What is the role of researchers
in the blockchain world?

What is my role?

What is a researcher anyway?

Some researchers are seen as gods.

Some play god.

nature

NEWS | 26 November 2018

Genome-edited baby claim provokes international outcry

The startling announcement by a Chinese scientist represents a controversial leap in the use of genome editing.

By David Cyranoski & Heidi Ledford

A Chinese scientist claims to have helped make the world's first genome-edited babies – twin girls, who were born this month. The announcement has provoked shock and outrage among scientists around the world.

Others are oracles.

Impossibility of Distributed Consensus with One Faulty Process

MICHAEL J. FISCHER

Yale University, New Haven, Connecticut

NANCY A. LYNCH

Massachusetts Institute of Technology, Cambridge, Massachusetts

AND

MICHAEL S. PATERSON

University of Warwick, Coventry, England

Abstract. The consensus problem involves an asynchronous system of processes, some of which may be unreliable. The problem is for the reliable processes to agree on a binary value. In this paper, it is shown that every protocol for this problem has the possibility of nontermination, even with only one faulty process. By way of contrast, solutions are known for the synchronous case, the "Byzantine Generals" problem.

But the blockchain world no longer needs gods and oracles.

At least I am not good enough to be one.

My true talent: making others unhappy, and being the cause of this unhappiness brings me great happiness.

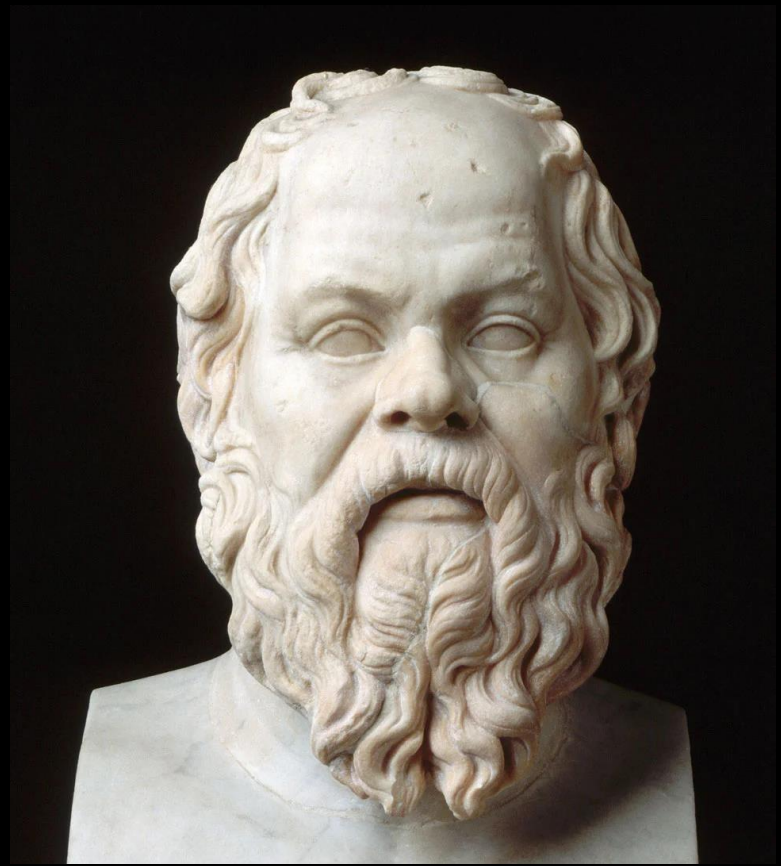
Schadenfreude

/ˈʃɑːdənˌfrɔɪdə/

Making others unhappy, and being the cause of this unhappiness brings one great happiness.

I hope to be …

a gadfly.



… sting people and whip them into a fury, all in the service of truth.

What is my role? A wannabe gadfly.

What am I doing here? To disseminate bias.

A Ph.D. equips one to convince others of their biases. How boring a person would be without any biases!

— Yefu Zheng

My Biases

Ren Zhang

Researcher @ Cryptape and Nervos

@Nirenzang

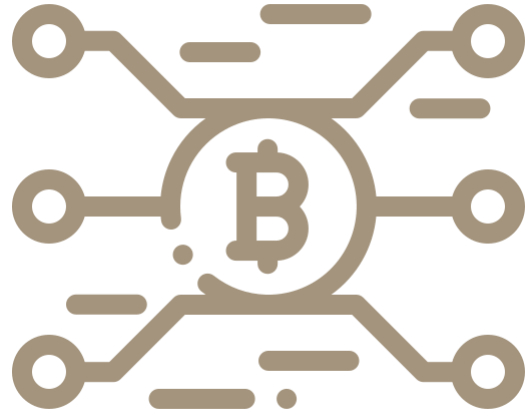
ren@nervos.org

Outline

1. Against Bitcoin Unlimited
2. Against 9 Other PoW Protocols
3. Against 7 Sharding Designs
4. Against 2 DAG-based Protocols
5. Against All PoS Protocols (including Ethereum)

1

Against Bitcoin Unlimited



Bitcoin is about to split into two chains. Maybe there is something you can do.

— Yonatan Sompolinsky in 2017

Analyzing BU Mining Protocol

Bitcoin Unlimited:

- A Bitcoin scaling proposal that received the largest mining power support (40%) until late June, 2017
- *"A tool to raise the blocksize limit without splitting the network"*

Secure?

