Better Consensus In The Bitcoin Model

Prateek Saxena
Computer Science

NUS National University of Singapore | School of Computing

Blockchains: Origin & Today

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.

2008

Top 100 Cryptocurrencies by Market Capitalization

Cryptocurrencies ▾ | Exchanges ▾ | Watchlist | USD ▾ | Next 100 → | View All

#	Name	Market Cap	Price	Volume (24h)	Circulating Supply	Change (24h)	Price Graph (7d)
1	Bitcoin	$59,580,761,374	$3,399.59	$4,939,435,528	17,525,862 BTC	-0.49%	
2	XRP	$12,001,134,334	$0.291508	$356,976,506	41,169,202,069 XRP *	-0.25%	
3	Ethereum	$10,974,571,873	$104.75	$2,280,623,059	104,766,118 ETH	-0.48%	
4	EOS	$2,126,001,619	$2.35	$472,575,374	906,245,118 EOS *	-0.64%	
5	Bitcoin Cash	$2,041,982,753	$115.96	$198,734,194	17,609,650 BCH	0.05%	
6	Tether	$2,026,509,895	$1.00	$3,511,890,558	2,021,103,317 USDT *	0.10%	
7	Litecoin	$2,000,776,268	$33.14	$636,413,250	60,369,927 LTC	0.12%	
8	TRON	$1,712,362,099	$0.025684	$136,340,725	66,671,422,606 TRX	-0.61%	
9	Stellar	$1,422,240,776	$0.074196	$114,737,113	19,168,570,823 XLM *	0.28%	
10	Binance Coin	$1,101,770,088	$7.80	$84,783,682	141,175,490 BNB *	-4.79%	
11	Bitcoin SV	$1,091,169,120	$61.97	$83,503,727	17,608,711 BSV	-1.61%	
12	Cardano	$940,904,576	$0.036290	$12,298,410	25,927,070,538 ADA *	-0.51%	
13	Monero	$727,519,153	$43.36	$46,156,605	16,777,423 XMR	0.27%	

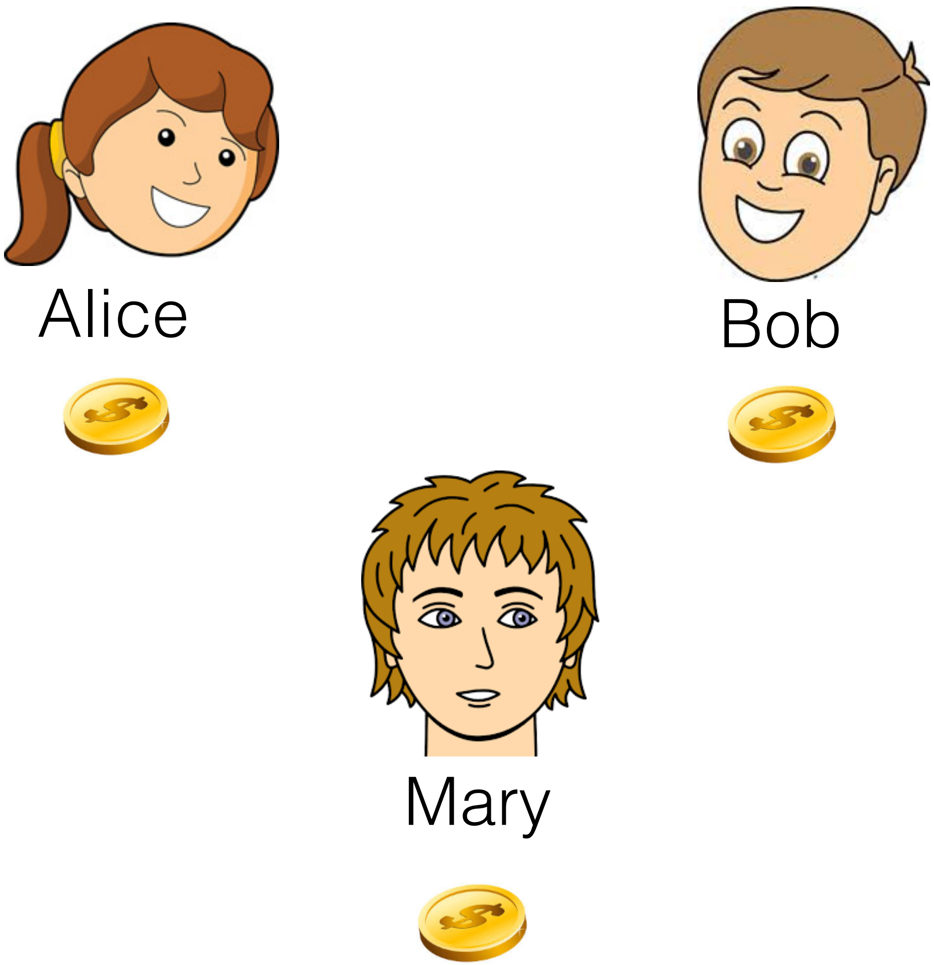
2019

A New Model of Trust

- Basis For Trust In Prior Systems:
  - Blind Faith / Assumption
  - Reputation
  - Incentives
  - Regulation

- A New Model: Self-regulation
  - Anyone can audit the operations
  - (Extremely) High Availability
  - No permission needed, no centralized coordinator

