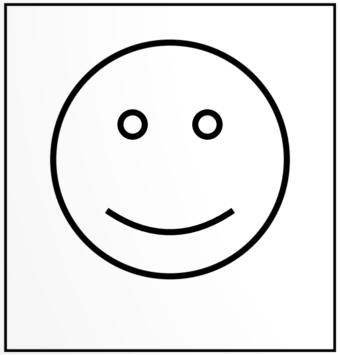
Bitcoin-NG

A Scalable Blockchain Protocol

Ittay Eyal



Adem Efe Gencer

Emin Gün Sirer

Robbert Van Renesse

Computer Science, Cornell University

Initiative for Cryptocurrencies and Contracts

NSDI, Santa Clara, CA, March 2016

Cryptocurrency

Exchanges

Security

Payment Services

Hardware

○ ○ ○

The Blockchain Promise

- Bank-to-bank settlements
- Cheap remittance
- Device-to-device payments (IoT)

citibank NASDAQ® intel®

S.W.I.F.T. UBS vmware® IBM

BARCLAYS HYPERLEDGER

The Blockchain Promise

Requires a bigger and faster boat

- Bank-to-bank settlements
- Cheap remittance
- Device-to-device payments (IoT)

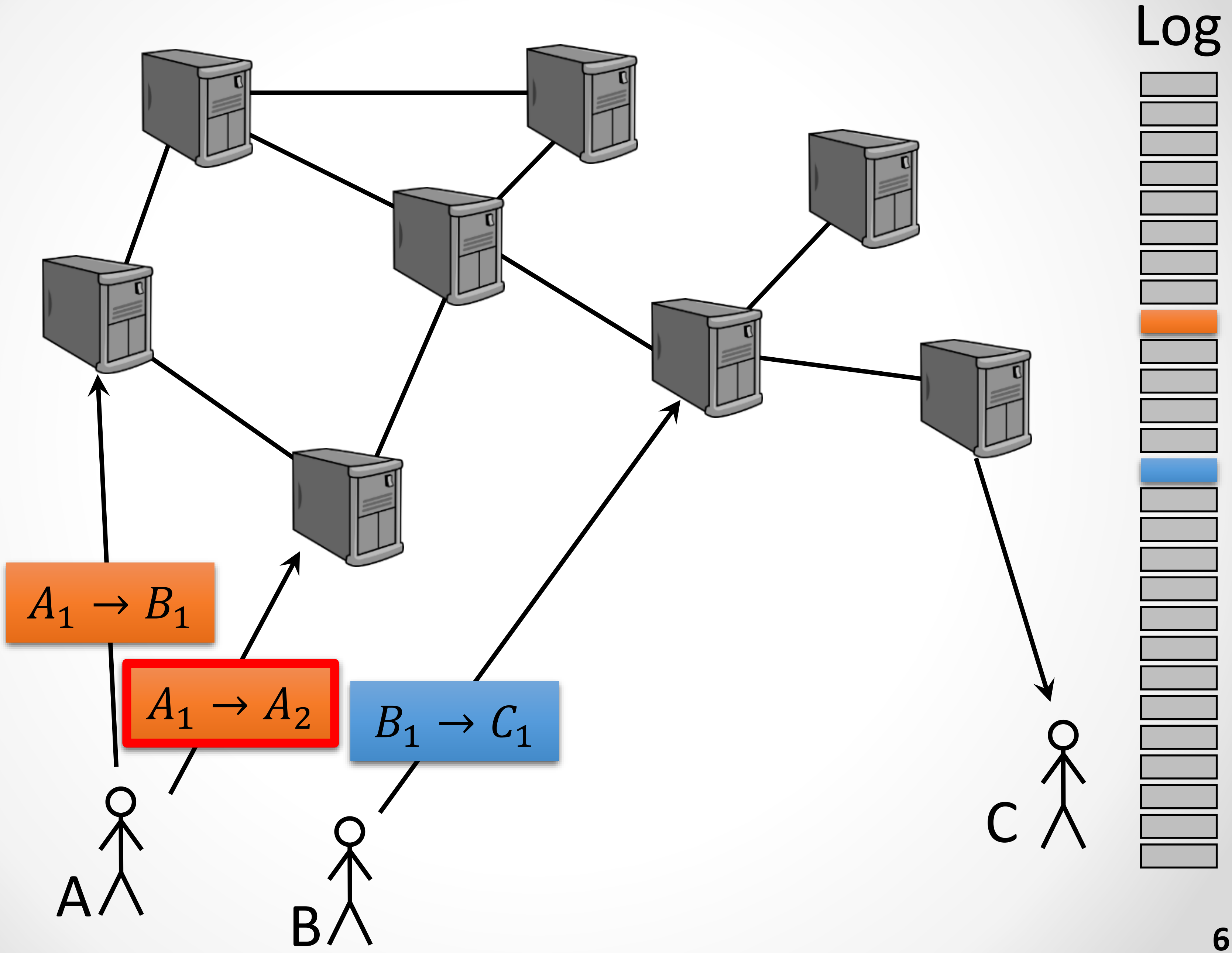
Bitcoin-NG: A Scalable Blockchain Protocol

- A replicated state machine (Monte-Carlo)
- Extreme-churn robustness
- High performance
  (10x throughput, fraction of latency)

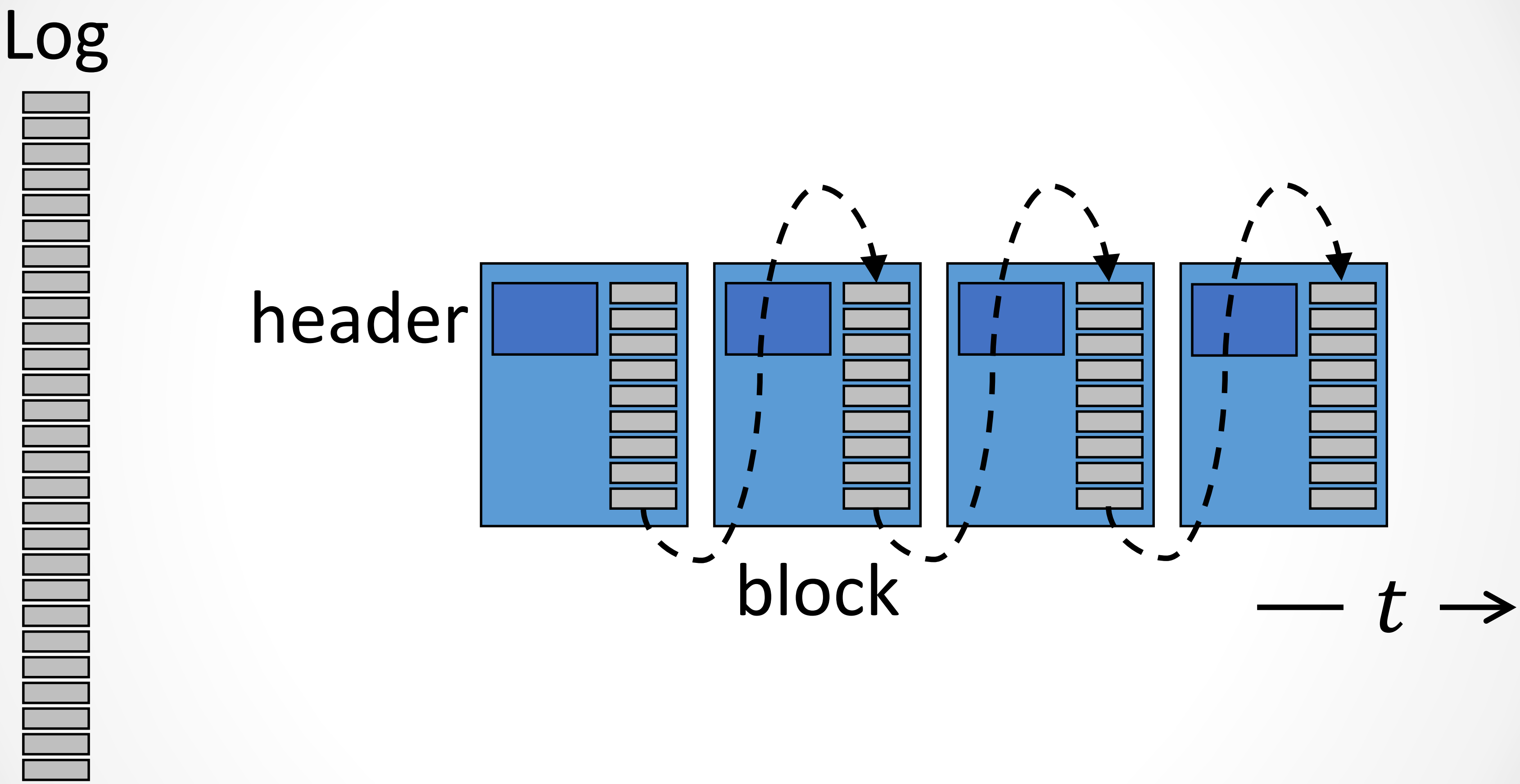
Evaluation

- Novel performance metrics
- Experiments with unmodified nodes
  - Low latency
  - High throughput

