## **Better Consensus In The Bitcoin Model**

#### **Prateek Saxena** Asst. Professor, Computer Science, NUS

Blockchain Winter School, Switzerland

#### Blockchains: Origin & Today

tom.	
Bitcoin: A Peer-to-Peer Electronic Cash System	
p or Electronic Cur	
Peer-to-Peer	
Bitcoin: A 100	
Satoshi Nakamoto	
Satoshi Nasam satoshin@gmx.com www.bitcoin.org	
www.black	
Abstract. A purely peer-to-peer version of electronic cash would allow online and through a party of another without going through a party to another without going through a party of the solution, but the main another to be sent directly from one party to another without going there are prevented and the prevent double-spreading.	
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 hough a comparison of the solution. Digital signatures provide part of the solution, but the main comparison of the solution of the solution of the solutio	
service peer version of the another with each the man	
A purely face from one parvide part of the prevent double-spectral directly from one parvide part of the prevent double-spectral directly from one parvide part of the prevent double-spectral directly for the prevent directly for	
The network timestand forming a term of the largest pool of CFO poperating to	
financial institutation in the double-sepending protocol minimum into an one- benefits are lost if a trusted dirict period by bashing them into an one- We propose a solution to the double-sepending the solution to be changed without redome. We propose a solution to the double-sepending a record that cannot be changed without redome The network interstamps transactions of while servers as groof of CPU power. As hash-based proof-of-work. The longest chain not only serves as tero of cooperations to the proof-of-work. The longest chain not only serves and outpace cooperations. The events witnessed, but proof that it came from the largest pool of CPU power. The events witnessed, but proof that it generate output, Message are broadcast on a best effort is an anjointy of CPU power is controlled by nodes that are not cooperations.	
The network intro-Forcek, forming. hash-based proveds, forming and only server and the largest pool of Cooperating to the proof-of-work. The longest chain not only server and outpace and the cooperating to the proof-of-work chain and the largest chain and outpace and the server long as a majority of CPU power is centrolled by nodes that are not ecoepering the long as a majority of CPU power is controlled by nodes that are not ecoepering the long as a majority of CPU power is controlled by nodes that are not ecoepering the long as a majority of CPU power is controlled by nodes that are not ecoepering the matter the network, they ill gererature there. Messages are broadcast on a best effort 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.	
network itself and nodes can leave and hyperical the	
public and the second s	
<b>1. Introduction</b> Commerce on the Internet has come to rely almost exclusively on financial institutions enough for instead third parties to process electronic payments. While the system works well enough for instead third parties to process electronic payments. While the system works well enough for instead third parties to process electronic payments. While the system works well enough for instead third parties to process electronic payments. While the system works well enough for instead third parties to process electronic payments. While the system works well enough for instead third parties to process electronic payments. While the system works well enough institutions eanor instead third parties to process electronic payments. The test of mediation increases transaction coefficients instead to the system and entities of the possibility to make non-reversible payments for non- avoid mediating disputes. The cost of mediation in the end of the they would open uncertainties in the system and the system and the end of the payments for anory	
1. Introduction Commerce on the Internet has come to rely almost care. While the 39-of the trust curves cannot commerce on the Internet has come to rely almost care. While the 39-of the trust curves cannot invited third parties to process electronic payments. The value of the second curves the structure of the second curves the possible, since financial institutions cannot completely non-reversible transactions are not really possible, since financial institutions cannot completely non-reversible transactions are not really possible, since and curves of the second curves of the second curves the possibility for second curves of the second curves. The need for trust spreads. Merchants must avoid mediating disputes and curves of ability to make non-reversible payment uncertainties of the loss of ability of curves, the need for trust spreads. Merchants must append curve of the loss of ability of the second information are costs and payment uncertainties are spinibility of the second information curves of the payments.	
1. Interee on the Internet has come to anymento. See the second paymento in the second parties to process electronic paymento. See the second parties to process the transactions are not really possible, since financial instancement of the second parties to process the transaction increases transaction const. It is the second parties to proceed the payment of the payment of the payment of the payment pay	
trusted third parties it still sufficience and an endiation increases used and assessed for non-	
most transaction por reversible under the cost of meride off the possible por versible P-Merchans med.	
Completely and the state of the state of ability to the need for trust spir would other the state of the stat	
avoint practicul coder cost in utility of reverses information users and payments	
Commerce on the inner process electron the inner@ ossible, since ooss, irransactions, i rusted third parties to process electrons are not really possible, since and irransactions, completely non-reversible transactions are not really possible parties for small casual transactions avoid mediating disputes. The cost of mediation increases transactions, where the innimum practical transaction size and euting 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 reversel, the need for trust spreads. Merchanis musi- reversible services. With the possibility of reversel, then each other without be made many and reversible services. An extra scenter das unavoidable. These costs and payment ucertainties to wary of their customers, hassing them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment used and rusted and the oxided in person by using physical currency, but no mechanism exists to make payment over a communications channel without a trusted party. What is needed is an electronic payment system based. What is needed is an electronic payment system for environ payment when each other without the needs of trust.	
and three services. We may apprecipate as unavoidable and an avoidable services and the customers, hasting the anavoidable and the customers, hasting the anavoidable and the customers, but no mechanism. A certain percentage of fraud is accepted as unavoidable and the customers, but no mechanism. A certain percentage of fraud is percentage and the service of the customers, but no mechanism. A certain percentage of fraud is percentage and the service of the customers, but no mechanism. A certain percentage of the service of the customers, but no mechanism. A certain percentage of the service of the customers, but no mechanism. A customers and the service of the customers of the customer of the customer of the customer of the customer of the customers of the customer of the customer of the customers of the customer of the customers of the customer of the customers of t	
a stain percentage asson by using the ut a trusted the based on cryptic without the net expected sellers	
the avoided in Figure channel with payment system with each other reverse would not buyers. In	
over a communication of the second state of th	
What is you will be a section with the section of t	
be wary of their classes frauds is deceived in the physical currency. A certain percentage of frauds is deceived physical currency. Can be avoided in person by using physical currency. What is needed is an electronic payment system based on envytographic proof instead set of the physical currency. What is needed is an electronic payment system based on envytographic proof as electronic payment system based on the without the need of the system and the set of the physical currency. What is needed is an electronic payment system based on envytographic proof physical currency. In this payment system based on the system based on envytographic proof of the system. In this payment and the system based on the system based on envytographic proof of transactions. The physical currency and physical currency are physical currency. In this payment and the system based on the system based on the system with each other without the physical currency and the system is secure as long as honest nodes collectively control more CPU power than any system is secure as long as honest nodes.	ł
from fraud, and propose a solutional protectively conduction	1
this paper, server to generate house	
system is secure as the secure of attacker nodes.	
timestamp server to e as long as hand- system is secure as long as hand- cooperating group of attacker nodes.	Ī