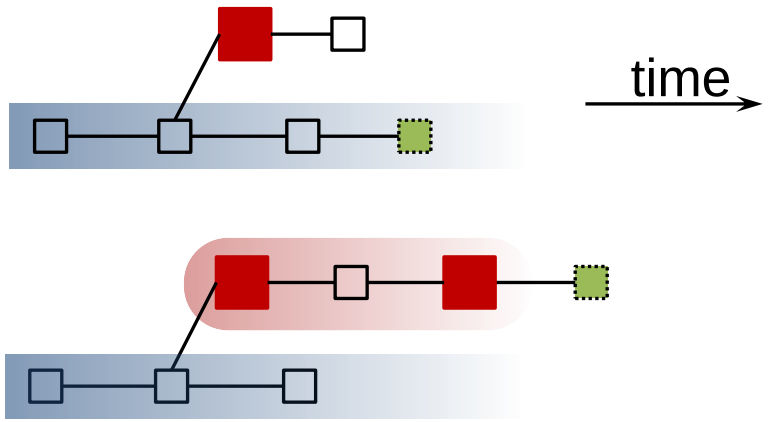
- Attacks will *"cost the attacker far more than the victim"*

How BU Works

"the blocksize limit should never have been a consensus rule in the first place"

- Miners decide their local block size limit *EB*, and stick to their choices
- Until it is *AD* blocks behind the longest chain

→ No **block validity consensus** (BVC)



□ ≤ *EB* block

■ > *EB* block

▩ block that the miner tries to mine

block size limit = *EB*

block size limit = 32MB

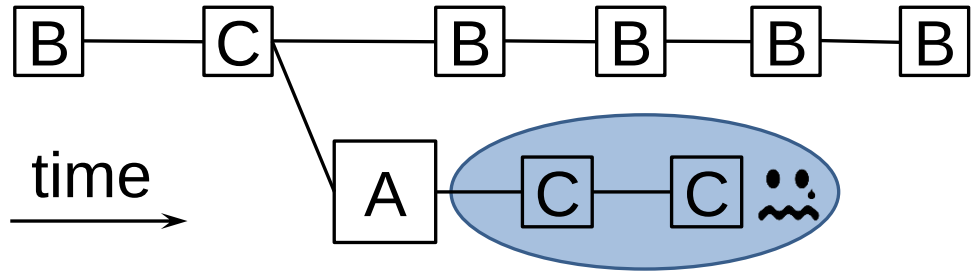
What We Did: Compare BU and Bitcoin

Incentive models / Security claims	BU is secure when BVC is absent	BVC will emerge
Compliant & Profit-Driven		
Non-Compliant & Profit-Driven		Not meaningful
Non-Profit-Driven		

Non-Profit-Driven Attacker

- Alice's goal: to orphan as many Bob and Carol's blocks as possible with the least number of Alice's blocks

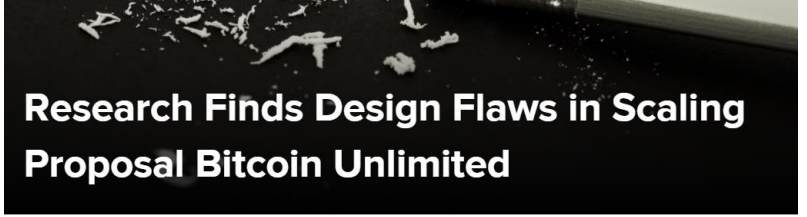
- A typical execution



Alice orphans two Carol's blocks with only one block


bitcoinunlimited
release the potential attacks

Impact



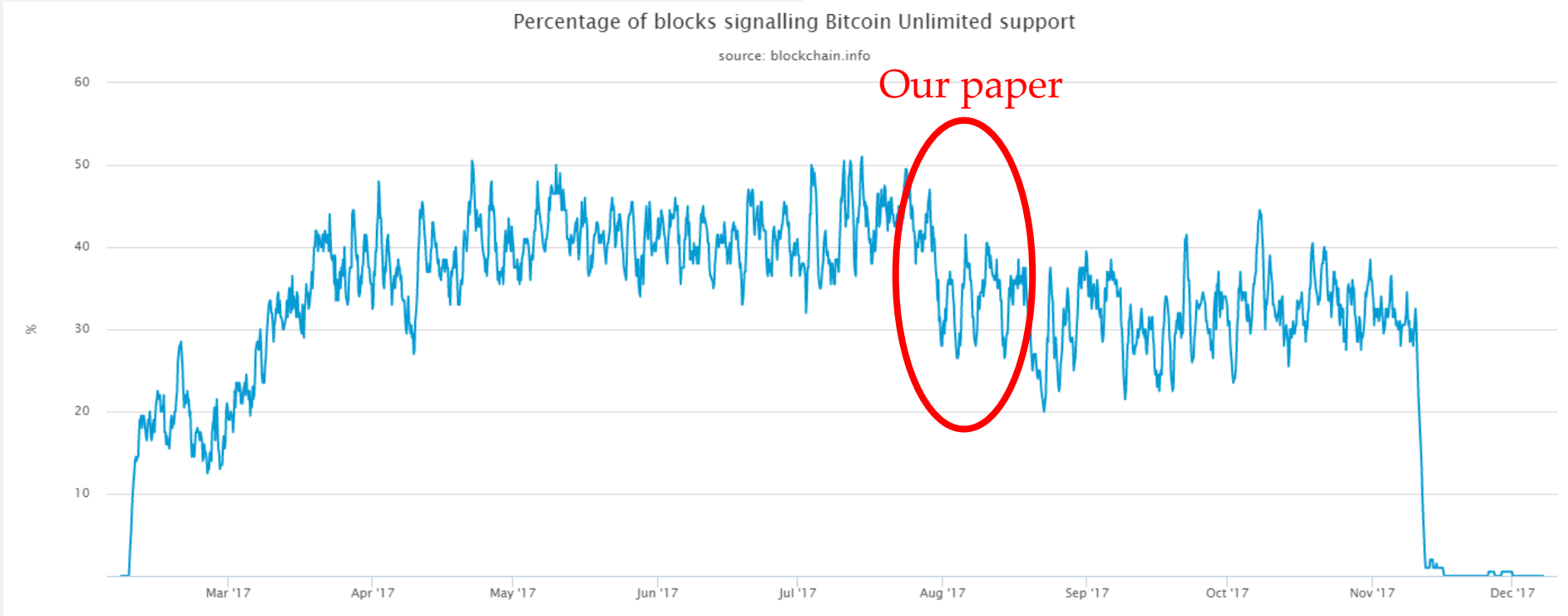
Research Finds Design Flaws in Scaling Proposal Bitcoin Unlimited

6 13

Pete Rizzo
Jul 19, 2017 at 14:45 UTC

NEWS

A new research paper from international analyst group IMEC has found that changes to bitcoin proposed by a software implementation called Bitcoin Unlimited would "magnify the effectiveness" of attacks on the network.