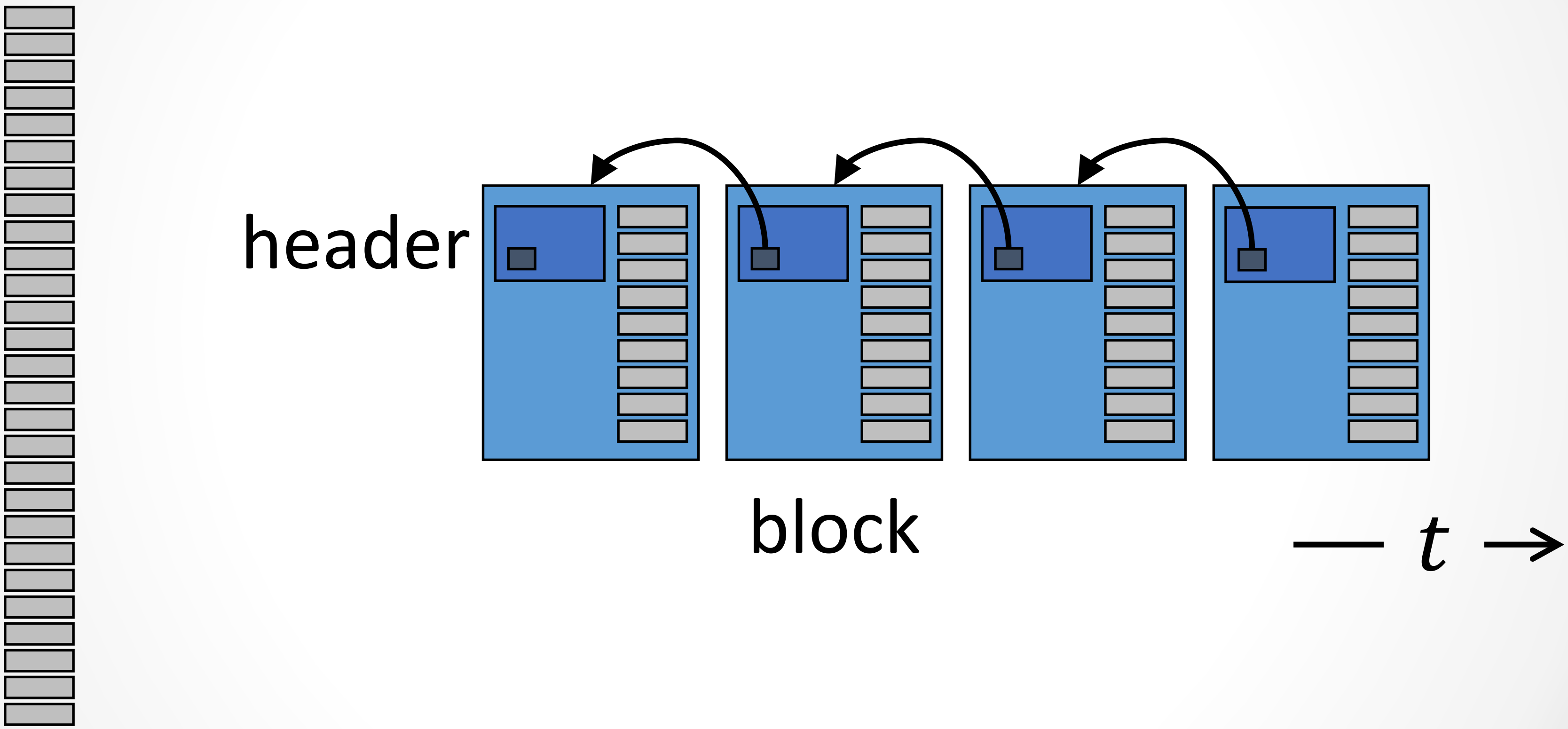
Blockchain: A Replicated State Machine



The Blockchain



The Blockchain



Log

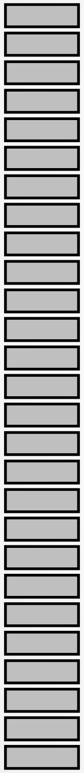
header

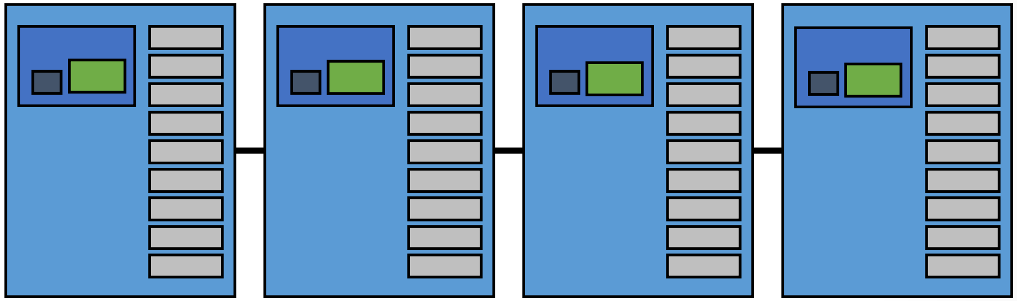
block

— t →

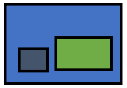
The Blockchain

Log



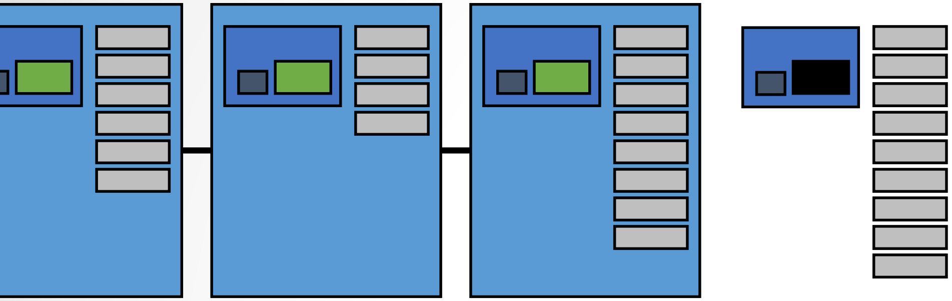


— *t* →

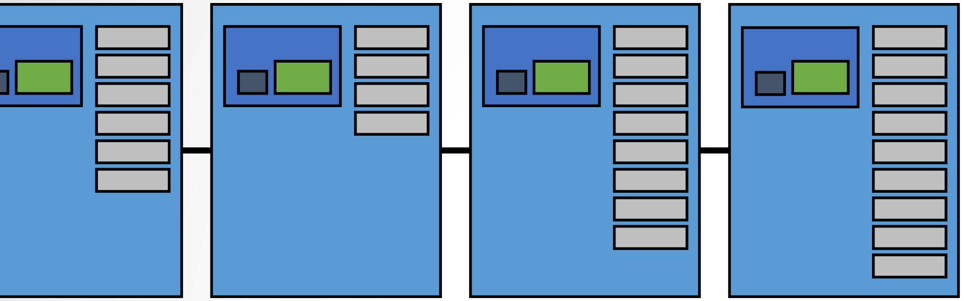
hash() < target*

* *target*: a deterministic function of previous blocks

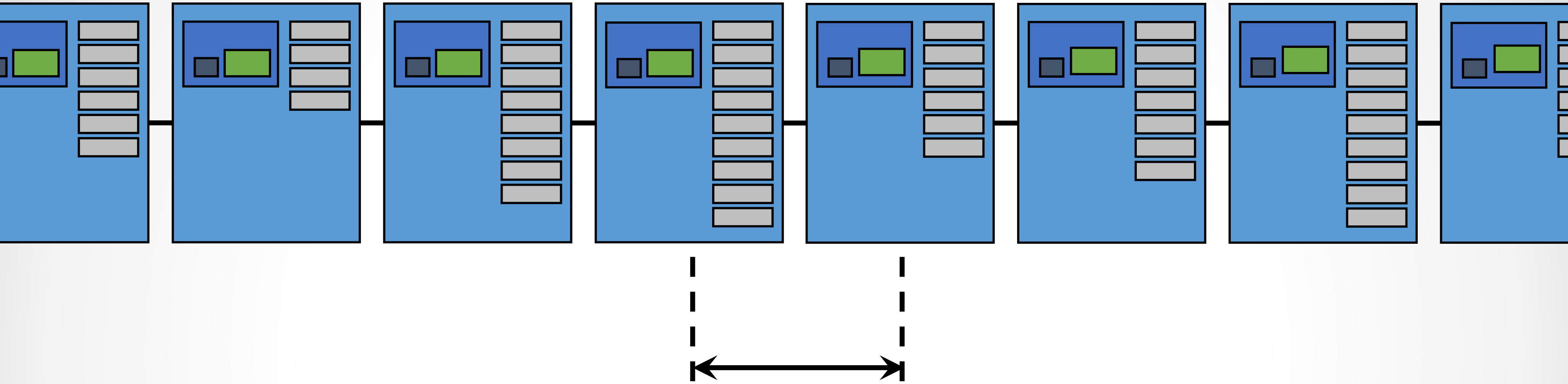
The Blockchain



The Blockchain



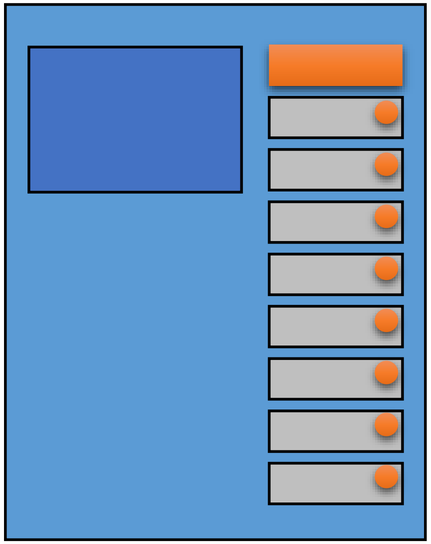
The Blockchain

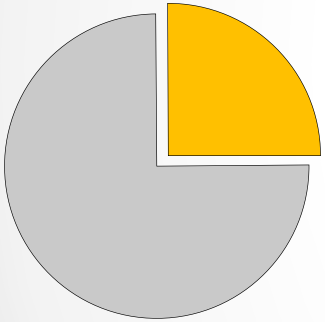


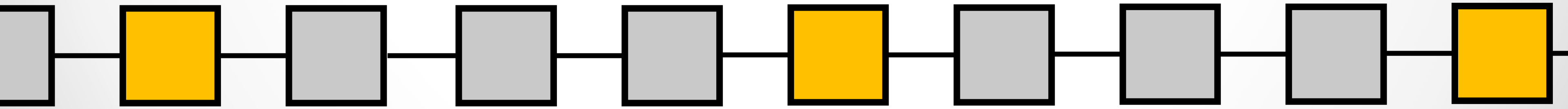
Exponential, with
constant mean interval

Incentive for Mining

- **Internal** Prize:
  - Minting
  - Fees

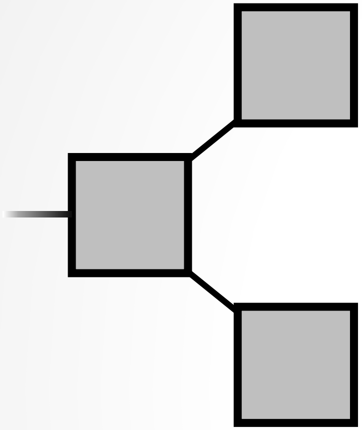






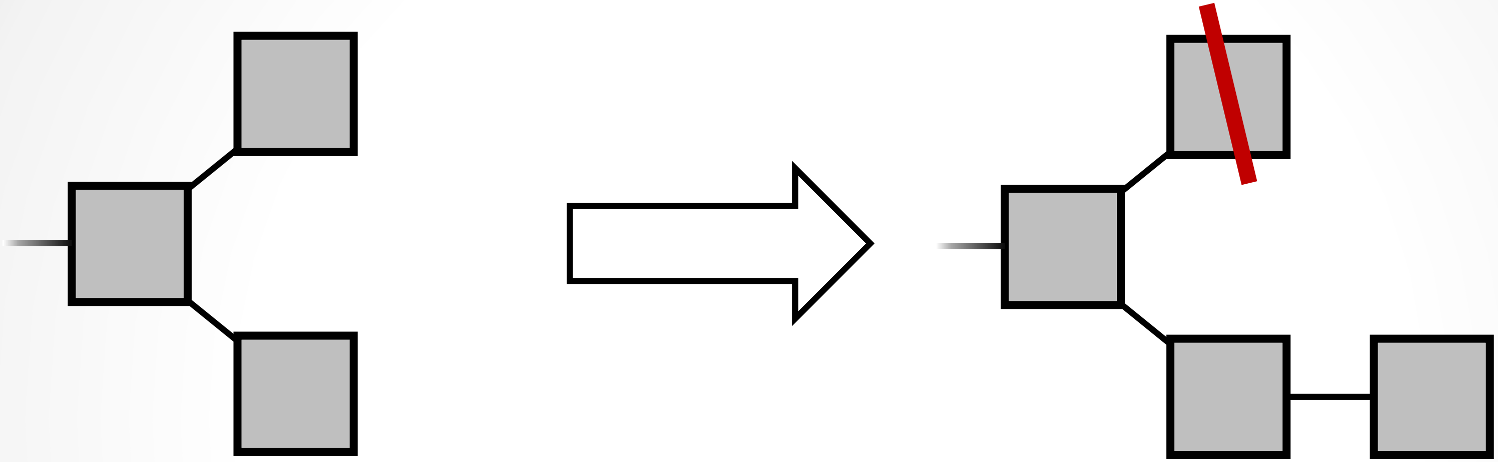
Wins proportional to computation power

Forks



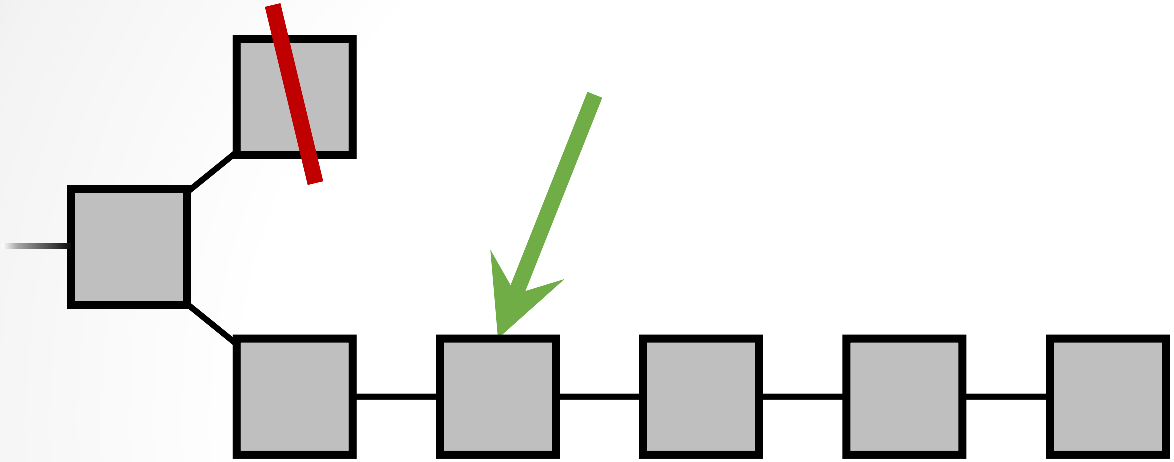
- Natural in a distributed system

Fork Resolution



- **Longest** chain wins
- Transactions are reverted
- Double-spending a threat

Fork Resolution

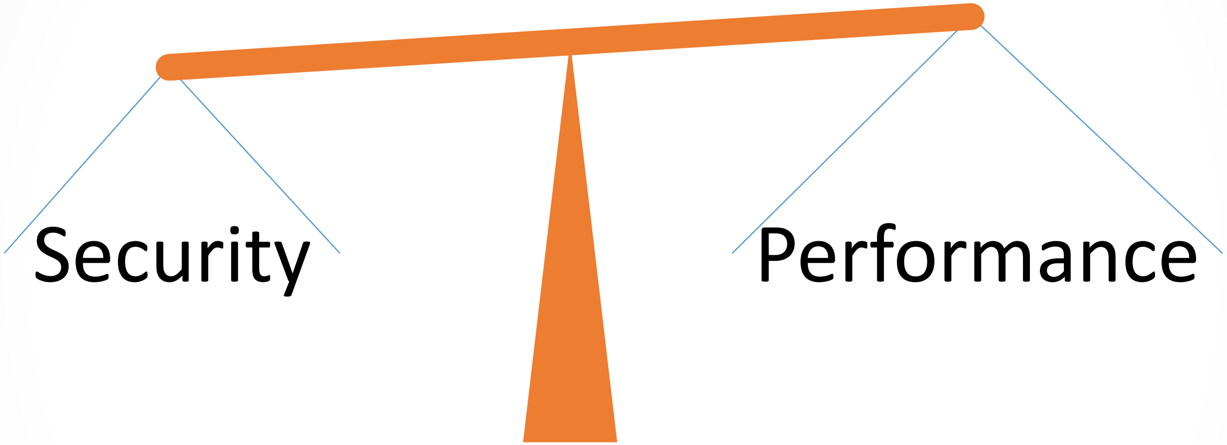


A transaction is **confirmed** when it is **buried** “deep enough”

Security-Performance Tradeoff

Nakamoto’s Blockchain exhibits a tradeoff:

[Sompolinsky+’15, Lewenberg+’15]



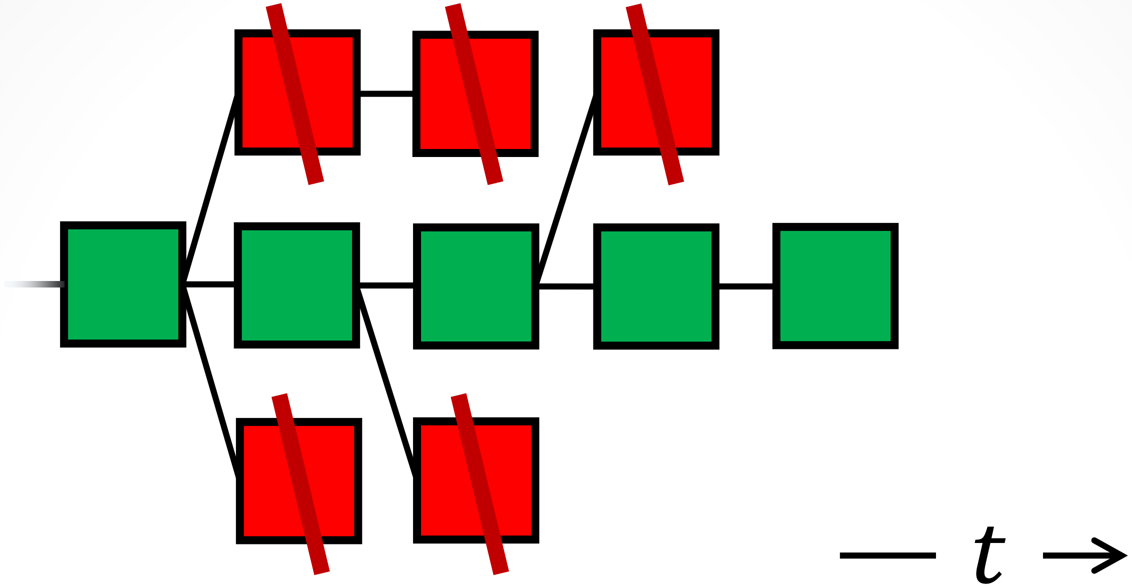
Security

Performance

Metrics

- **Bandwidth**
- **Latency**
  - Consensus delay
- **Security**
  - Mining power utilization
  - Fairness

