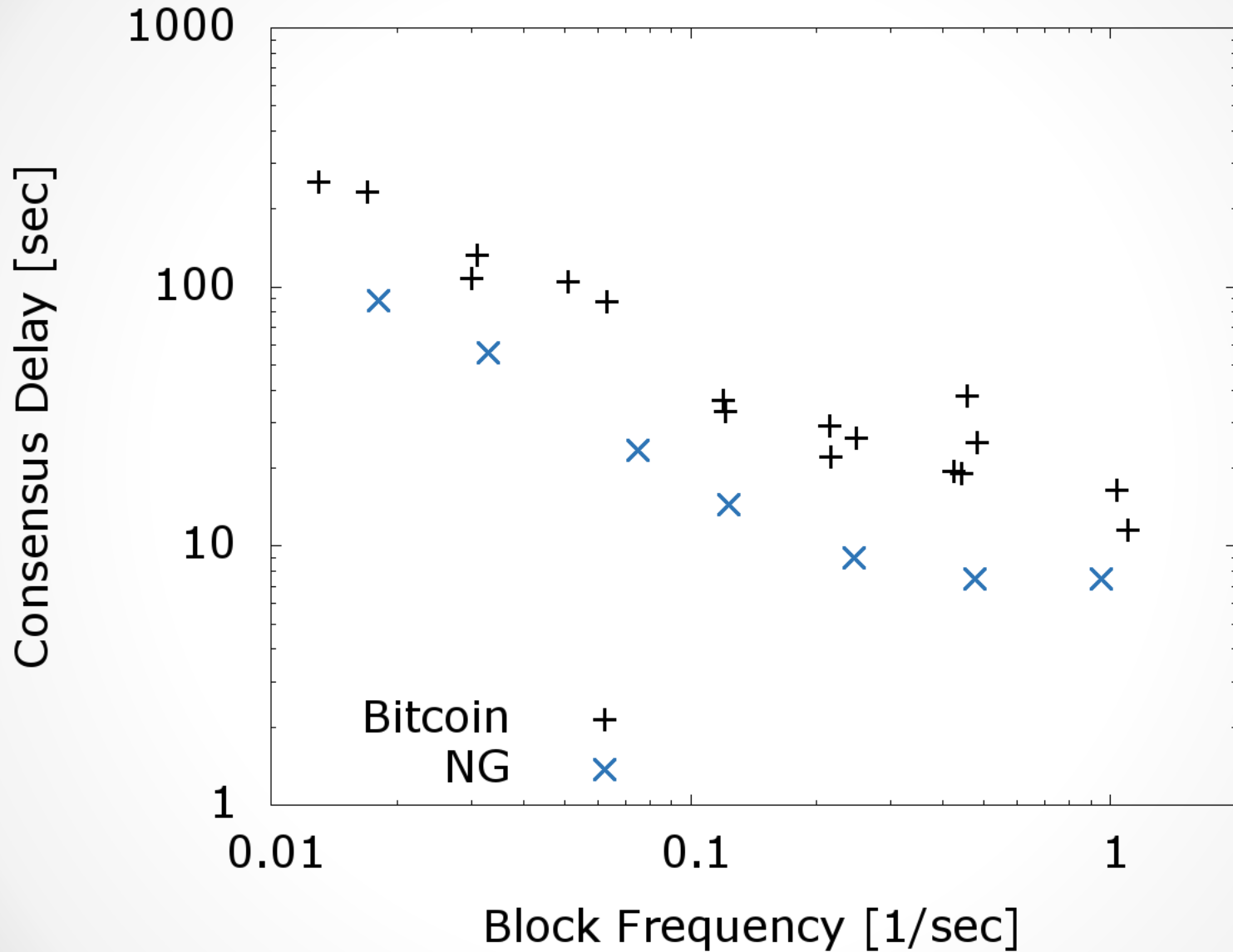


Double Spending

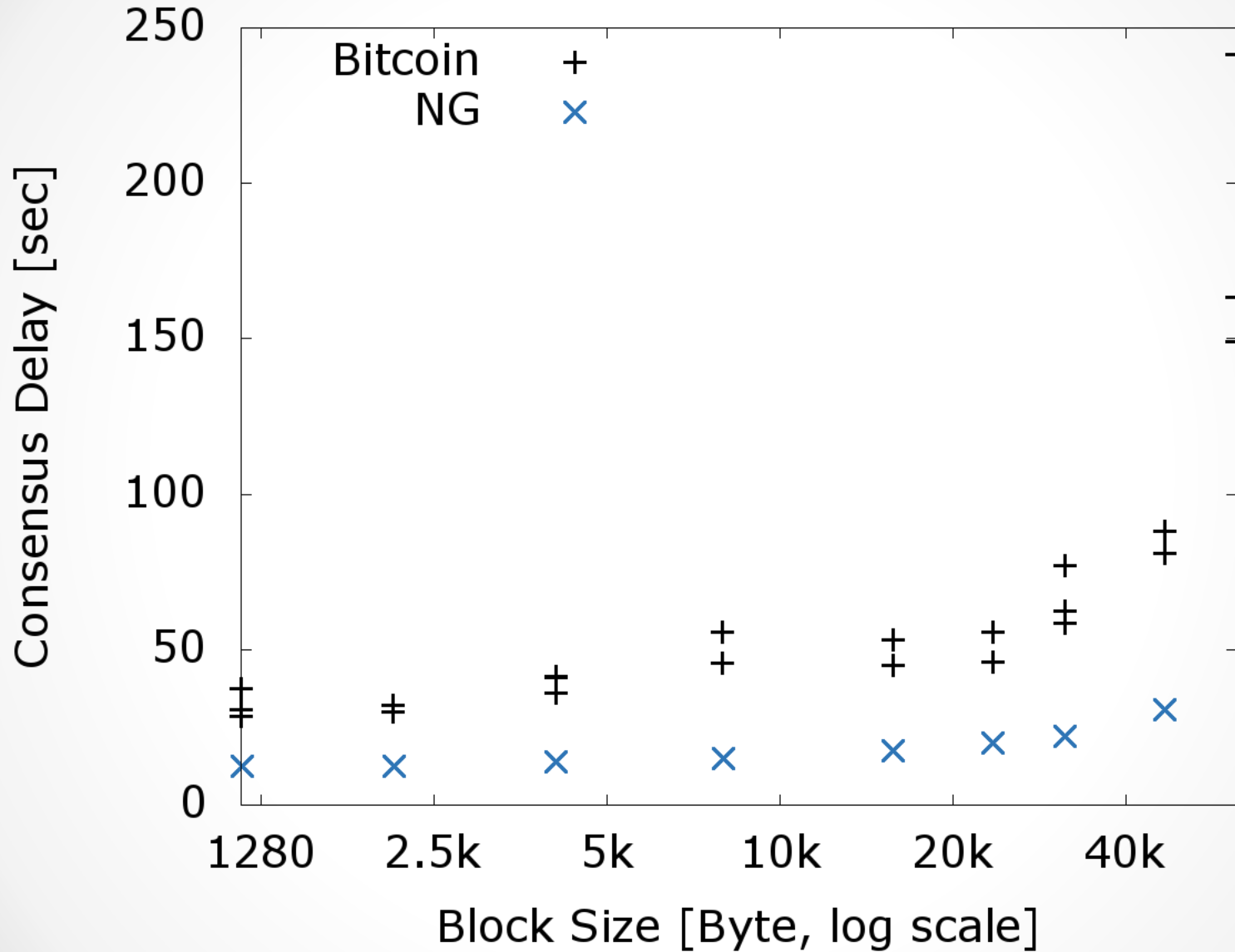


