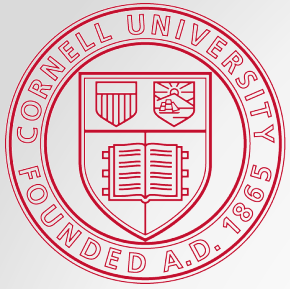


IC3

Bitcoin-NG

Building the next generation of blockchains

Ittay Eyal
Cornell CS, IC3

With Adem Efe Gencer, Emin Gun Sirer, and Robbert van Renesse

IC3 Retreat, May 2016

Blockchain's Promise and Limits

Promises

- Global currency, IoT money
- Bank to bank transactions (money, securities)
- Smart contracts infrastructure

Blockchain's Promise and Limits

Promises

- Global currency, IoT money
- Bank to bank transactions (money, securities)
- Smart contracts infrastructure

With Nakamoto's blockchain:

Performance – security tradeoff

We present a novel blockchain:

Same guarantees, but

no protocol limits on performance

Blockchain's Promise and Limits

The concepts apply to most blockchain instances

Test case: Bitcoin

Today's Bitcoin

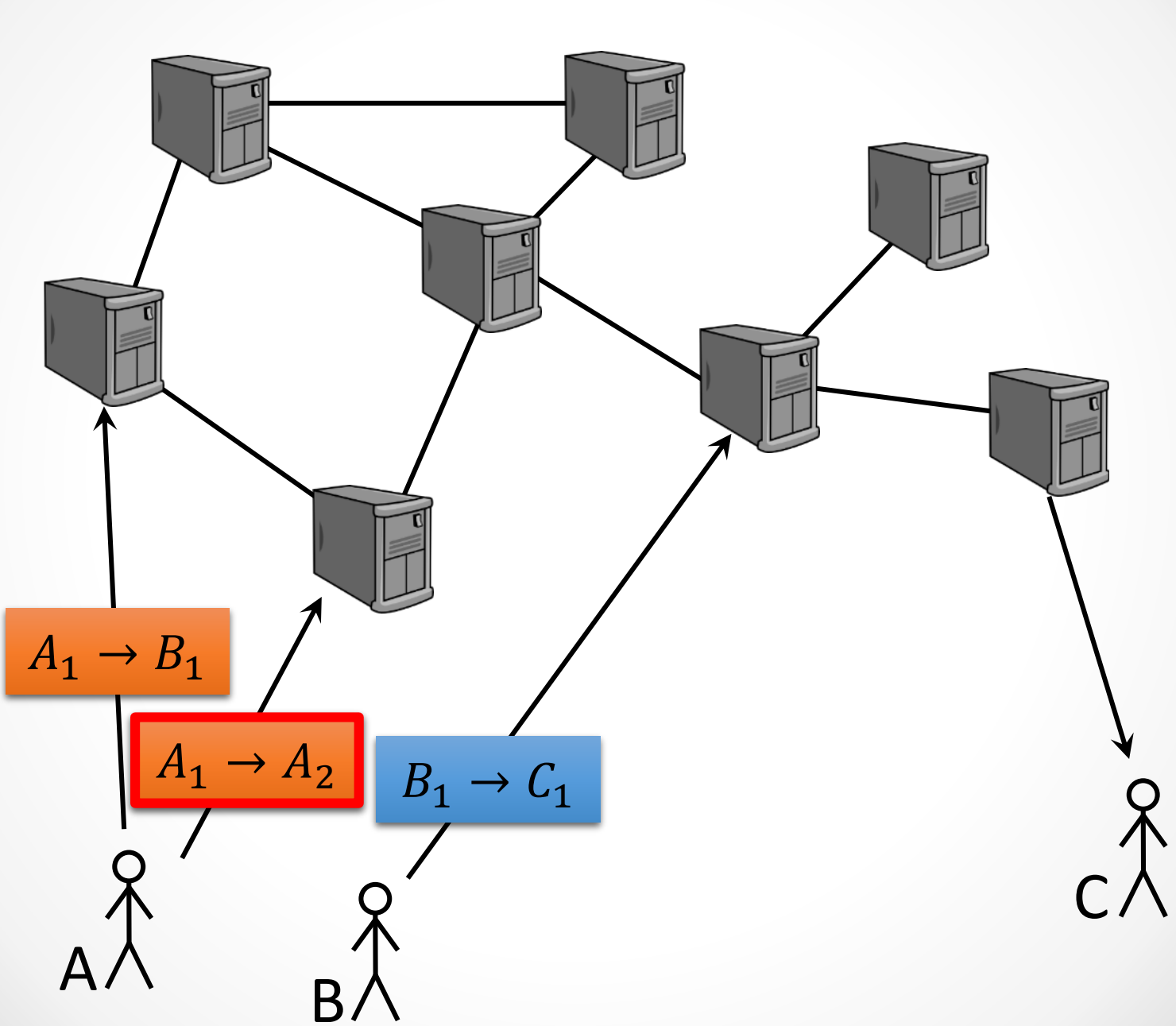
- About **2 txn/sec**
- About **10 minutes** latency

Bitcoin-NG

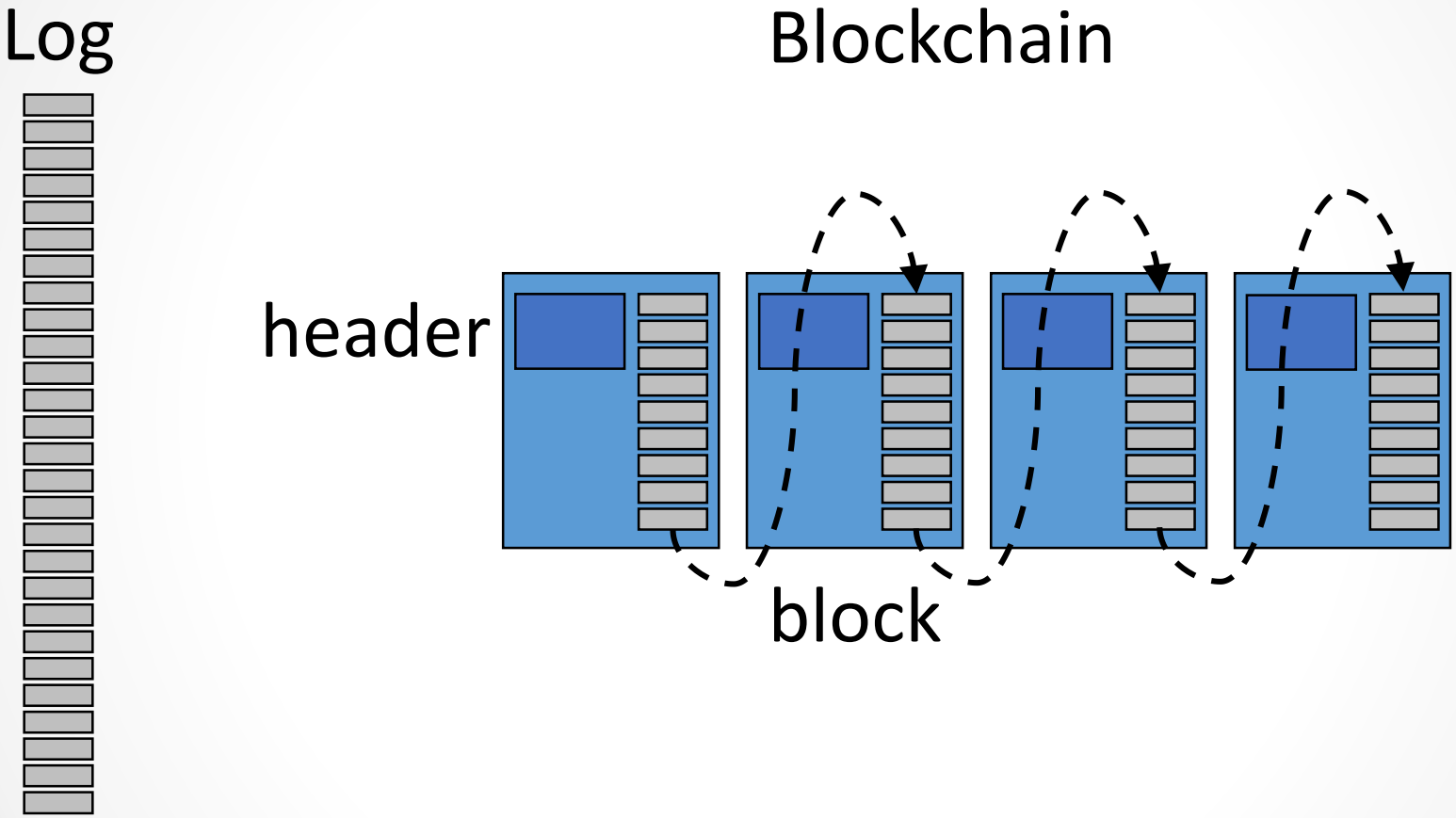
- About **100 txn/sec**
- About **10 second** latency

- **Nakamoto's performance-security tradeoff**
- Bitcoin-NG
- Performance experiments
- Demonstration

