Max Attestation Matters: Making Honest Parties Lose Their Incentives in Ethereum PoS

Mingfei Zhang
Shandong University

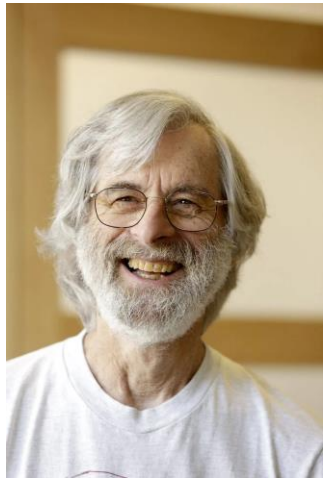
Rujia Li
Tsinghua University

Sisi Duan
Tsinghua University

16 Aug, 2024

USENIX Security 2024

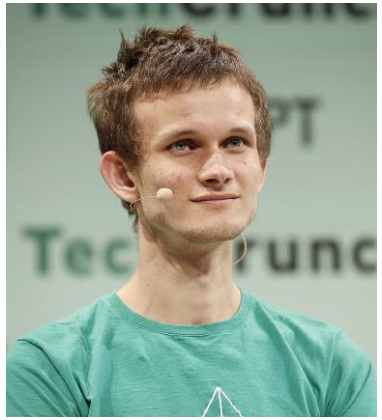
The History of Distributed System



Leslie Lamport
Byzantine Generals Problem

Babara Liskov
First practical BFT

Satoshi Nakamoto
Bitcoin



Vitalik Buterin
Ethereum

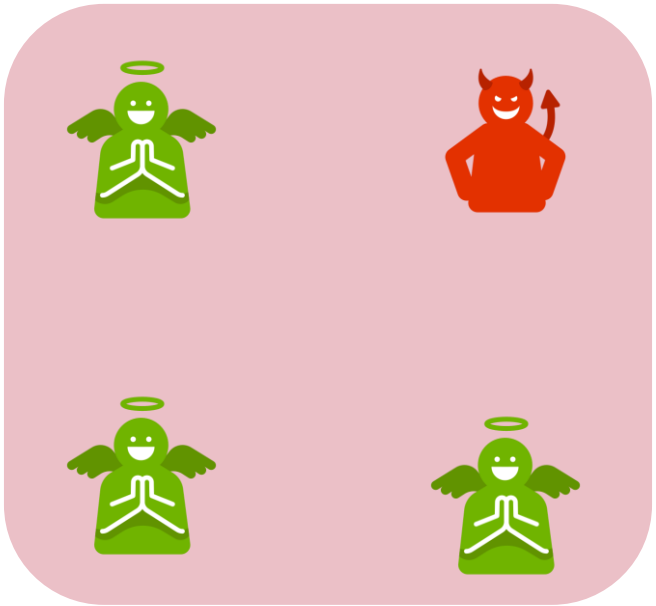
1982 1999 2008 2013

Figure source: Wikipedia

Understanding Blockchain Security

System model

- The system is maintained by a group of nodes;
- Allowing for the existence of some malicious nodes;
- The majority of nodes are honest.

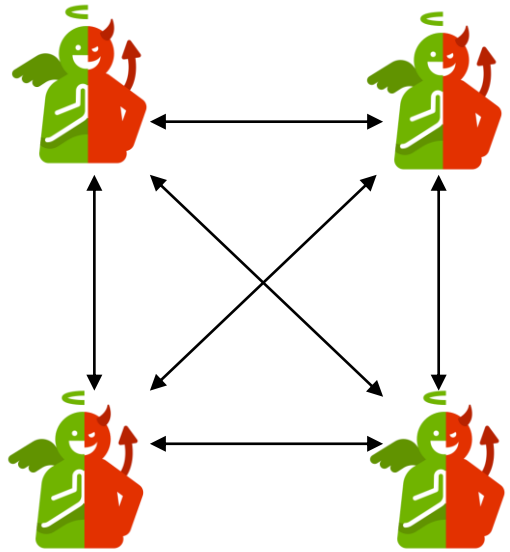


Security goals

- **Safety**: ensures that all honest nodes have a consistent view of the system's state at all times.
- **Liveness**: ensures that the system can continue to process and confirm new transactions

