The Performance of Selfish Mining in GHOST

Qing Xia, Wensheng Dou, Fengjun Zhang, Geng Liang

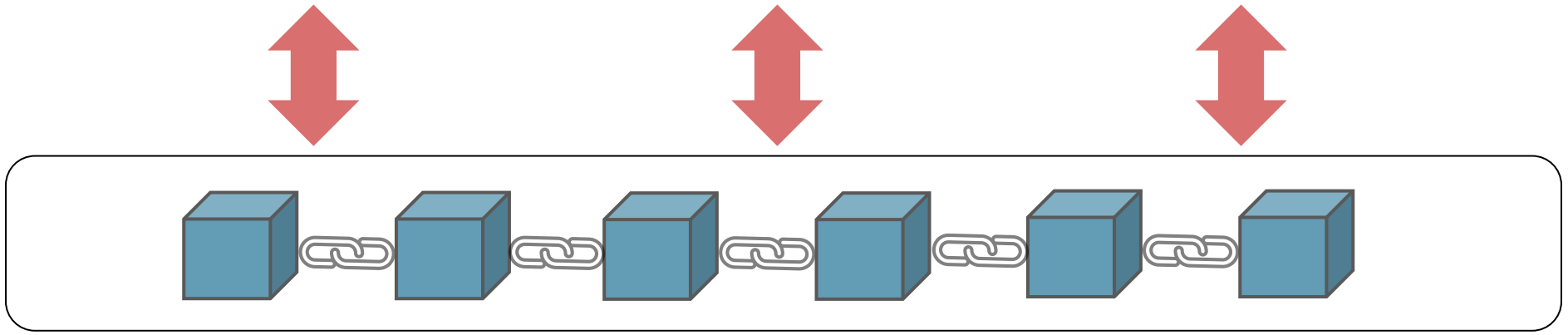
Institute of Software, Chinese Academy of Sciences