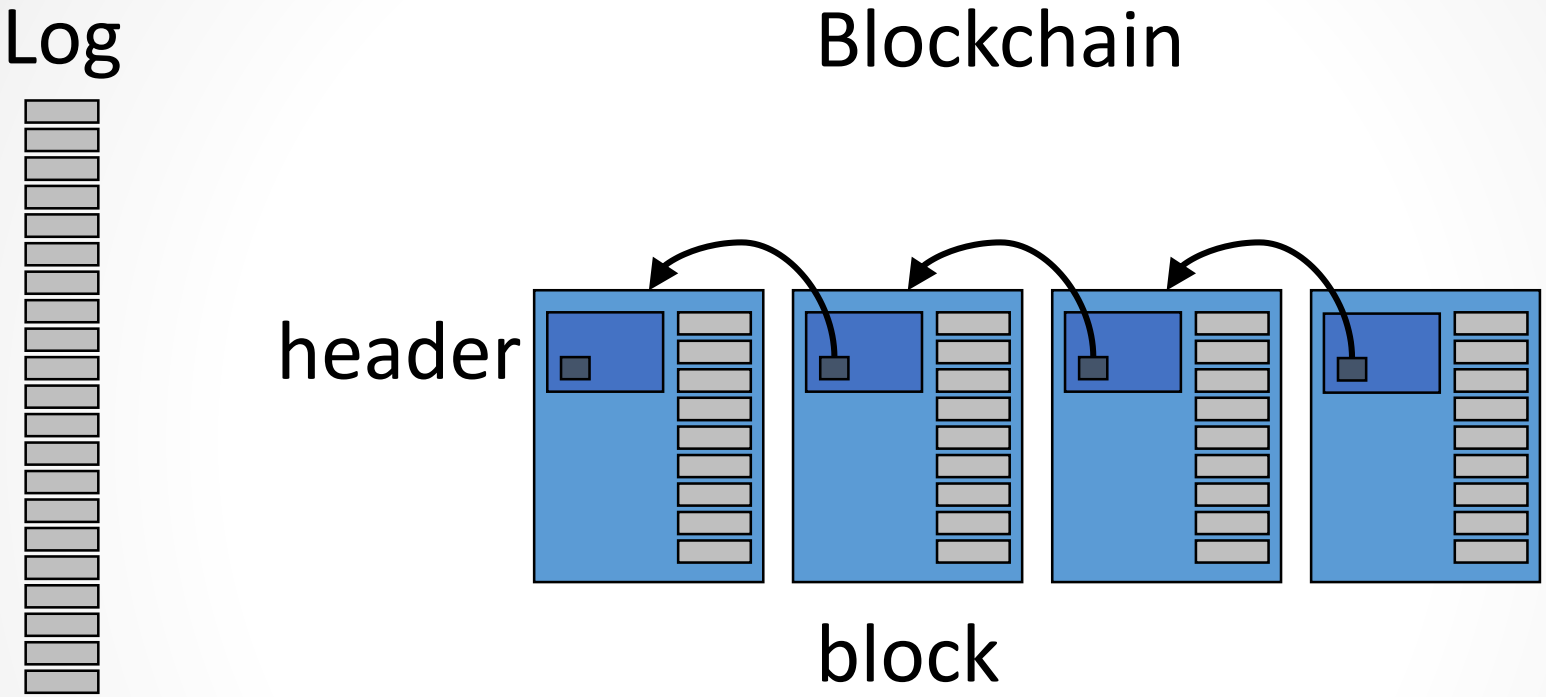
A Replicated State Machine



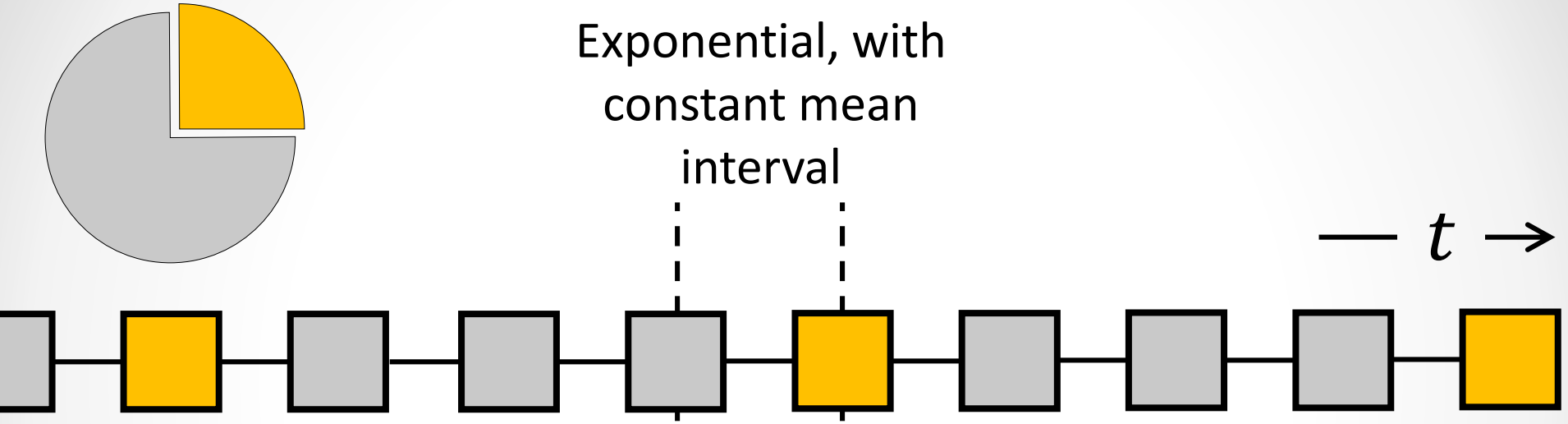
The Blockchain



The Blockchain

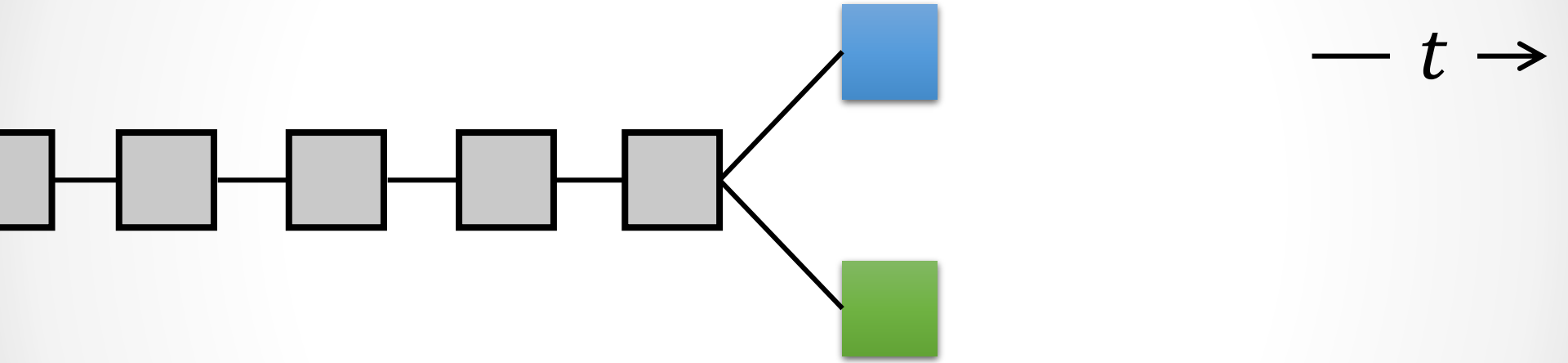


Incentive for Mining

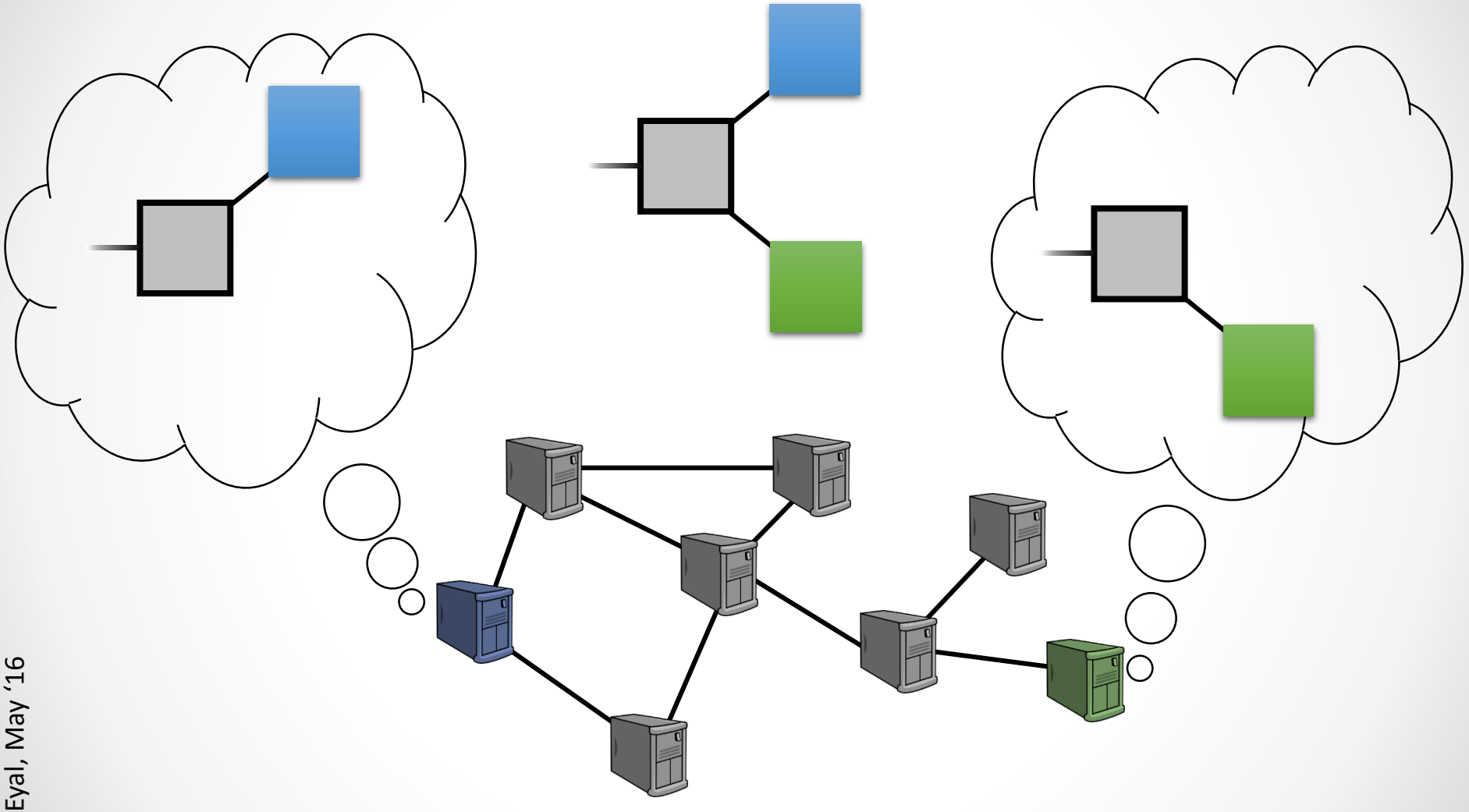


Wins proportional to computation power

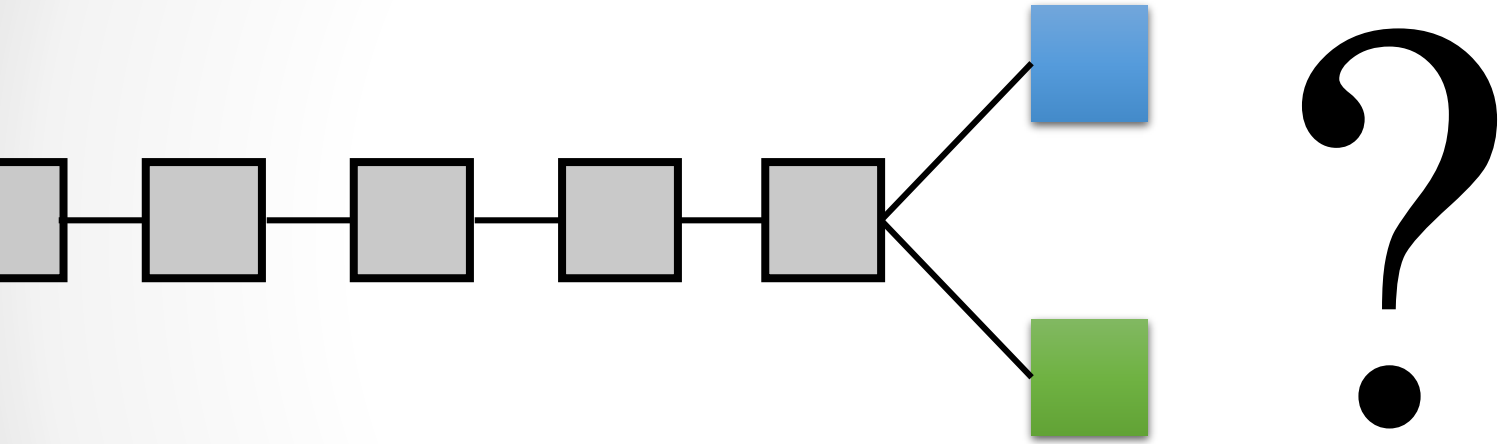
Forks



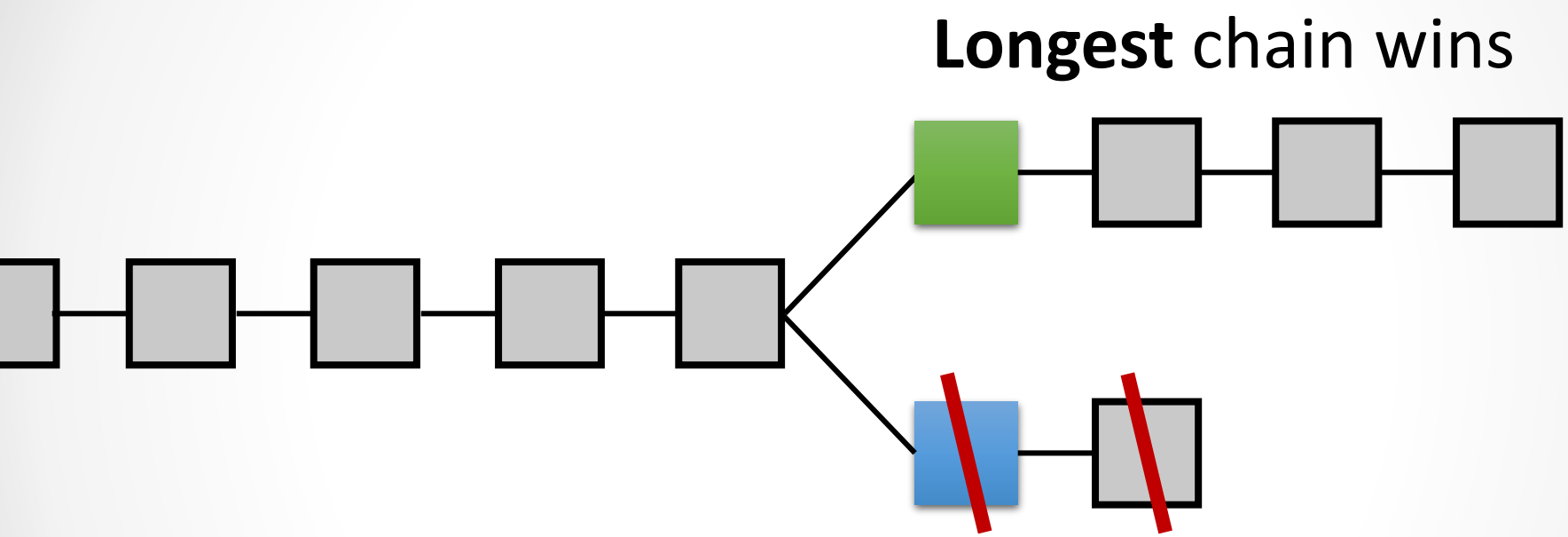