Mining Power Utilization



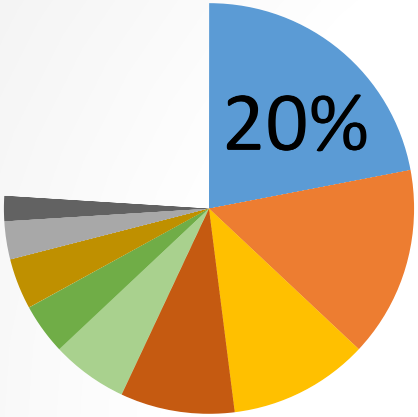
$$\frac{\Sigma\,\text{🟩}}{\Sigma(\text{🟩}+\text{🟥})}$$

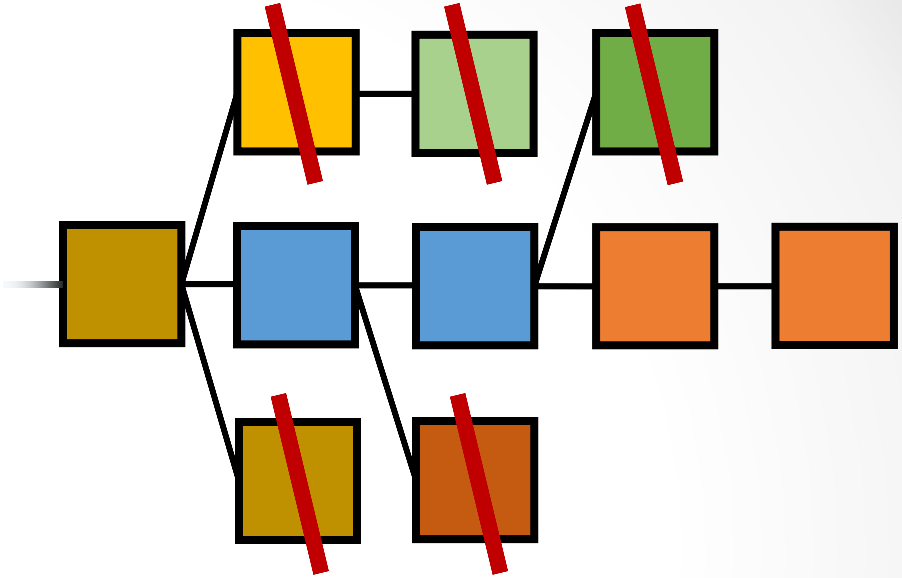
==> vulnerability to rollback

Fairness

Known Miner Sizes

[blockchain.info, April 2015]





Presence:

Fair

$$\frac{\sum_{all} \neg \blacksquare}{\sum_{all} \square} = 80\%$$

Actual

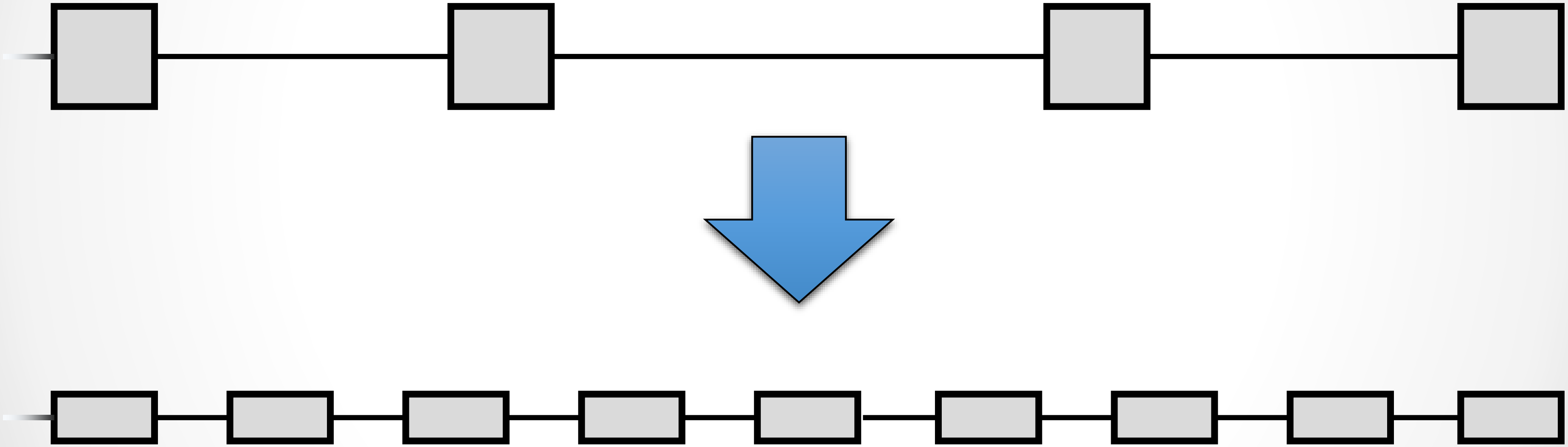
$$\frac{\sum_{main} \neg \blacksquare}{\sum_{main} \square} = 60\%$$

$$\text{Fairness: } \frac{\textbf{Actual presence}}{\textbf{Fair presence}} = \frac{60\%}{80\%} = 3/4$$

==> tendency towards centralization

Block Frequency Experiments

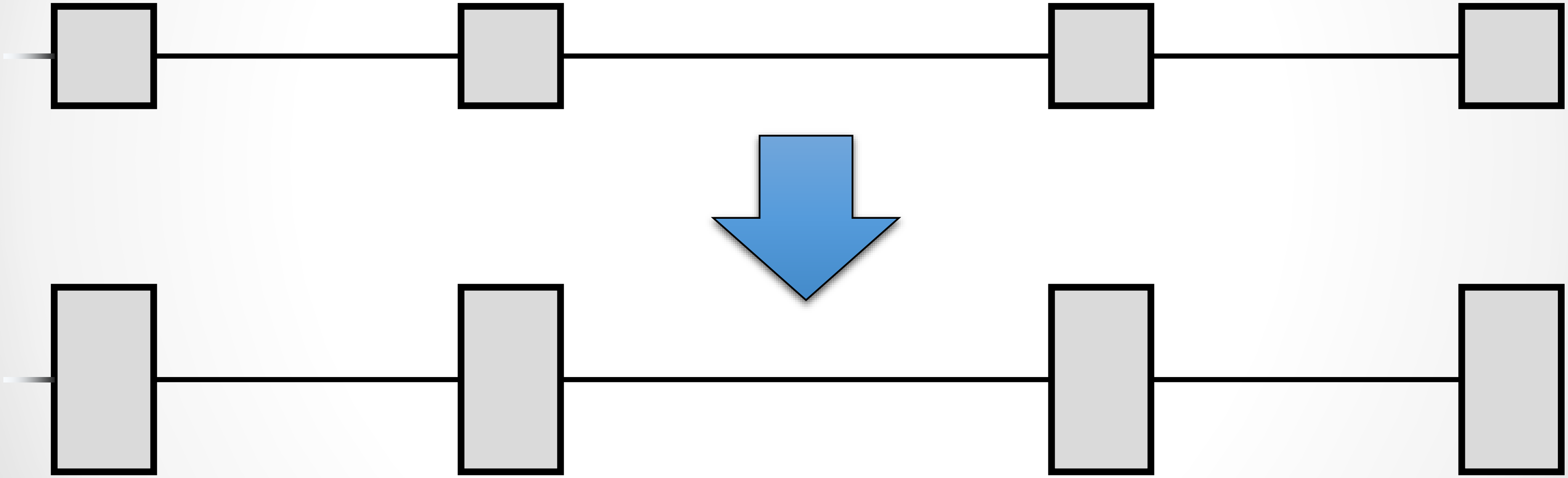
- Increasing block frequency
- Static bandwidth



==> More forks ==> worse security

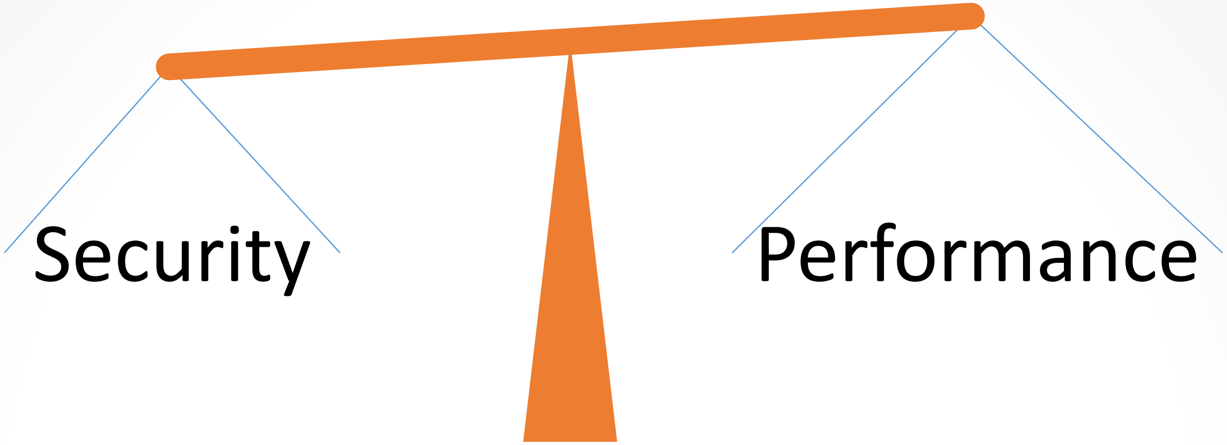
Block Size Experiments

- Static block frequency
- Increasing block size



==> More forks ==> worse security

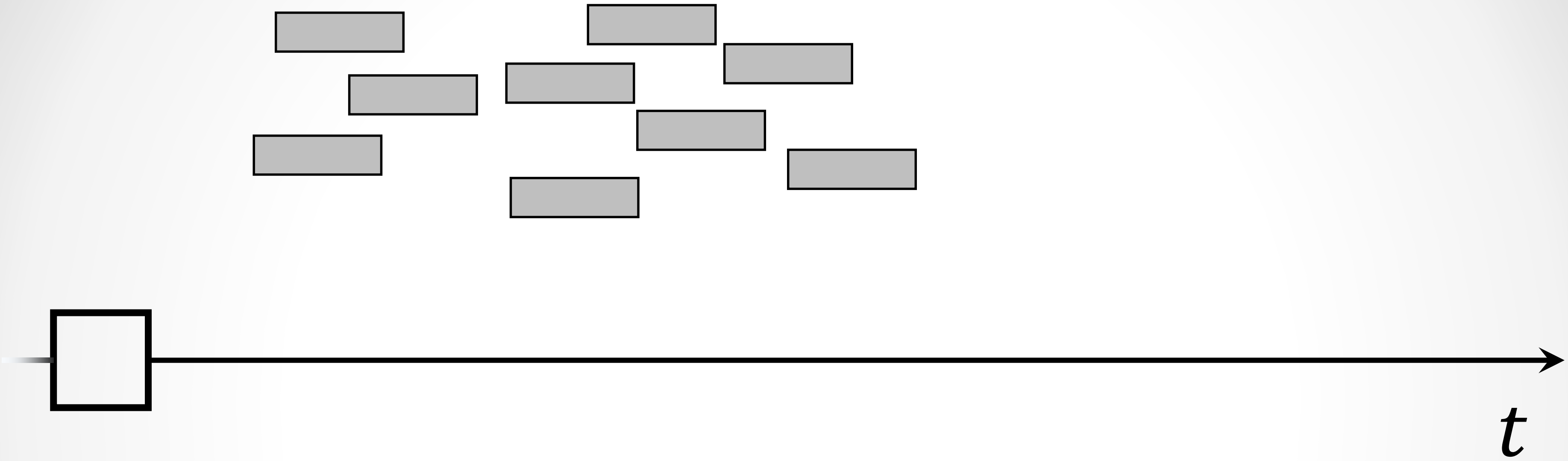
An Inherent Tradeoff?