Poison transaction cancels cheater reward
Poisoner receives nominal prize

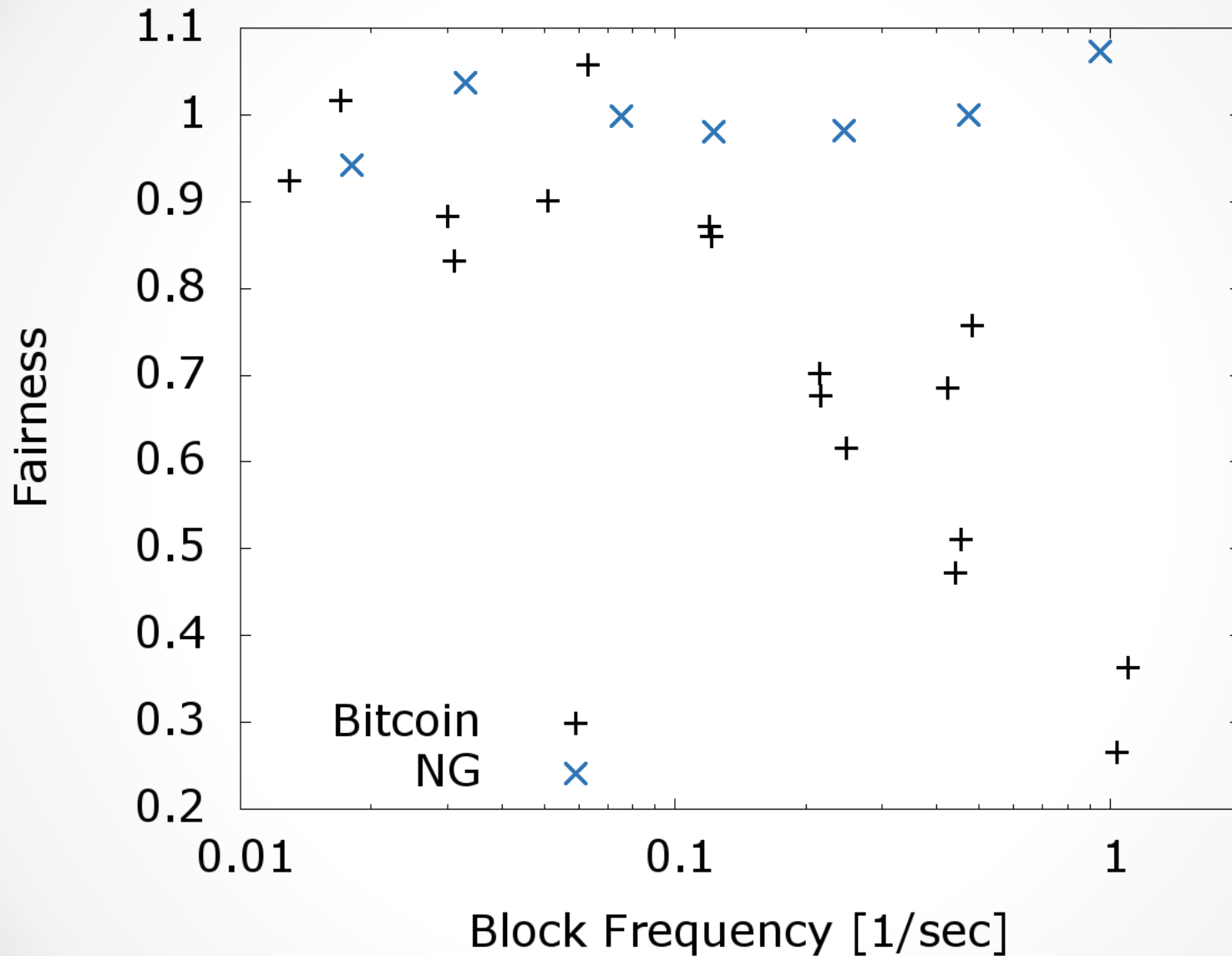
Consensus Delay