Forks



Forks

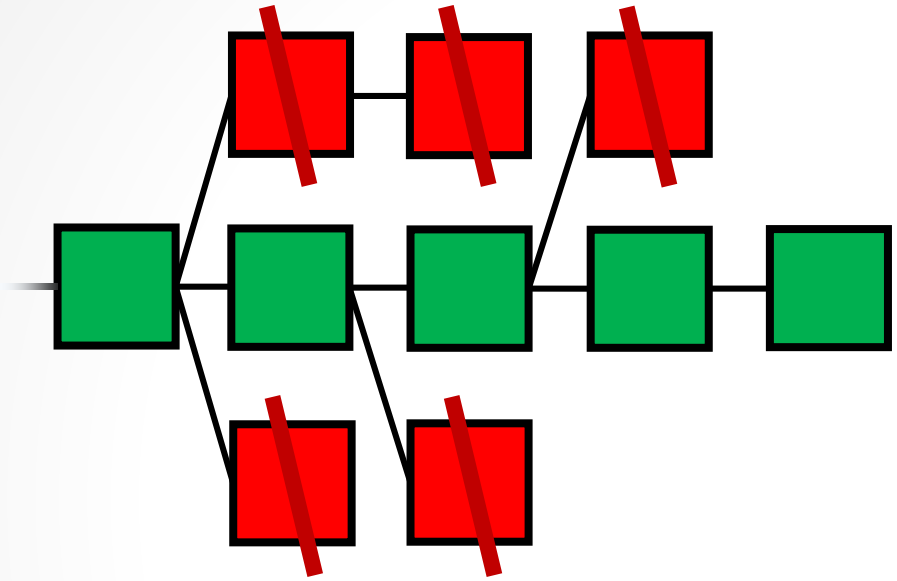


Fork Resolution



Minority attacker cannot out-run honest parties

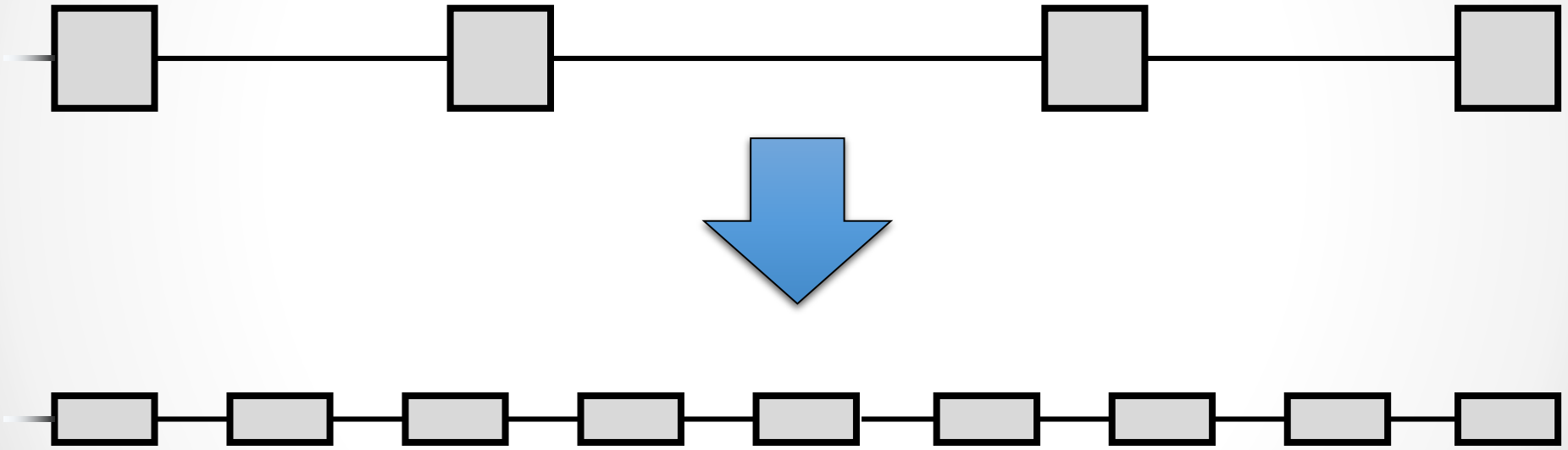
Mining Power Utilization



$$\frac{\sum \blacksquare}{\sum (\blacksquare + \blacksquare)}$$

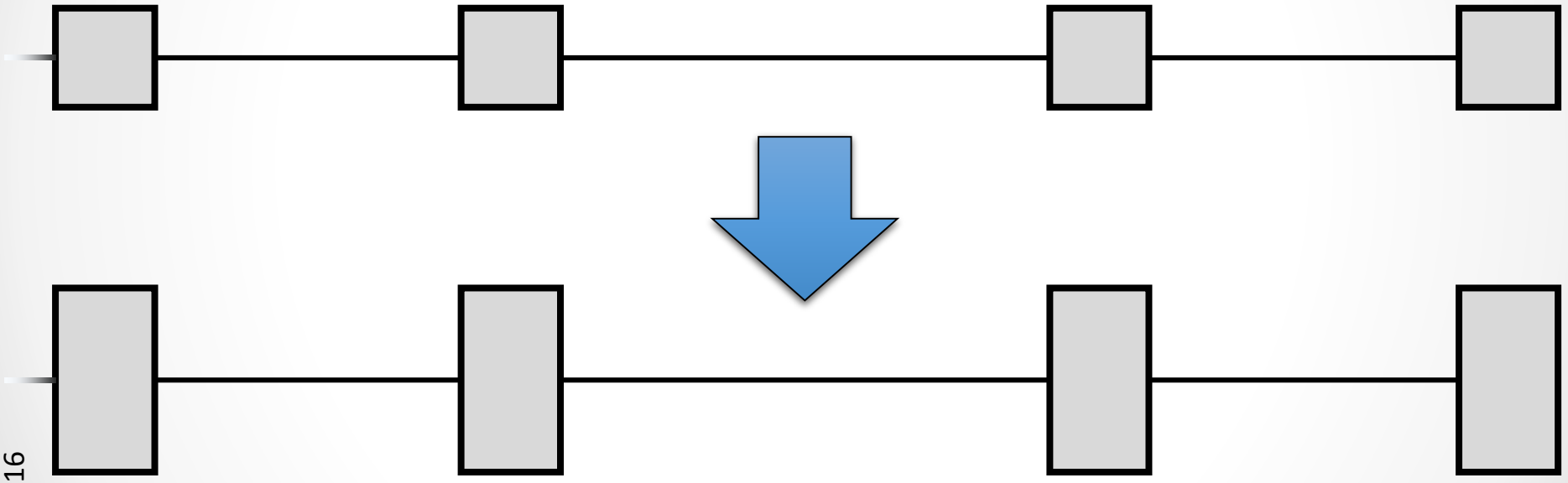
Attacker only has to out-run the main chain