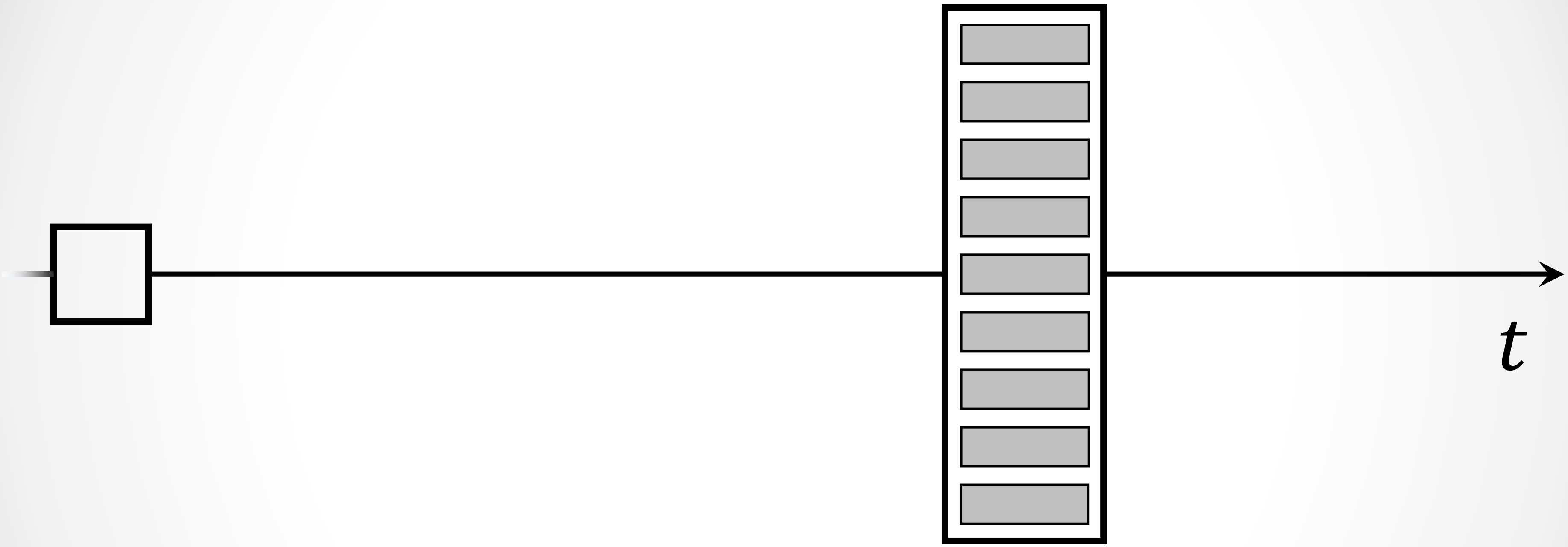
Replicated state machine performance is typically bounded by single node performance

Can this be achieved for the blockchain model?