Publication

- Ren Zhang and Bart Preneel. On the necessity of a prescribed block validity consensus: Analyzing Bitcoin Unlimited mining protocol. In *13th International Conference on emerging Networking EXperiments and Technologies (CoNEXT)*, pages 108–119. ACM, December 2017
- https://ia.cr/2017/686
- https://www.youtube.com/watch?v=P35M74KcLmA

2

Against 9 Other PoW

The Story Behind

- To improve NC, I designed, modeled and evaluated dozens of ideas, but none is perfect
- But these flawed ideas kept being published with none or partial security evaluation
- I think people need to be informed

Protocol	Citations (till 2019)
Fruitchains	131
Bitcoin-NG (btw, I like it!!!)	631
Byzcoin	321
Subchains	19
DECOR+	3

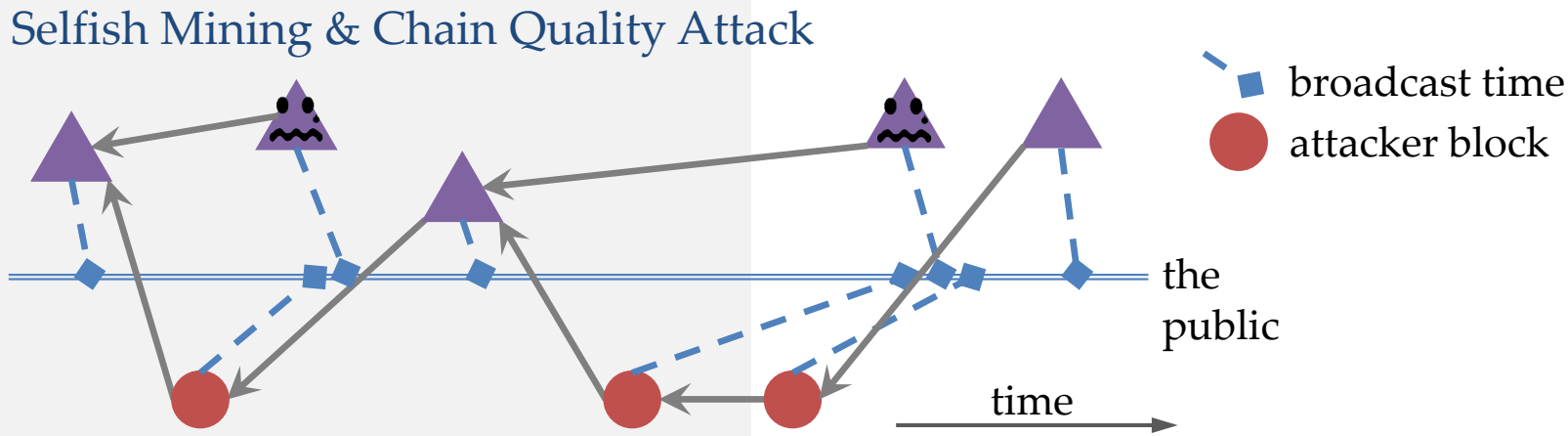
Crab Mentality:
If I don't get it, you don't get it either.

Alternative PoW Protocols

?


bitcoin
2
1

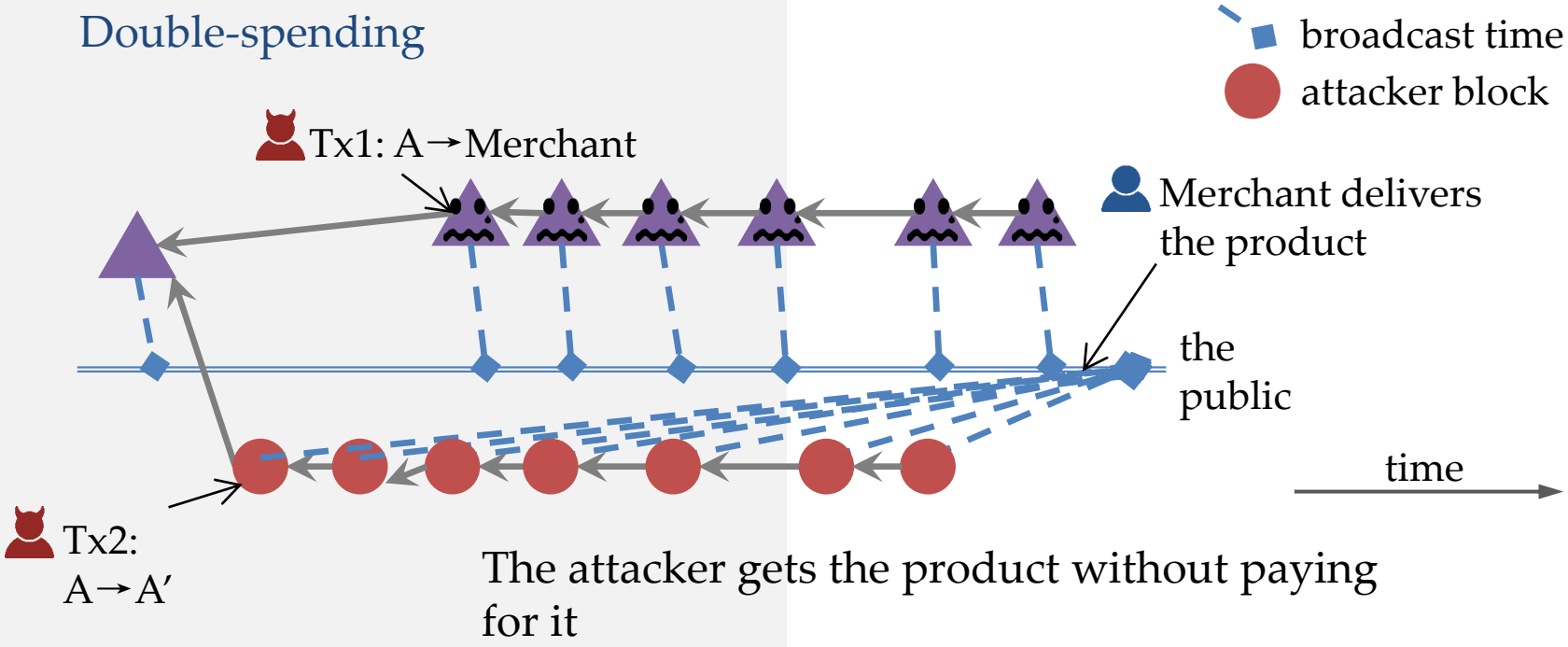
The Imperfect Chain Quality → Three Attacks