Tune Nakamoto's Performance?



==> More forks ==> worse security

Tune Nakamoto's Performance?

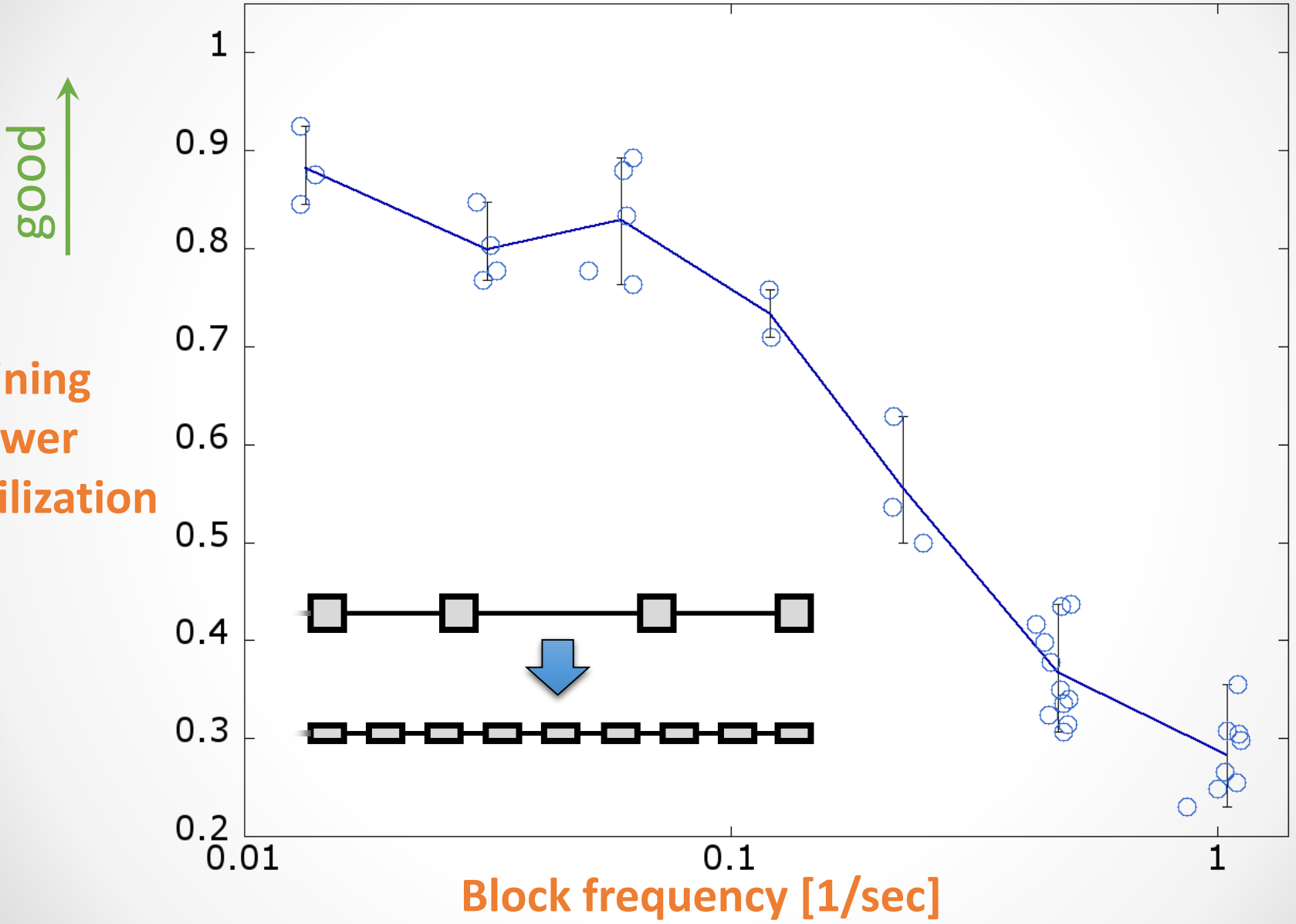


==> More forks ==> worse security

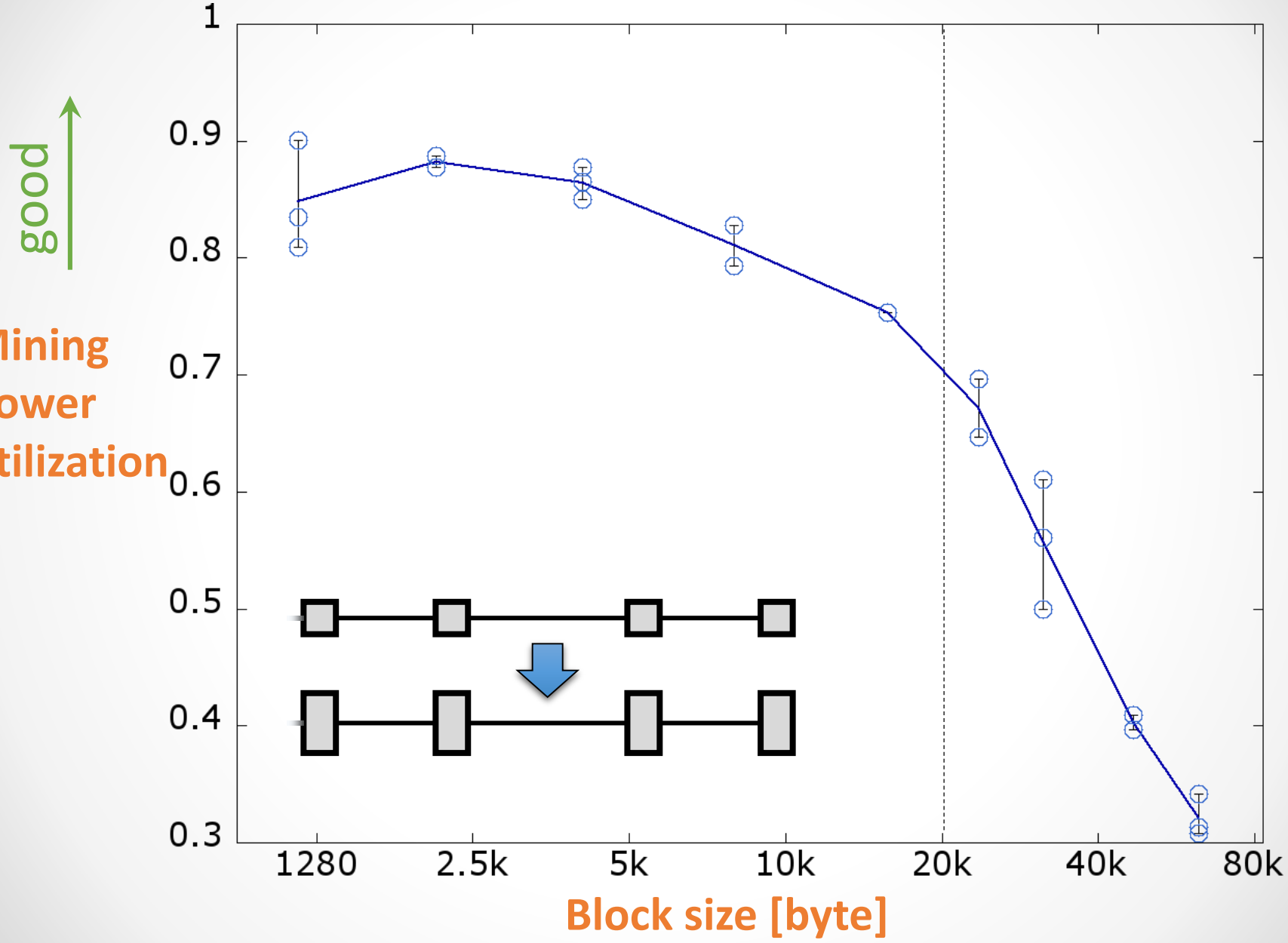
Metrics

- **Bandwidth**
- **Latency**
  - Consensus delay
  - Subjective time to prune
- **Security**
  - Mining power utilization
  - Fairness