Using Economic Incentive to Bridge the Gap

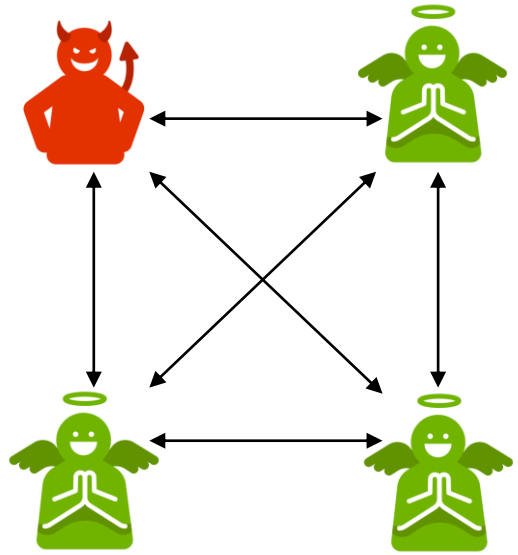
Real-world



Any node is rational and may choose to do evil for its interest

Economic Incentive

Real-world



Using incentives to keep the majority honest

Ethereum

- Ethereum is the second biggest blockchain.
- In September 2022, Ethereum transitions from Proof-of-Work to a Proof-of-Stake consensus mechanism, Gasper.

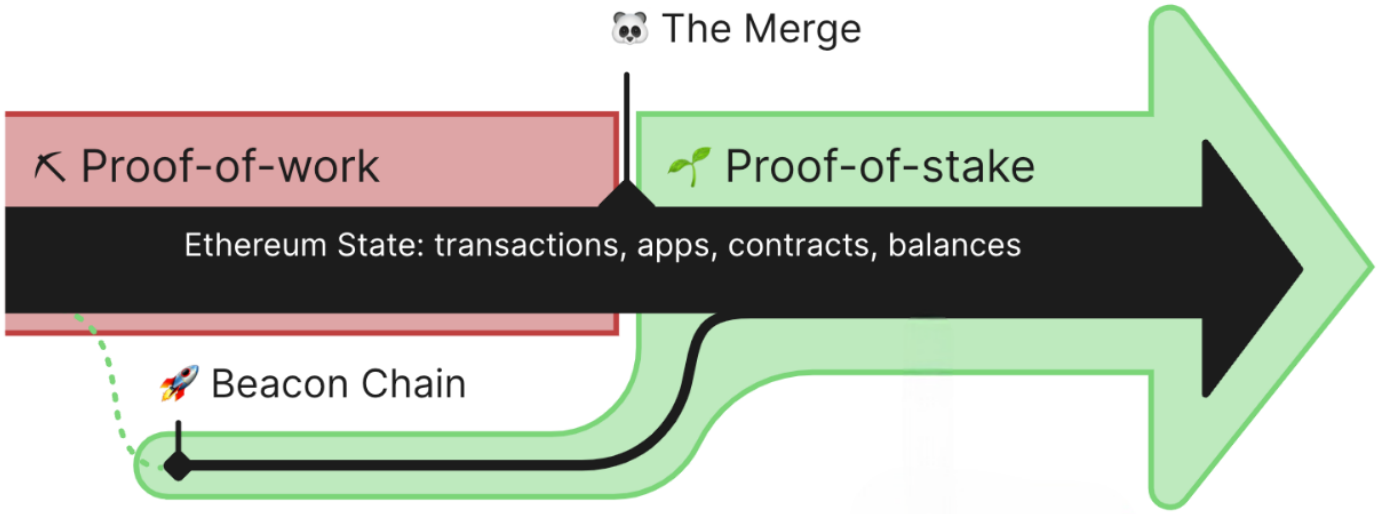
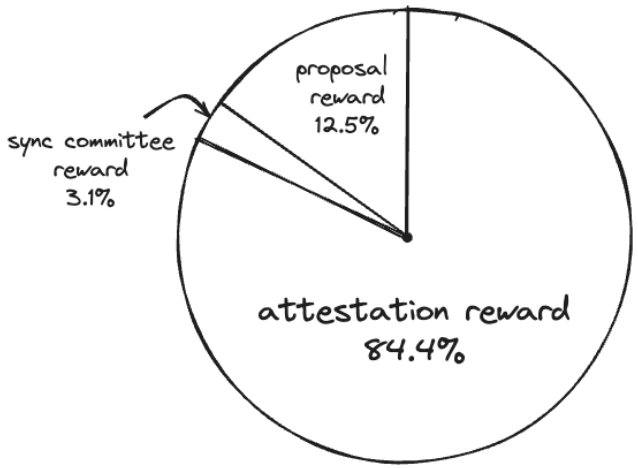
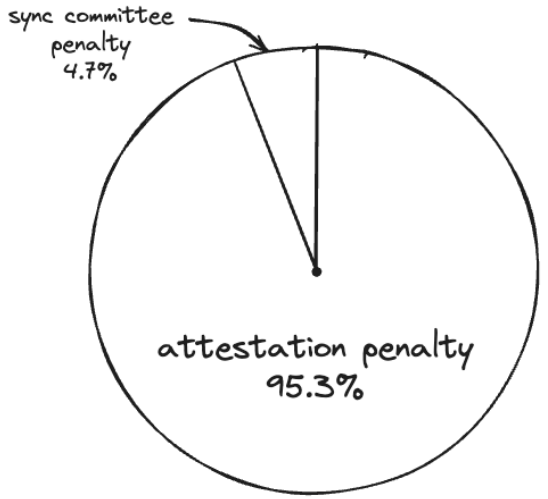