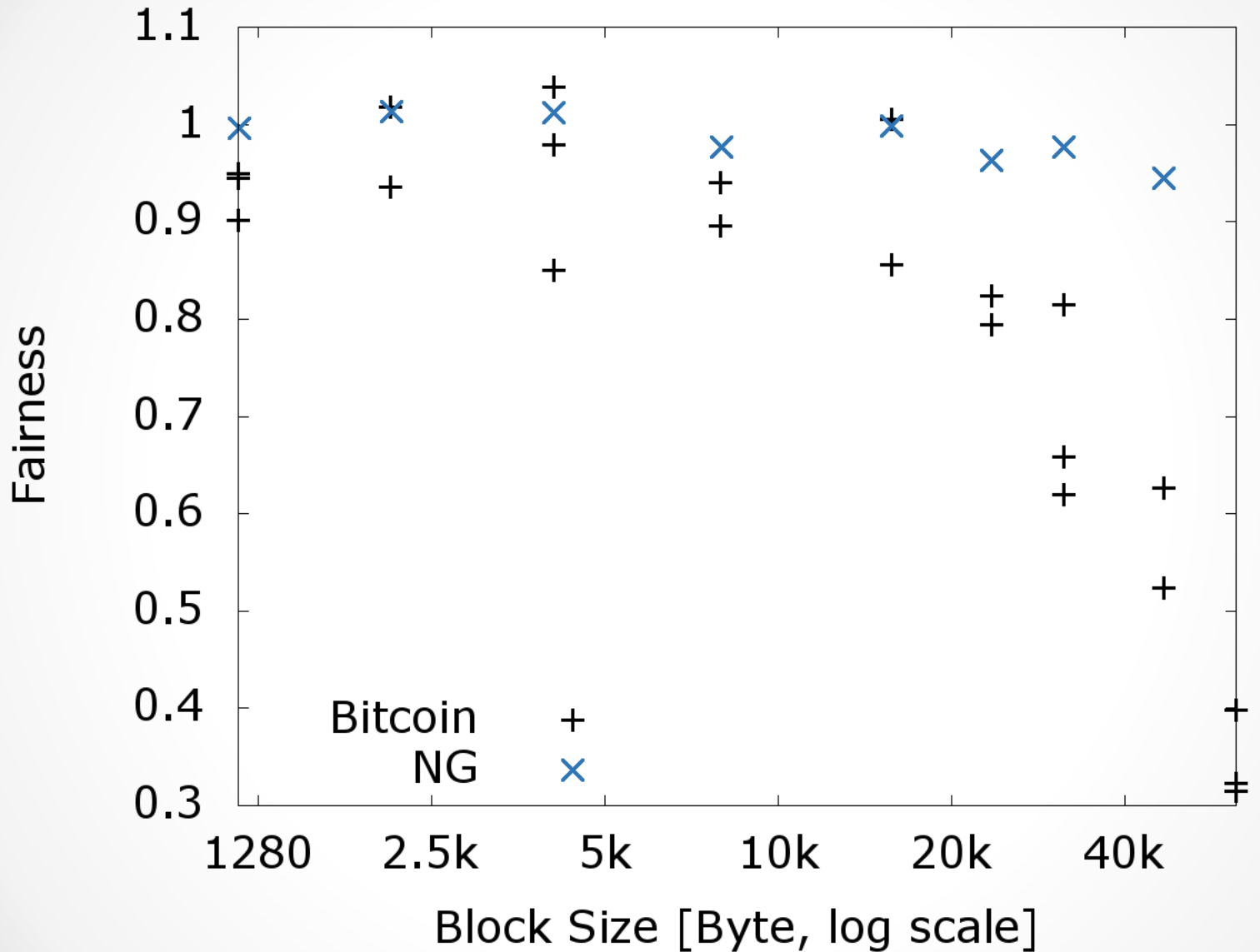
Consensus Delay



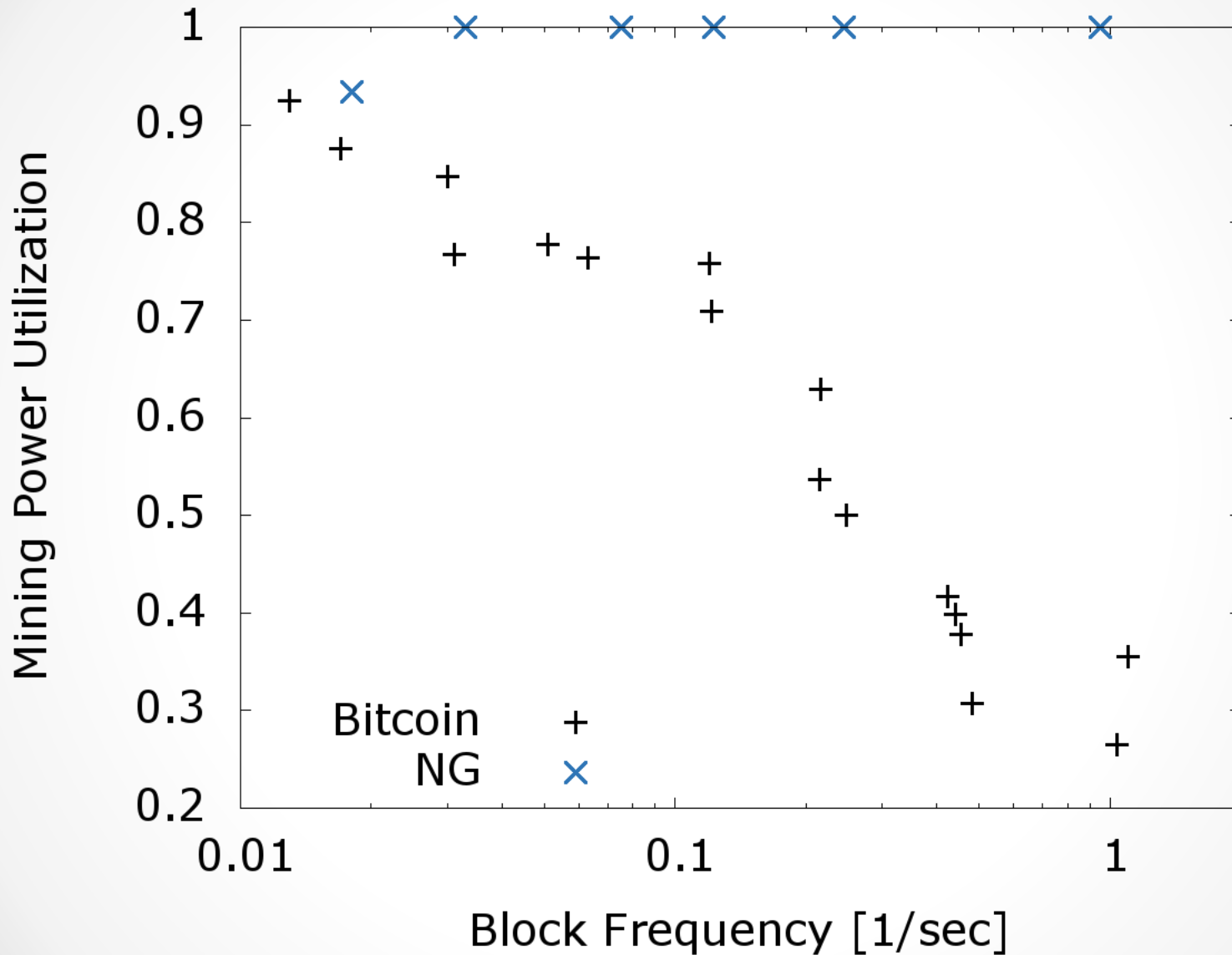
Fairness