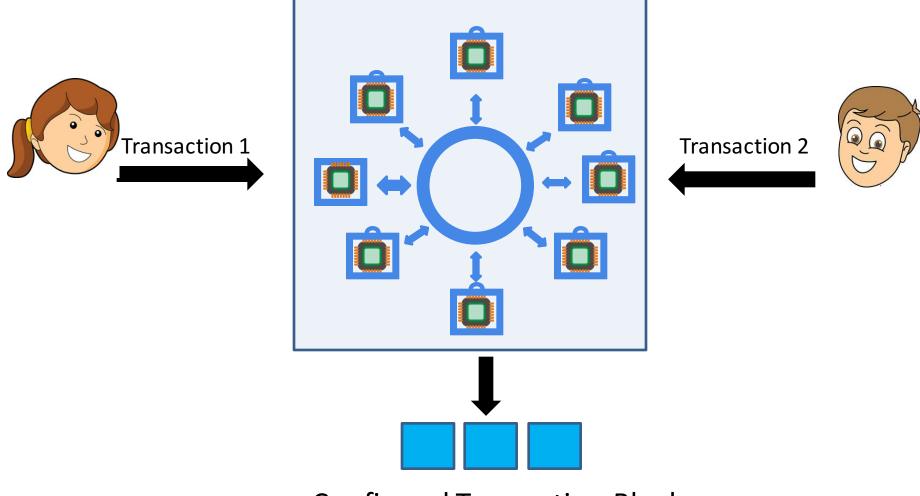
2008

#### Top 100 Cryptocurrencies by Market Capitalization

Cry	yptocurrencies 👻	Exchanges -	Watchlist				USD 🕶	Next 100 $\rightarrow$ View All
#	Name		Market Cap	Price	Volume (24h)	Circulating Supply	Change (24h)	Price Graph (7d)
1	8 Bitcoin		\$59,580,761,374	\$3,399.59	\$4,939,435,528	17,525,862 BTC	-0.49%	man
2	X XRP		\$12,001,134,334	\$0.291508	\$356,976,506	41,169,202,069 XRP *	-0.25%	mun
3	Ethereum		\$10,974,571,873	\$104.75	\$2,280,623,059	104,766,118 ETH	-0.48%	mym
4	₿ EOS		\$2,126,001,619	\$2.35	\$472,575,374	906,245,118 EOS *	-0.64%	son
5	🛯 Bitcoin Cash		\$2,041,982,753	\$115.96	\$198,734,194	17,609,650 BCH	0.05%	m m
6	😯 Tether		\$2,026,509,895	\$1.00	\$3,511,890,558	2,021,103,317 USDT *	0.10%	my m
7	() Litecoin		\$2,000,776,268	\$33.14	\$636,413,250	60,369,927 LTC	سر 0.12%	mm
8	🌾 TRON		\$1,712,362,099	\$0.025684	\$136,340,725	66,671,422,606 TRX	-0.61% 🔨	mm
9	🦸 Stellar		\$1,422,240,776	<b>\$0.074</b> 196	\$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%	m m
12	🔅 Cardano		\$940,904,576	\$0.036290	\$12,298,410	25,927,070,538 ADA *	-0.51%	m m
13	🔊 Monero		\$707 519 153	<b>\$</b> 43.36	\$46 156 605	16 777 423 XMR	n 27% 🔨	\m _ ^