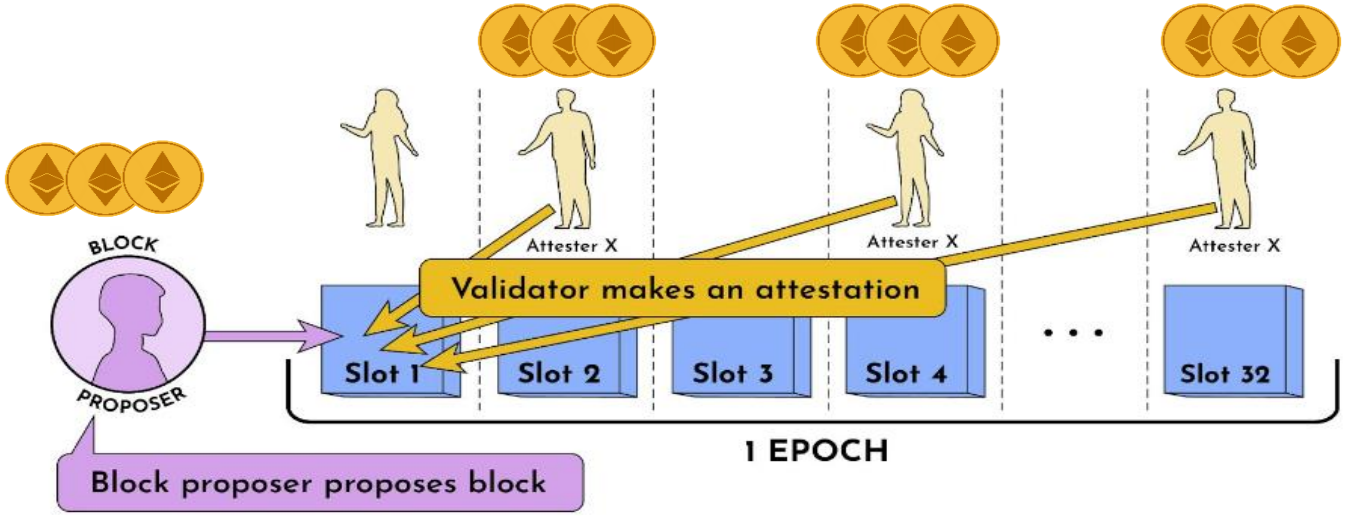
Figure source: https://ethereum.org/en/roadmap/merge/