Application: Self-regulating Currency



TX-1: Bob -> Mary
TX-2: Alice -> Mary

TX-1: Alice -> Bob
TX-2: Bob -> Mary

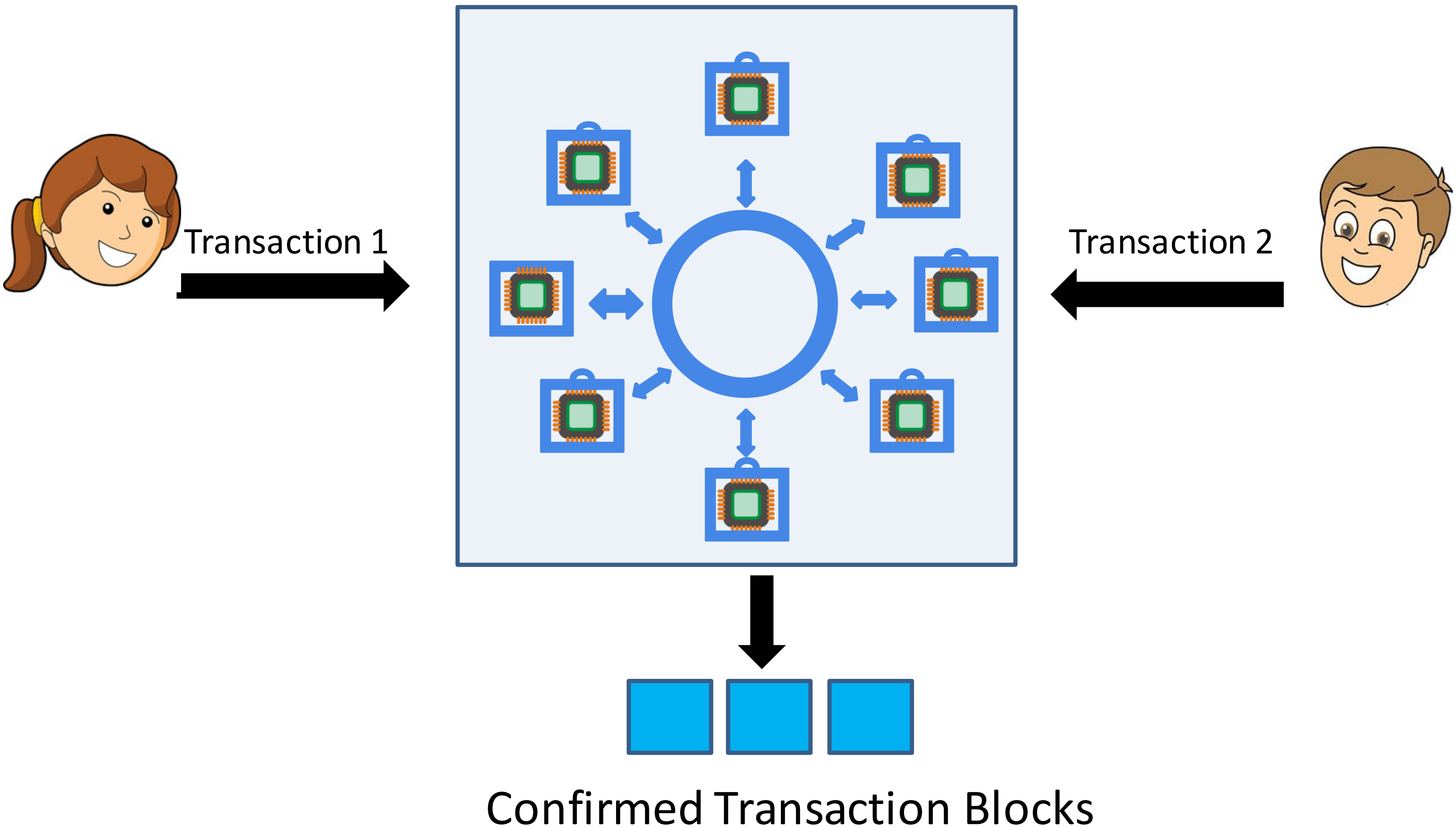
TX-1: Alice -> Bob
TX-2: Alice -> Mary

↑

Double-spending

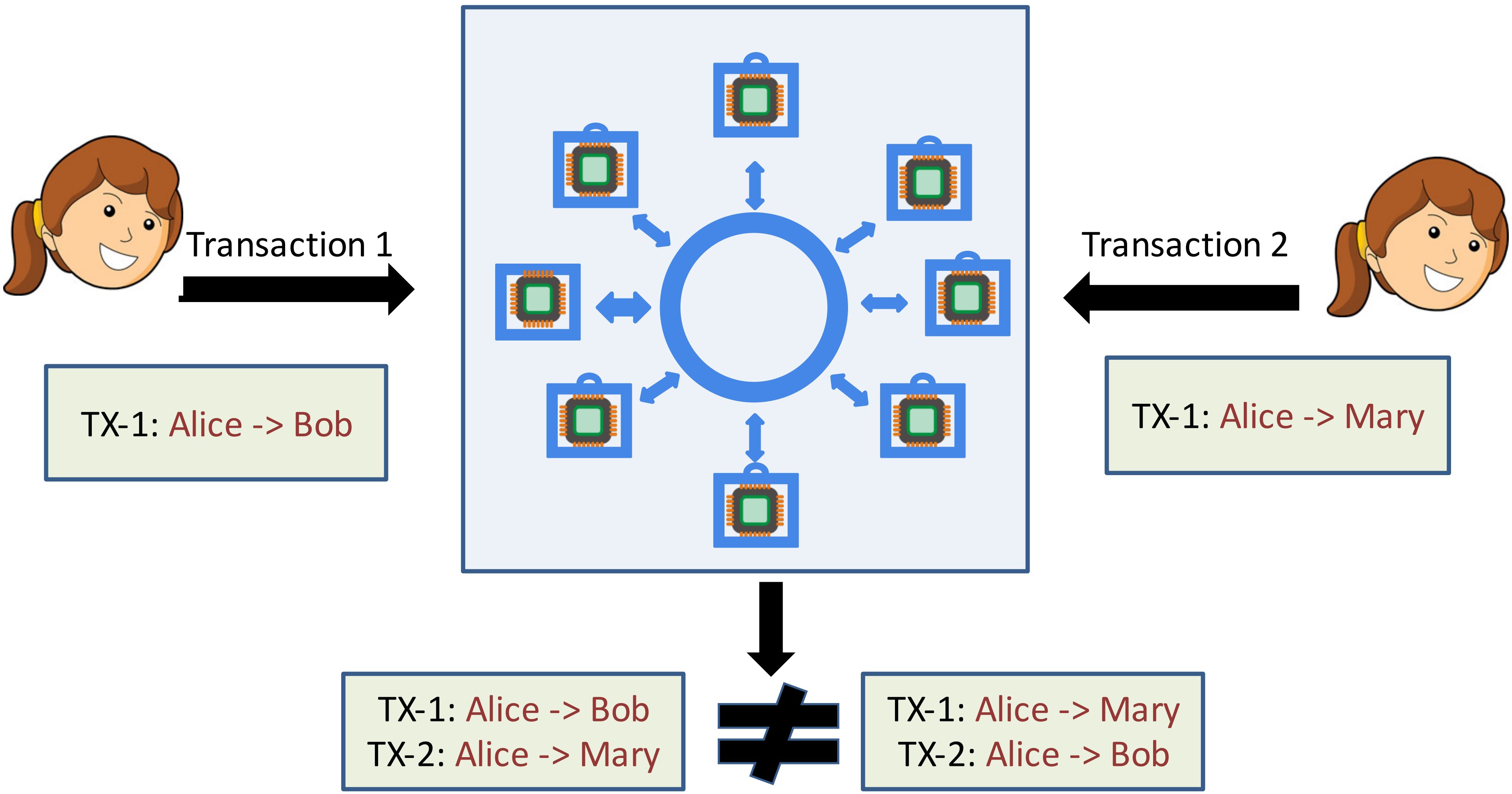
The Blockchain Consensus Problem

The Problem



Transaction 1
Transaction 2
Confirmed Transaction Blocks

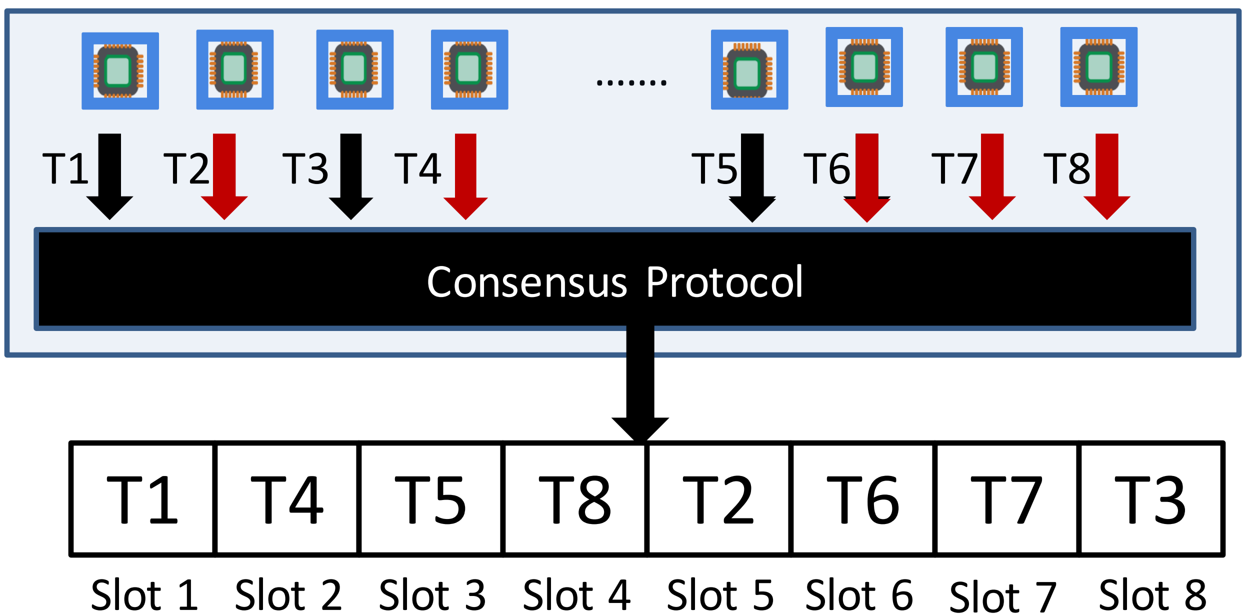
Key Challenge:
Agreement over Transaction Ordering



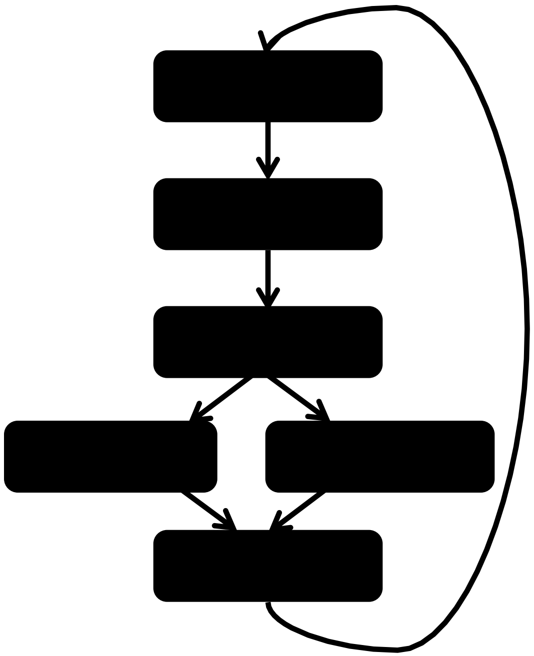
Ordering Transactions is sufficient to prevent double-spends!

Why Total Order?

- Replicated State Machines *[Lamport84, Schnieder90]*
  - Useful for backups, snapshots, distributed locks, …
  - A sequence of commands transition from state to state

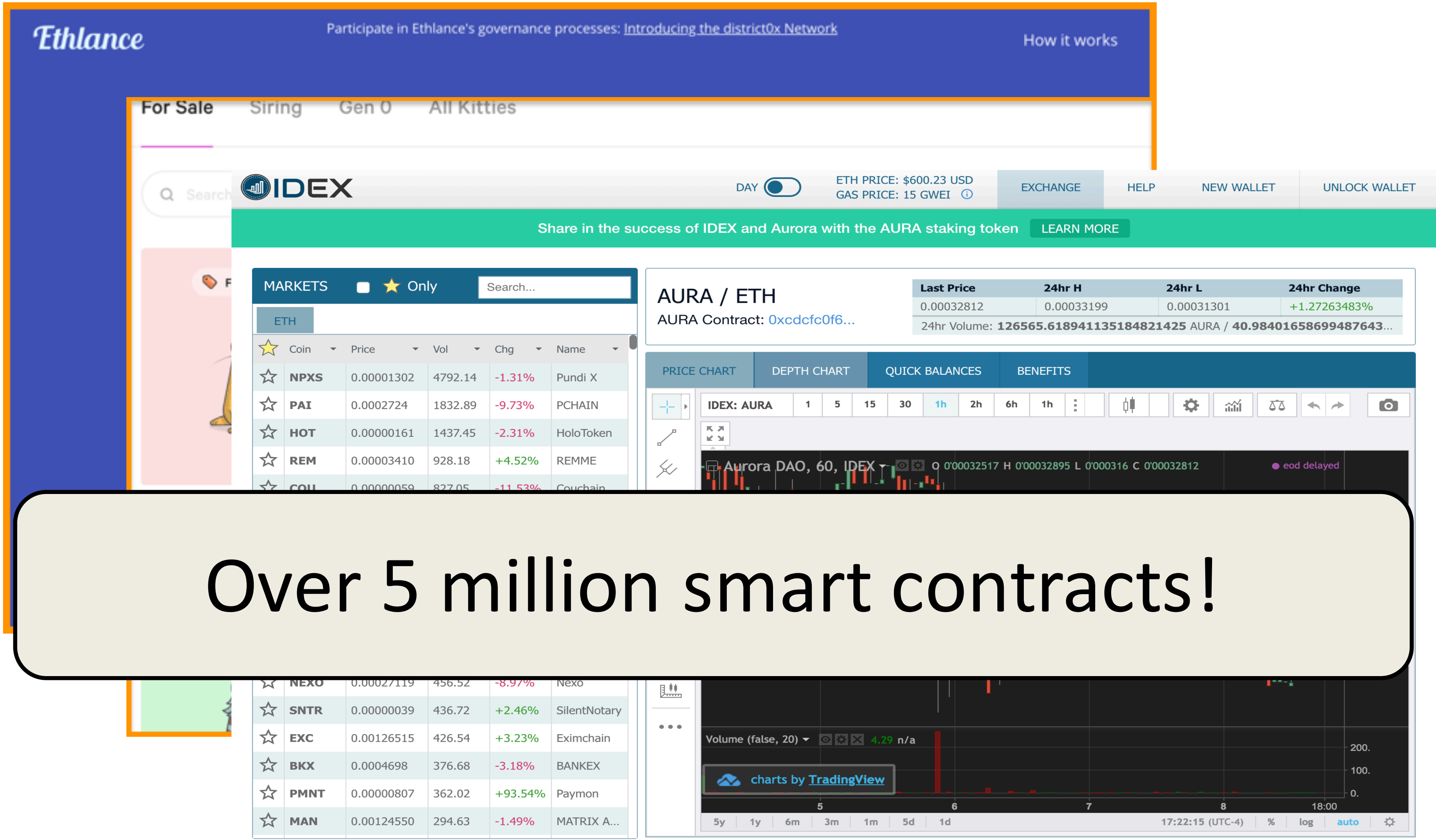


Replicated Log



Deterministic State Machine

Enables General-Purpose Computing



Over 5 million smart contracts!

The Bitcoin Security Model

- Assumptions:
  - A trusted "genesis" block
  - No pre-established identities, joining is **permissionless**
  - A fraction "f" (< ½) of the computational power is malicious
  - Network is synchronous (Blocks transmitted within some delay)
- Security Properties:
  - **Safety:** Nothing bad happens
    - **Stability:** A block once confirmed can't be changed
    - **Agreement:** All miners order blocks same way
  - **Liveness:** Honest blocks are accepted eventually
  - **Fairness:** Your confirmed blocks are proportional to your computational power