The attacker gains **unfair** block rewards; rational miners would join the attacker, which damages decentralization

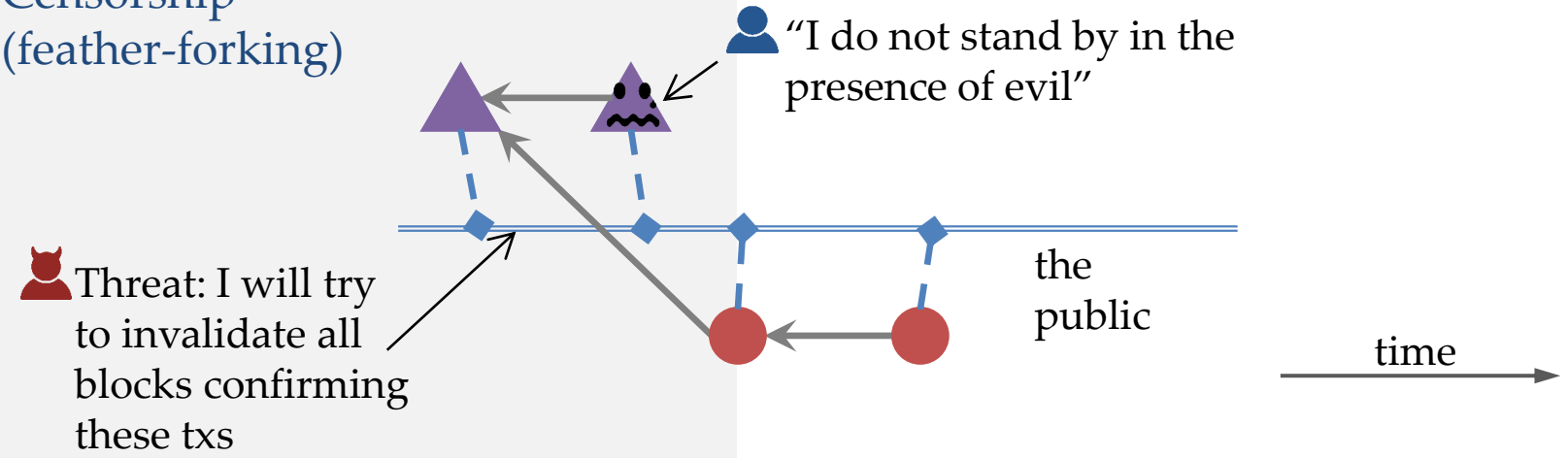
The Imperfect Chain Quality → Three Attacks

Double-spending



The Imperfect Chain Quality → Three Attacks

Censorship (feather-forking)



Rational choice: join the attacker in censorship
The attacker becomes a *de facto* owner

Our Evaluation Framework: Four Metrics

A better-than-NC protocol needs to

- Achieve better chain quality ❶❷
- **Or** resist better against all three attacks:
  - Selfish mining 👉 incentive compatibility ❶
  - Double-spending 👉 subversion gain ❶
  - Censorship 👉 censorship susceptibility ❷

❶ profit-driven adversary

❷ byzantine adversary

Better-than-NC Candidates

Better-chain-quality protocols:
"I can raise the chain quality"

- UTB: Ethereum PoW, Bitcoin-NG (Aeternity, Waves)
- SHTB: DECOR+ (Rootstock)
- UDTB: Byzcoin, Omniledger
- Publish or Perish

In the paper

Attack-resistant protocols:
"I don't need to raise the chain quality, I can defend against the attacks"

- Reward-all ("compensate the losers"): Fruitchains, Ethereum PoW, Inclusive, SPECTRE, PHANTOM, …
- Punishment ("fine all suspects"): DECOR+, Bahack's idea
- Reward-lucky (content-based reward): Subchains, Bobtail

Simplified Results

😀 better
😟 it depends
😵 worse

"Better-chain-quality"	Chain Quality
Uniform tie-breaking	😵
Smallest-hash tie-breaking	😵
Unpredictable deterministic tie-breaking	😵
Publish or perish	😟

"Attack-resistant"	Incentive compatibility	Subversion gain	Censorship susceptibility
Reward-all 👉Fruitchains	😵	😵	😀
Punishment 👉Reward-splitting	😀	😀	😵
Reward-lucky 👉Subchains	😵	😵	😵

Insight: Rewards Don't Solve the Attacks

A dilemma: "Rewarding the bad vs. punishing the good"

- Reward all -> no risk to double-spend
- Punish -> aid censorship
- Reward lucky -> lucky≠good

A common mistake

- Attackers have different incentives; no reward scheme discourages all of them

Insight: What Not to DO

- Designing protocols too complicated to analyze
- Security analysis
  - against one attack strategy
  - against one attacker incentive
  - with unrealistic parameters

If it is provably secure, it is probably not.

— Lars Knudsen on block ciphers

If a protocol is not provably secure, it is probably not secure.