Incentive Mechanism in Ethereum

- Attestation Incentives
  - Rewards
  - Penalties
- Block Rewards
- Sync Committee Incentives

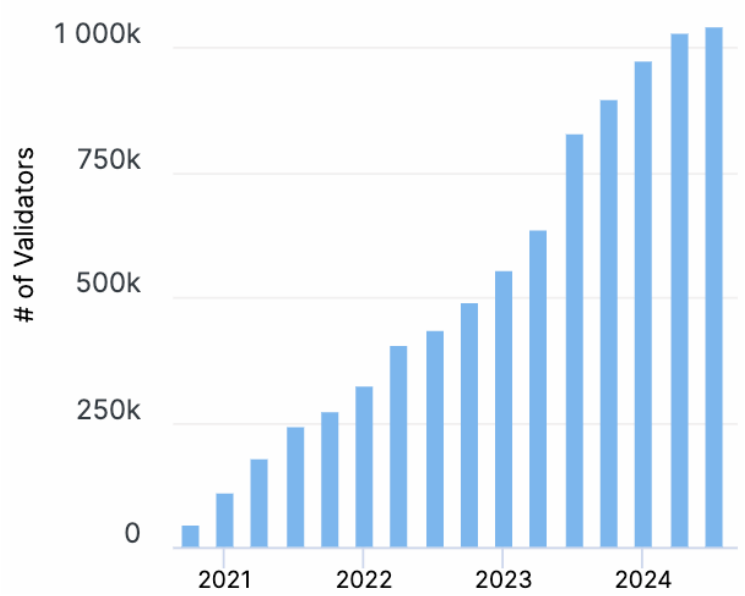






Incentive Mechanism is Successful

- Up to now, more than one million validators are in the system.
- Ethereum uses an incentive mechanism to keep validators active.
- The participation rate is very high, exceeding 99%.



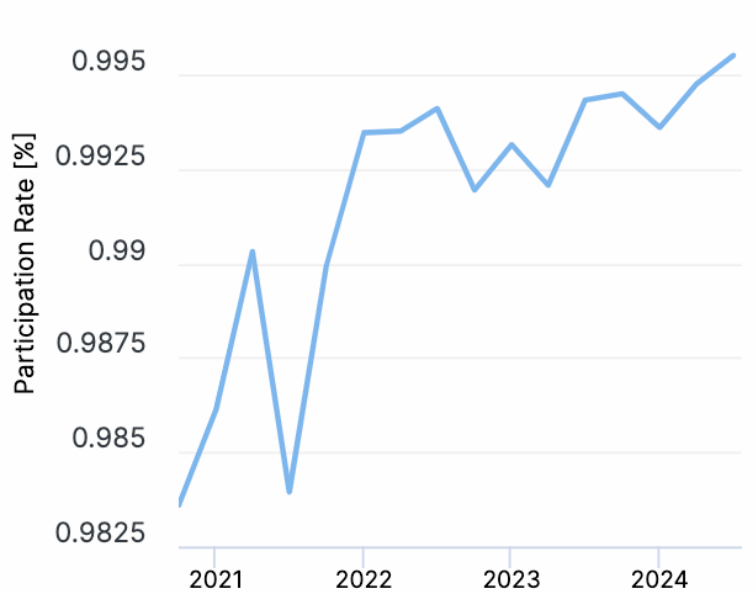


Figure source: beaconcha.in

Research Problems

Can we make honest players suffer from penalties (at least without receiving rewards) even if they strictly follow the protocol?