Bitcoin's Solution: Nakamoto Consensus

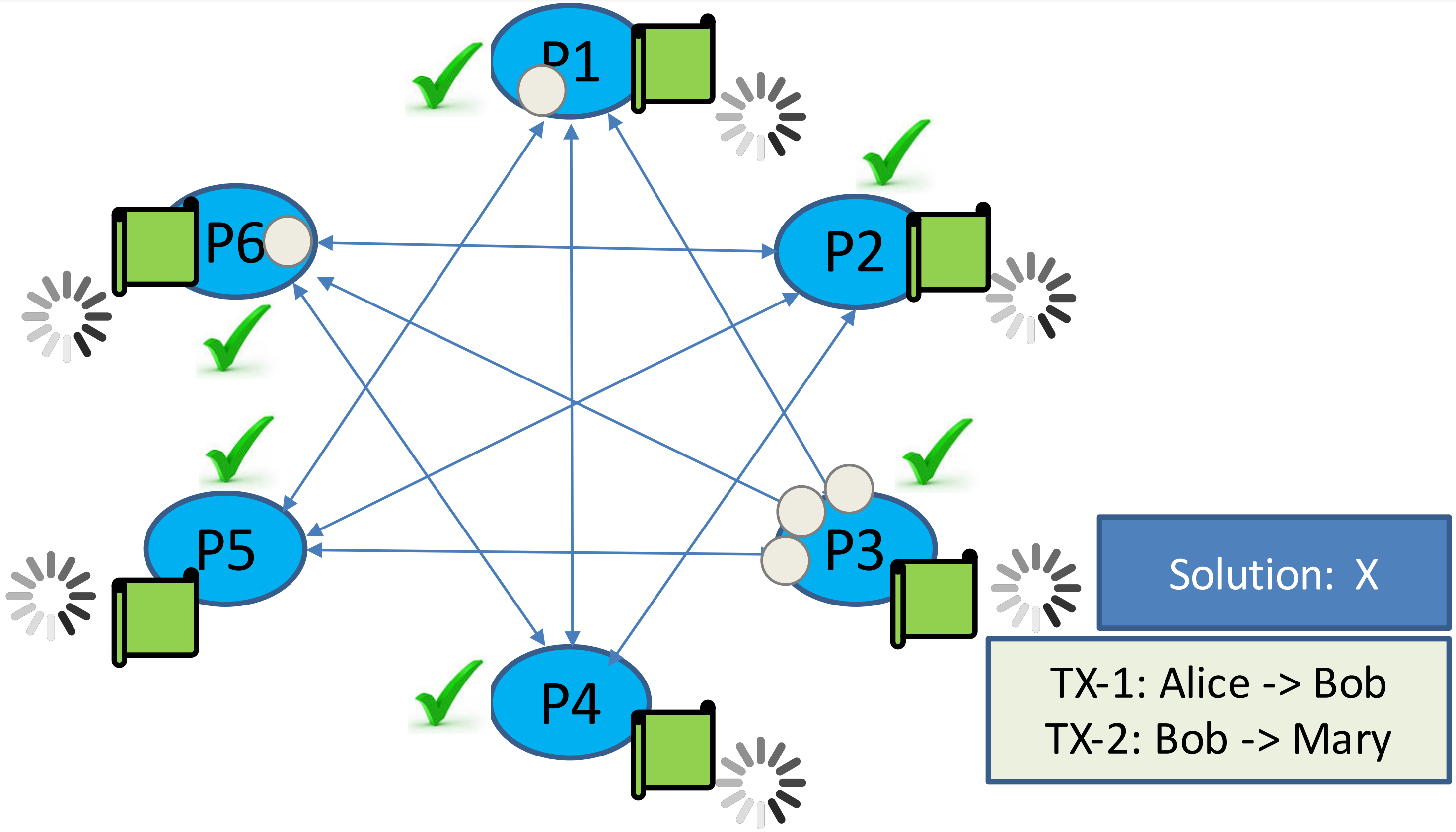
Nakamoto Consensus Protocol

- Miners keep a local copy of the blockchain
- Miners solve a computational Proof-of-Work puzzle:

- **H**(**s** || last_block_hash || new_block) < **d**

- Successful miners (usually <u>one</u>) broadcast solution
- Miners check the received solutions, and if valid:
  – Extend their chain's last block with that block
- Confirm block on the <u>longest chain</u> after it is k-deep
    - Bitcoin proposes k = 6

Nakamoto Consensus: Overview



PoW solver (block founder) is a **leader**. Everyone accepts his solution, if valid.

- We didn't know how many computers connected, yet we elected one block!
- Miners only select **valid** blocks per round

Problems with Nakamoto Consensus: **Poor Throughput**

bitcoin

- 2-4 Kilobytes / second
- 6-12 TXs per second
- 3-60 minutes latency

ethereum

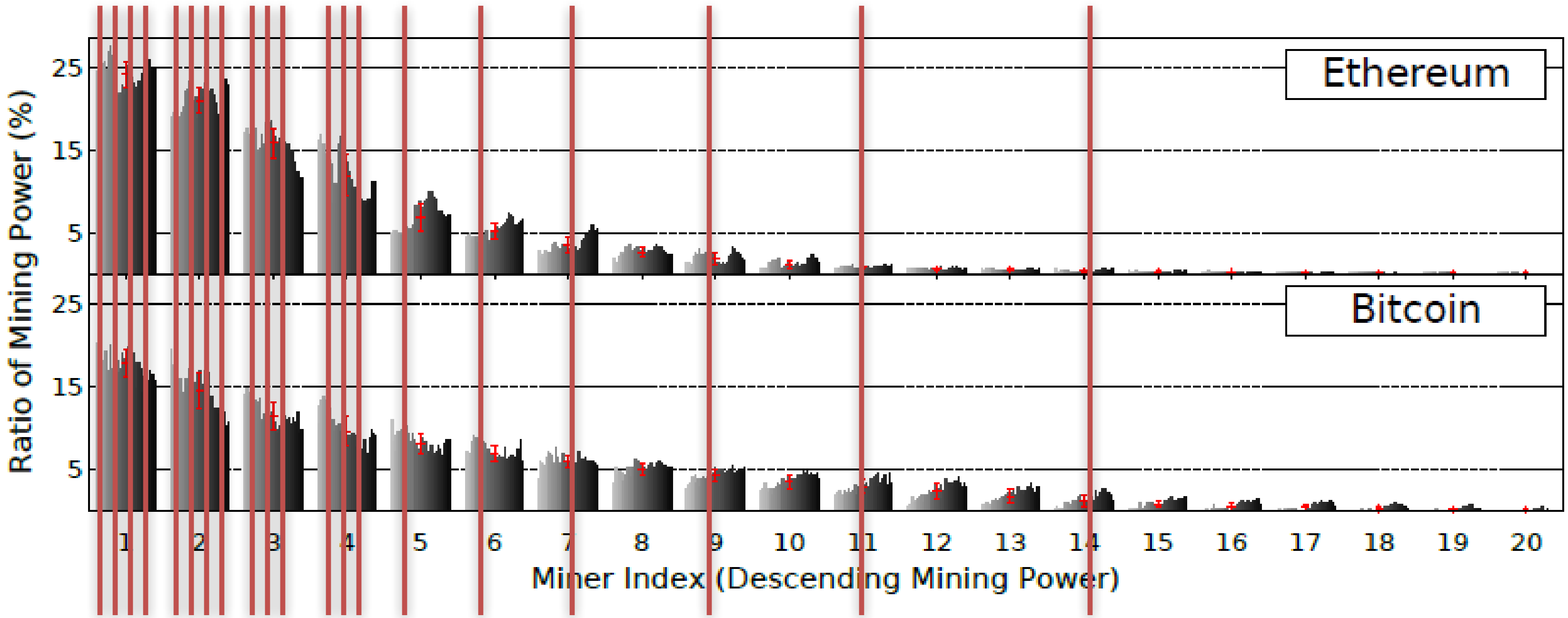
- Support limited computations
- Outages and Unavailability
- A cryptoKitties app clogged the entire network

Demand from Practice: 1,200 - 50,000 TXs/s

PayPal VISA MasterCard

Poor Decentralization

- In anonymous, permissionless setup
  - Mining concentration reflects “real” wealth distribution

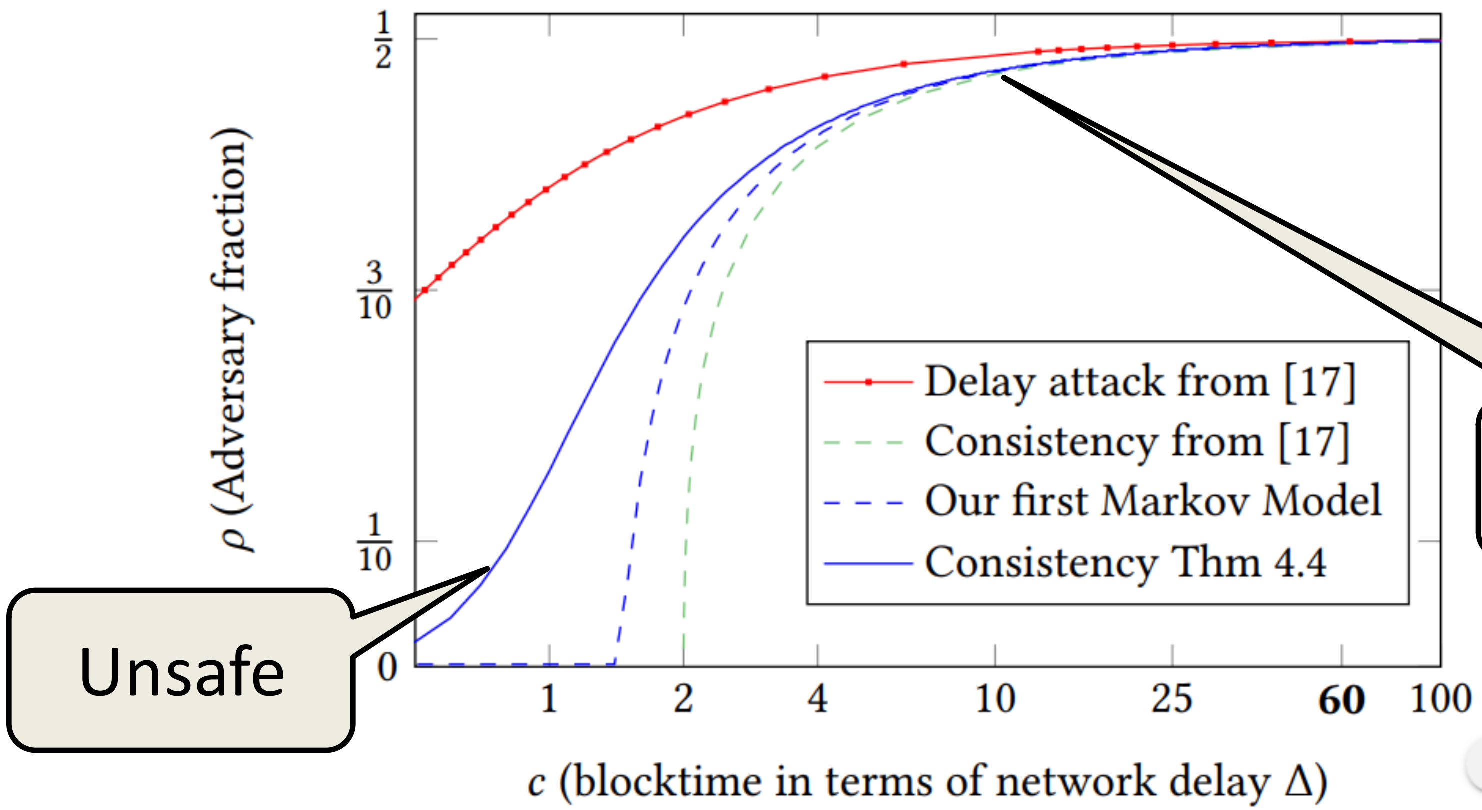


- Goal of decentralization: Maximize block miners/sec
- Optimal Decentralization is $\Theta(\beta)$, where β is bandwidth

[Decentralization in Bitcoin and Ethereum Networks – Gencer et. al.]