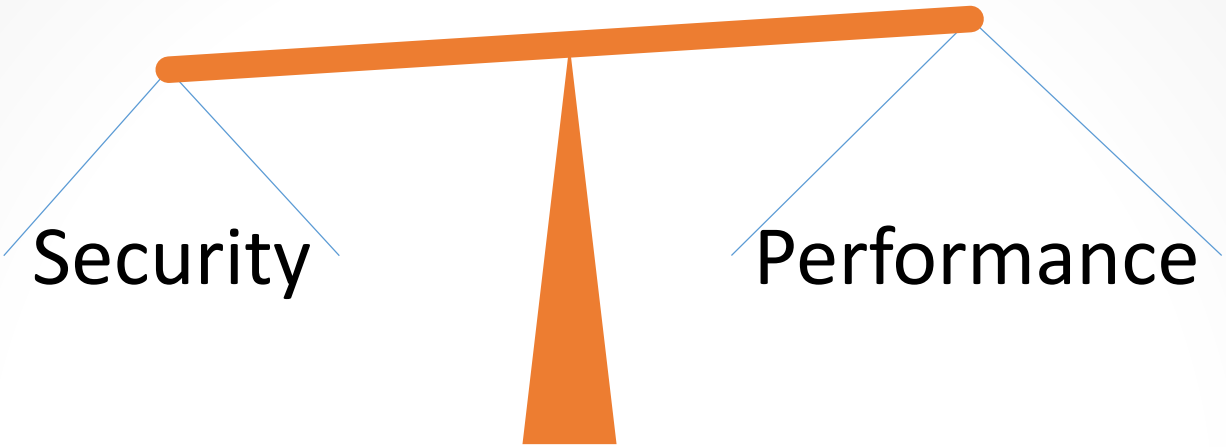
Block Frequency



Block Size


good
Mining Power utilization
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]

Nakamoto's Tradeoff



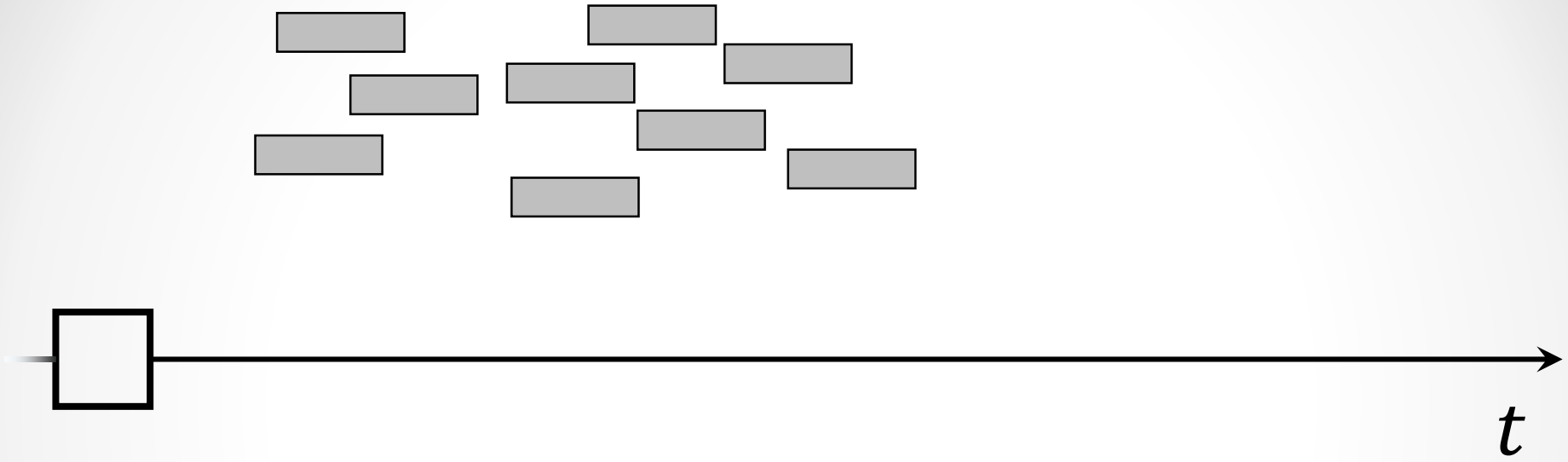
Replicated state machine performance typically bounded by single node performance

What went wrong?

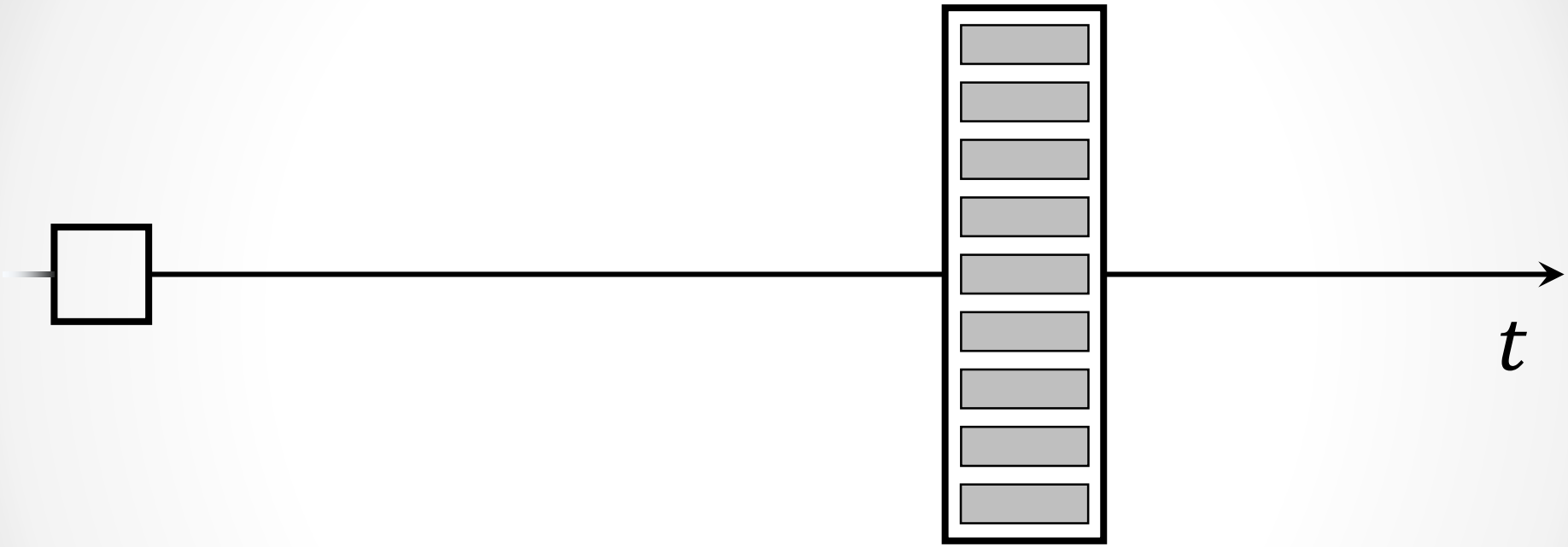
This is not an inherent limit.

- Nakamoto’s performance-security tradeoff
- **Bitcoin-NG**
- Performance experiments
- Demonstration