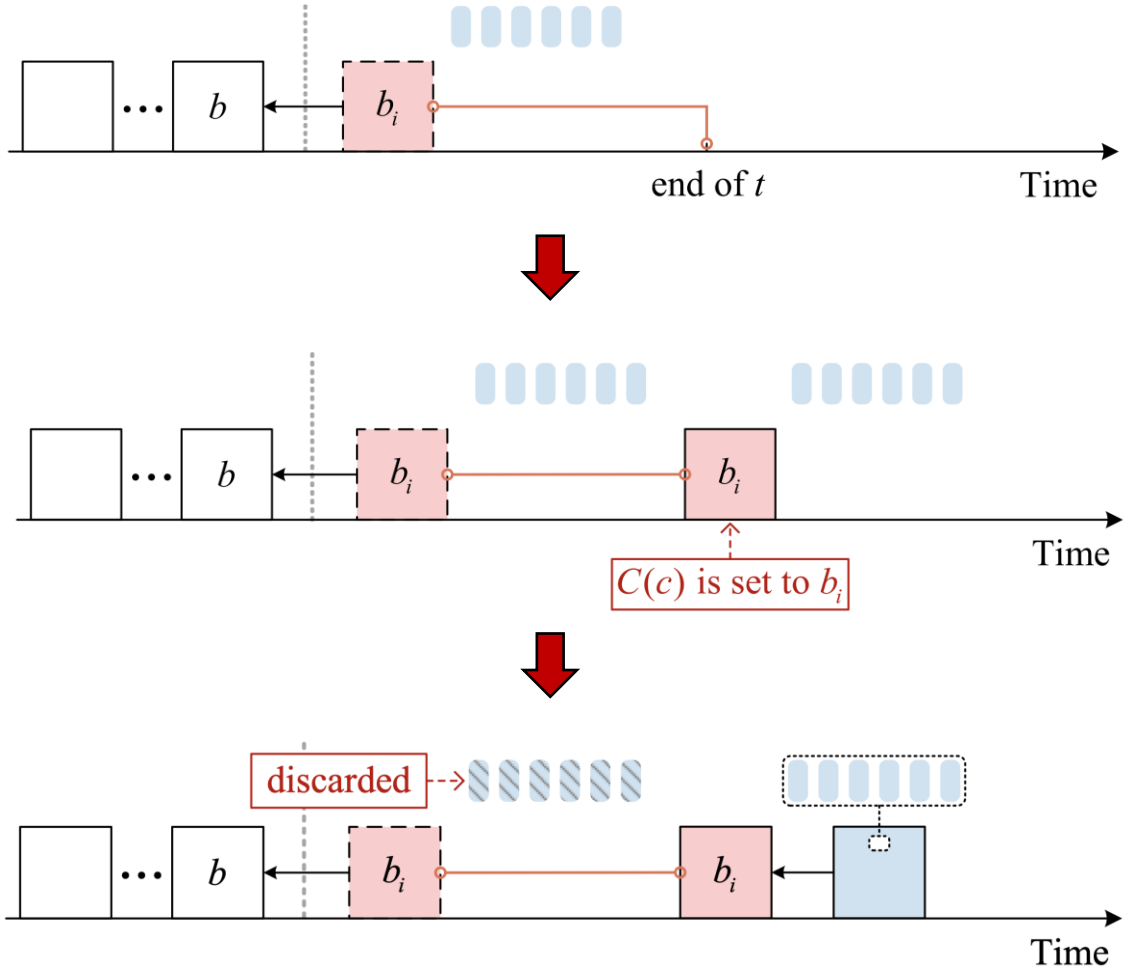
- Attacks on the attestation incentive mechanism causing honest validators to lose their incentives.