Problems with Nakamoto Consensus: **Resilience Reduces with Decentralization**

- For Nakamoto consensus,
  - **Resilience** (f) is "near-optimal" at blk. interval > 3Δ

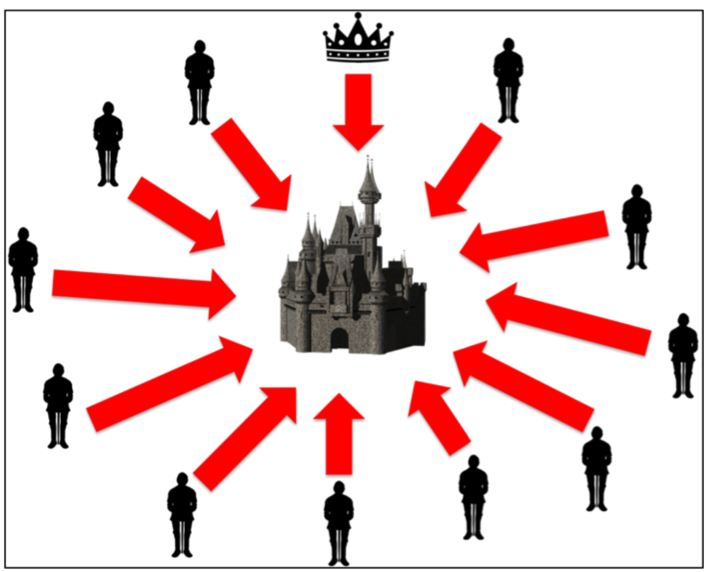


A Better Method to Analyze Blockchain Consistency" – KRS'18. (Also see GK'15, GKL'17, PSS'17)

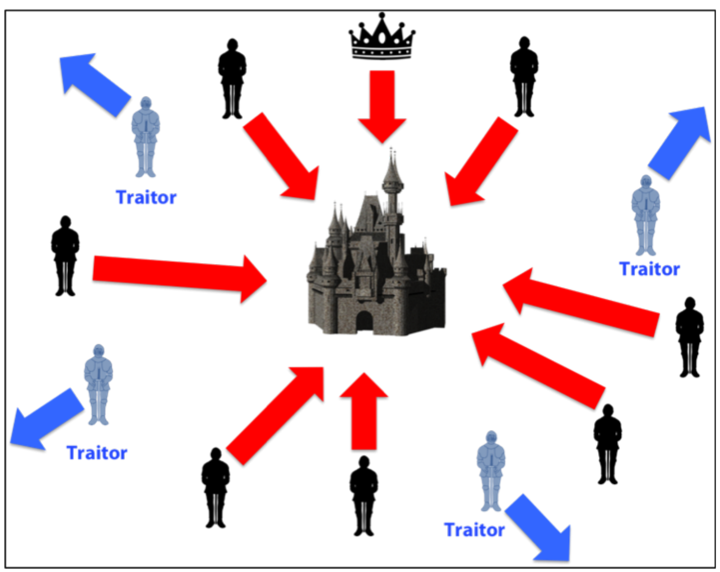
Can We Do Better?

Classical Byzantine Agreement (BA)

- Byzantine Agreement Problem (Lamport et al. 82):
  - A set of parties {P1, P2, ... Pn} have inputs
  - A fraction **f** out of **n** are malicious, i.e., Byzantine
  - Goals:
    - Ensure that all honest parties **agree on the same** value
    - The agreed value is **valid**, i.e. input of some honest node



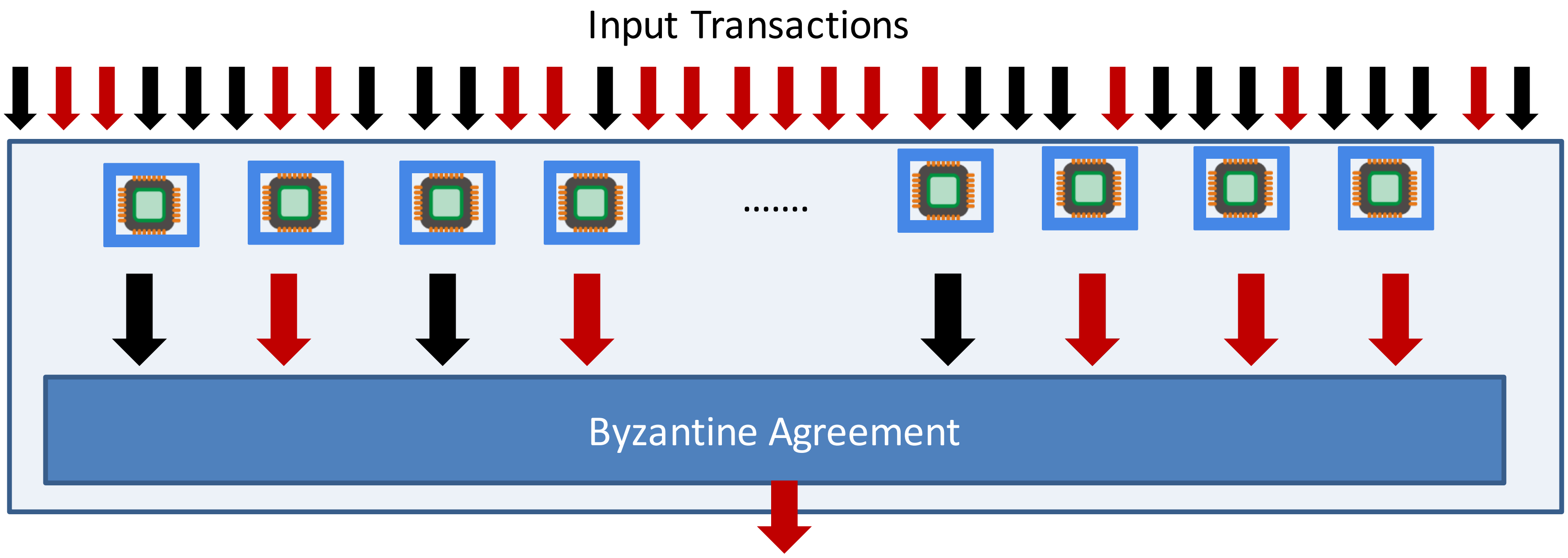
Coordinated Attack Leading to Victory



Uncoordinated Attack Leading to Defeat

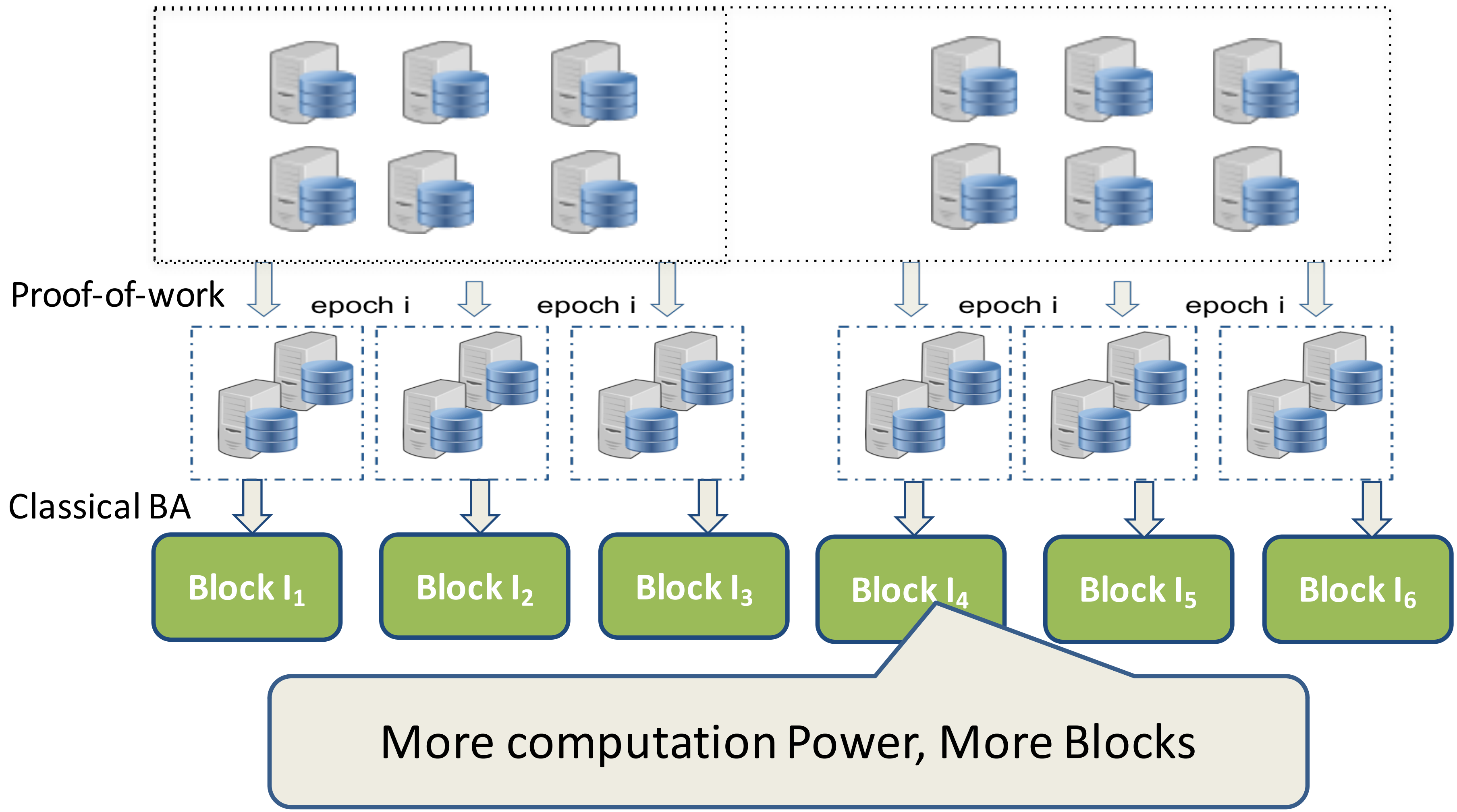
Repurposing BA Protocols?

- Yes, repeated rounds of BA
- Agree on 1 block per round
- Honest miners sign that block with round id.



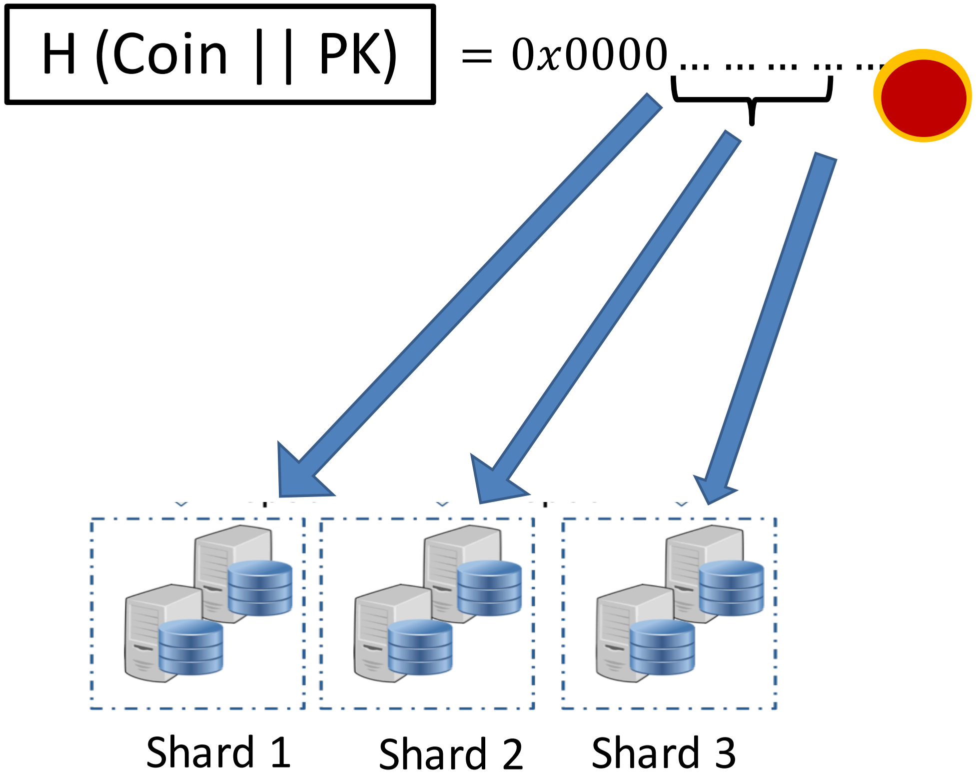
- Challenge: Participants must be <u>known a-priori</u>
  – Chicken-n-egg: Agreeing on participants is itself…