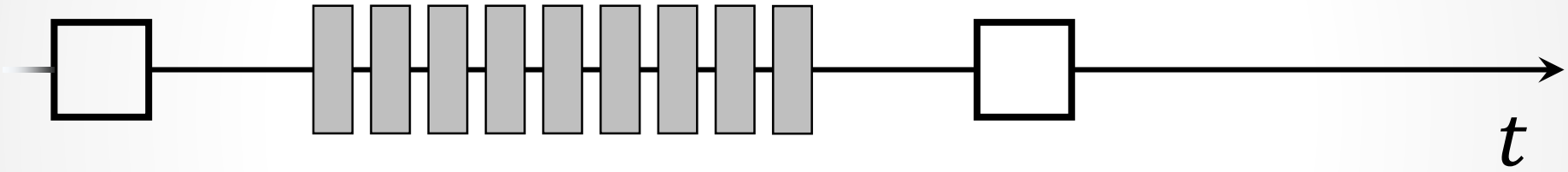
Nakamoto Blocks



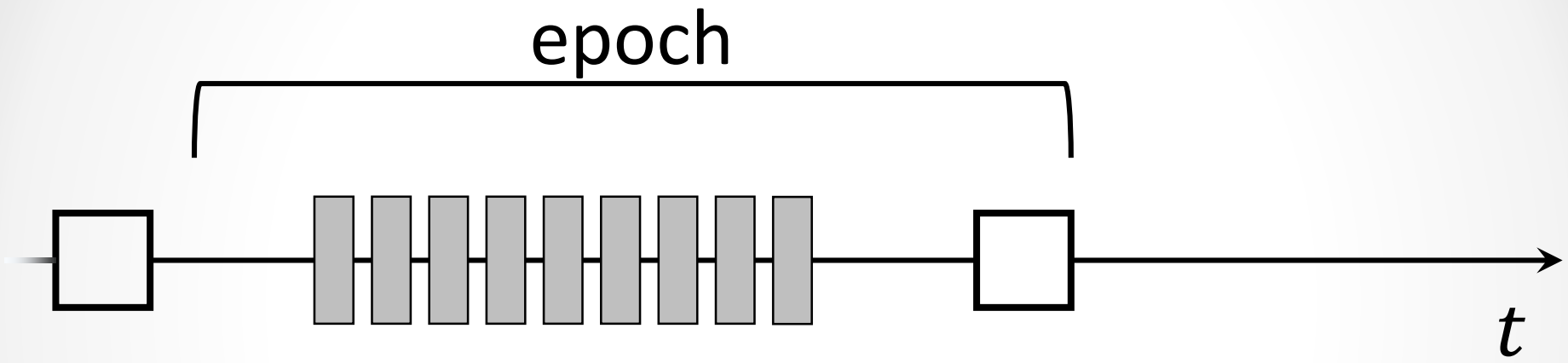
Nakamoto Blocks



Nakamoto Blocks

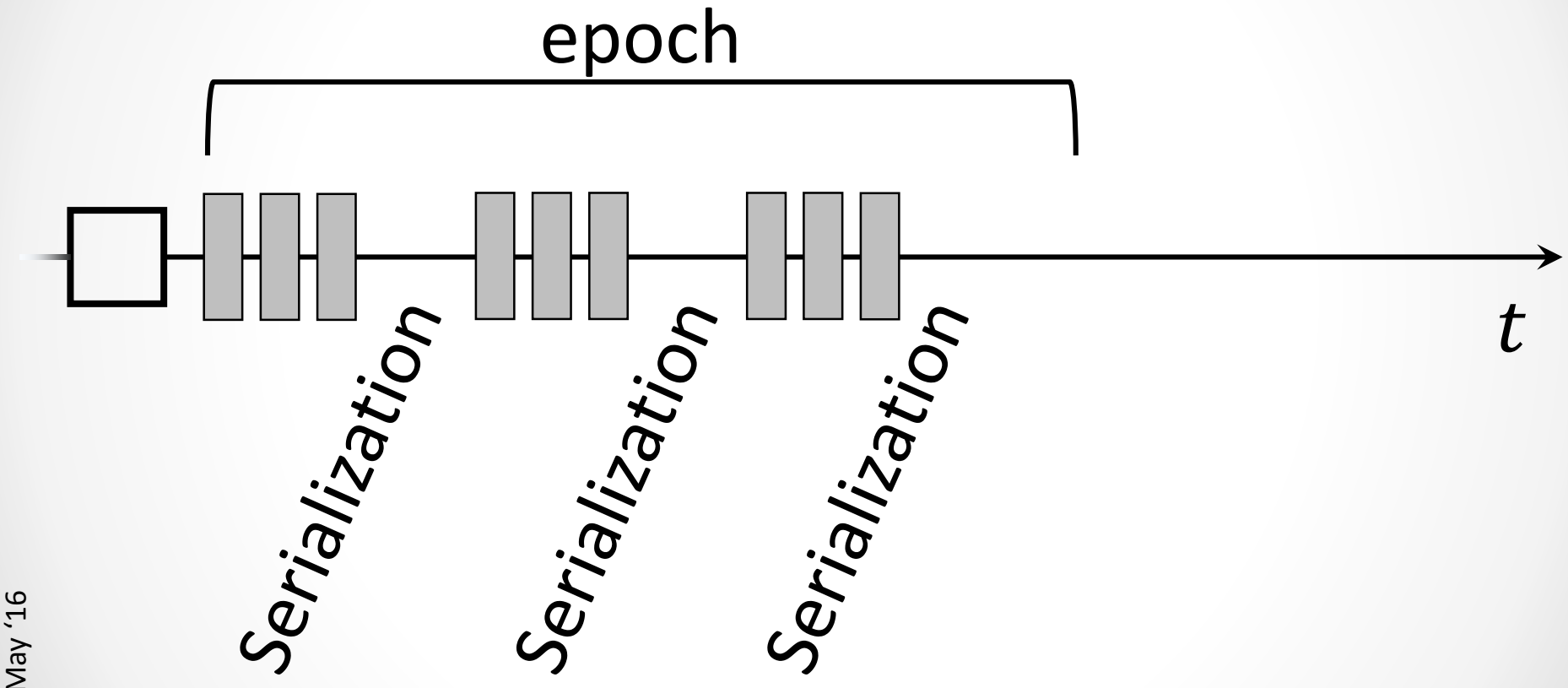


Nakamoto Blocks

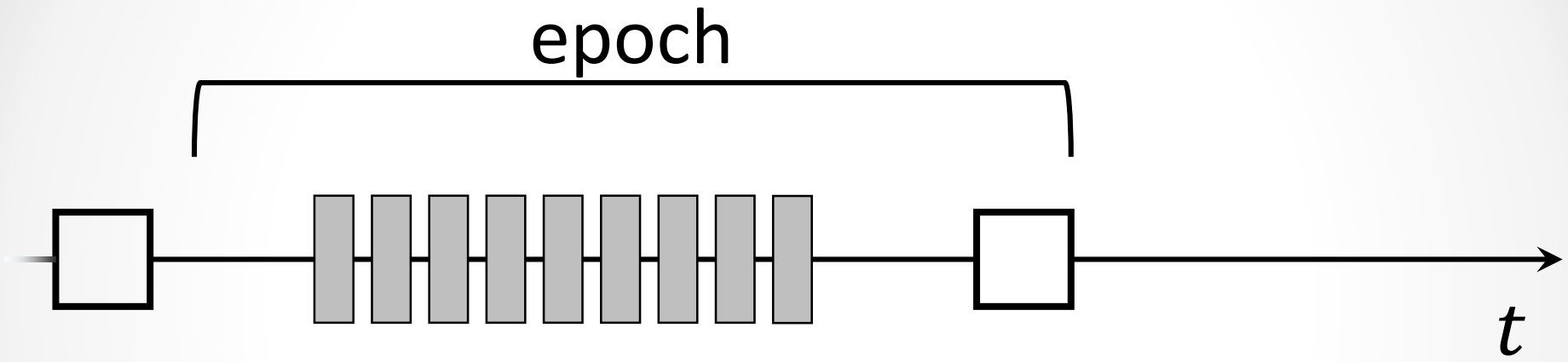


Serialization

Nakamoto Blocks

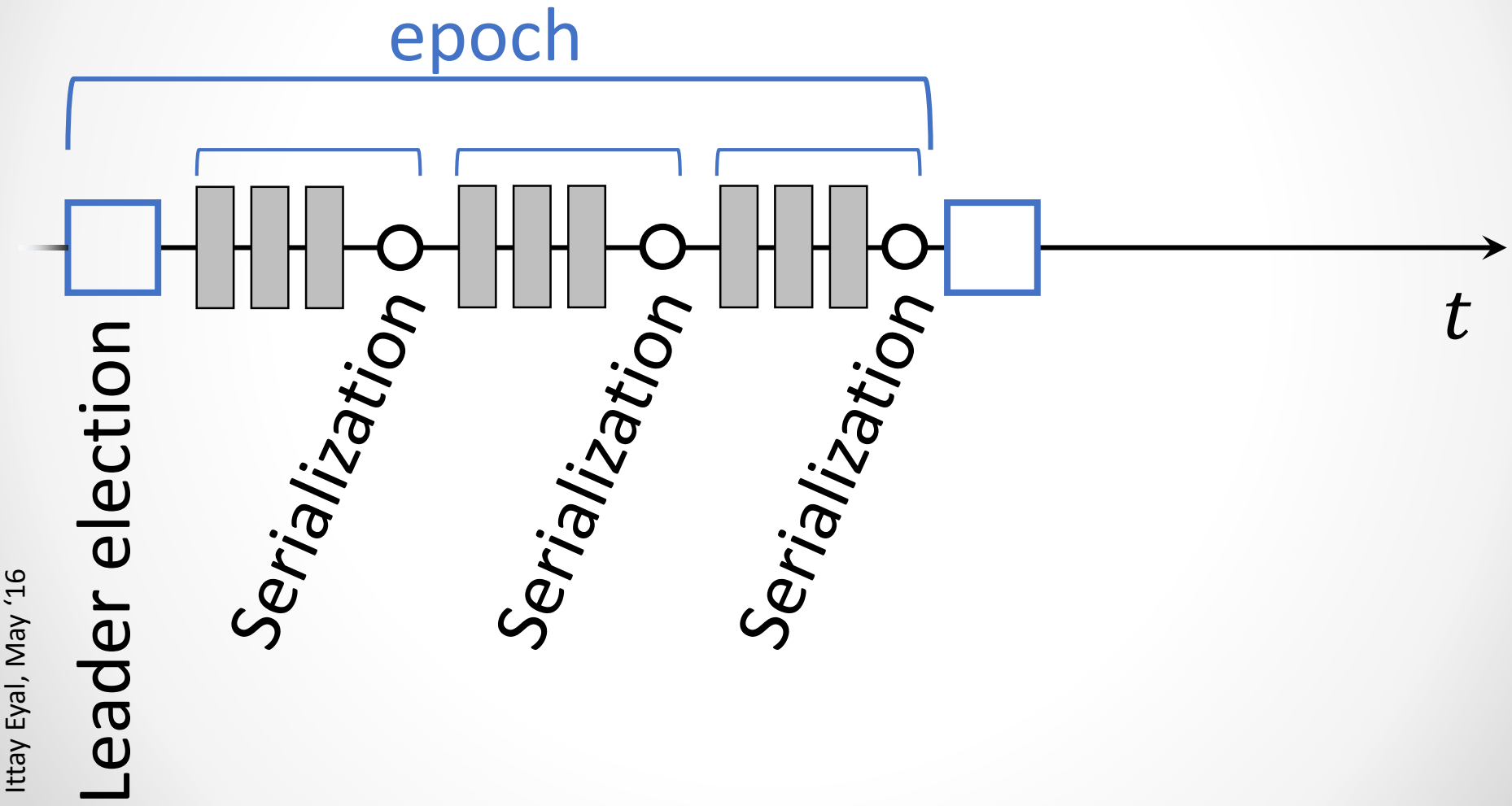


Nakamoto Blocks



1. Leader election
2. Serialization

Bitcoin-NG

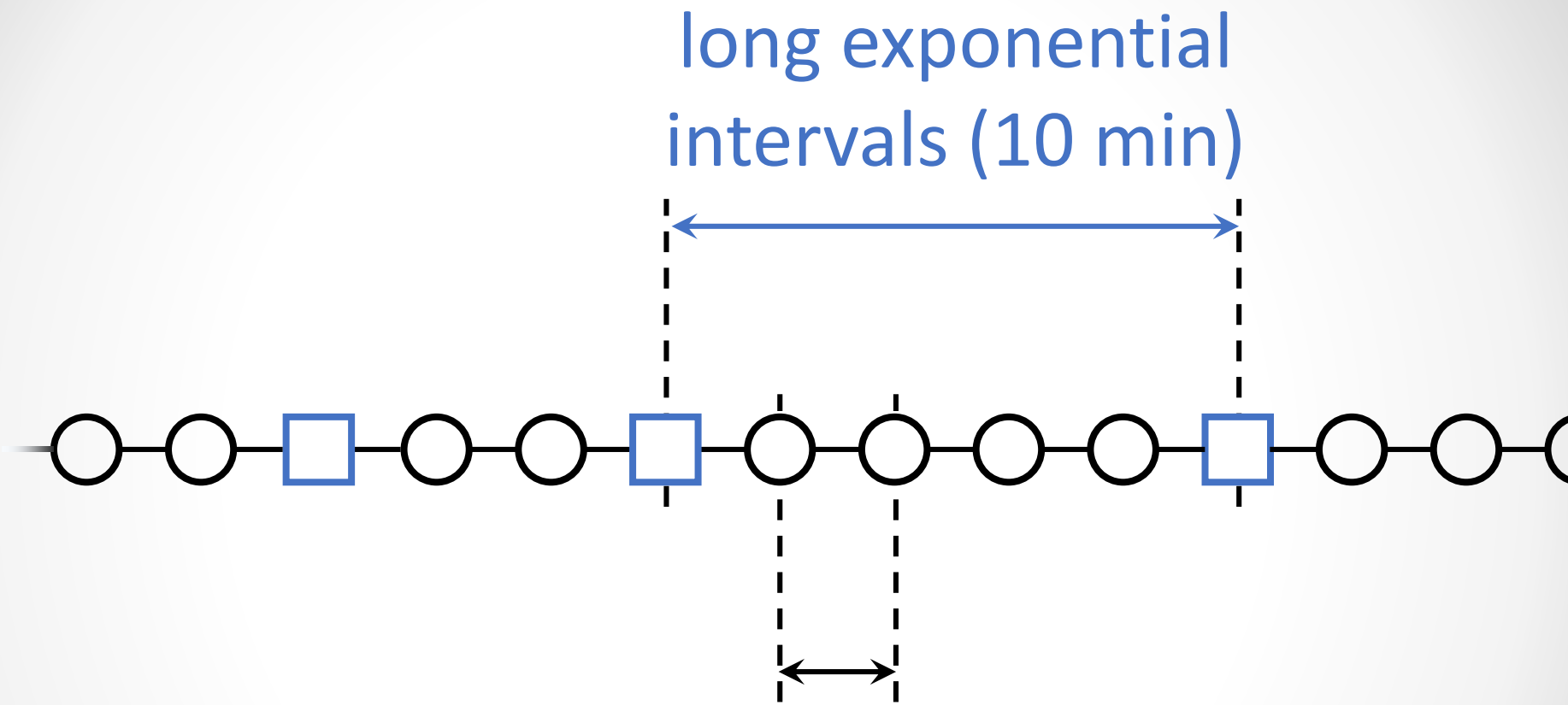

epoch
Leader election
Serialization
Serialization