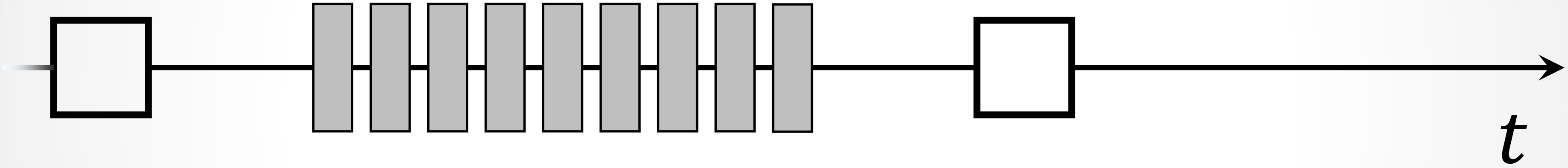
Nakamoto Blocks



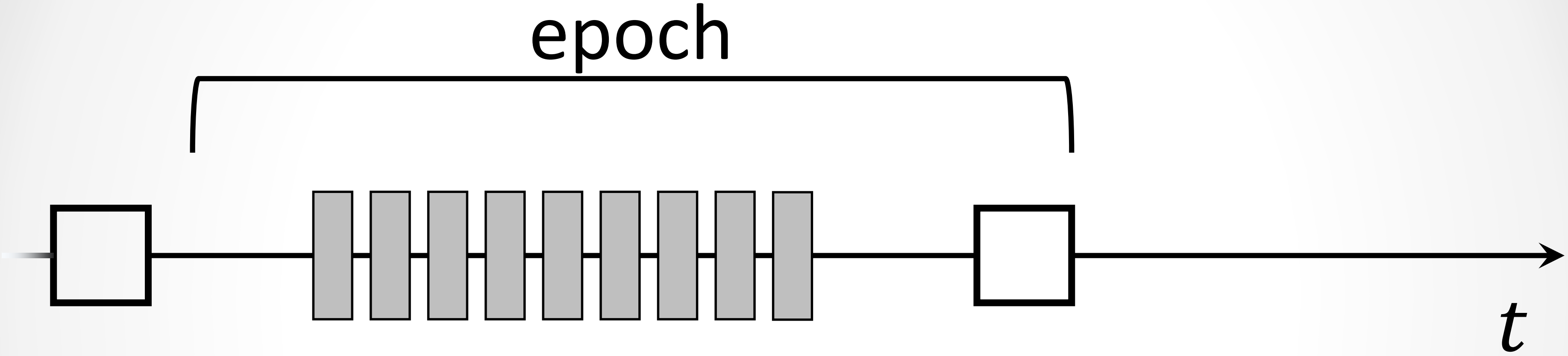
Nakamoto Blocks



Nakamoto Blocks

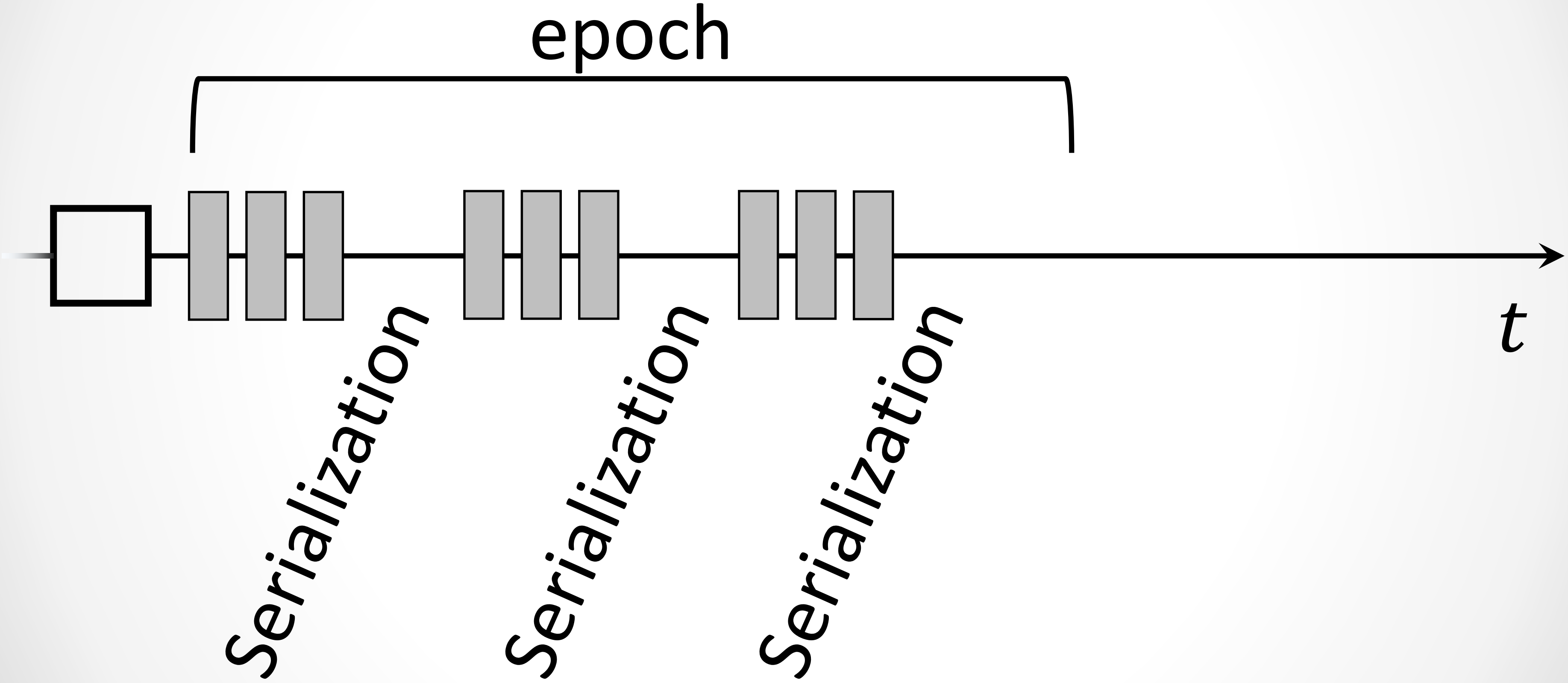


Nakamoto Blocks

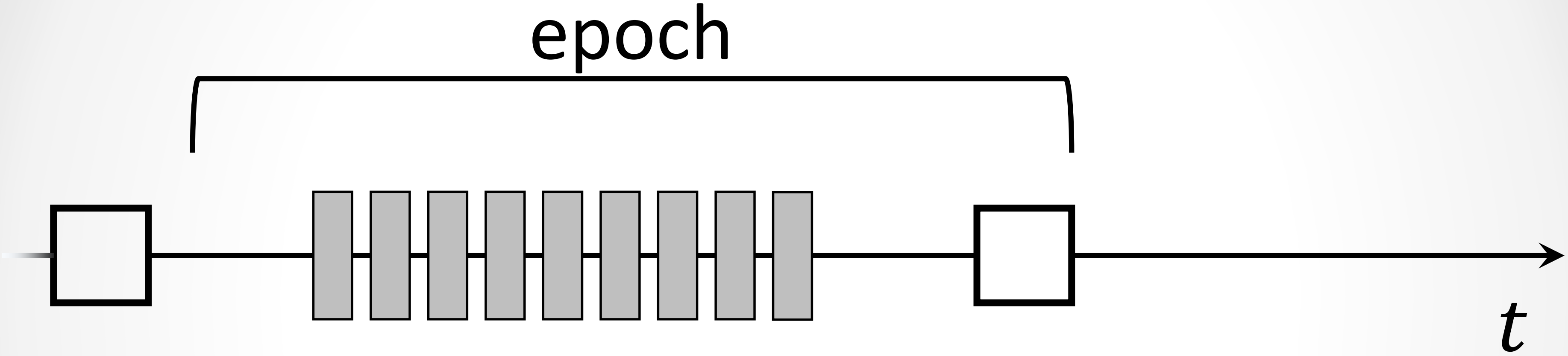


Serialization

Nakamoto Blocks

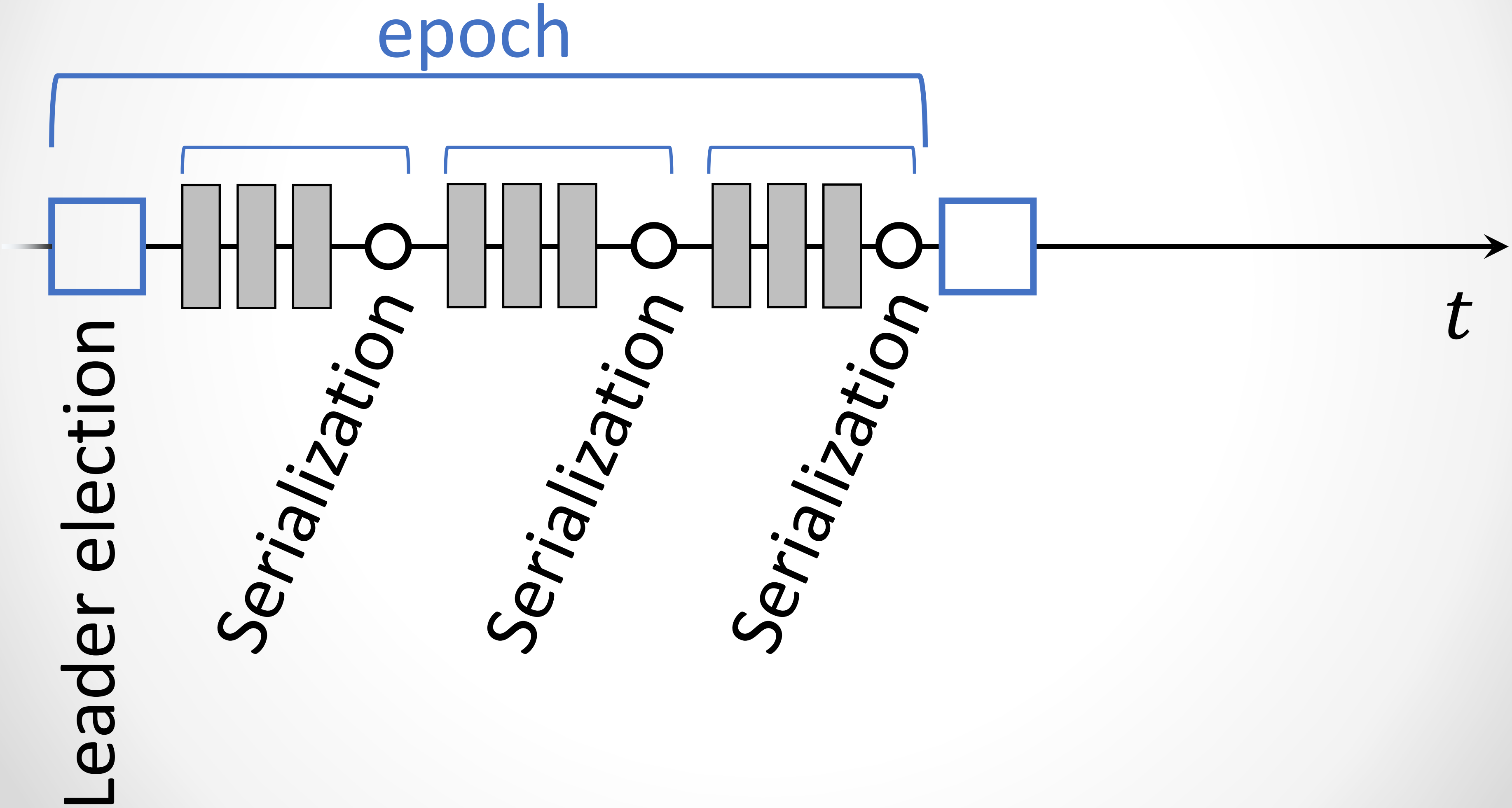


Nakamoto Blocks

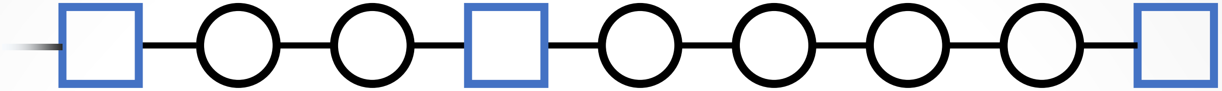


1. Leader election
2. Serialization

Bitcoin-NG


epoch
Leader election
Serialization
Serialization
Serialization
t

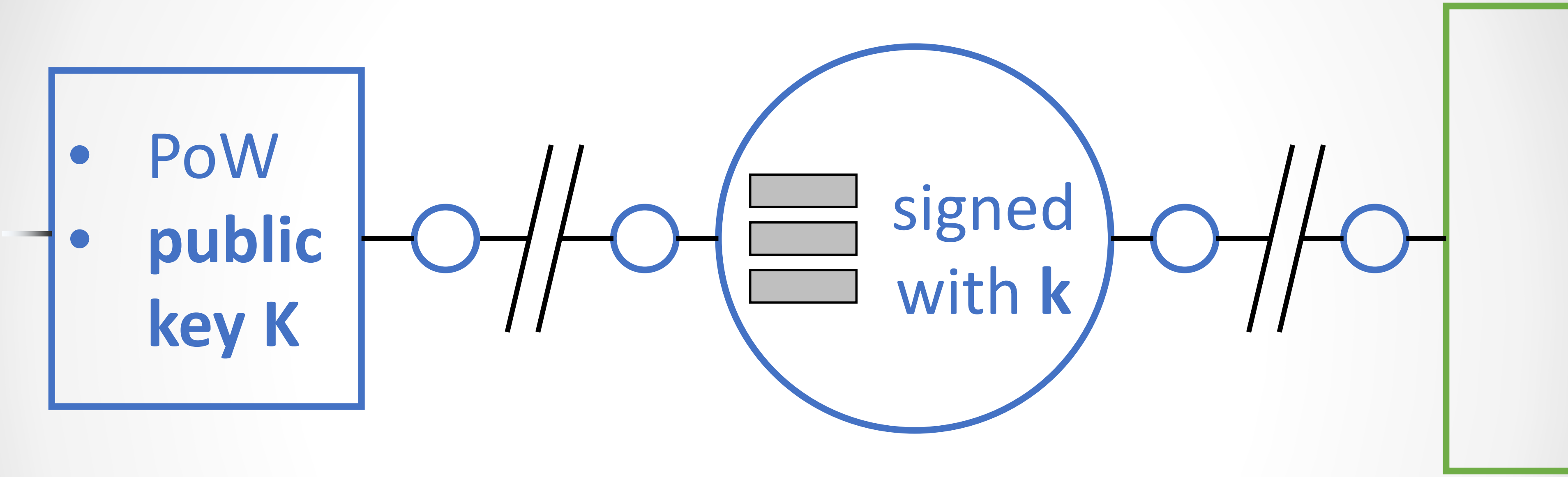
Bitcoin-NG



- Key blocks:
  - No content
  - Leader election

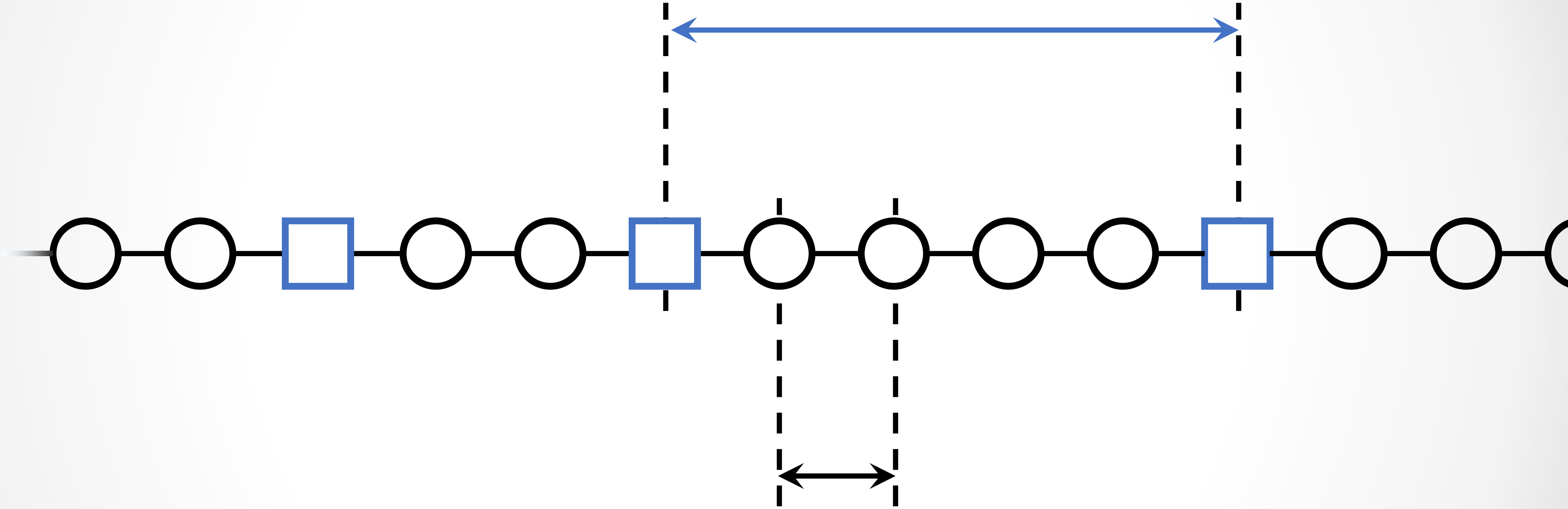
- Microblocks:
  - Only content
  - No contention

Bitcoin-NG



Bitcoin-NG

long exponential intervals (10 min)



short deterministic intervals (10 sec)

Bitcoin-NG Incentives

Next miner: **Include previous microblocks**
Leader: **Place transactions in microblocks**

Counting microblocks for chain selection breaks security (Selfish Mining)

Bitcoin-NG Incentives

Next miner: Include previous microblocks

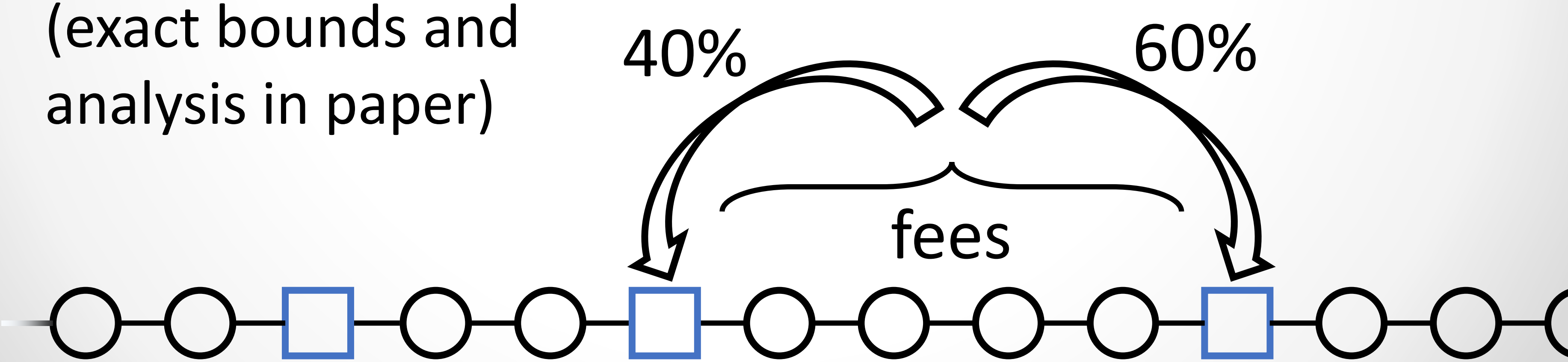
Leader: Place transactions in microblocks

Chain selection rule

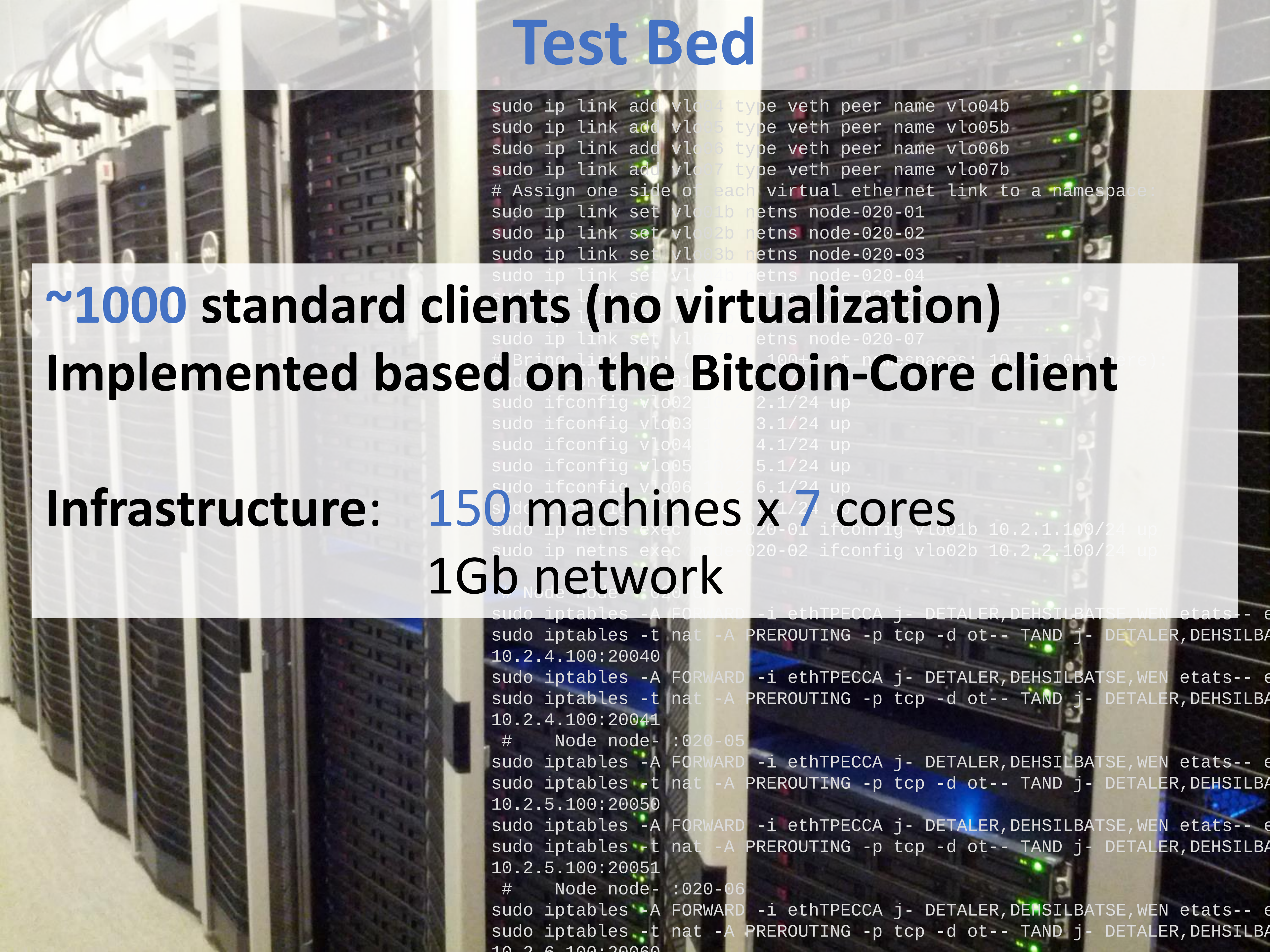
- Heaviest chain
- Microblocks carry no weight

Fee distribution

(exact bounds and analysis in paper)



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 each virtual ethernet link to a namespace:
sudo ip link set vlo01b netns node-020-01
sudo ip link set vlo02b netns node-020-02
sudo ip link set vlo03b netns node-020-03
sudo ip link set vlo04b netns node-020-04
[illegible]
[illegible]
sudo ip link set vl[illegible]7b netns node-020-07
# Bring links up: ([illegible] 100+i at namespaces: 10.2.1.0+i here):
[illegible]
sudo ifconfig vlo02 [illegible] 2.1/24 up
sudo ifconfig vlo03 [illegible] 3.1/24 up
sudo ifconfig vlo04 [illegible] 4.1/24 up
sudo ifconfig vlo05 [illegible] 5.1/24 up
sudo ifconfig vlo06 [illegible] 6.1/24 up
[illegible] 1/24 up
sudo ip netns exec [illegible] 020-01 ifconfig vlo01b 10.2.1.100/24 up
sudo ip netns exec [illegible] 020-02 ifconfig vlo02b 10.2.2.100/24 up