The Concept: Blockchain Sharding



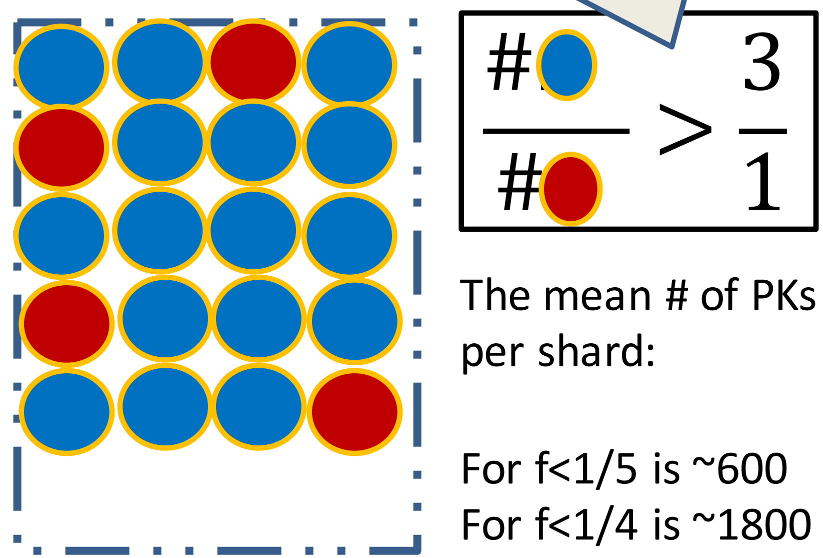
Elastico – CCS'16

How to do it Securely?



The identity "PK" is assigned to corresponding shard

For safety of the classic BA



The mean # of PKs per shard:

For f<1/5 is ~600
For f<1/4 is ~1800

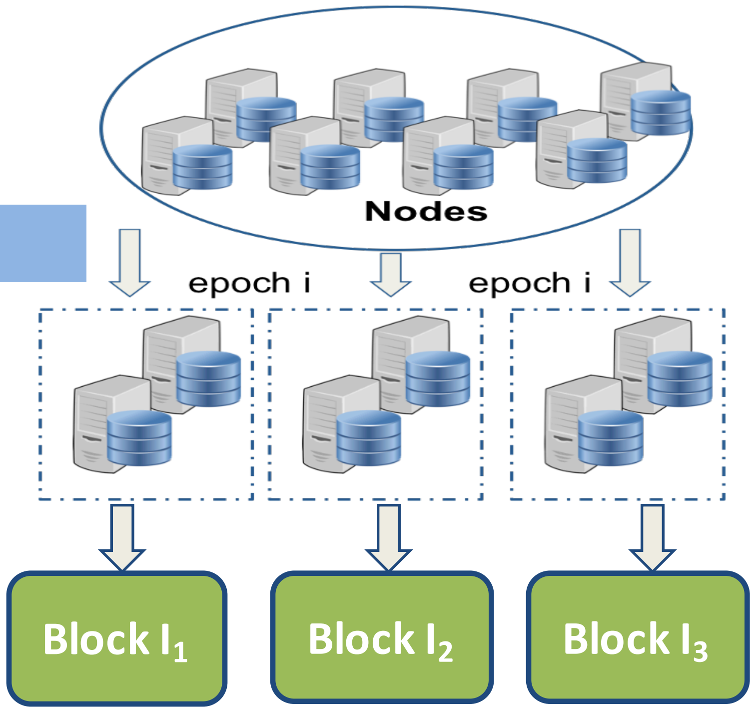
Elastico – CCS'16 (Also see Omniledger – Oakland'18, RapidChain-CCS'18)

Sharding: A Straw-man Solution

H (Coin || PK)

Run BFT Protocols

Broadcast all blocks



Assumptions

A known list of nodes joining simultaneously

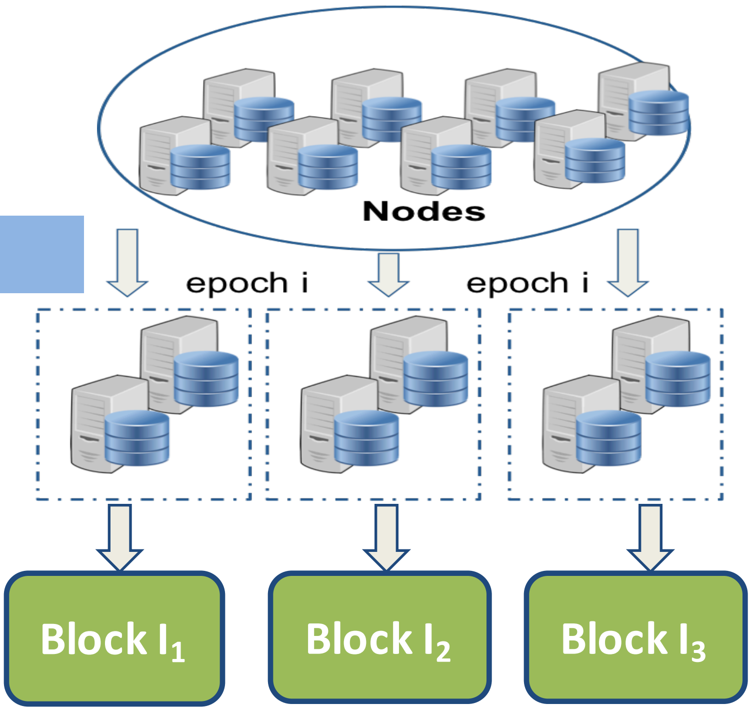
Common random coin

Improvements over the Basic Solution

H (Coin || PK)

Run BFT Protocols

Broadcast all blocks



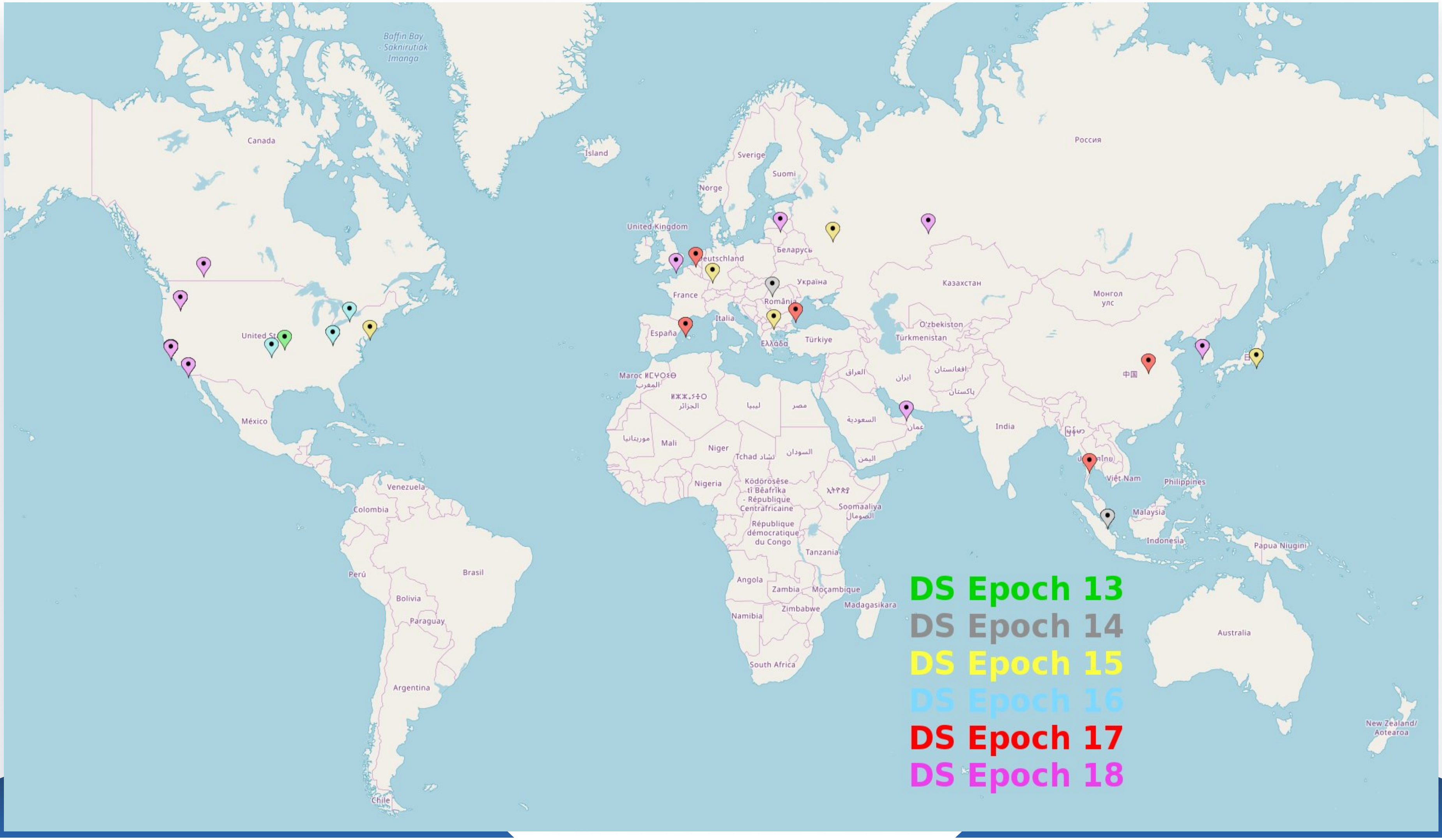
Additional Considerations

- $O(N^2)$ -> $O(NC)$ messages to broadcast hash values, using a dedicated shard that runs BA
- $O(C^2)$ messages for BFT protocols, which can be optimized with signature aggregation
- Generating a shared common coin each round, without excessive bias
- Minimize the size of broadcast data to pipeline BA and block verification

Elastico – CCS'16 (Some improvements in the Zilliqa whitepaper)

Commercialized as the Zilliqa public blockchain platform

Open to public mining (Feb 2019)



Security vs. Performance: State-of-the-art

Approach	Resilience	Throughput	Decentralization	Latency
Nakamoto with reduced block intervals	$f < \frac{1}{3}$	Low	Medium	Good
Nakamoto with large blocks	$f < \frac{1}{2}$	High	Low	Medium
AlgoRand (with BA) [SOSP'17]	$f < \frac{1}{5}$	High	Low	Good
Sharding (with BA) [CCS'16, S&P'18,CCS'18]	$\mathbf{f < \frac{1}{3}}$	**High**	**Medium**	**Good**

~1-3 proposers per sec

~30 sec.