Serialization
t

Bitcoin-NG

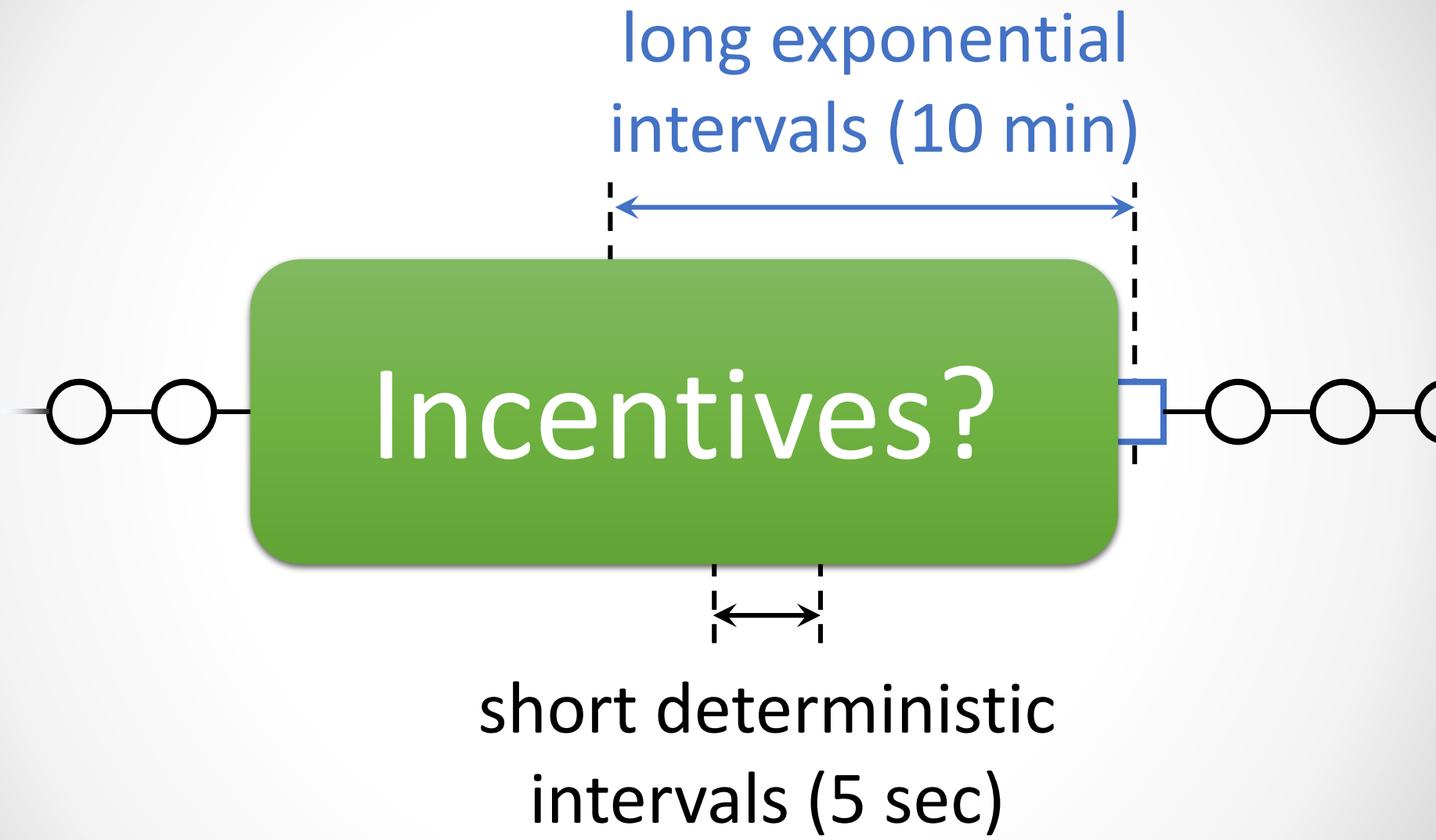
- Key blocks:
  - No content
  - Leader election

- Microblocks:
  - Only content
  - No contention

Bitcoin-NG


long exponential
intervals (10 min)
short deterministic
intervals (5 sec)

Bitcoin-NG


long exponential
intervals (10 min)
Incentives?
short deterministic
intervals (5 sec)

- Nakamoto’s performance-security tradeoff
- Bitcoin-NG
- **Performance experiments**
- Demonstration