—Lars Knudsen, as I recalled

But he never said this.

But the modified quote is also valid, I believe.

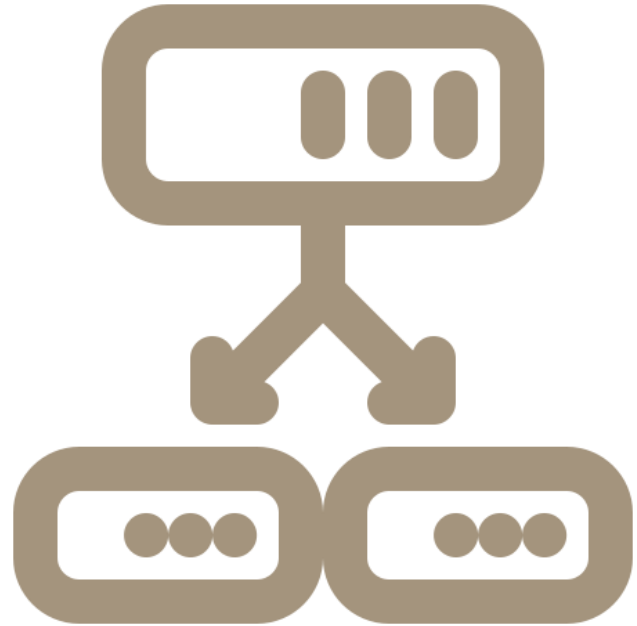
Unless you are Satoshi Nakamoto.

Publication

- Ren Zhang and Bart Preneel. Lay down the common metrics: Evaluating proof-of-work consensus protocols' security. In *40th IEEE Symposium on Security and Privacy (S&P)*, pages 1190–1207. IEEE, May 2019
- https://www.esat.kuleuven.be/cosic/publications/article-3005.pdf
- https://www.youtube.com/watch?v=UV5E-DjCHn4

3

Against 7 Sharded Blockchains



Sharding: A Problem Solver of Troublemaker?

Motivation:

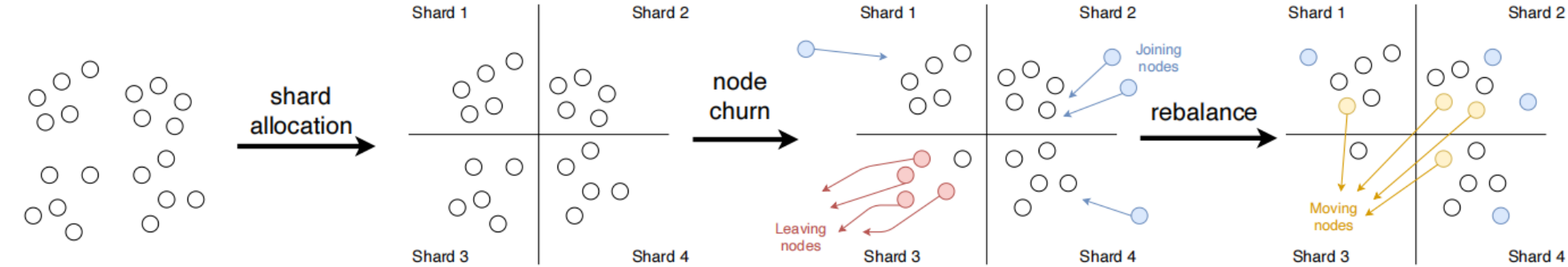
- Sharding—distributing the tasks to different servers—is successful in scaling databases
- Can we apply that to permissionless blockchains?

Challenges

- Cross-shard transactions are expensive dangerous
- and—

Protocol	Citations (till 2024)
Elastico	1424
Omniledger	1218
Rapidchain	1052
Monoxide	449
Chainspace	366
Ethereum 2.0	Industry, abandoned
Zilliqa	Industry

Shard (Re)Allocation



Desirable Properties

Why is reallocation indispensable?

- When no one moves, the attacker can gradually take over a shard
- Network churn also leads to unbalanced shard sizes

Suspicious preconditions we don't challenge

- Everyone knows when to do reallocation
- No Sybil attacks
- Trustworthy global randomness

Desirable properties

- **Self-balance**: (roughly) shards are uniformly distributed despite churn
- **Operability**: some nodes don't shuffle
- Public verifiability, Liveness, Allocation randomness, Unbiasability, privacy, …

Selected Results

- **Evaluation**: all existing designs choose an extreme between self-balance and operability
- **Proof**: impossible to achieve the optimal values on both properties
- **Design**: a new design to parametrize between them

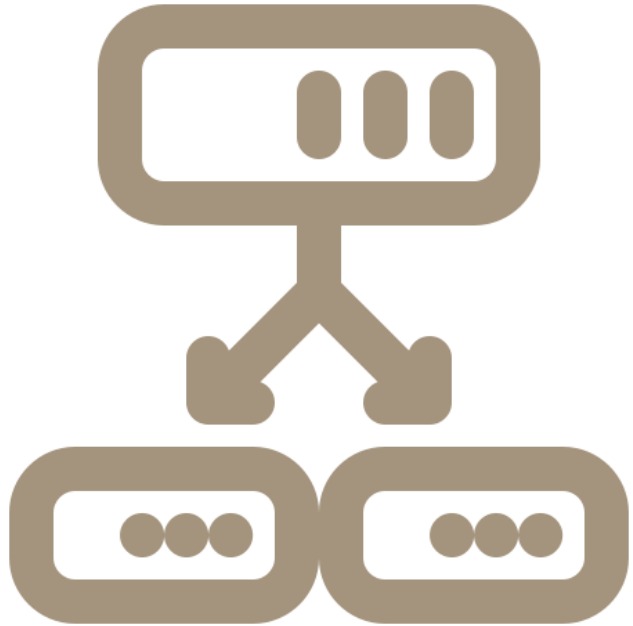
- **Self-balance**: (roughly) shards are uniformly distributed despite churn
- **Operability**: some nodes don't shuffle