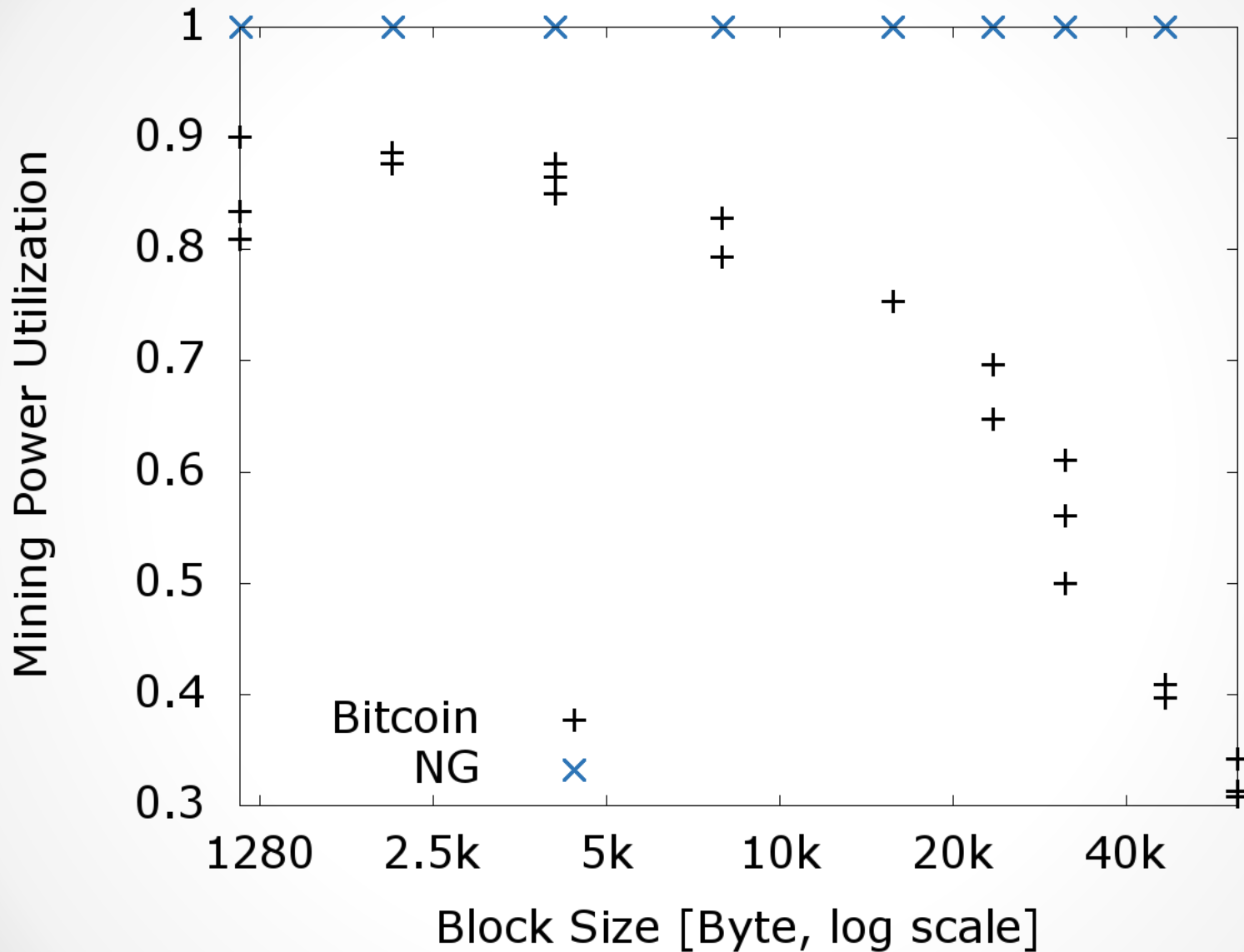
Fairness



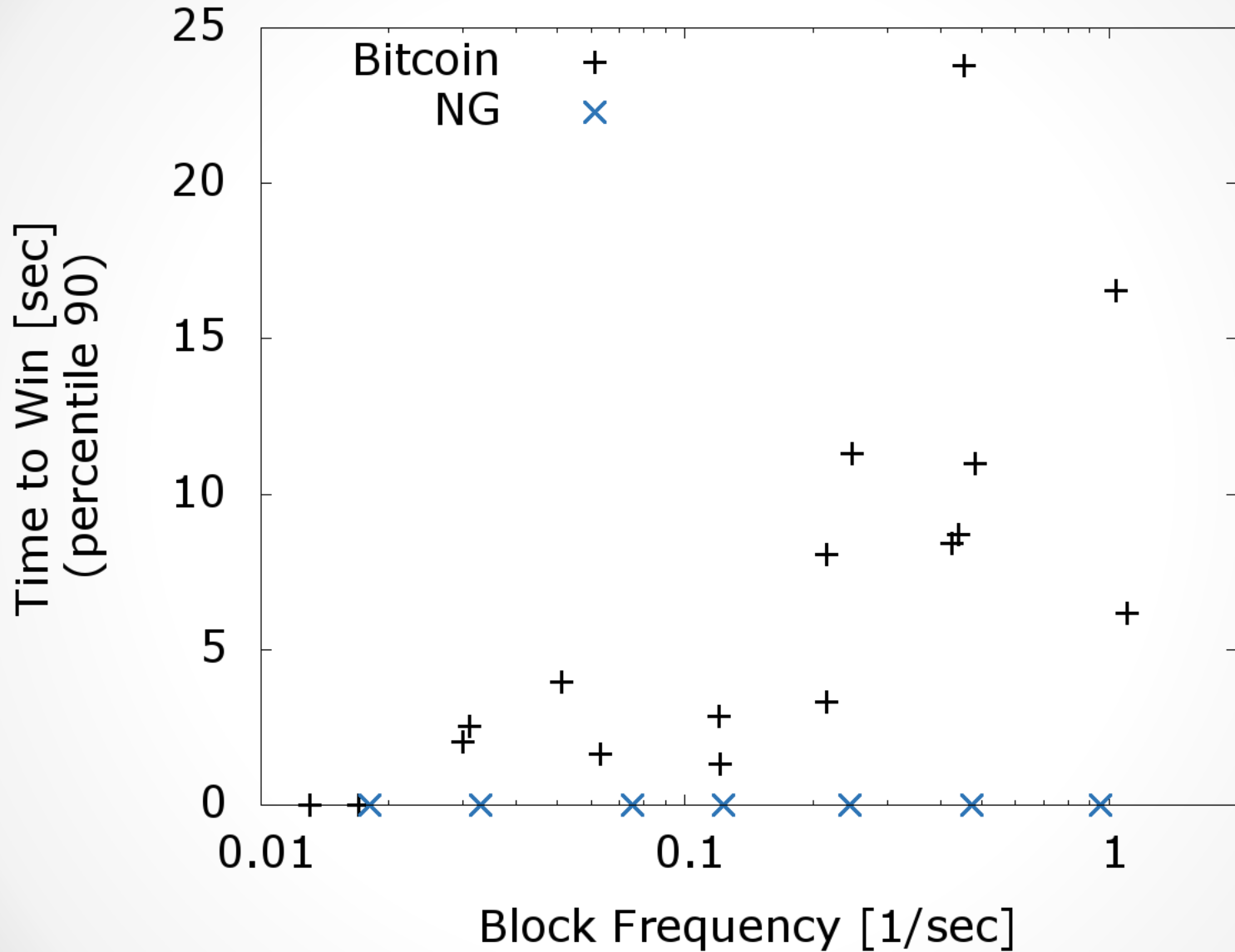
Mining Power Utilization