 # Node node- :020-0[illegible]
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
```

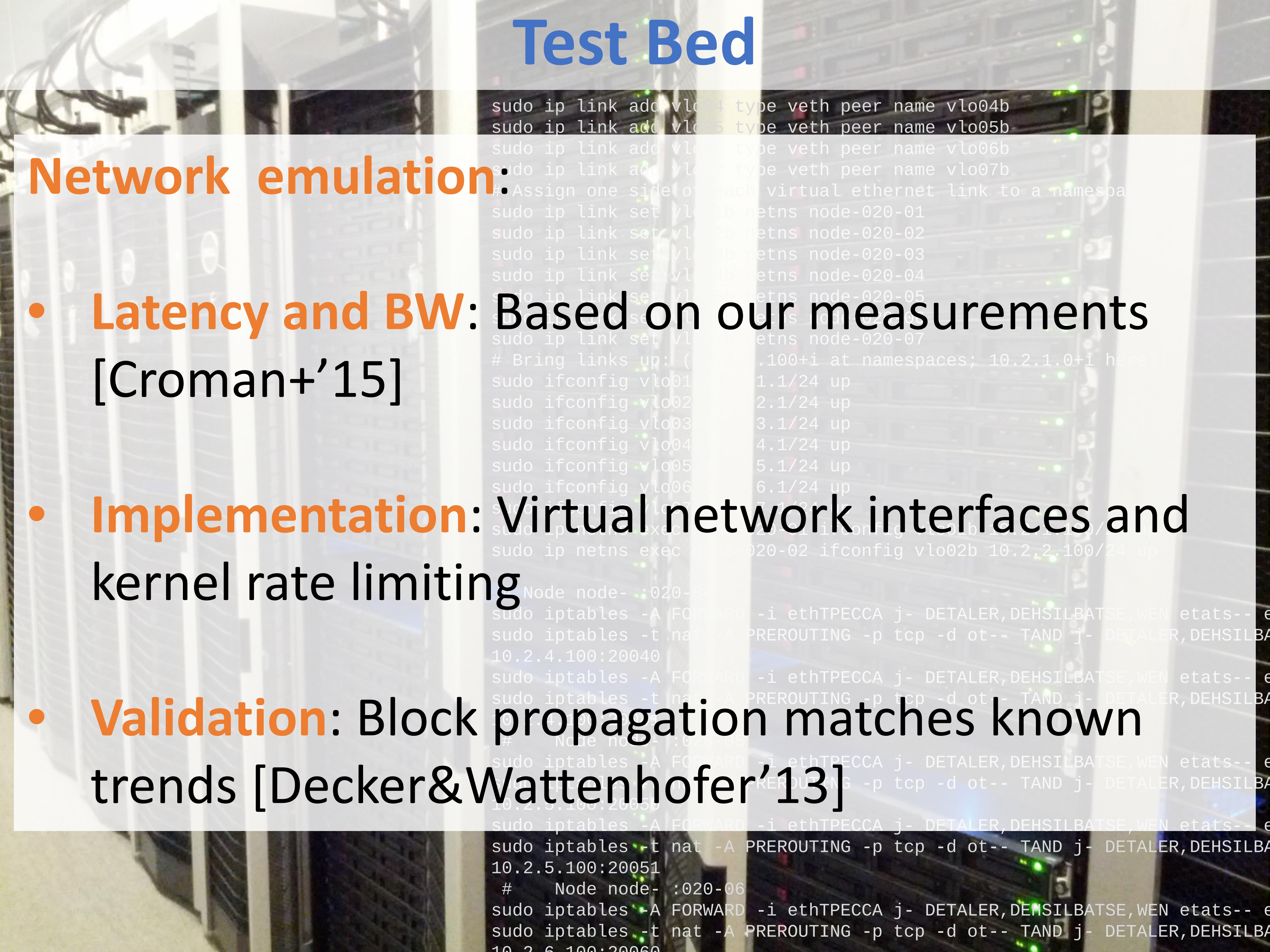
~1000 standard clients (no virtualization)

Implemented based on the Bitcoin-Core client

Infrastructure: 150 machines x 7 cores

1Gb network

Test Bed



Network emulation:

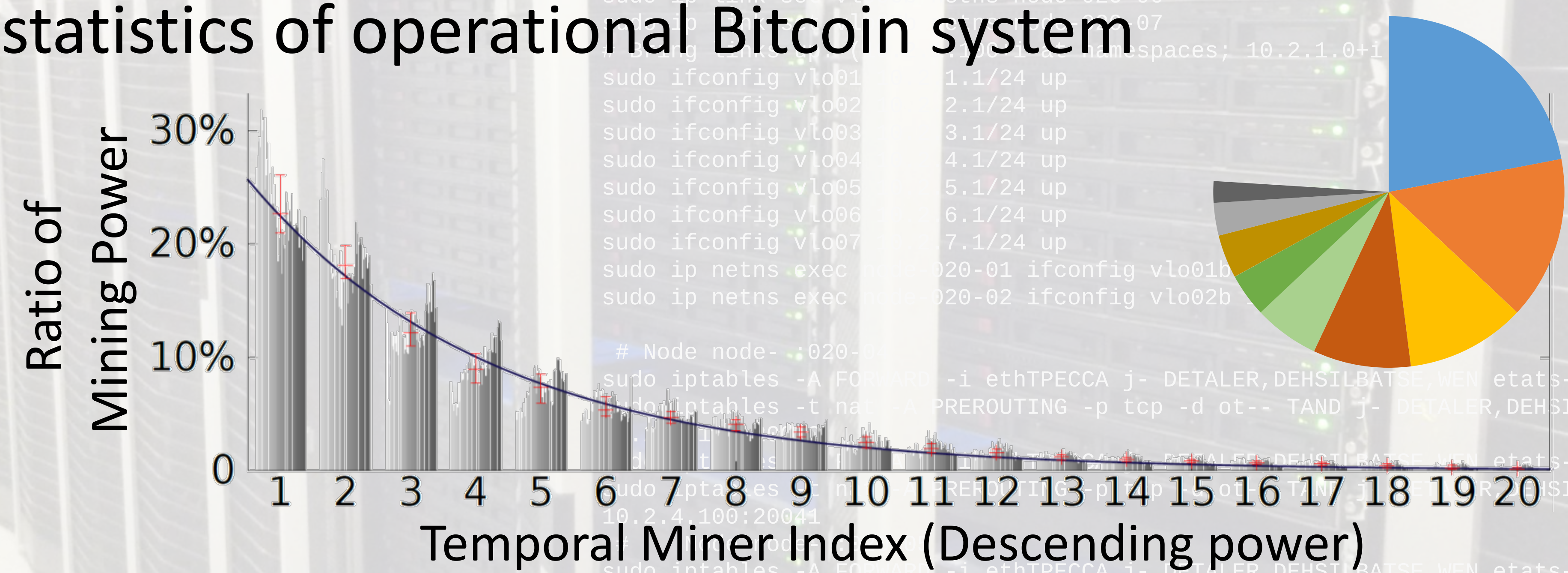
- **Latency and BW**: Based on our measurements [Croman+'15]
- **Implementation**: Virtual network interfaces and kernel rate limiting
- **Validation**: Block propagation matches known trends [Decker&Wattenhofer'13]

```
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 each virtual ethernet link to a namespa
sudo ip link set vlo01b netns node-020-01
sudo ip link set vlo02b netns node-020-02
sudo ip link set vlo03b netns node-020-03
sudo ip link set vlo04b netns node-020-04
sudo ip link set vlo05b netns node-020-05
sudo ip link set vlo06b netns node-020-06
sudo ip link set vlo07b netns node-020-07
# Bring links up: (10.2.i.100+i at namespaces; 10.2.1.0+i host):
sudo ifconfig vlo01 10.2.1.1/24 up
sudo ifconfig vlo02 10.2.2.1/24 up
sudo ifconfig vlo03 10.2.3.1/24 up
sudo ifconfig vlo04 10.2.4.1/24 up
sudo ifconfig vlo05 10.2.5.1/24 up
sudo ifconfig vlo06 10.2.6.1/24 up
sudo ifconfig vlo07 10.2.7.1/24 up
sudo ip netns exec node-020-01 ifconfig vlo01b 10.2.1.100/24 up
sudo ip netns exec node-020-02 ifconfig vlo02b 10.2.2.100/24 up
#    Node node- :020-04
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
```

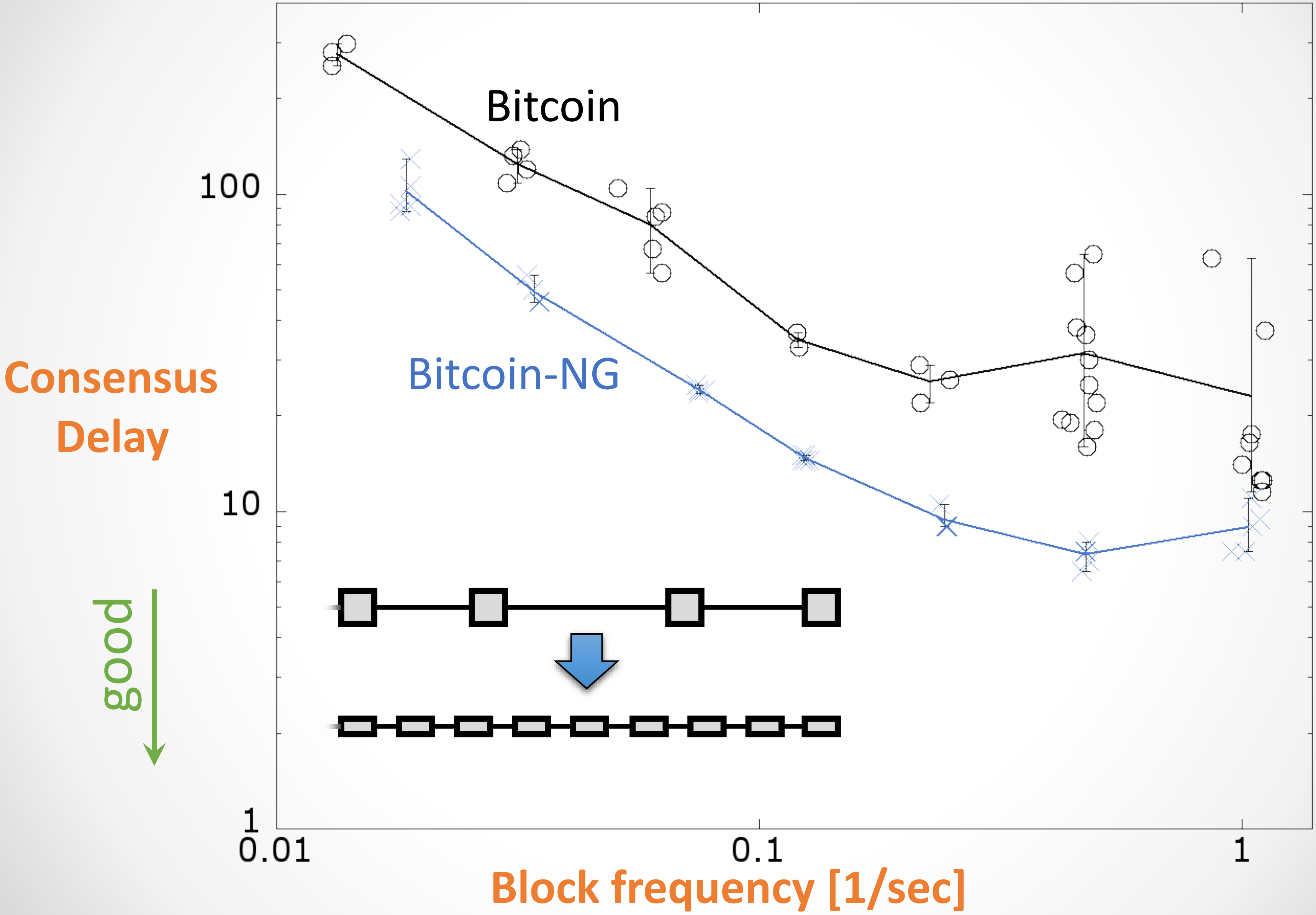
Test Bed

```
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 each virtual ethernet link to a namespace:
sudo ip link set vlo01b netns node-020-01
sudo ip link set vlo02b netns node-020-02
sudo ip link set vlo03b netns node-020-03
sudo ip link set vlo04b netns node-020-04
sudo ip link set vlo05b netns node-020-05
sudo ip link set vlo06b netns node-020-06
sudo ip link set vlo07b netns node-020-07
# Bring links up: (  in namespaces; 10.2.1.0+i
sudo ifconfig vlo01 10.2.1.1/24 up
sudo ifconfig vlo02 10.2.2.1/24 up
sudo ifconfig vlo03 10.2.3.1/24 up
sudo ifconfig vlo04 10.2.4.1/24 up
sudo ifconfig vlo05 10.2.5.1/24 up
sudo ifconfig vlo06 10.2.6.1/24 up
sudo ifconfig vlo07 10.2.7.1/24 up
sudo ip netns exec node-020-01 ifconfig vlo01b
sudo ip netns exec node-020-02 ifconfig vlo02b