Test Bed

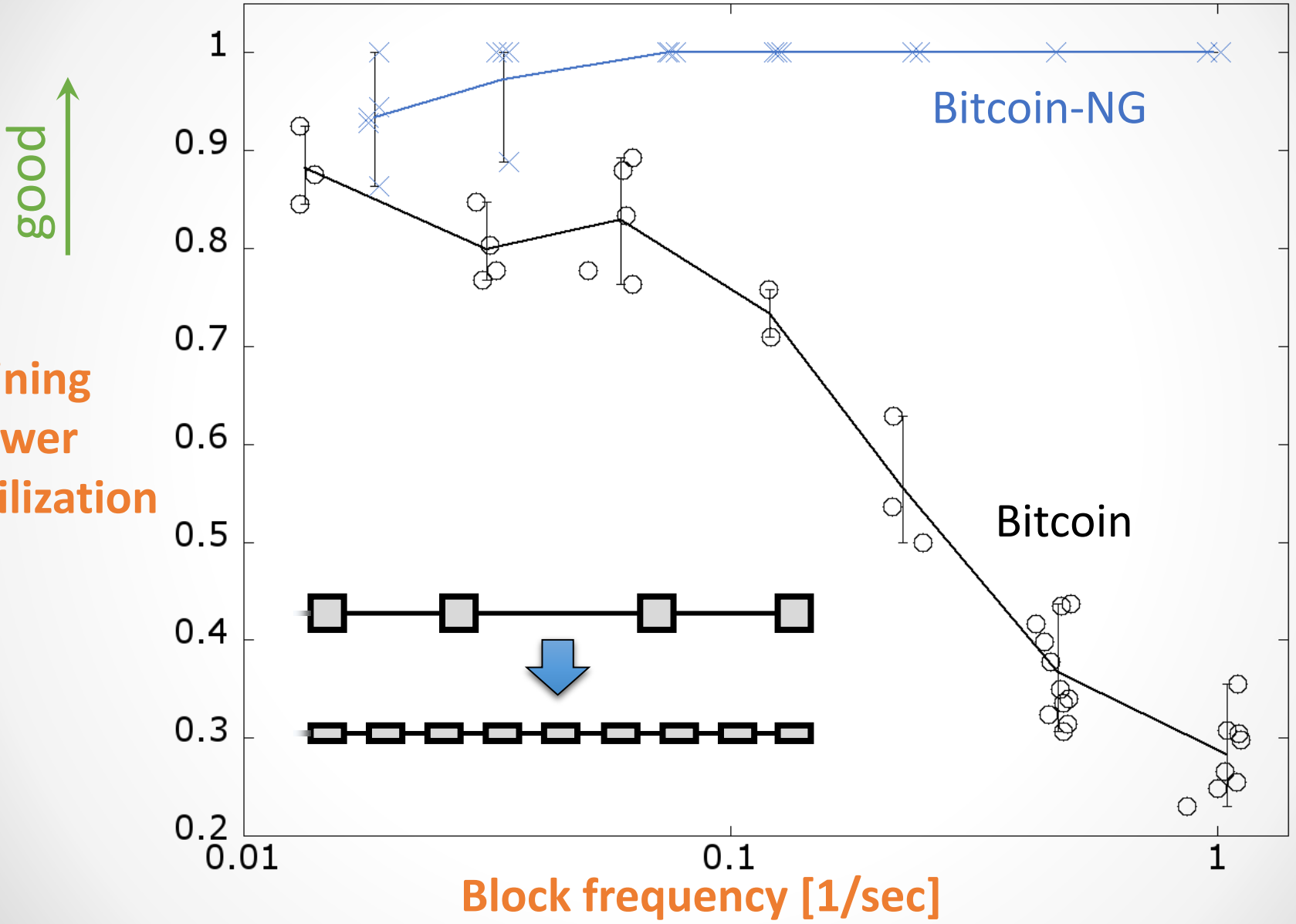
~1000 standard clients

Infrastructure: **150** machines x **7** cores
1Gb network

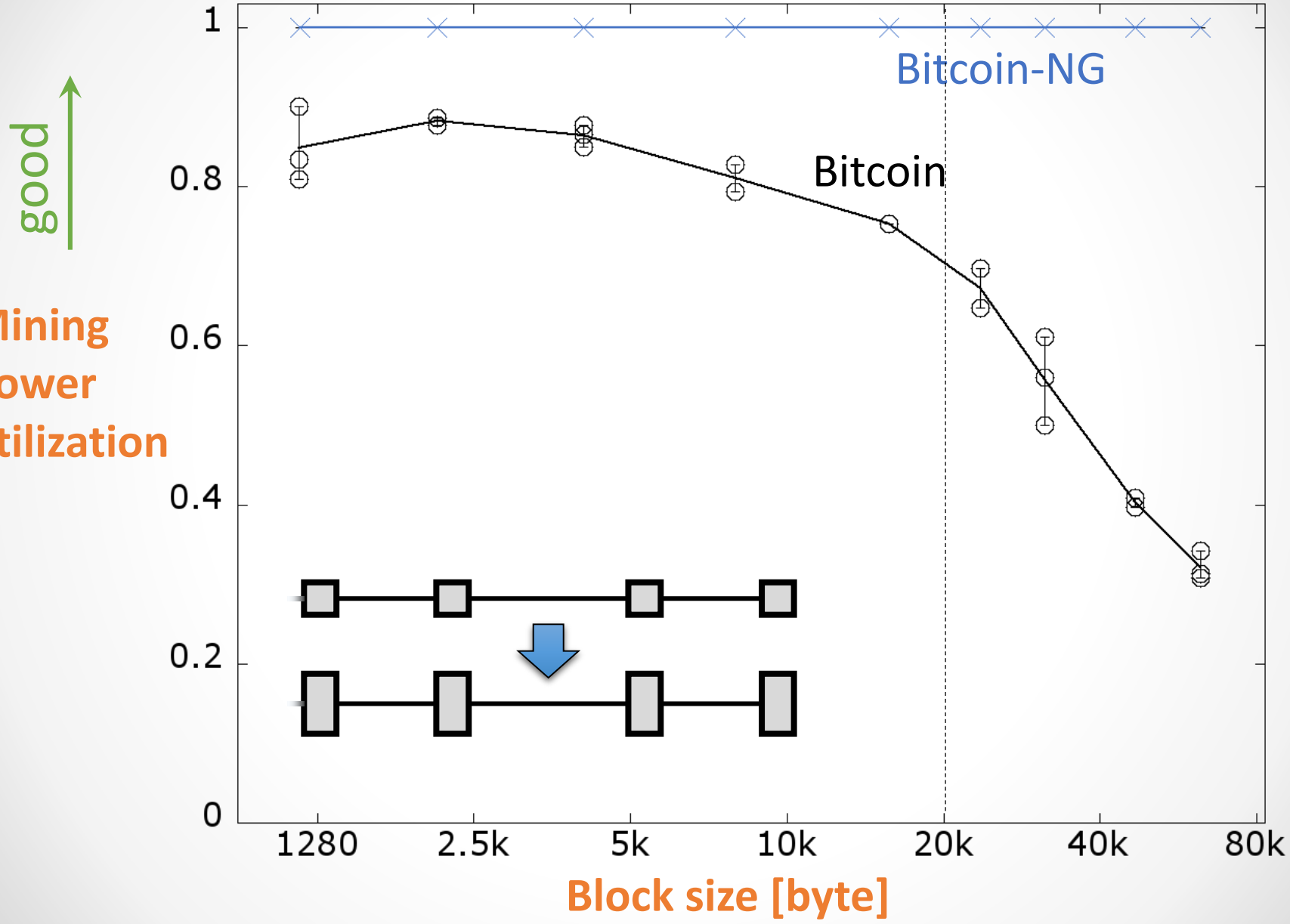
Network, mining: Emulated based on real-world measurements

Validated against known network properties

Block Frequency

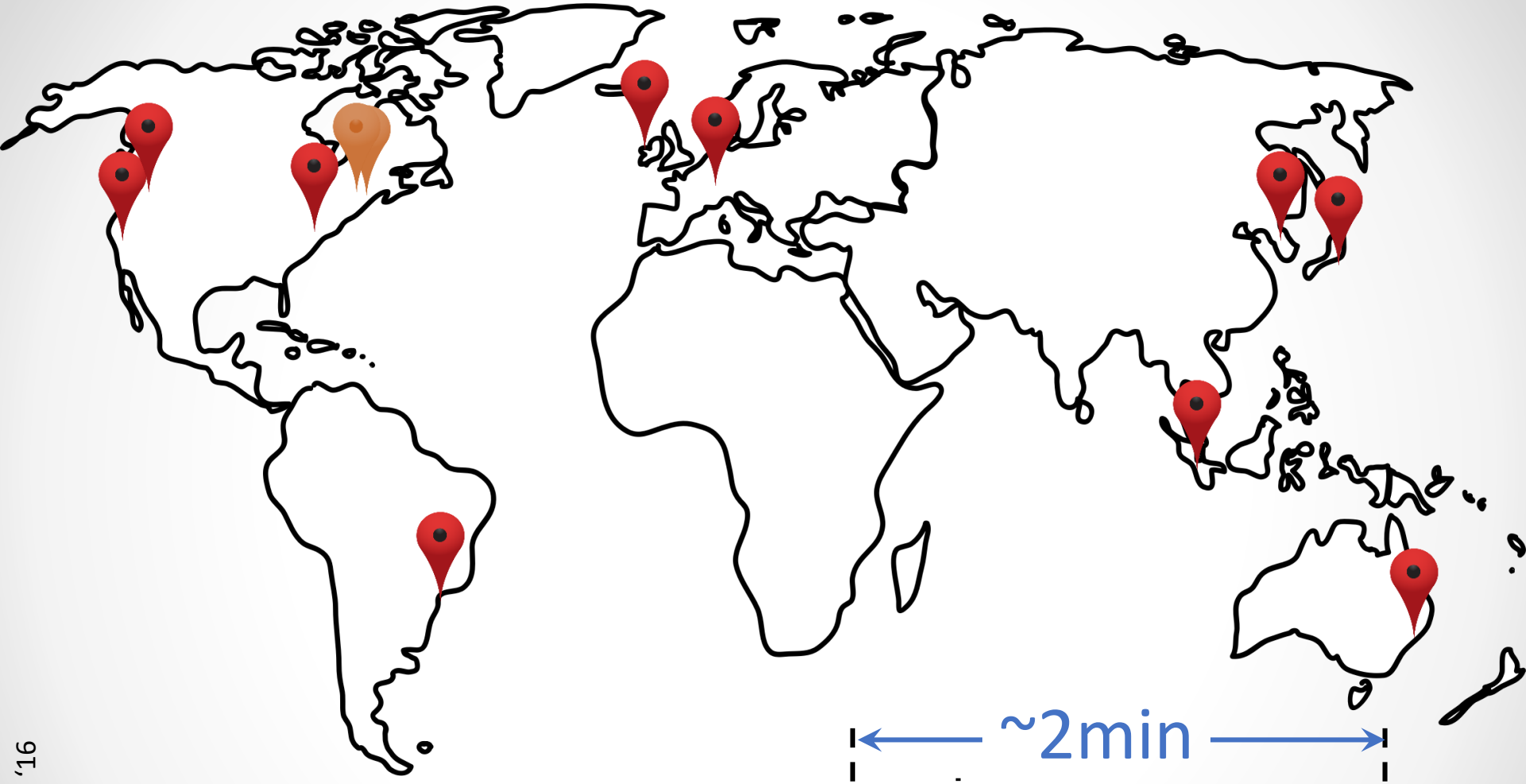


Block Size


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]

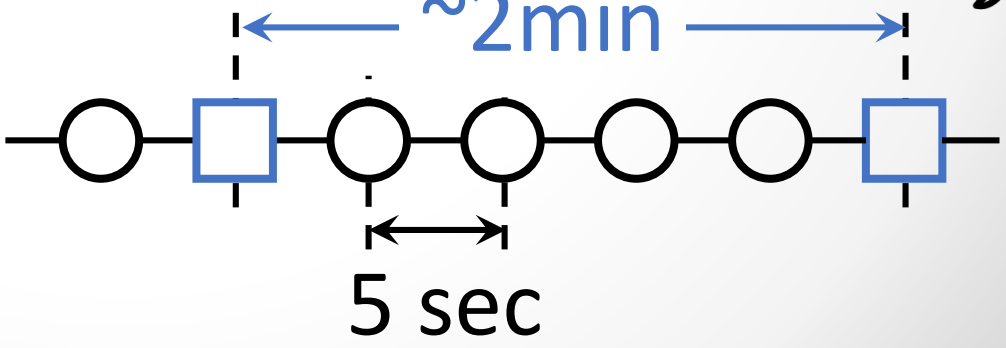
- Nakamoto’s performance-security tradeoff
- Bitcoin-NG
- Performance experiments
- **Demonstration**

Bitcoin-NG Demonstration



Cornell (2)

Amazon EC2 (10)



Related Work

GHOST protocol [SZ15], inclusive blockchains [LSZ15]

Improve censorship resistance.

Might be combined with Bitcoin-NG

Centralized solutions of the BFT consensus family

Classical efficient techniques

Payment channels [DW15, Lightning Network]

Offload to alternative channels

Bitcoin-NG maintains Bitcoin's weak model

Byzcoin, Hybrid Consensus

Use Bitcoin-NG's technique with epoch-length quorums to improve security and latency even further

Conclusion

- Bitcoin-NG – a next-generation blockchain
  - High bandwidth
  - Low latency
  - Maintain Nakamoto's security guarantees
- Measurements on 1000-node test-bed
- Demonstration – quick transactions
- Next up: Beyond single-machine capacity

Ittay Eyal, Adem Efe Gencer, Emin Gun Sirer, and Robbert van Renesse. ***Bitcoin-NG: A Next-Generation Blockchain***. NSDI'16.