Publication

- Runchao Han, Jiangshan Yu, Ren Zhang. Analysing and improving shard allocation protocols for sharded blockchains. In *4th ACM Conference on Advances in Financial Technologies (AFT)*, pages 198–216. ACM, September 2022
- https://ia.cr/2020/943

4

Against 2 DAG-Based Protocols



NC's Security-Performance Tradeoff

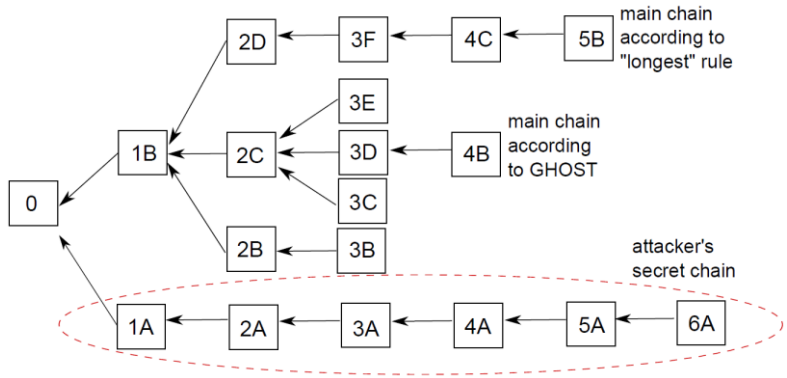
To raise performance:
↑ block size or ↓ block interval

👇

orphaned blocks ↑

👇

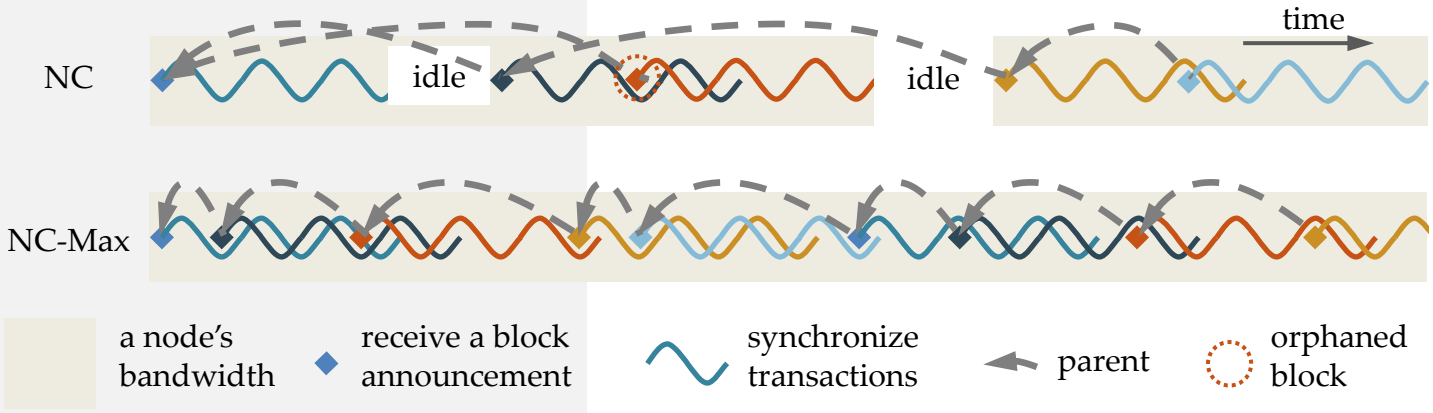
security ↓ (, performance ↓)



Sompolinsky et al. Secure High-Rate Transaction Processing in Bitcoin. In FC'15

NC-Max: Consensus of Nervos CKB

- **Decoupling** tx synchronization and confirmation 👉 allows **parallel tx processing**—similar to DAG—while preserving the chain-based structure
- **Recoupling** the two-step in an updated block structure 👉 inherits NC's **security** properties and **simplicity** in reward distribution



Submitted Several Times Before Accepted

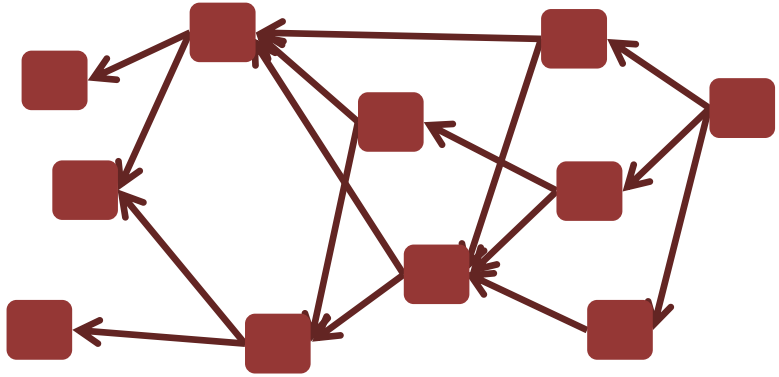
- Ren Zhang, Dingwei Zhang, Quake Wang, Shichen Wu, Jan Xie, Bart Preneel. NC-Max: Breaking the Security-Performance Tradeoff in Nakamoto Consensus. In *The Network and Distributed System Security (NDSS) Symposium*. April 2022
- https://ia.cr/2020/1101
- https://www.youtube.com/watch?v=CyT3mPOROes
- https://www.bilibili.com/video/BV1XP411n7qV/?share_source=copy_web&vd_source=5b7cb08c03174c2368cdf12a61382f63

*Why a **chain-based** protocol when **DAG** protocols solve the security-performance tradeoff already?*

— Reviewers in 2020 and 2021

Early DAG-based Protocols

- Motivation: higher throughput
- Solution: chain → Directed Acyclic Graph (≥1 predecessors, ≥1 concurrent blocks)
- Security
  - Weak guarantees (inclusive, meshcash)
  - Partial analysis (SPECTRE, PHANTOM, Conflux)