 # Node node- :020-04
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
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
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
```

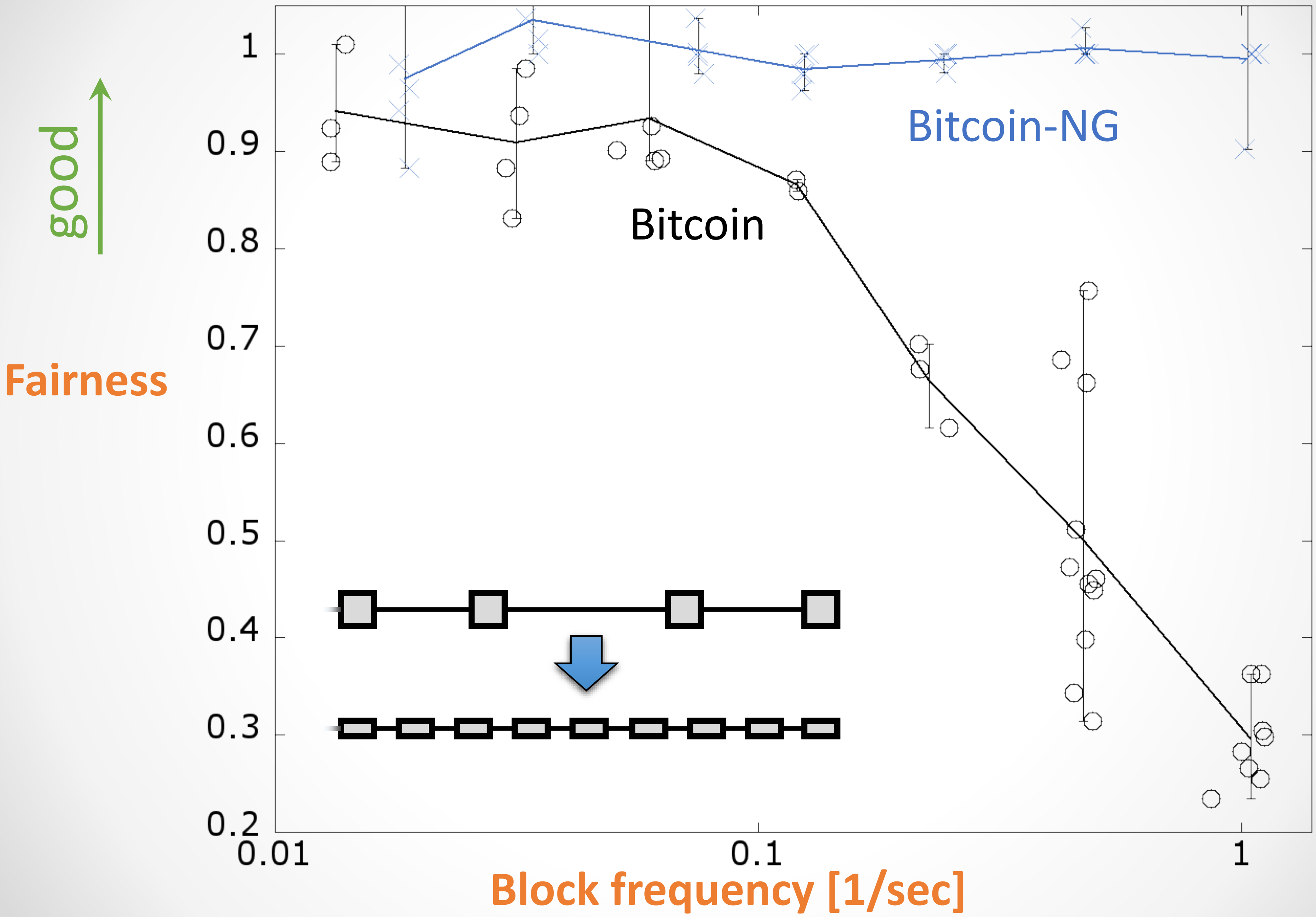
Mining power distribution: Based on one-year statistics of operational Bitcoin system



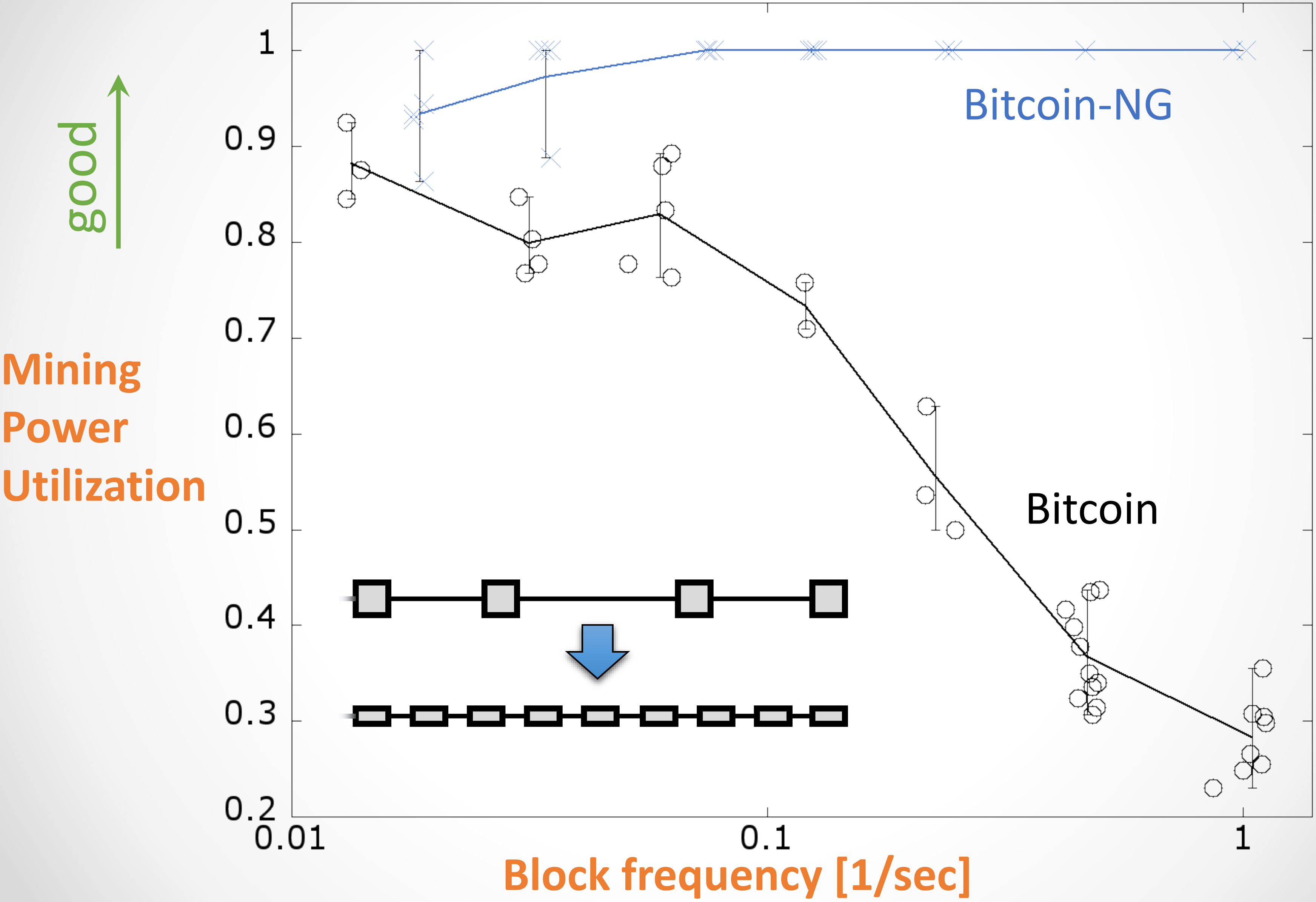
Block Frequency



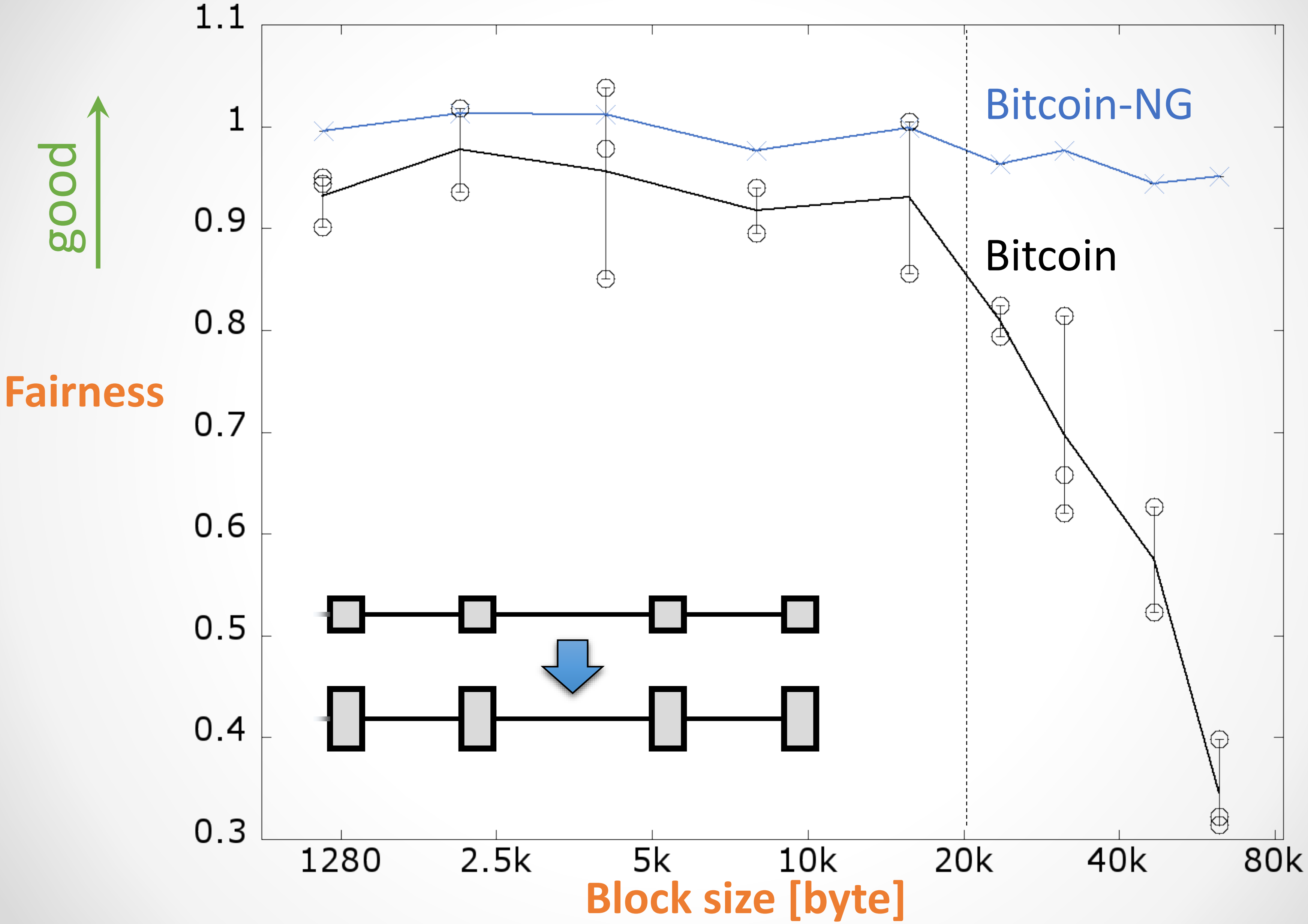
Block Frequency



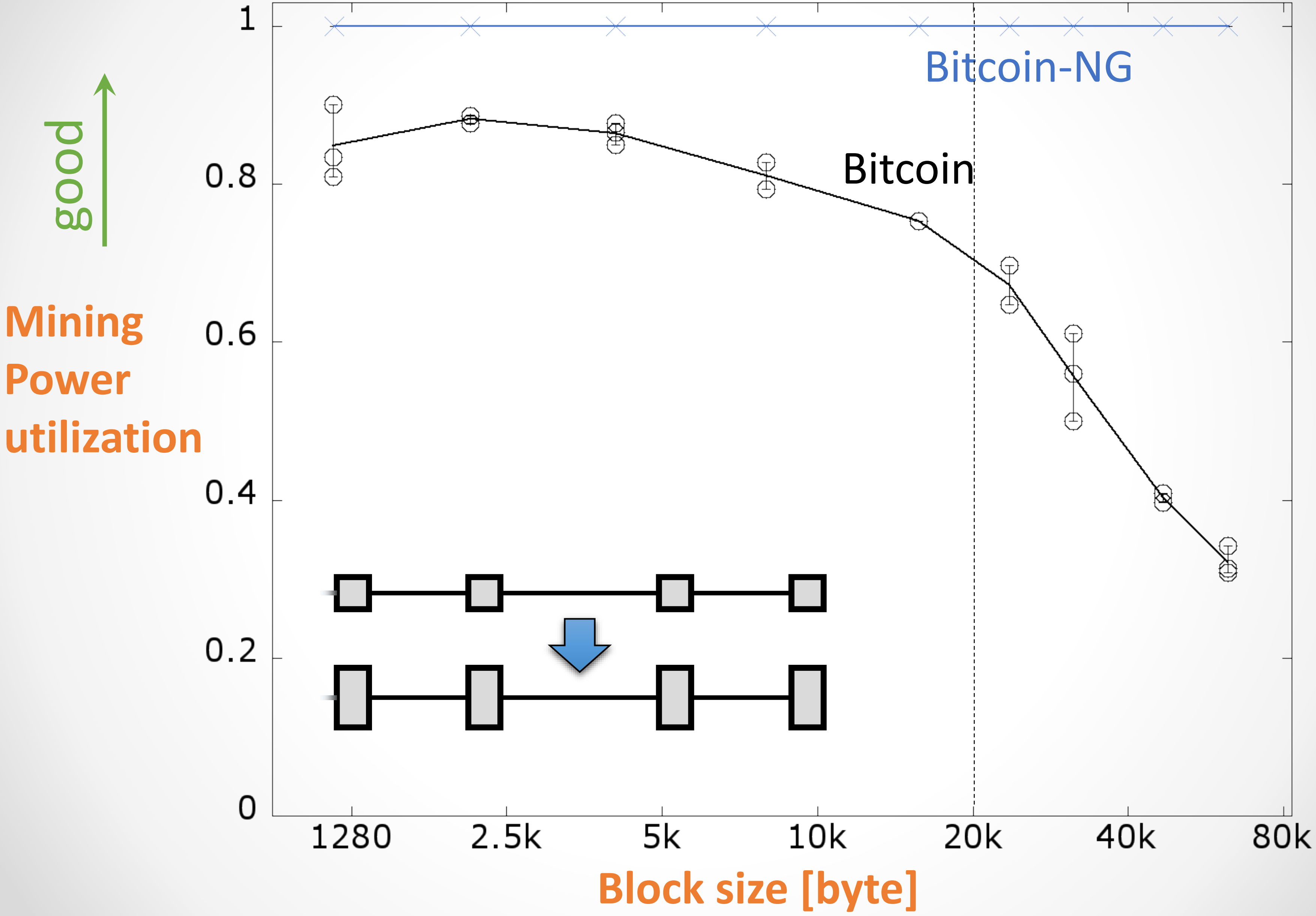
Block Frequency



Block Size


good
Fairness
1.1
1
0.9
0.8
0.7
0.6
0.5
0.4
0.3
1280
2.5k
5k
10k
20k
40k
80k
Block size [byte]
Bitcoin-NG
Bitcoin

Block Size


good
Mining Power utilization
1
0.8
0.6
0.4
0.2
0
Bitcoin-NG
Bitcoin
1280
2.5k
5k
10k
20k
40k
80k
Block size [byte]

Related Work

“The Block Size Debate”

Bitcoin-NG solves an inherent protocol shortcoming.

GHOST protocol, inclusive blockchains

Partial solutions. Perhaps could be used in concert with NG

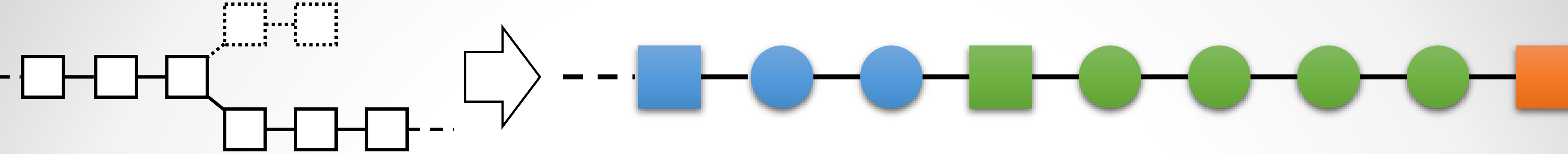
Centralized solutions of the BFT consensus family

Bitcoin-NG maintains Bitcoin’s weak model

Byzcoin, Hybrid Consensus

Uses Bitcoin-NG’s technique with epoch-length quorums to improve security and latency even further.

Summary



Bitcoin-NG

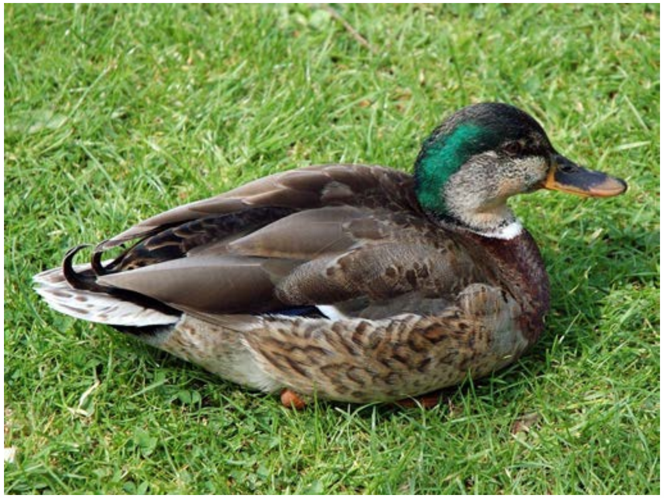
```
sudo ip link add vlo04 type veth peer name
vlo04b
sudo ip link add vlo05 type veth peer name
vlo05b
sudo ip link add vlo06 type veth peer name
vlo06b
sudo ip link add vlo07 type veth peer name
vlo07b
sudo ifconfig vlo05 10.2.5.1/24 up
sudo ifconfig vlo06 10.2.6.1/24 up
sudo ifconfig vlo07 10.2.7.1/24 up
sudo ip netns exec node-020-01 ifconfig vlo01b
10.2.1.100/24 up
sudo ip netns exec node-020-02 ifconfig vlo02b
10.2.2.100/24 up