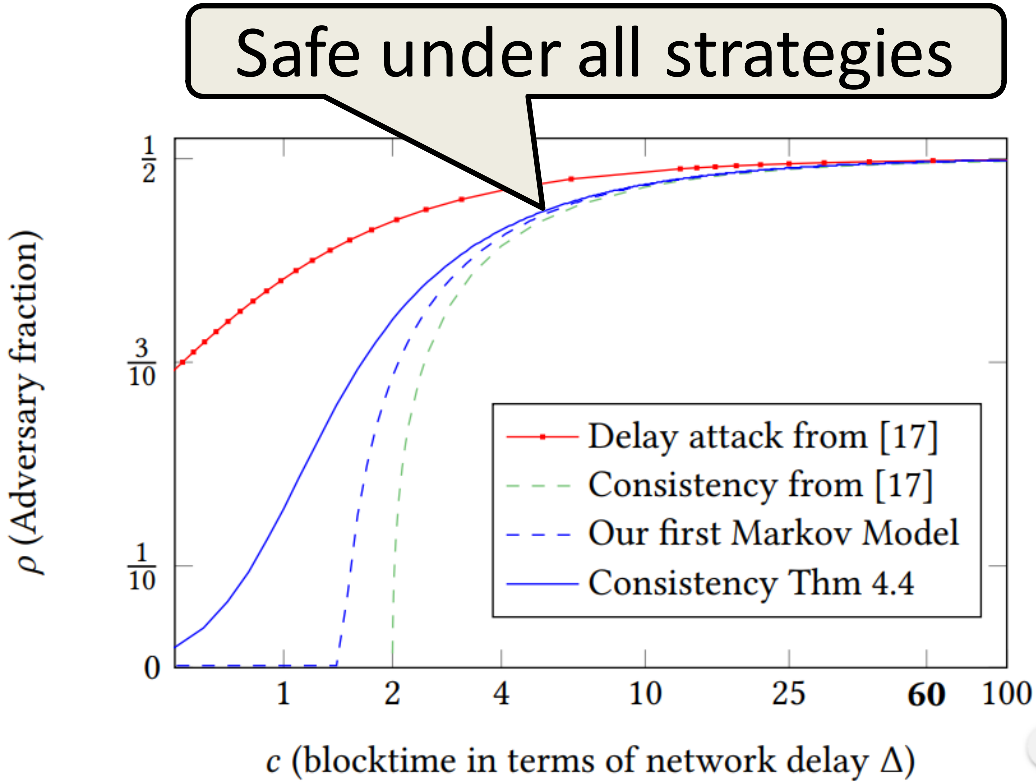
But, Resilience and Decentralization are not optimal!

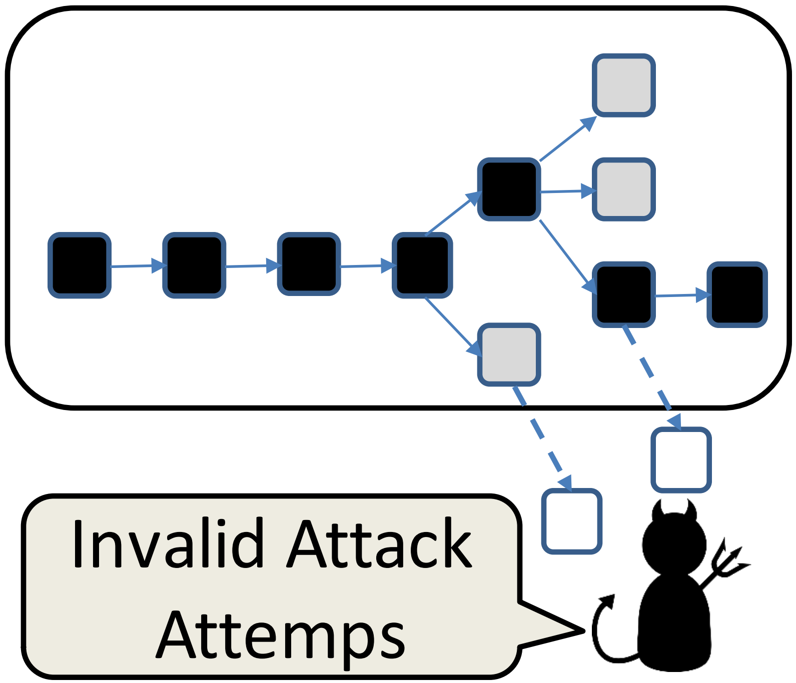
OHIE:
A Principled Approach To Scale Nakamoto

Joint work with Haifeng Yu, Ivica Nikolic, and Ruomu Hou (IEEE S&P 2020)

Starting From Proven Foundations

- There is a safe way to run Nakamoto consensus
  - **Resilience** (f) is "near-optimal" at blk. interval > 3Δ

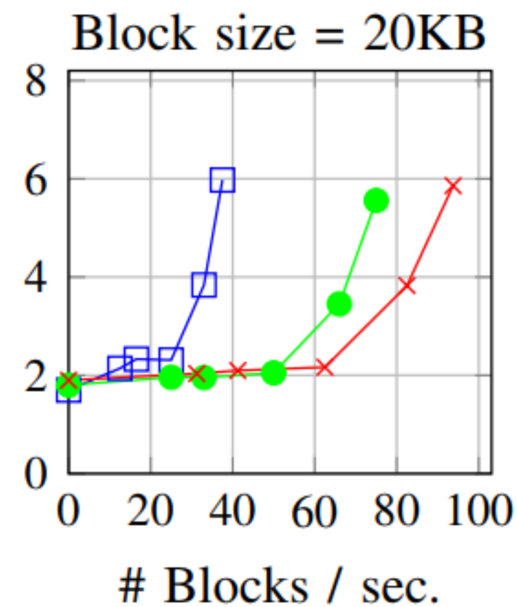




A Better Method to Analyze Blockchain Consistency" – KRS'18. (Also see GK'15, GKL'17, PSS'17)

Key Observations

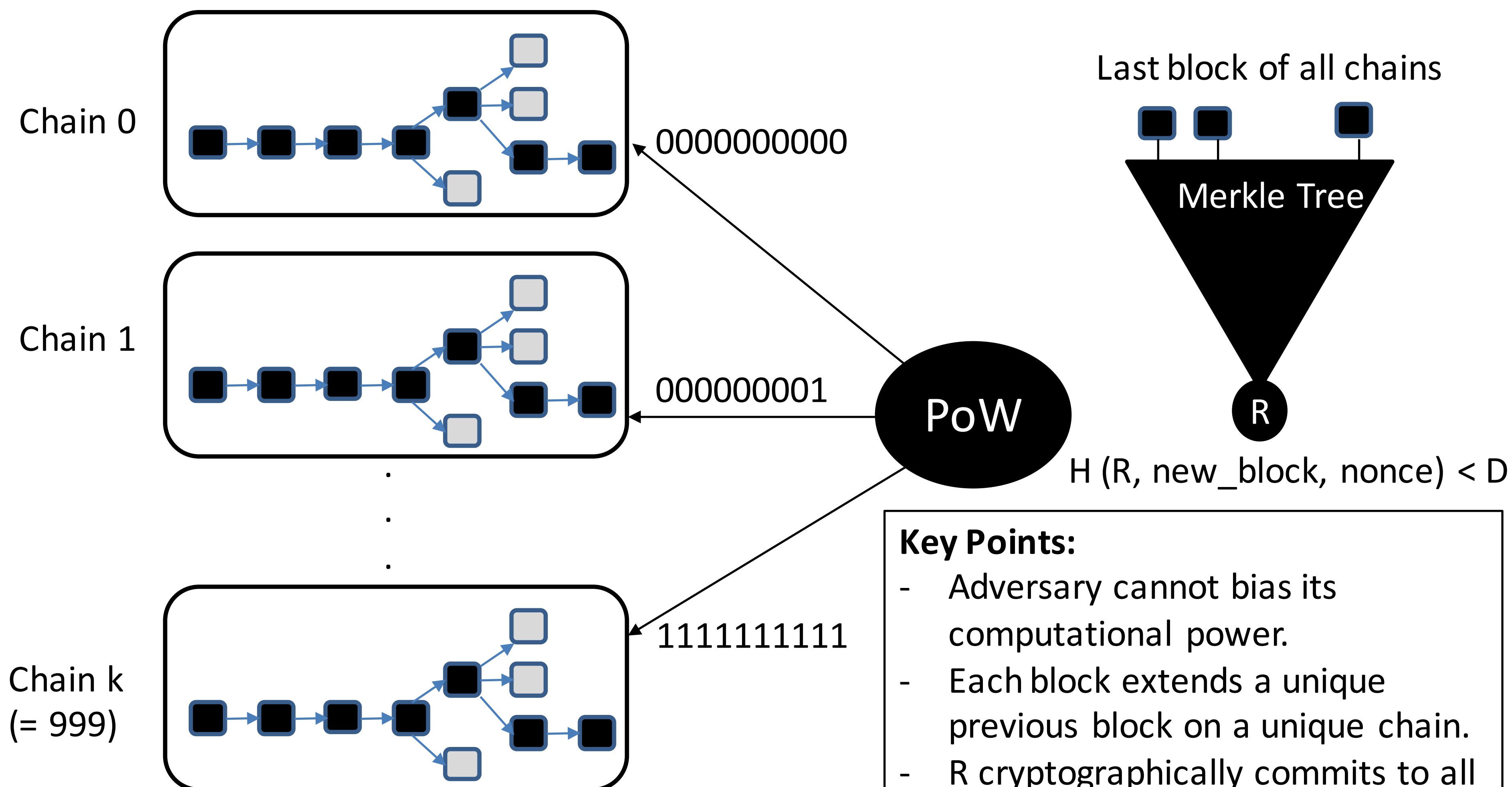
- Experimental Observations:
  - Block propagation delay (Δ) proportional to graph diameter (1-2 seconds)
  - **Parallel broadcasts don't impact latency (Δ)**



- Independence of Design Parameters
  - Block interval depends only on desired f and Δ
  - Confirmation latency depends only on block interval
  - Throughput depends only on available bandwidth (β)
  - Decentralization depends only on number of blocks/sec.

OHIE: Blockchain scaling made simple – Yu,Nikolic, Saxena,Hu (To Appear at Oakland'20)

The OHIE Protocol: Run “k” parallel chains!



Key Points:

- Adversary cannot bias its computational power.
- Each block extends a unique previous block on a unique chain.
- R cryptographically commits to all “k” blocks that the miner sees.

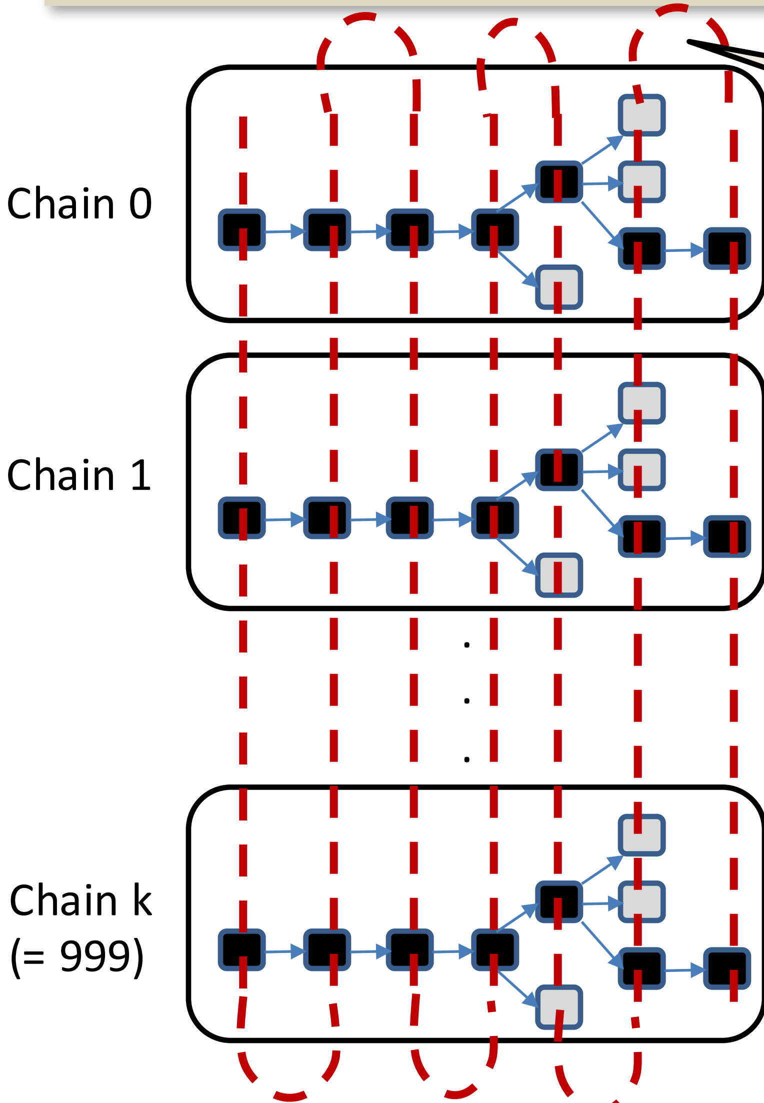
[OHIE: Blockchain scaling made simple](#) – Yu,Nikolic, Saxena,Hu (To Appear at Oakland’20)