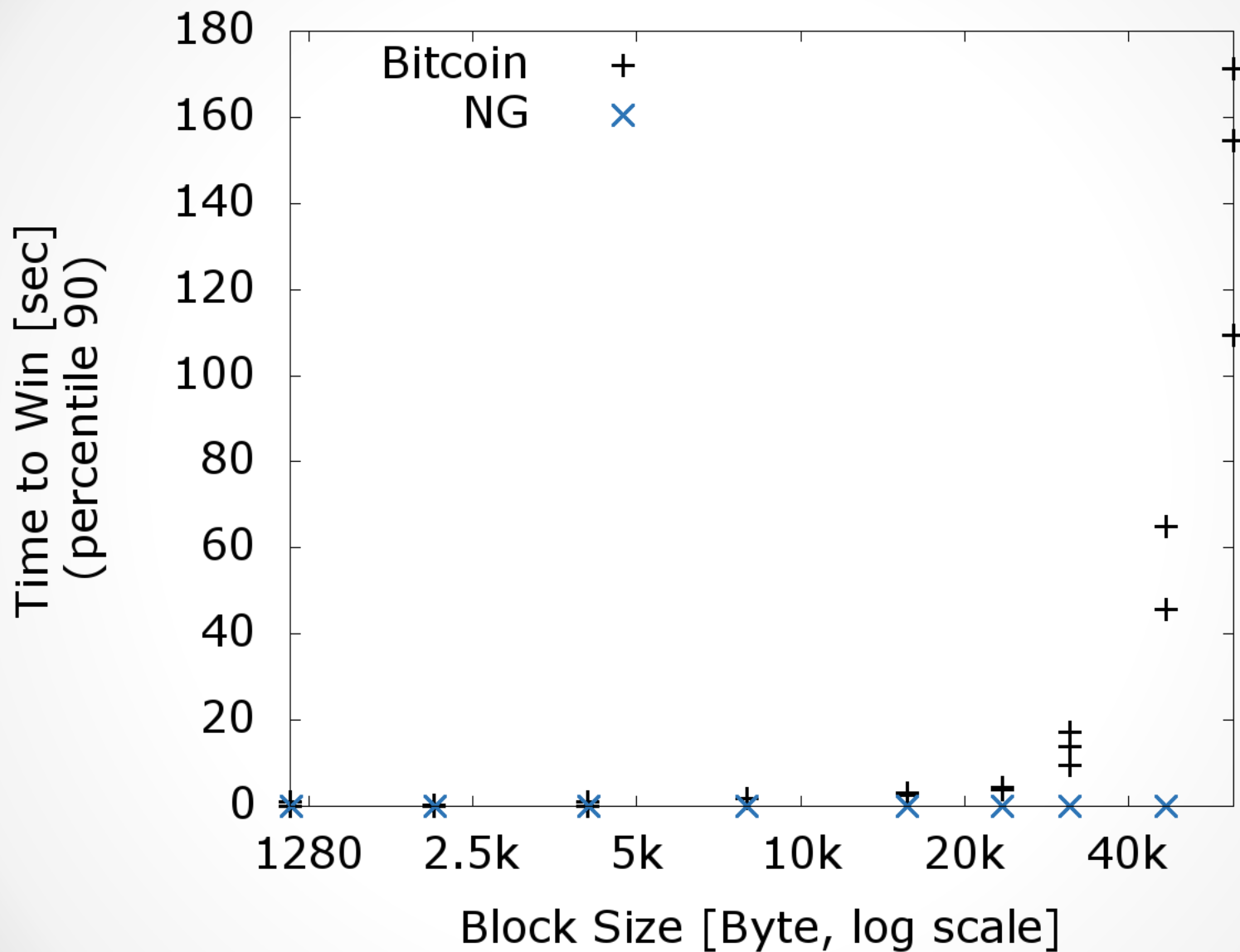
Mining Power Utilization



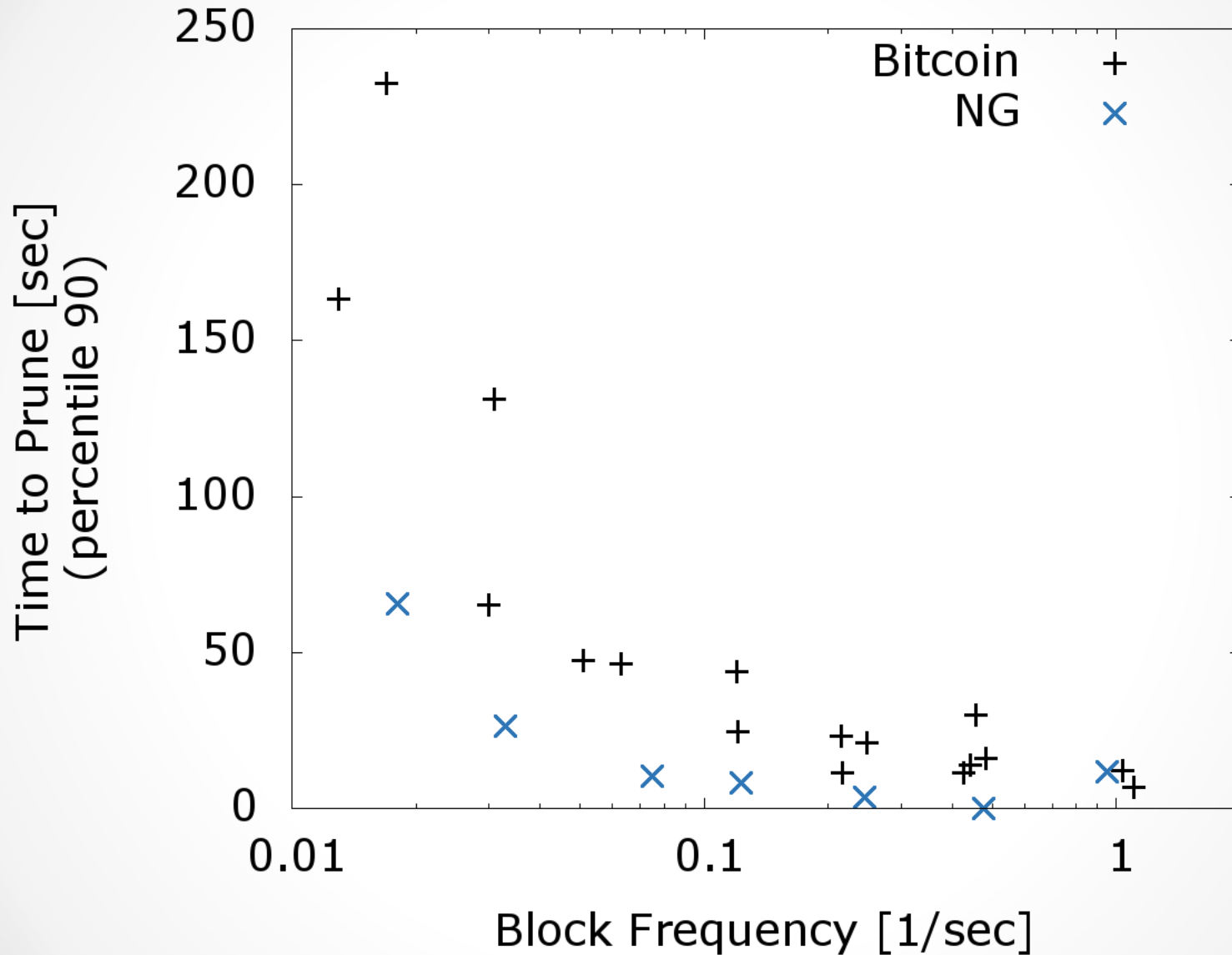
Time to Win