Attacks Overview

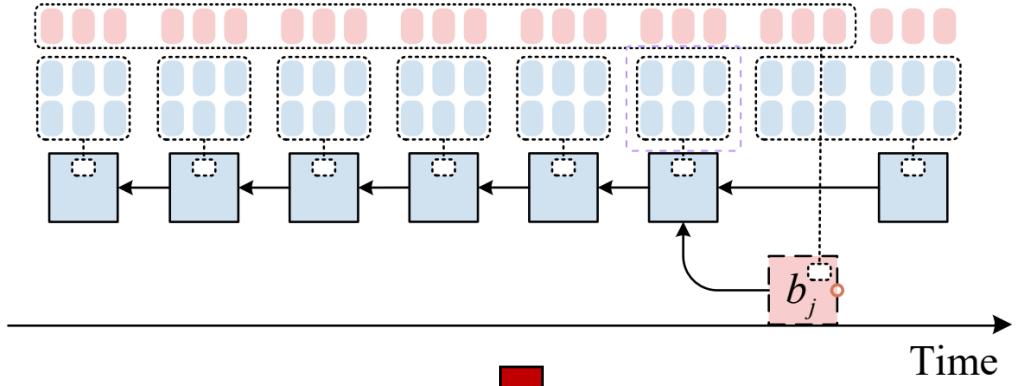
- We have identified two kinds of attacks:
  - Warm-up attack
  - Staircase attack
- In the warm-up attack, a single Byzantine validator can cause the honest validators to lose their attestation incentives.
- In the staircase attack, the adversary can cause the honest validators to lose all their attestation incentives, even lose their stake.

Warm-up Attack

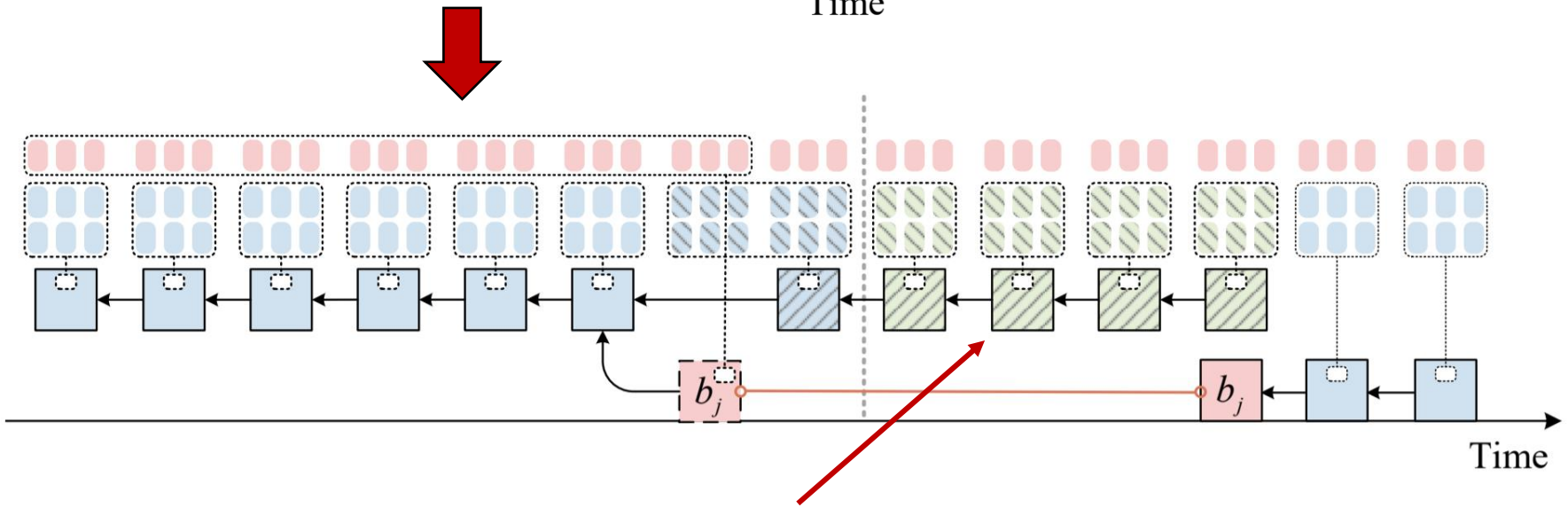
- Only one Byzantine validator is required to conduct the attack.
- To conduct the attack, the Byzantine validator must be the proposer at the first slot of an epoch.
- The adversarial strategy is withholding its blocks for 4 seconds.
- Approximately 1/32 honest validators will receive penalties after the attack.