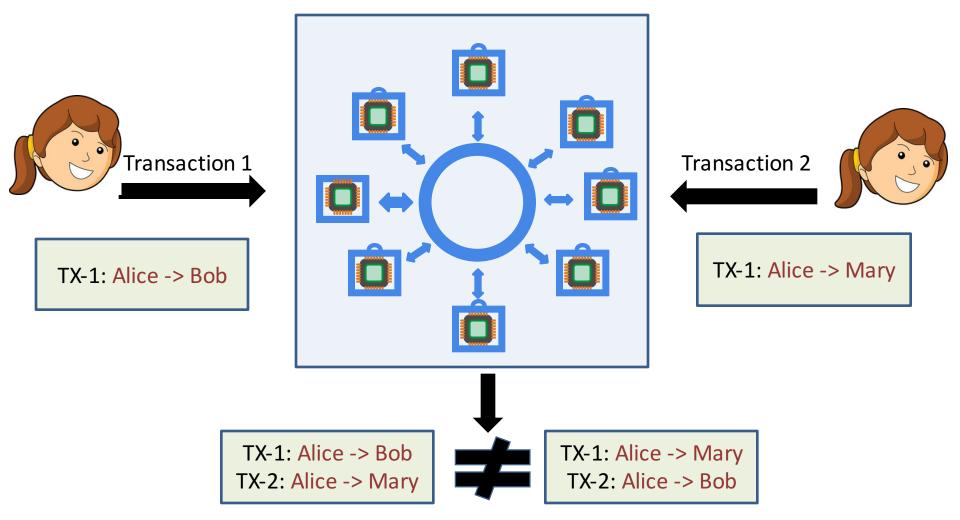
# The Blockchain Consensus Problem

# The Problem



**Confirmed Transaction Blocks** 

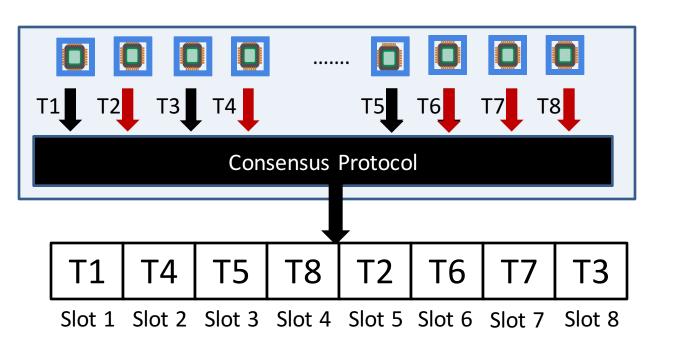
# Key Challenge: Agreement over Transaction Ordering



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**

Ethlance		Participate in Ethlan	ce's governance processes: <u>In</u>	troducing the district0x Network	How it works					
F	or Sale	Siring Gen 0 All	Kitties							
	Q Search			DAY C ETH PRICE: \$6 GAS PRICE: 15		P NEW WALLET UNLOCK WALLET				
	_	Share in the success of IDEX and Aurora with the AURA staking token LEARN MORE								
	S F	F MARKETS T A Only Search		AURA / ETH AURA Contract: 0xcdcfc0f6	Last Price         24hr H           0.00032812         0.00033199           24hr Volume:         126565.61894113518483	24hr L         24hr Change           0.00031301         +1.27263483%           21425 AURA / 40.98401658699487643				
	1		Chg         Name           22.14         -1.31%         Pundi X           22.89         -9.73%         PCHAIN	PRICE CHART DEPTH CHART QUIC	K BALANCES BENEFITS					
	4	☆         HOT         0.00000161         143           ☆         REM         0.00003410         928           ☆         COLL         0.00000558         837		★	O 000032517 H 000032895 L 0000316 C 0	000032812 ● eod detayed				
	Over 5 million smart contracts!									
	44	☆         NEXO         0.0002/119         456           ☆         SNTR         0.00000039         436				P***				
		★ EXC 0.00126515 426		•••• Volume (false, 20) ▼		- 200.				
		☆         BKX         0.0004698         376           ☆         PMNT         0.0000807         362		charts by <u>TradingView</u>		- 100.				
		→ MAN 0.00124550 294		5 5 5 1m 5d	6 7	8 18:00 17:22:15 (UTC-4) % log auto 🔆				

# The Bitcoin Model

- Assumptions:
  - A trusted "genesis" block
  - No pre-established identities, joining is permissionless
  - 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

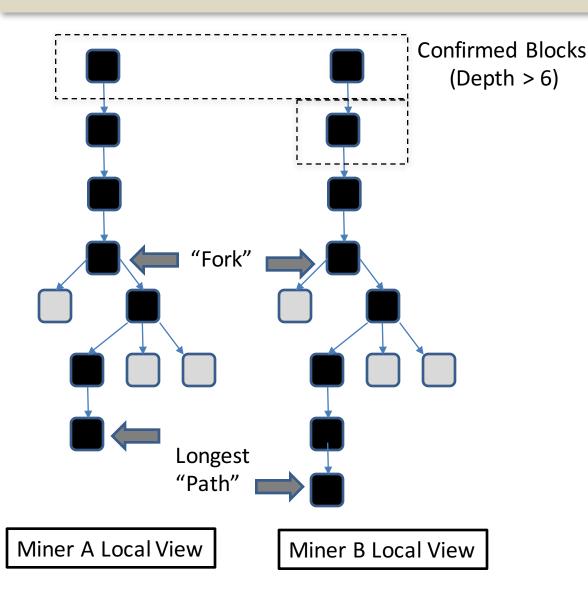
# Nakamoto Consensus Protocol

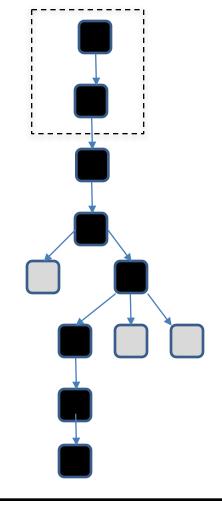
- Miners keep a local copy of the blockchain
- Miners solve a computational Proof-of-Work puzzle:



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

# Nakamoto Consensus: Overview





Combined System View (Taking comp. majority)