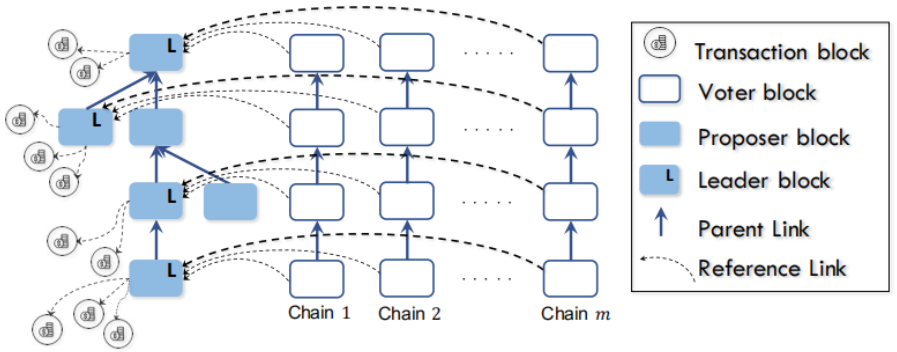


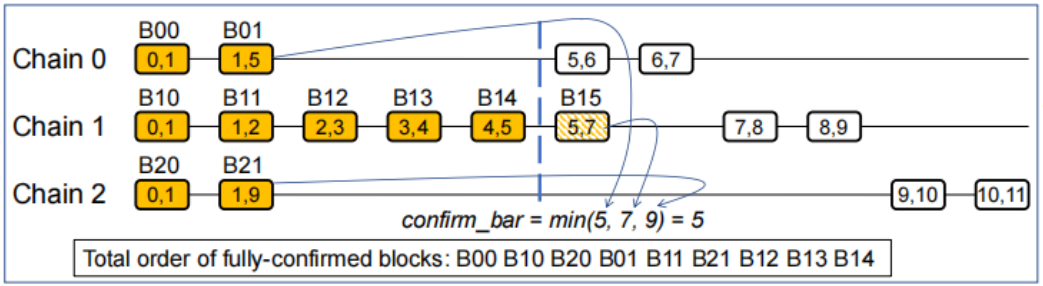
Provable Secure DAG-based Protocols

- Decoupling tx synchronization and **confirmation** (like NC-Max)
- 👆 with **NC chains** of small blocks
- Borrowing 👆NC's security proof

Can they really get away with the security-performance tradeoff?

- Prism and OHIE





The Hidden Assumption of Decoupling

Prism and OHIE's assumption:
all "small blocks"

- Enjoy a short and constant delay
- Are always accepted immediately

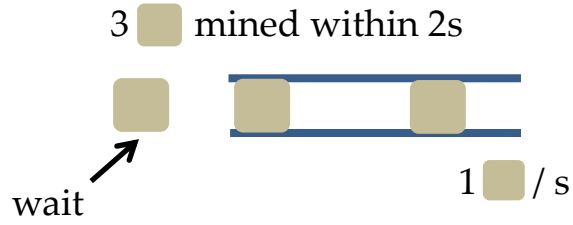
But it does not always hold, because 👉

We did some clever mathematical analysis 📝

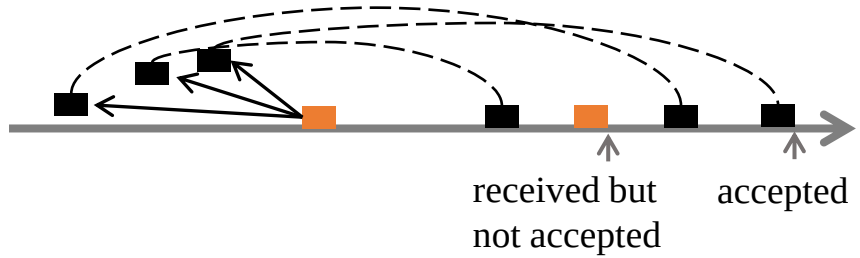
Result: they also suffer from the security-performance tradeoff

Not easy to get it published, either …

- Block jam



- Late predecessor



*Why a **chain-based** protocol when **DAG** protocols solve the security-performance tradeoff already?*

— Reviewers in 2020 and 2021

*Why analyzing **DAG** when **chain-based** protocols solve the security-performance tradeoff already?*

— Reviewers in 2022 and 2023

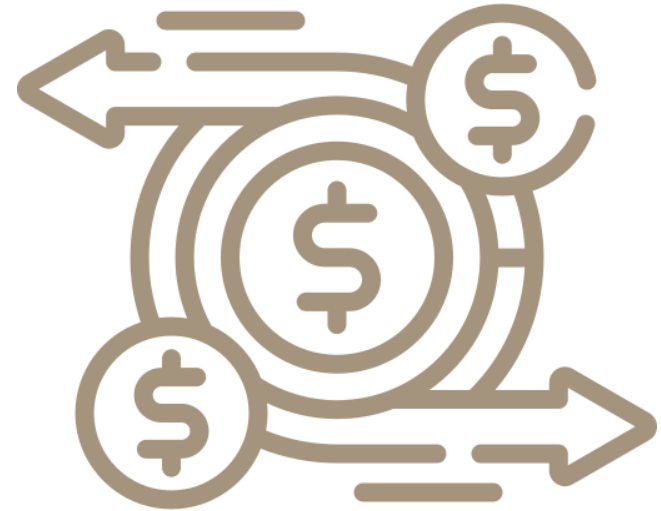
To DAG-based protocols:

Please don’t die until I am done with you.

Luckily

- Shichen Wu, Puwen Wei, Ren Zhang, Bowen Jiang. Security-Performance Tradeoff in DAG-based Proof-of-Work Blockchain Protocols. In *The Network and Distributed System Security (NDSS) Symposium*. February 2024
- https://ia.cr/2023/1089

Against All PoS Protocols



~~Life~~ This talk is too short to be wasted on attacking PoS protocols.