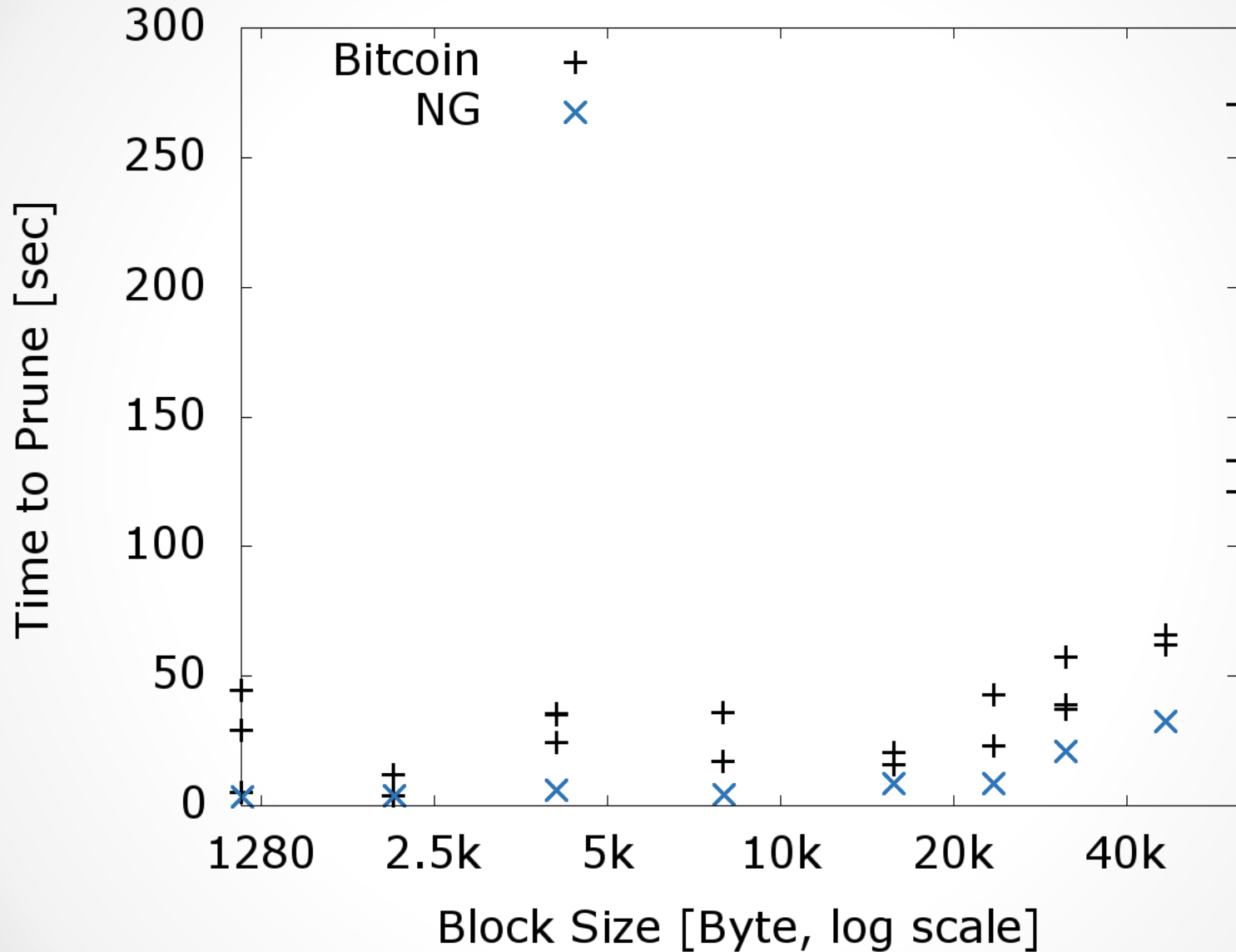
Time to Win



Subjective Time to Prune



Subjective Time to Prune