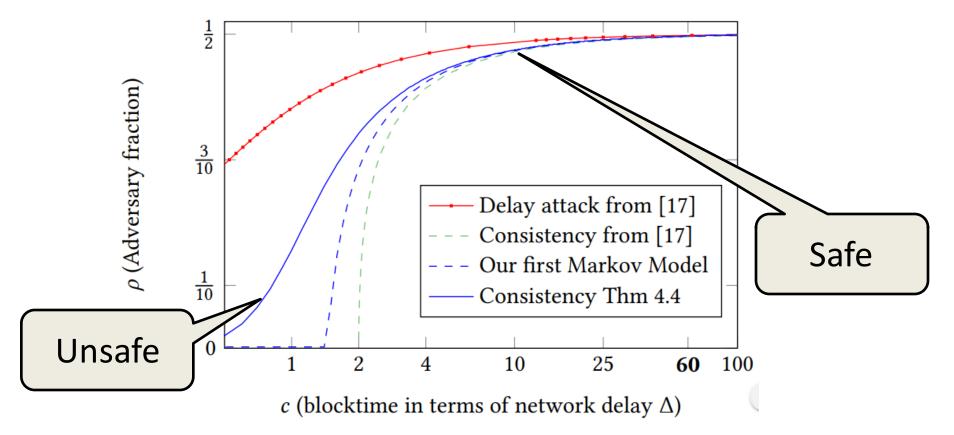
## Can We Do Better?

# Fundamental Limits & Optimality: Latency

- Limit 1: Block Propagation Delay ( $\Delta$ )
- Optimal Transaction confirmation latency is  $\Theta(\Delta)$
- A random (ER) graph with N nodes and degree d
  - Avg. hops between nodes =  $(\log N)/(\log d)$ 
    - Bitcoin N = 12,000, d = 16, avg. hops = 3.36
    - Ethereum N = 35000, d = 25, avg. hops = 3.25
    - (Hypothetical) N = 1M, d=40, avg. hops = 4.29
  - $-\Delta \sim = avg. hops \times hop \ latency$ 
    - On Amazon EC2 (geo-distributed) about 1-2 seconds
    - Changes minimally with (N,d)

# Nakamto Consensus: Safety & Liveness are Near-Optimal

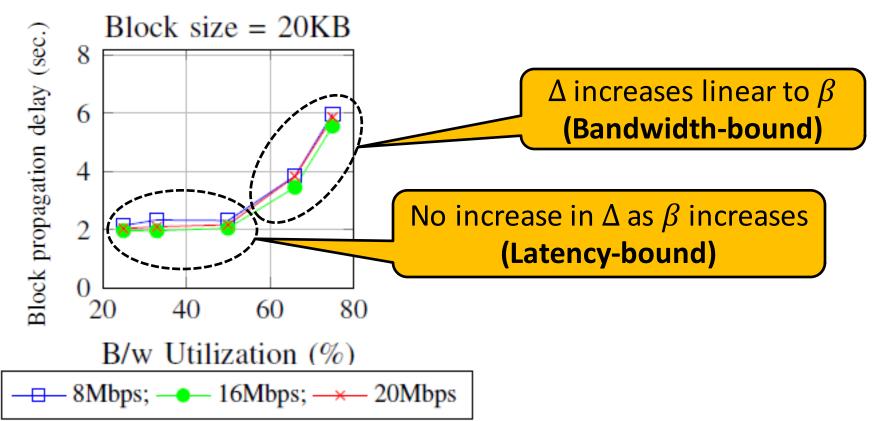
- For Nakamoto consensus,
  - **Resilience** (f) is "near-optimal" at blk. interval >  $3\Delta$



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

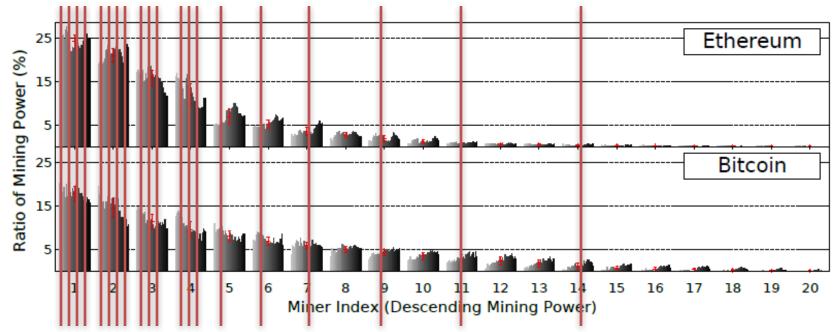
# Fundamental Limits & Optimality: Throughput

- Limit 2: Broadcast Throughput ( $\beta$ )
- Transactions per second =  $\beta$  / transaction size
- An experiment showing  $\Delta$  (un)correlation with eta



# Fundamental Limits & Optimality: Decentralization

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



- Goal of decentralization: Maximize miners/sec
- Optimal Decentralization is  $\Theta(\beta)$

# Nakamoto Consensus: Not Optimal In Throughput & Decentralization





- 6-12 TXs per second
- 3-60 minutes latency



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



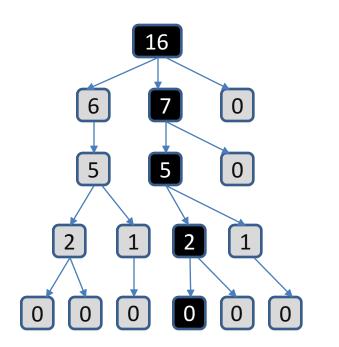
#### **Towards Better Consensus Protocols**