Blockchain has been widely adopted

Cryptocurrency payment

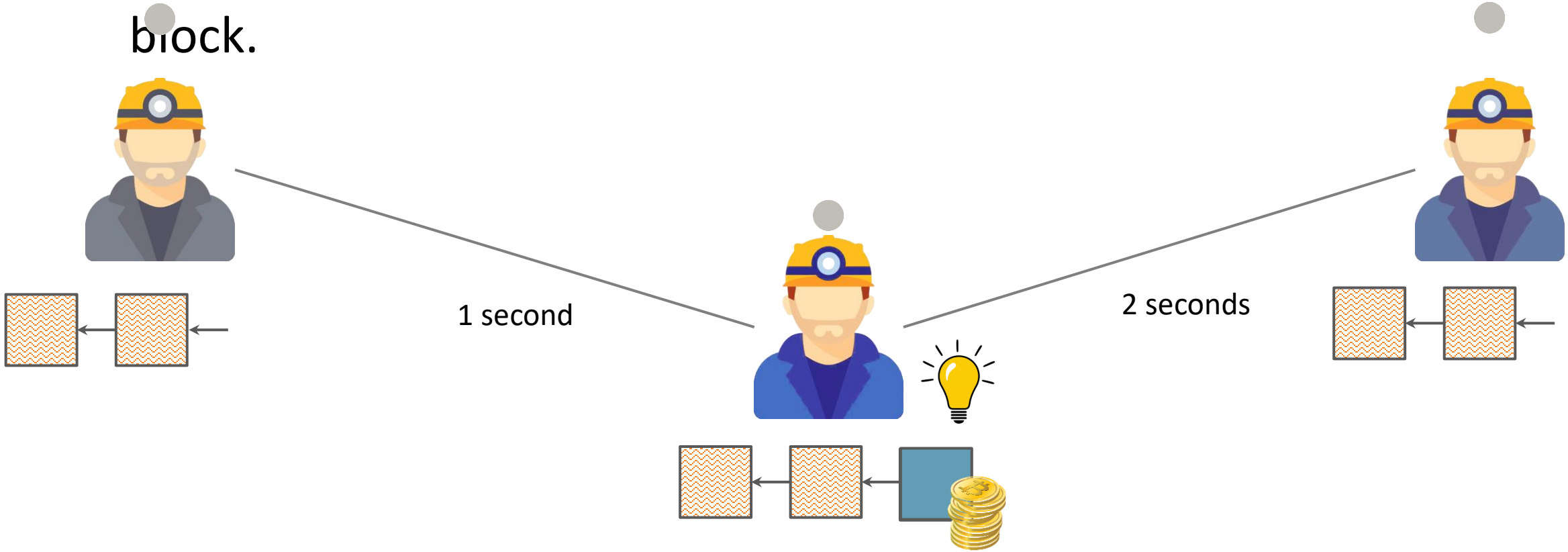
Supply chain management

Electronic government



Nakamoto consensus

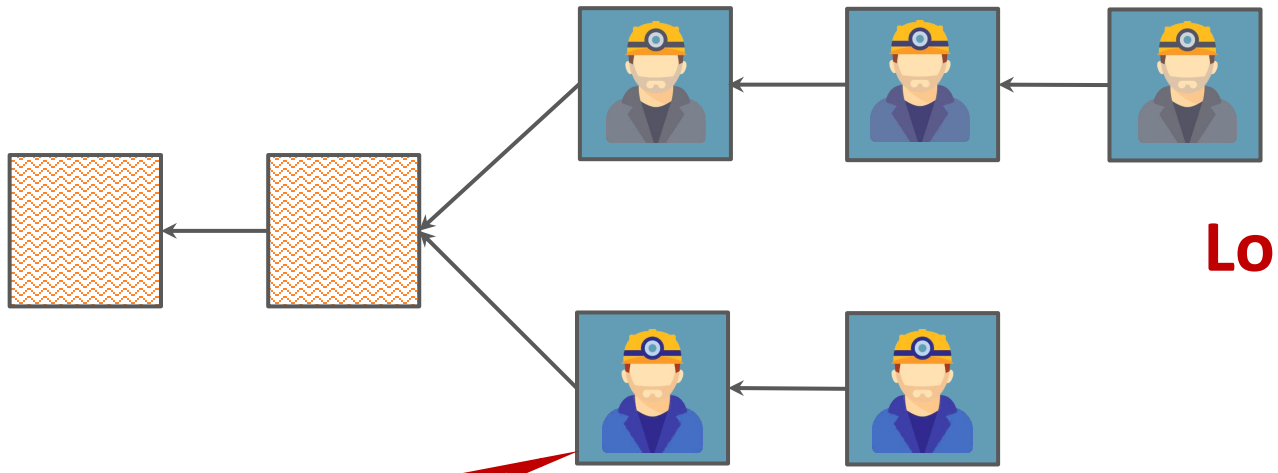
- **Proof of Work** is utilized to determine who can generate the new block.



Miner's reward is proportional to its mining power

Nakamoto consensus

- **The longest chain rule** is utilized to choose the main chain.



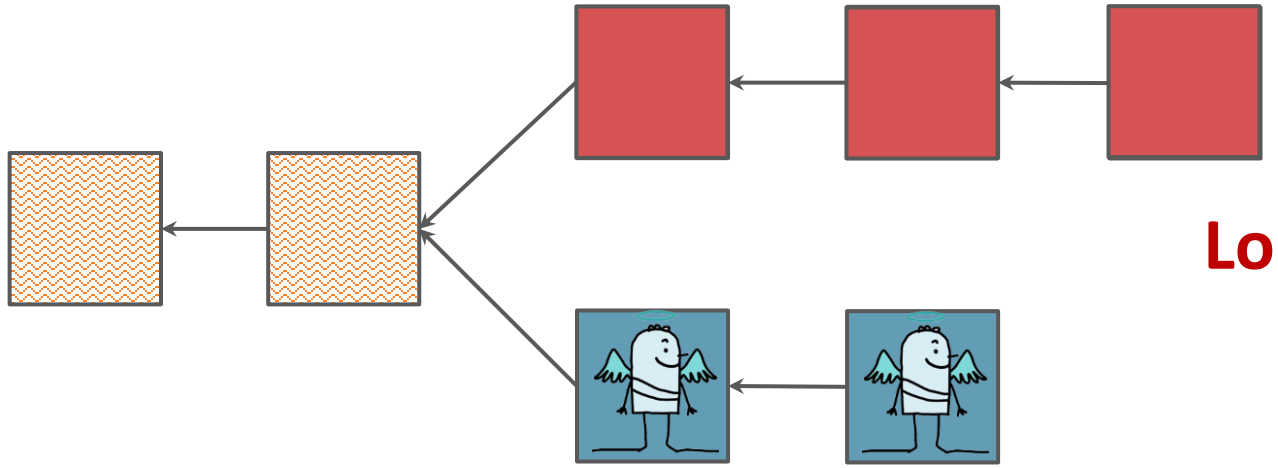
Fork happens when two miners generate blocks simultaneously.

Longest chain wins!

Blocks in the shorter chain are discarded as orphan blocks!