Staircase Attack: One-time Attack



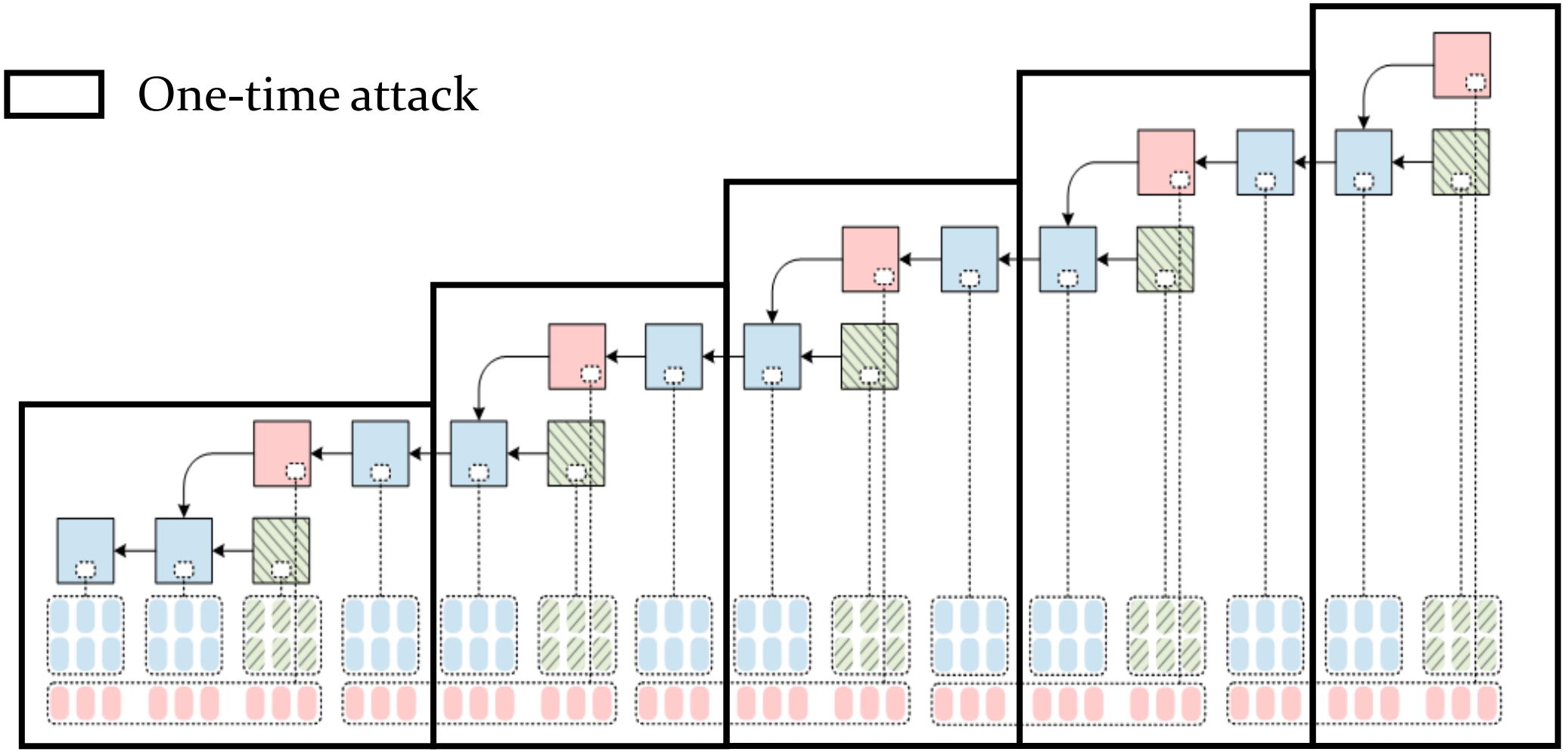
Step 1: The adversary creates and withholds a fork. The attestations from the adversary are included in the fork to affect the canonical chain.