# 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  $\underline{\text{not}} \Theta(\beta)$

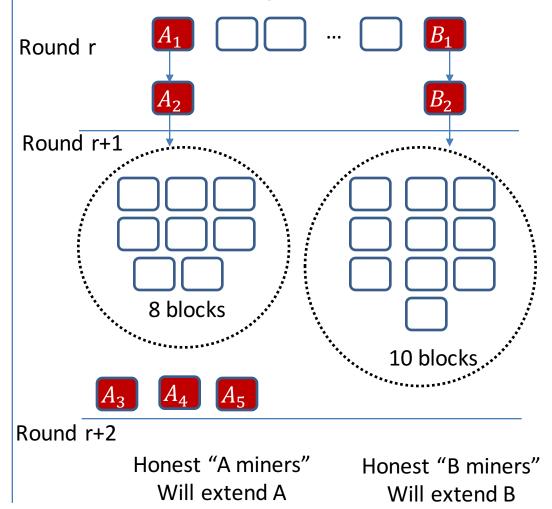
# Extending Nakamoto With Smaller Block Interval

The GHOST protocol



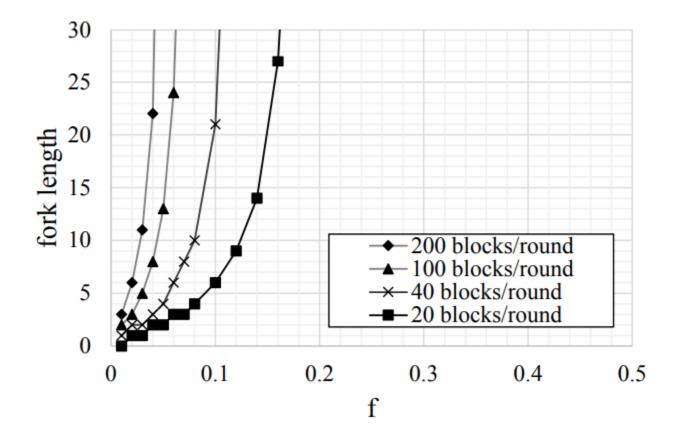
"Heaviest" rather than longest chain

#### Active Balancing Attack on GHOST



Secure High-Rate Transaction Processing in Bitcoin – SZ13

## **Attack Effectiveness on GHOST**

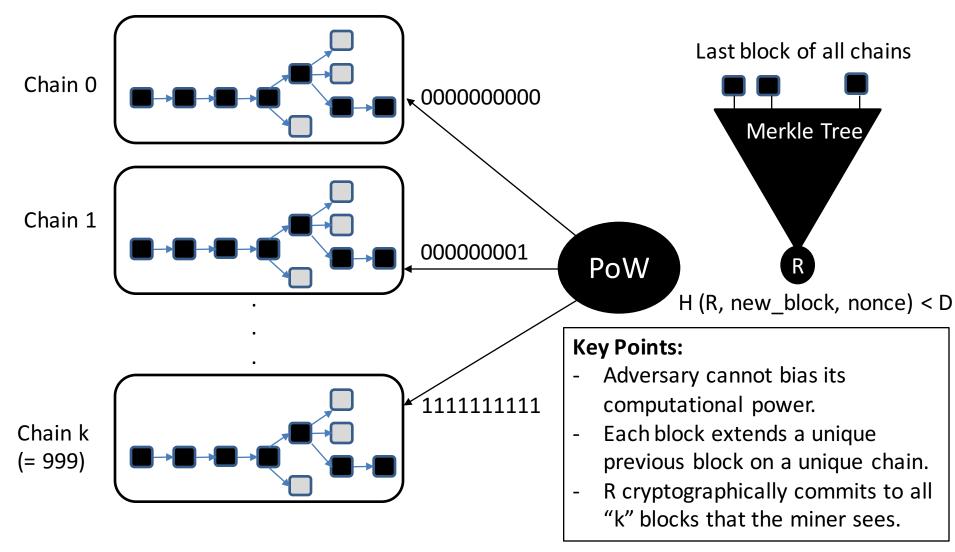


#### A Principled Approach To Scale Nakamoto

# **Key Observations**

- There is a safe way to run Nakamoto
  - Tolerates f ~ 0.5 if block interval exceeds  $3\Delta$
  - Have established proofs from prior works
- Independence of Design Parameters
  - Block interval depends <u>only</u> on desired f and  $\Delta$
  - Confirmation latency depends only on block interval
  - Throughput depends <u>only</u> on available bandwidth ( $\beta$ )
  - Decentralization depends <u>only</u> on number of blocks/sec.