Selfish mining in the longest chain rule

- The game between 1 selfish pool (Alice) and 1 honest pool (Bob)

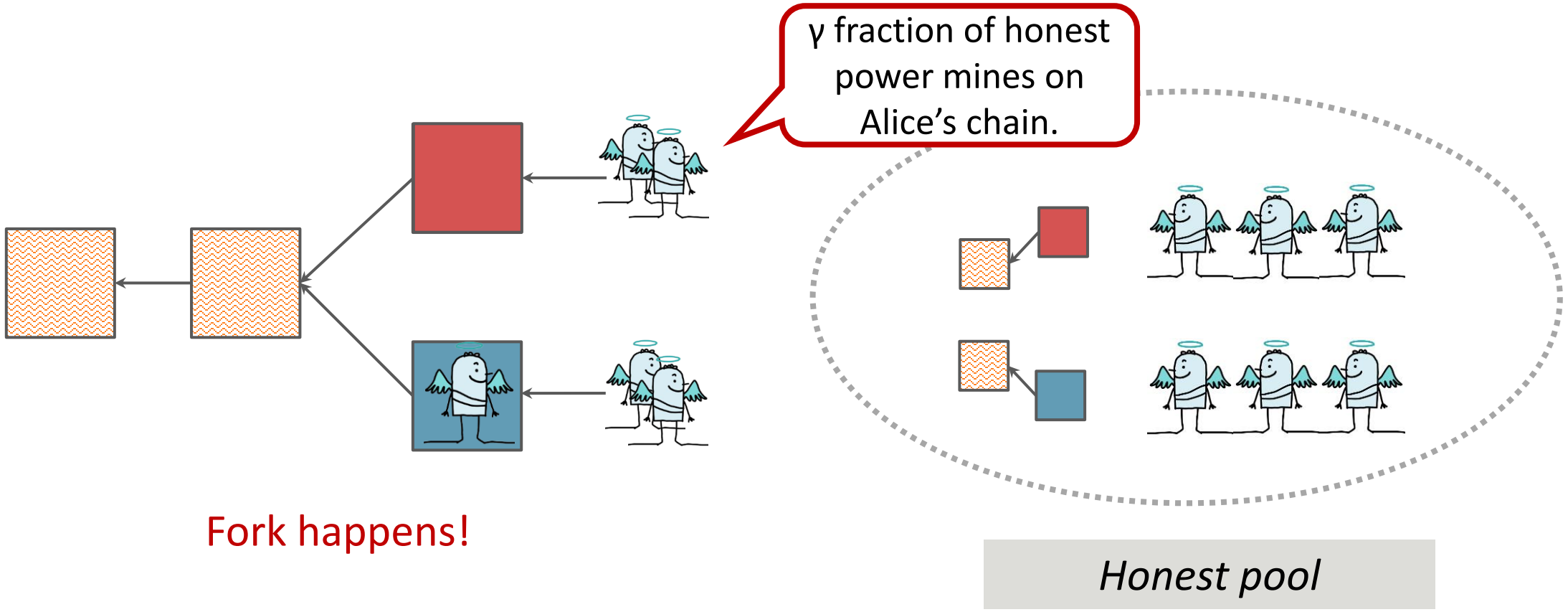


Longest chain wins!

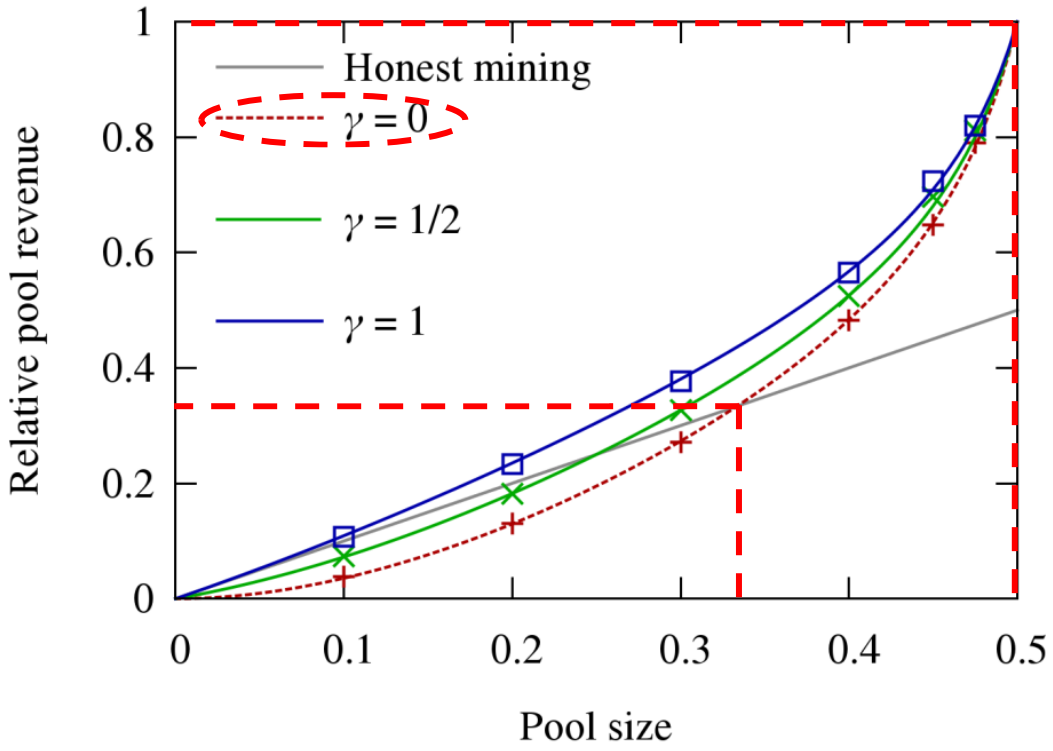
Bob wastes its power on orphan blocks!