Conclusion

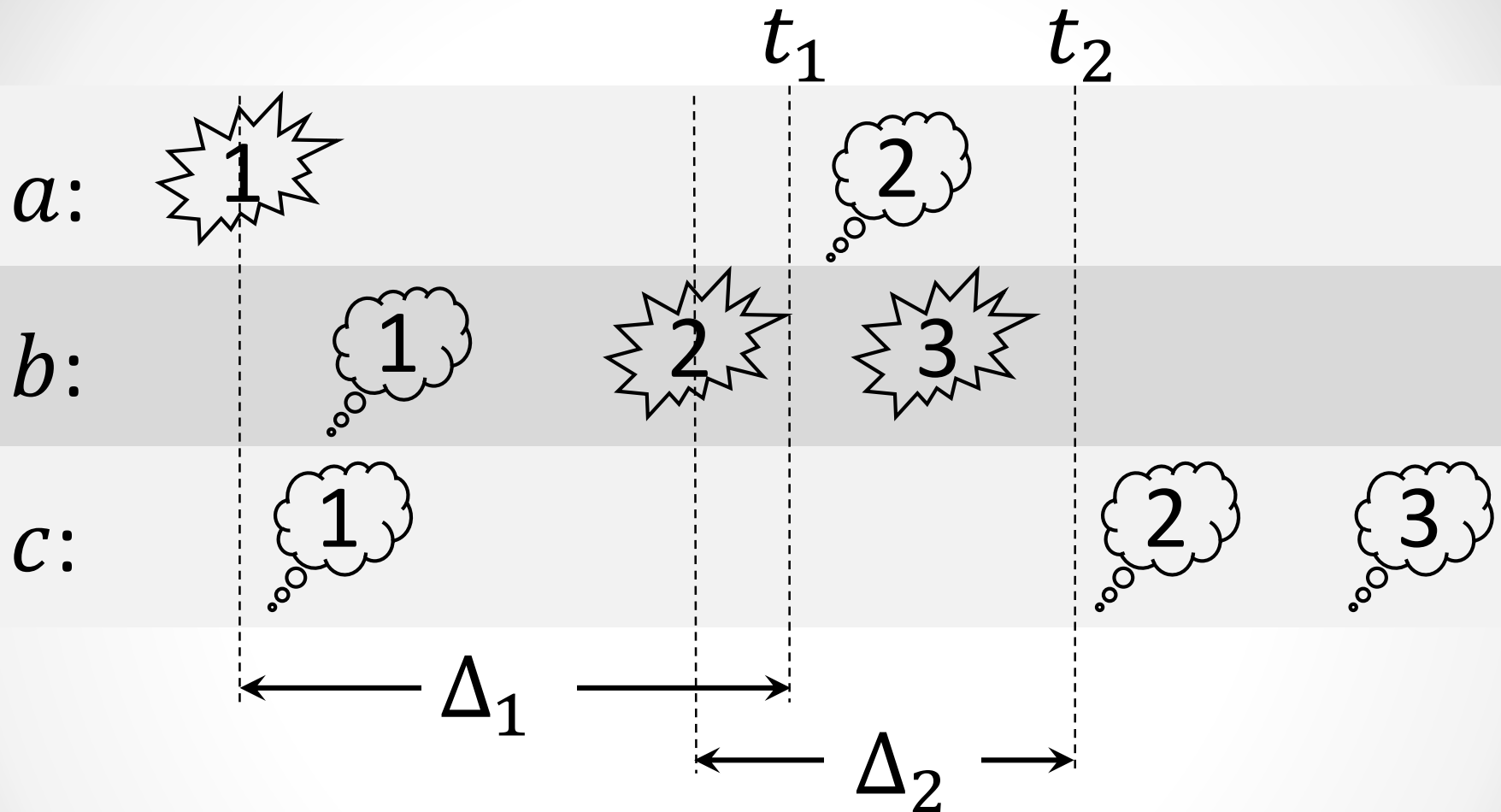
Test Bed

- Metrics
- P2P topology
- Properties to test

Bitcoin-NG

- Comments and concerns
- Adoption by Bitcoin

Consensus Latency



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