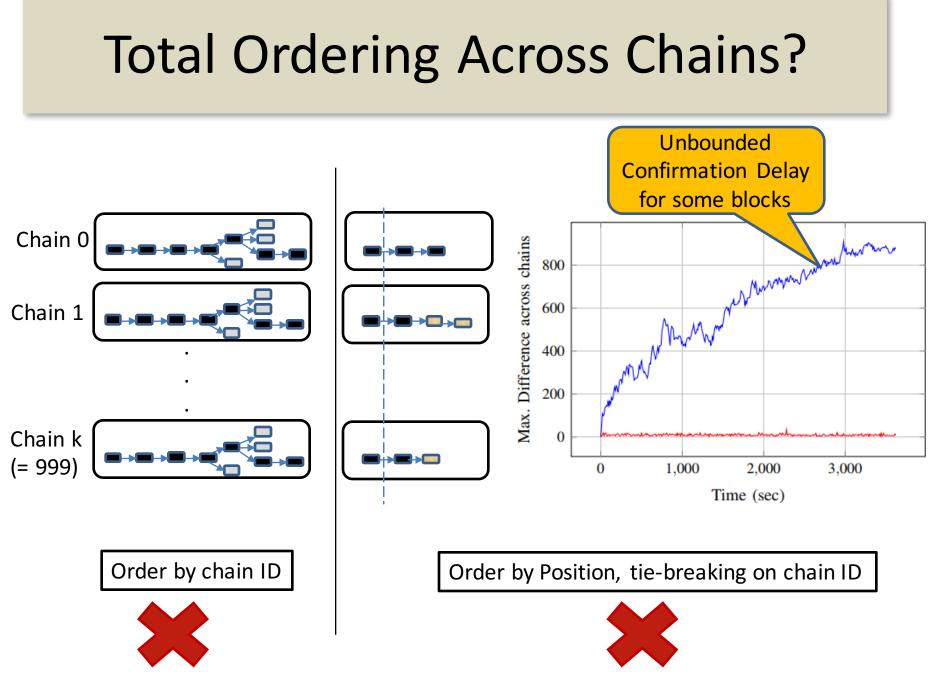
# The OHIE Protocol: Run "k" parallel chains!

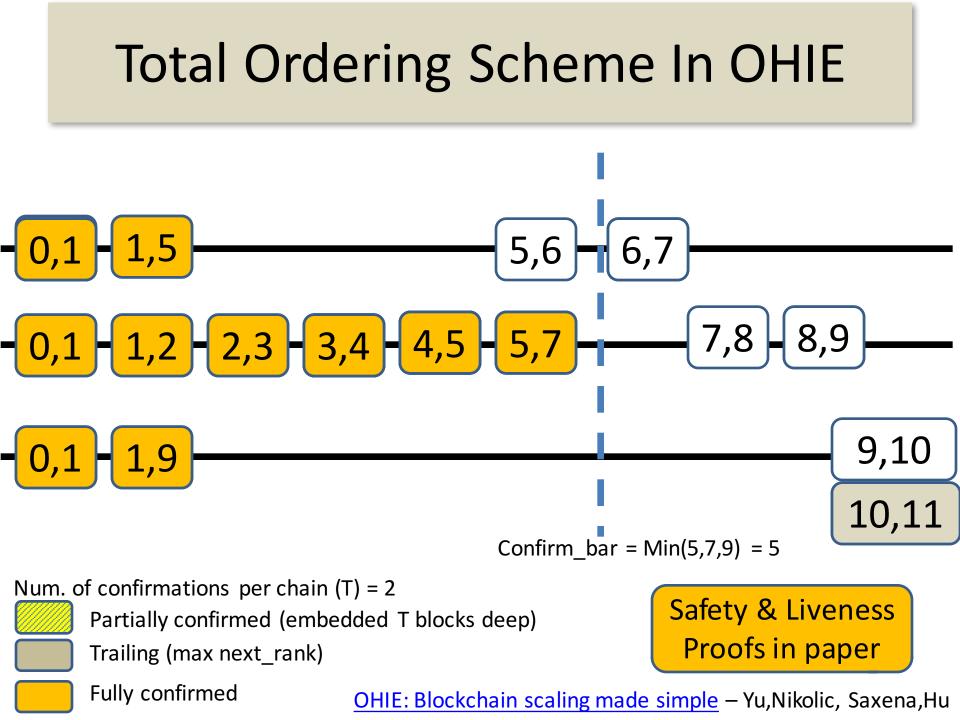


# The OHIE Protocol

- Construction is simple and modular
- Safety and Liveness Proof:
  - Reduces to that of Bitcoin backbone protocol
  - 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

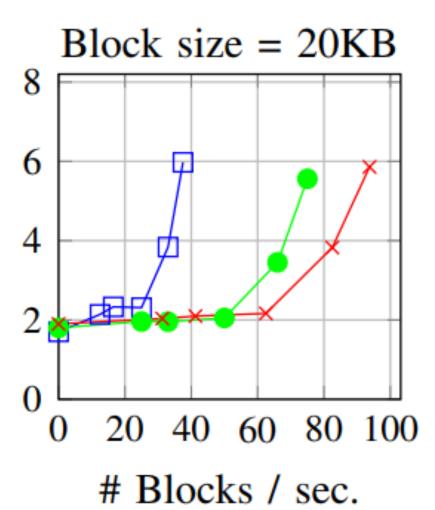
– Takes  $\Theta$  (log k) more confirmation blocks (union bound)