See my 2019 talk.

https://www.youtube.com/watch?v=gxFm1QieUdE

Statistics

In 585 papers presented at top CS conferences from 2020 to 2022

- 41 papers focus on PoW
  - Formal analysis of NC (10)
  - New design: DAG (7), non-DAG (6)
  - Mining attacks and ecosystem (18)
- 23 papers involve PoS
  - Analysis (11)
  - New design (12)

https://space.bilibili.com/1887870712/channel/seriesdetail?sid=3197977 (in Chinese)

Insights

- PoW: more secure than previously believed
- PoS: more attack vectors discovered (basically, instantiating my 2019 talk)
- New PoS Designs: not sure we can ever achieve PoW's security
- PoS ecosystems: lack of studies raises concerns

A Special Case: Ethereum PoS

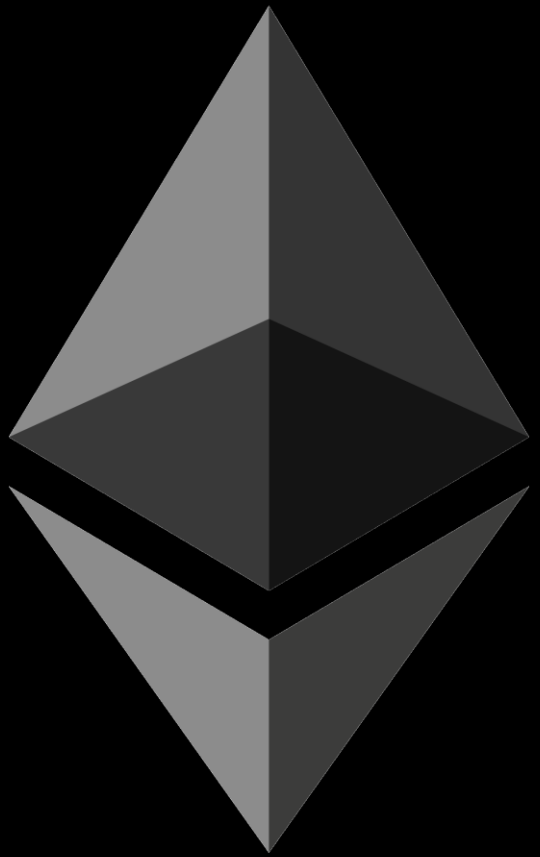
- A valid block to some may be invalid to others
- Synchronous model when issuing rewards, partially synchronous model when confirming blocks
- Thus, it could "reward the bad" and "punish the good"

- No block validity consensus
  (see "against BU")
- If a protocol is not provably secure, it is probably not secure
  (see "against 9 other PoW protocols")
- Rewards don't solve the attacks
  (see "against 9 other PoW protocols")

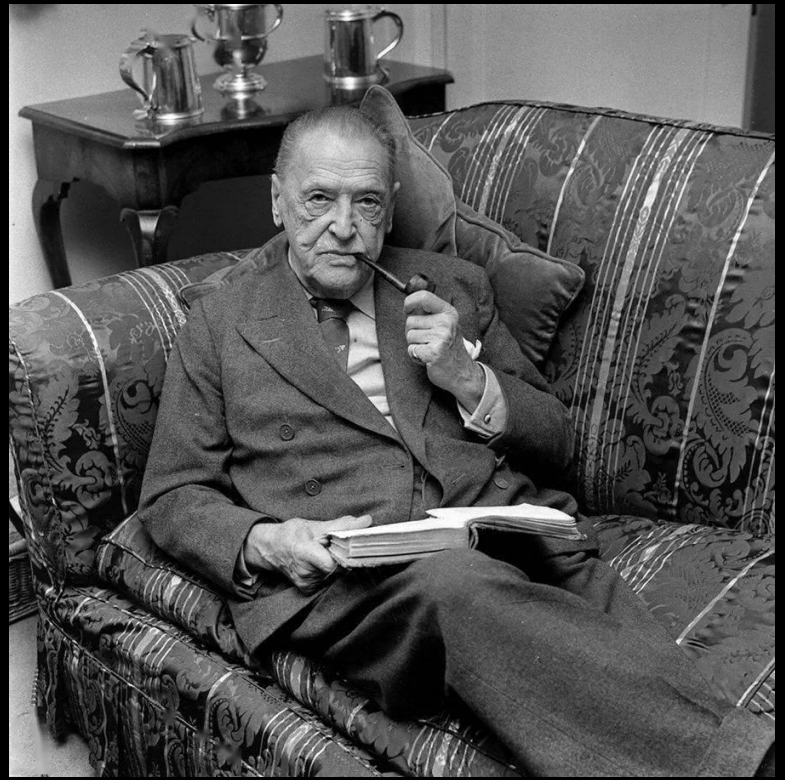
A Special Case: Ethereum PoS

- A valid block to some may be invalid to others
- Synchronous model when issuing rewards, partially synchronous model when confirming blocks
- Thus, it could "reward the bad" and "punish the good"

- Caspar Schwarz-Schilling, Joachim Neu, Barnabé Monnot, Aditya Asgaonkar, Ertem Nusret Tas, David Tse. Three Attacks on Proof-of-Stake Ethereum. *Financial Cryptography*, 2022, arXiv 2110.10086
- Joachim Neu, Ertem Nusret Tas, and David Tse. Two More Attacks on Proof-of-Stake GHOST/Ethereum. In *ACM Workshop on Developments in Consensus (ConsensusDay)*. ACM, 43–52.
- Mingfei Zhang, Rujia Li, Sisi Duan. Max Attestation Matters: Making Honest Parties Lose Their Incentives in Ethereum PoS. *Usenix Security 2024*. https://ia.cr/2023/1622



The future belongs to PoS Ethereum.



Those who cannot remember the past are condemned to repeat it.

—George Santayana

What's next?

With so many researchers attacking Ethereum, it is difficult to find a new angle.

Let alone a new message.

Yet I managed to find one.

But I write slowly.

To Ethereum:

Please don’t die …

until I am done with you.