The OHIE Protocol

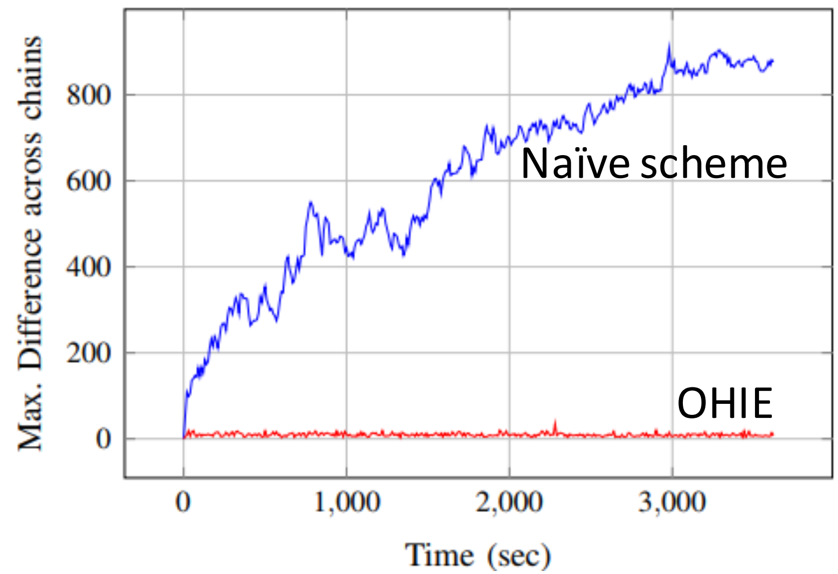
- Construction is simple and modular
- Safety and Liveness Proof:
  - Bitcoin backbone (Nakamoto) security reduces to OHIE
  - Intuition:
    - Probabilistic process on each chain is identical to Bitcoin
    - Each block extends a single prior block
    - The state that the block extends can't be forged
  - Takes Θ (log k) more confirmation blocks (union bound)

OHIE: Blockchain scaling made simple – Yu,Nikolic, Saxena,Hu (To Appear at Oakland'20)

Total Ordering Across Chains?



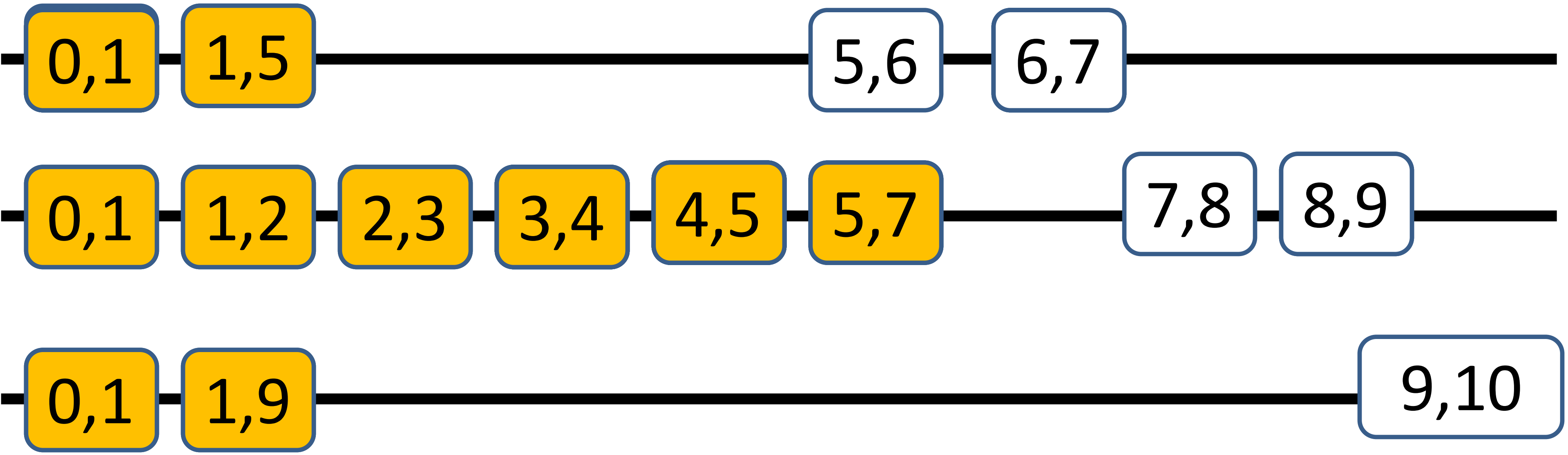
A Totally Ordered (Global) Chain



But, … works well when chains are of roughly equal length

OHIE: Blockchain scaling made simple – Yu,Nikolic, Saxena,Hu (To Appear at Oakland'20)

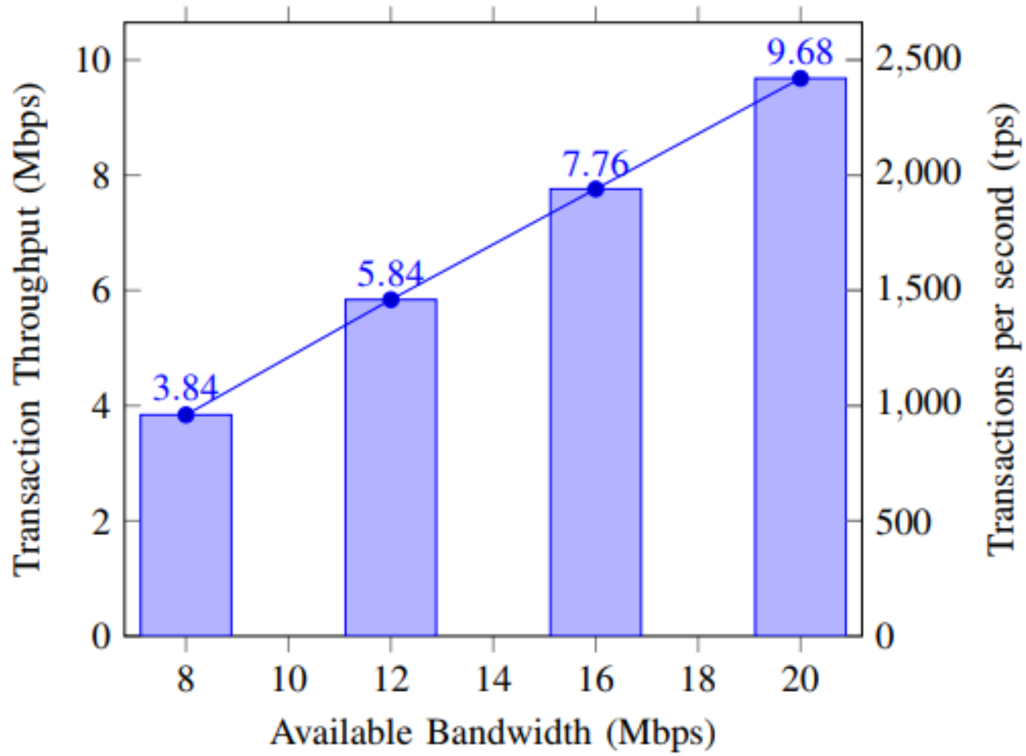
Total Ordering Scheme In OHIE



OHIE: Blockchain scaling made simple – Yu,Nikolic, Saxena,Hu (To Appear at Oakland'20)

Macro Experiments: Linear Scaling with Available Bandwidth

- 50,000 miners, 20 Mbps, resilience (f) ~ 0.43

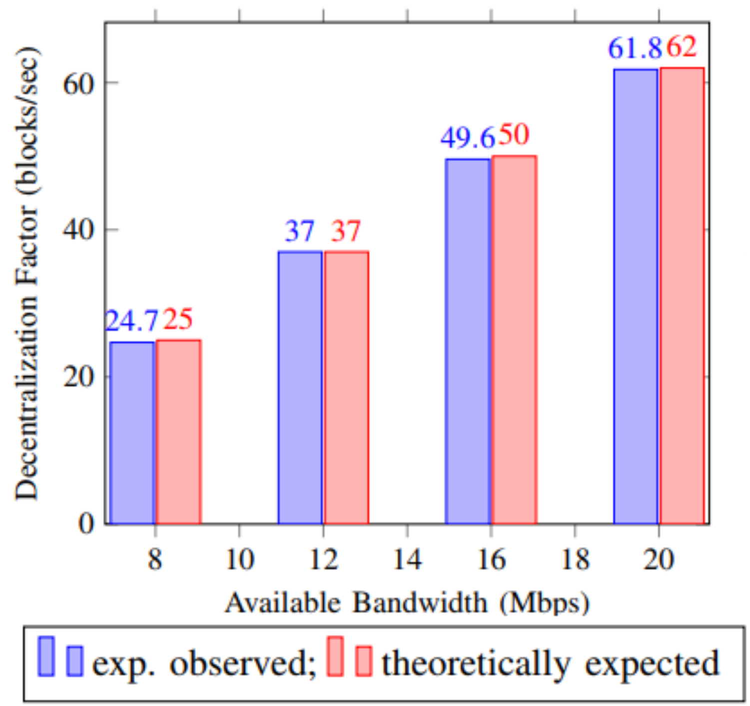


Num. of chains (k) = $0.5 \cdot 3\Delta \cdot \frac{\beta}{block\ size}$

OHIE: Blockchain scaling made simple – Yu, Nikolic, Saxena, Hou

Macro Experiments: Decentralization

- 50,000 miners, 20 Mbps, f ~ 0.43
- Decentralization: Scales linearly with bandwidth
  - k>60 blocks per second (20x higher than all prior work)

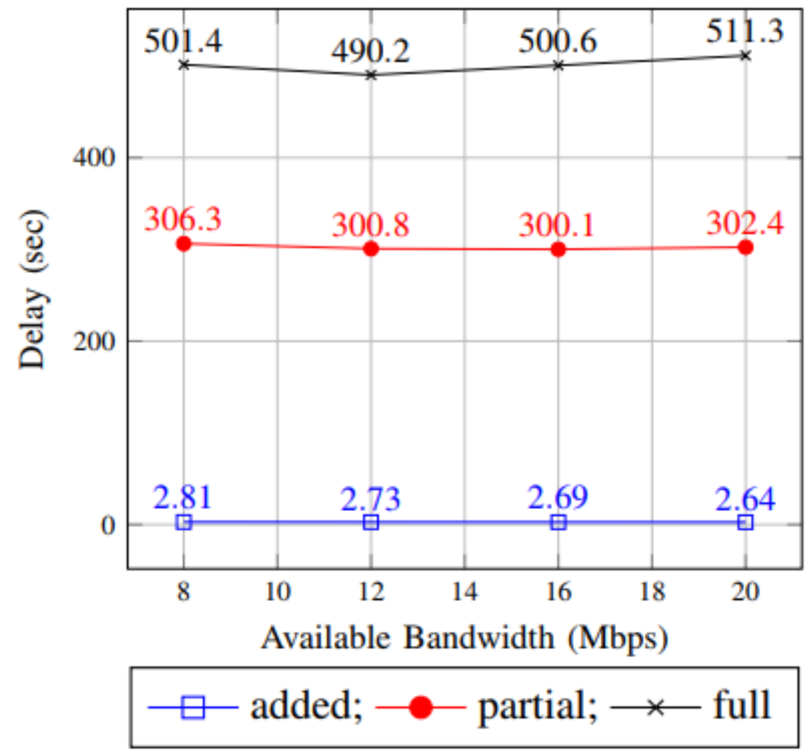


OHIE: Blockchain scaling made simple – Yu, Nikolic, Saxena, Hou

Macro Experiments: Confirmation Delay

- 50,000 miners, f ~ 0.43
- Confirmation Delay
  - **Under 10 minutes** $(3\Delta T)$
  - Independent of throughput!