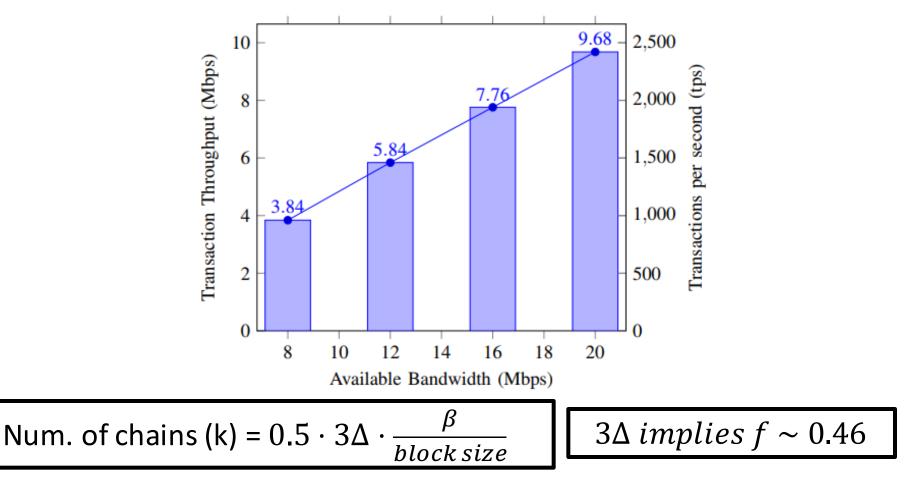
# Prototype & Micro Experiments

- Less than 5 KLOC of code
- Micro Experiments
   1000 miners, 20 Mbps
- Critical Observations:
  - Block propagation delay (Δ) proportional to graph diameter (1-2 seconds)
  - Parallel broadcasts don't impact latency (Δ)



# Macro Experiments: Linear Scaling with Available Bandwidth

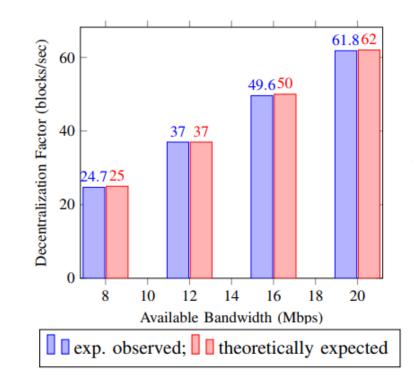
• 50,000 miners, 20 Mbps, resilience (f) ~ 0.46



# Macro Experiments: Decentralization

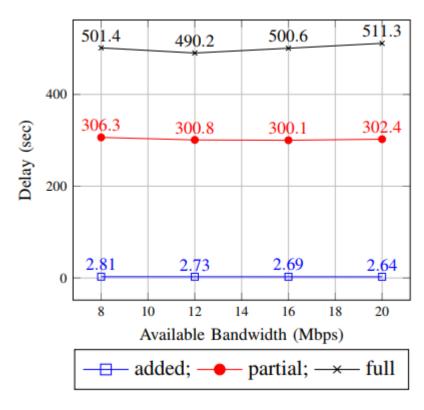
- 50,000 miners, 20 Mbps, f ~ 0.46
- Decentralization: Scales linearly with bandwidth

– k>60 blocks per second



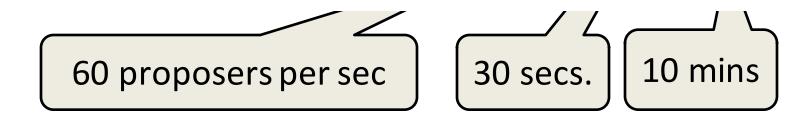
# Macro Experiments: Confirmation Delay

- 50,000 miners, f ~ 0.46
- Confirmation Delay
  - Under 10 minutes  $(3\Delta T)$
  - Independent of throughput!(once we fix "k")
- Conf. Blks (T) = 15 30 $-T_{BTC} + \Theta(\log k)$



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

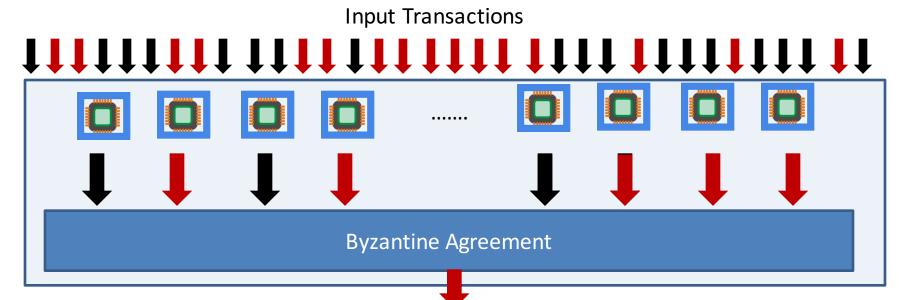
Approach	Resilience	Throughput	Decentralization	Latency
Nakamoto with reduced block intervals	$f < \frac{1}{3}$	Low	Medium	Good
Nakamoto with large blocks	$f < \frac{1}{2}$	High	Low	Medium
AlgoRand (with BA) [SOSP'17]	$f < \frac{1}{5}$	High	Low	Good