Step 2: After waiting for half of the honest validators to vote in the next epoch, the adversary releases the withheld block b_j.

The chain from honest validators is forked out and the attestations in the chain are discarded.

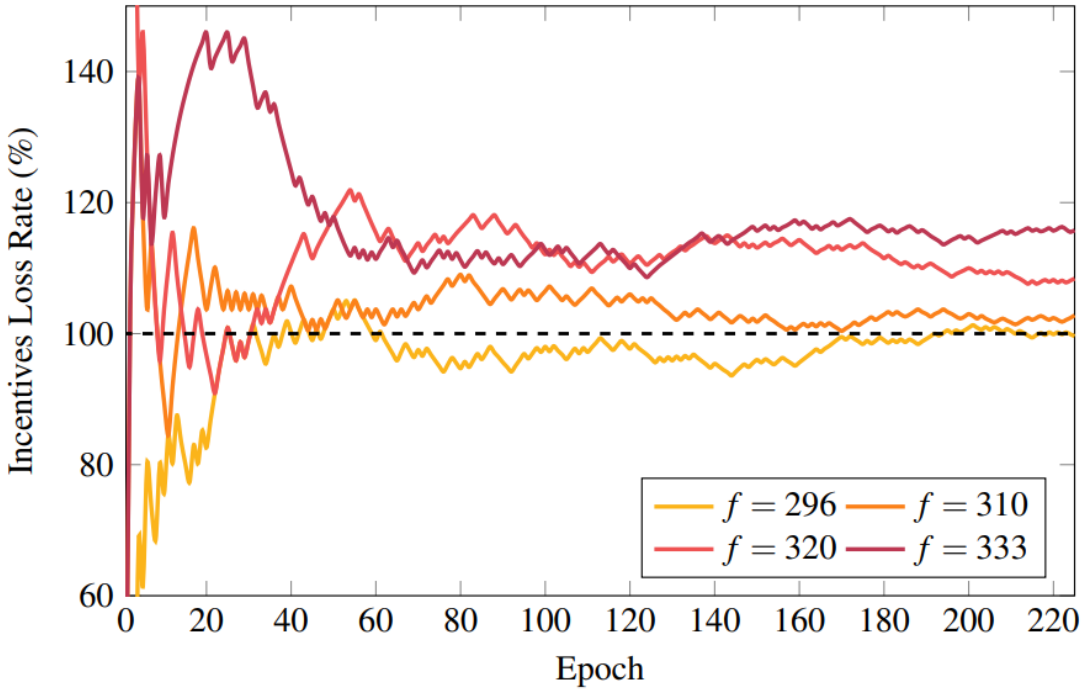
Staircase Attack: Repeat



Our Results

Theorem 1. *According to the configuration in Ethereum where* $W_r \leq 27W_p/20$ *(see Appendix A for more details), the expected incentive of any honest validators becomes lower than* 0 *when* $f \geq 8N/27 \approx 29.6\%N$.

- If there are 29.6% Byzantine validators, eventually all honest validators suffer from no attestation incentives;
- If the adversary controls a 33.3% stake, all honest validators are expected to suffer from a 20% stake loss compared to their fair share;



Attack Feasibility and Mitigation

- The feasibility of our attack is related to two parameters: the number of validators and the number of attestations each block can carry, i.e., the MAX_ATTESTATIONS parameter.

- Mitigation implemented by Ethereum significantly reduced the probability of continuing the attack in each epoch. The mitigation is already effective after the Deneb upgrade in March 2024.

Max Attestation Matters: Making Honest Parties Lose Their Incentives in Ethereum PoS

- Incentive mechanisms play an important role in the safety and liveness of the blockchain system.
- Two attacks against incentive mechanism in Ethereum PoS: warm-up attack and staircase attack.

Mingfei Zhang
mingfei.zh@outlook.com

Rujia Li
rujia@tsinghua.edu.cn

Sisi Duan
duansisi@tsinghua.edu.cn