  (once we fix "k")



- Conf. Blks (T) = 15 - 30
  - $T_{BTC} + \Theta(\log k)$

OHIE: Blockchain scaling made simple – Yu, Nikolic, Saxena, Hou

Security vs. Performance: State-of-the-art

Approach	Resilience	Throughput	Decentralization	Latency
Nakamoto with reduced block intervals	$f < \frac{1}{3}$	Low	Medium	Good
Nakamoto with large blocks	$f < \frac{1}{2}$	High	Low	Medium
AlgoRand (with BA) [SOSP'17]	$f < \frac{1}{5}$	High	Low	Good
Sharding (with BA) [CCS'16, S&P'18,CCS'18]	$\mathbf{f < \frac{1}{3}}$	**High**	**Medium**	**Good**

Takeaways

- Decentralized Systems propose exciting algorithmic problems
  - Build better crypto, distributed algorithms, verification tools, …
- Is there an Optimal Consensus Protocol?
  - Latency $\Theta(\Delta)$, Throughput $\Theta(\beta)$, Decentralization $\Theta(\beta)$, Res. f ~ 0.5
  - Simplicity
  - Improve the constants
- Need for new models and drawing new connections:
  - Consistency & Isolation properties offered by blockchains
  - Sybil resistance mechanisms: Proof-of-Stake vs. Proof-of-Work
  - Incentive mechanism design: Fairness, Variance,…
  - Trusting Off-chain computations

Thank you!

Collaborators:

- Loi Luu (PhD, NUS & CEO – Kyber Network)
- Haifeng Yu (Prof, NUS)
- Ivica Nikolic (Postdoc, NUS)
- Seth Gilbert (Prof., NUS)
- Hrishi Olickel (UG, Yale-NUS)
- Roumu Hou (UG, NUS)

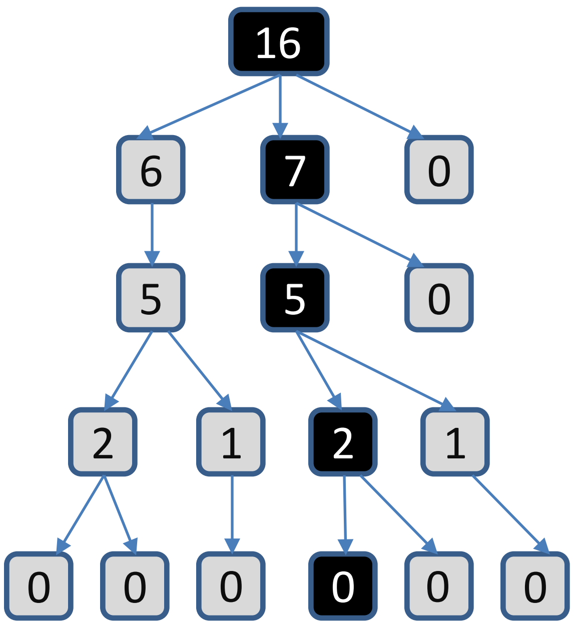
Prior Scaling Efforts

Extending Nakamoto: With Large Blocks

- Increase block size (e.g Bitcoin-NG)
  - May achieve near-optimal throughput, latency, resilience
    - Needs a careful implementation
  - Poor decentralization:
    - A single block proposer broadcasts tens of thousands of TXs
    - Number of miners participating is not $\Theta(\beta)$

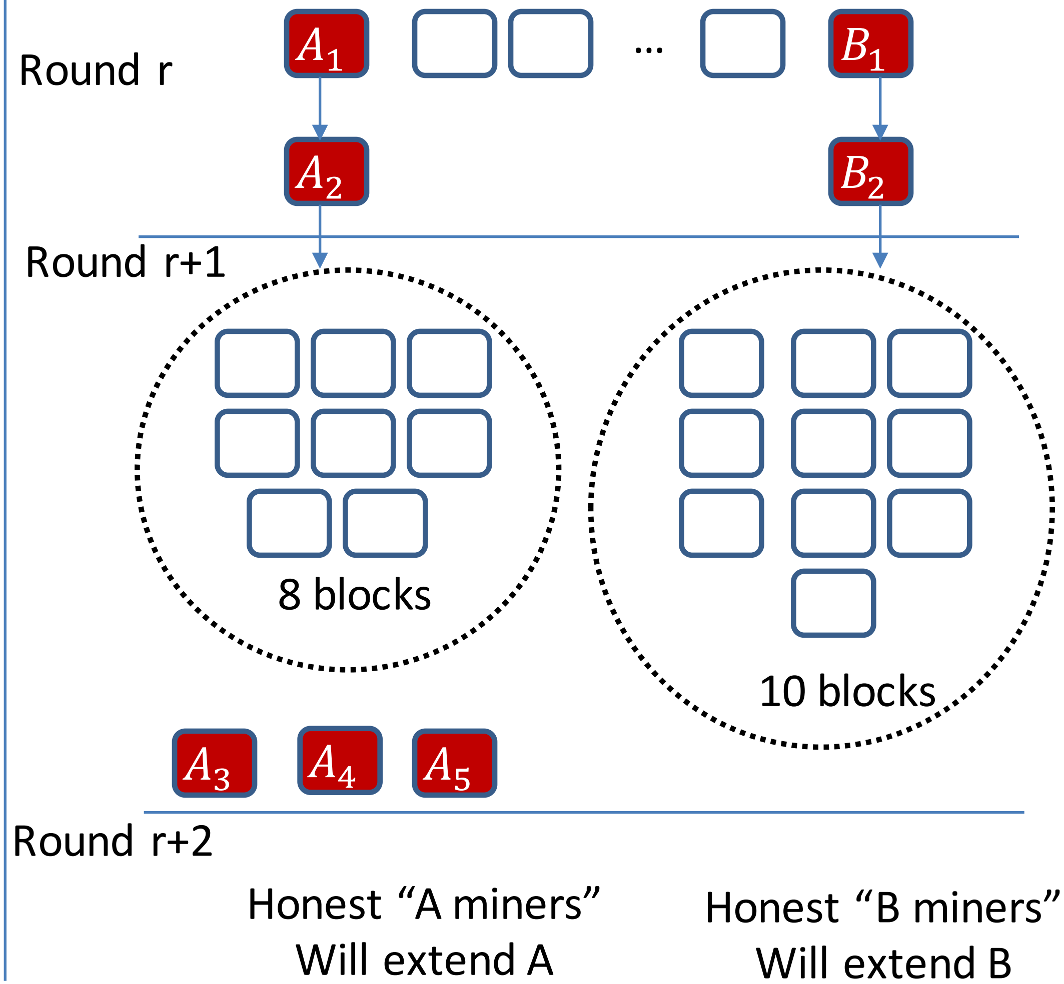
Extending Nakamoto With Smaller Block Interval

The GHOST protocol



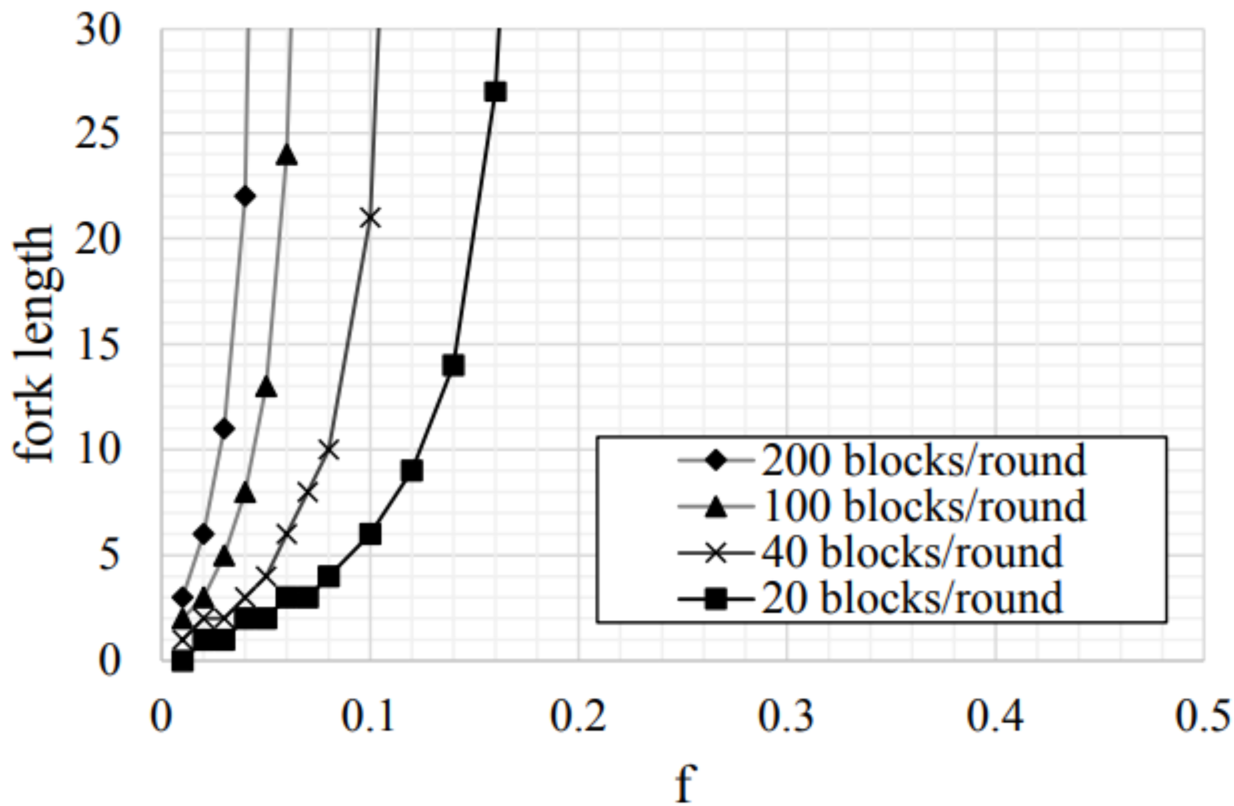
"Heaviest" rather than longest chain

Active Balancing Attack on GHOST



Secure High-Rate Transaction Processing in Bitcoin – SZ13

Attack Effectiveness on GHOST



OHIE: Blockchain scaling made simple – Yu, Nikolic, Saxena, Hou