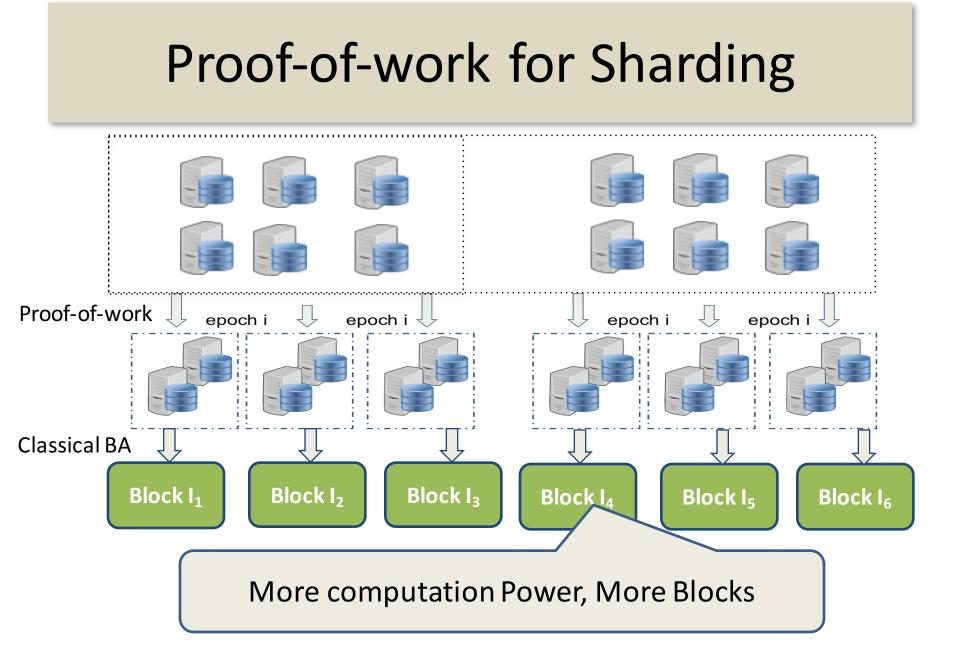
# State-of-the-practice

# Repurposing BA Protocols?

- Agree on 1 block per round with standard BFT / BA
- Honest miners sign that block with round id.

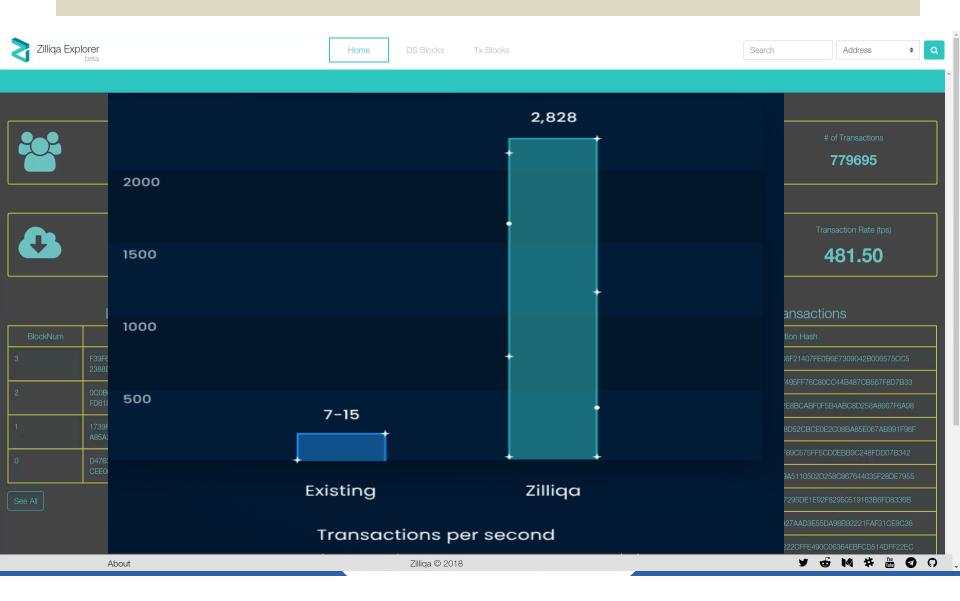


- Challenge: Participants must be <u>known a-priori</u>
  - Chicken-n-egg: Agreeing on participants is itself...

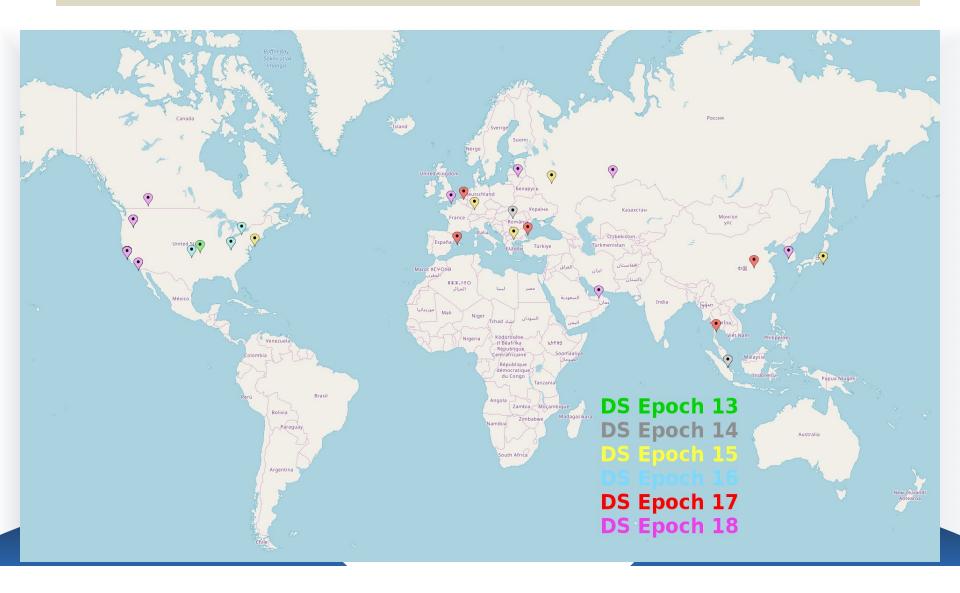


Elastico – CCS'16 (Also see Omniledger – Oakland'18, RapidChain-CCS'18)

#### Commercialized as the Zilliqa public blockchain platform



# Open to public mining (Feb 2019)



# 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)