 # Node node- :020-04
sudo iptables -A FORWARD -i ethp-04 olv o-0
```

- High bandwidth
- Low latency
- Secure

Ittay **Eyal**, Adem Efe **Gencer**, Emin Gün **Sirer**, and Robbert **Van Renesse**. **Bitcoin-NG, A Scalable Blockchain Protocol**.

Security Concern

- Unlike Nakamoto’s chain, Bitcoin-NG’s leader is a sitting duck
    - Only the leader’s key is static. Microblock generation can be distributed



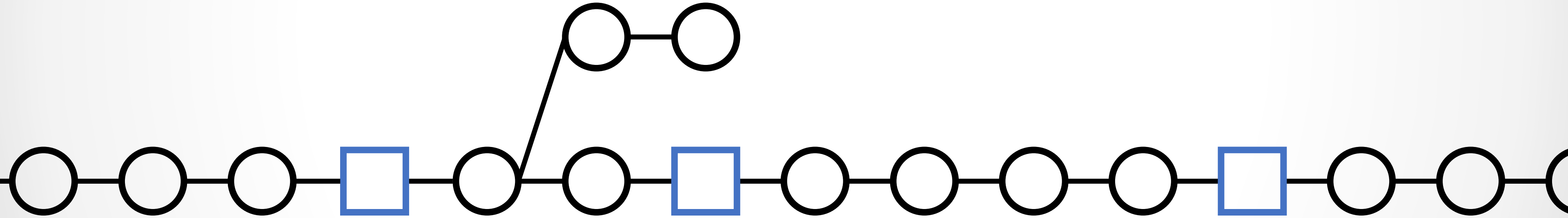
Microblock Guarantees

- With Nakamoto’s Blockchain:

  fork by risking block prize

- With Bitcoin-NG:

  Free forking?



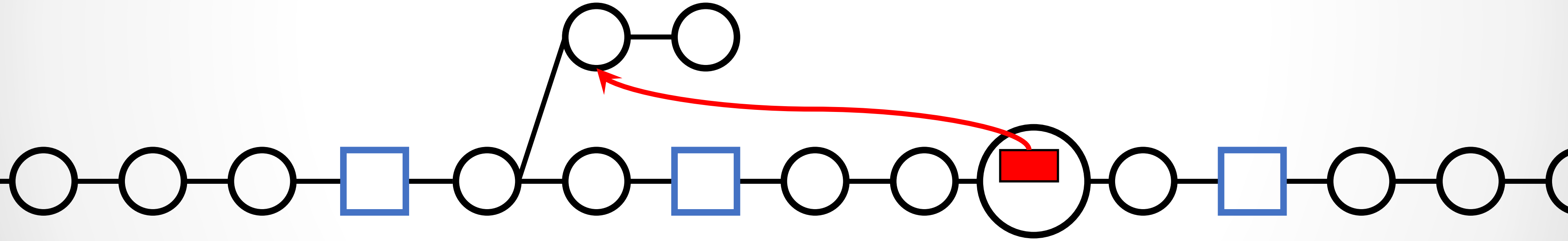
Microblock Guarantees

- With Nakamoto's Blockchain:

  fork by risking block prize

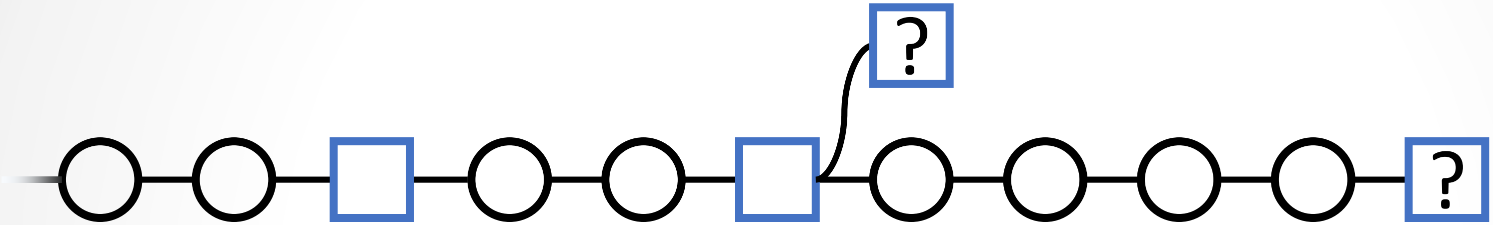
- With Bitcoin-NG:

  Free forking? No.



- Poison transaction cancels cheater reward
- Poisoner receives nominal prize

Incentive Compatibility



Broken Chain Selection Rule

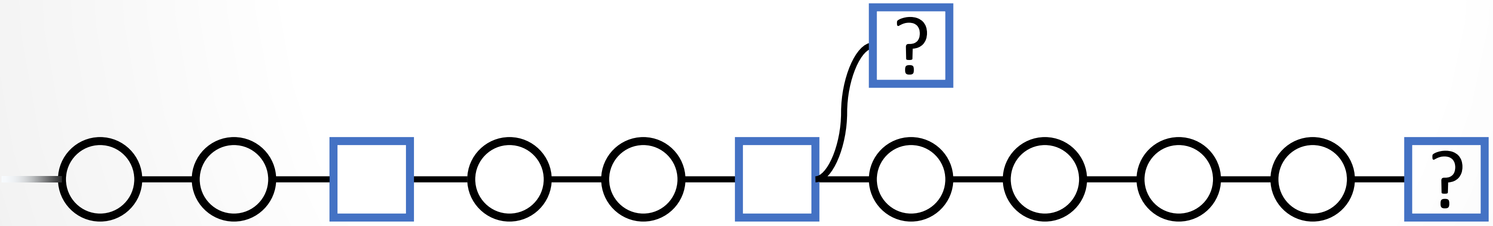
Next miner: **Include previous microblocks**

Microblocks carry small weight?

Leader: **Place transactions in micro blocks**

Leader gets fees?

Broken



Broken Chain Selection Rule

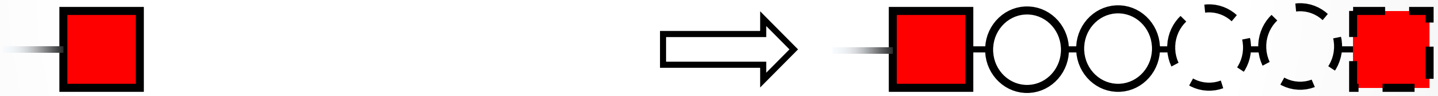
Next miner: Include previous microblocks

Microblocks carry small weight?

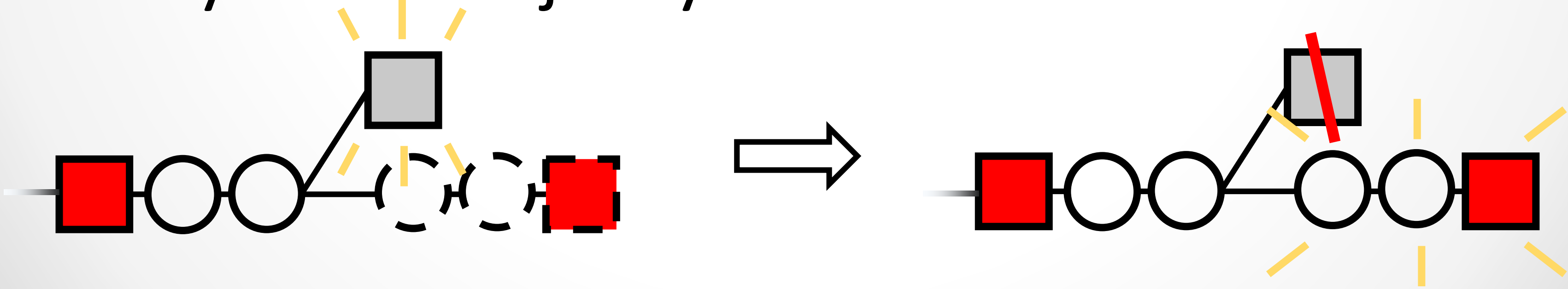
Leader: Place transactions in microblocks

Leader gets fees?

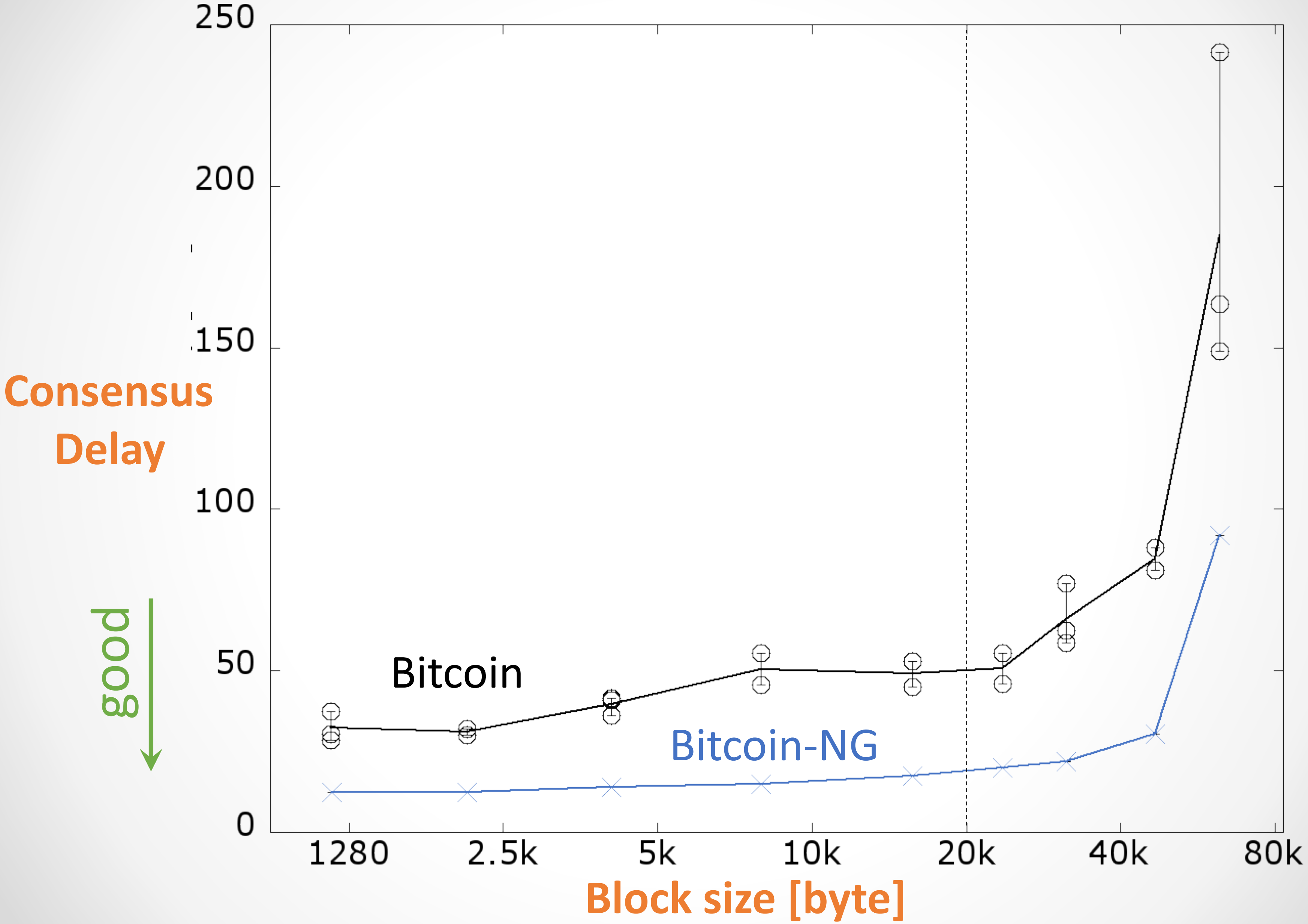
- Create secret chain:



- Always beat majority:



Block Size


250
200
150
100
50
0
Consensus Delay
good
Bitcoin
Bitcoin-NG
1280
2.5k
5k
10k
20k
40k
80k
Block size [byte]