Selfish mining in the longest chain rule

- The game between 1 selfish pool (Alice) and 1 honest pool (Bob)



Selfish mining in the longest chain rule

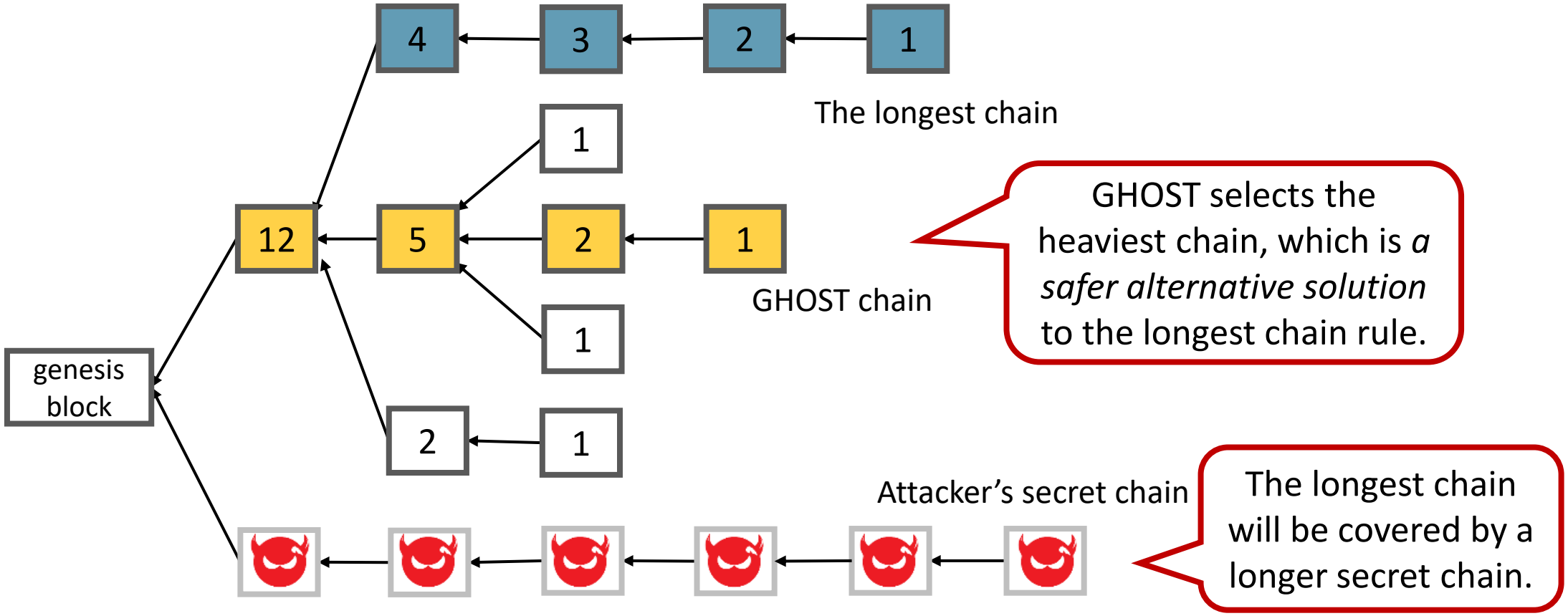


- When γ = 0, Alice with ≥ 33% mining power can gain more profit.
- No matter what γ is, with 50% mining power, Alice can gain almost all profit.

[1] I. Eyal and E. G. Sirer, Majority is not enough: Bitcoin mining is vulnerable, FC 2014.

GHOST (Greedy Heaviest Observed Subtree)

- Select the heaviest chain as the main chain.



A safer alternative solution to the longest chain rule.

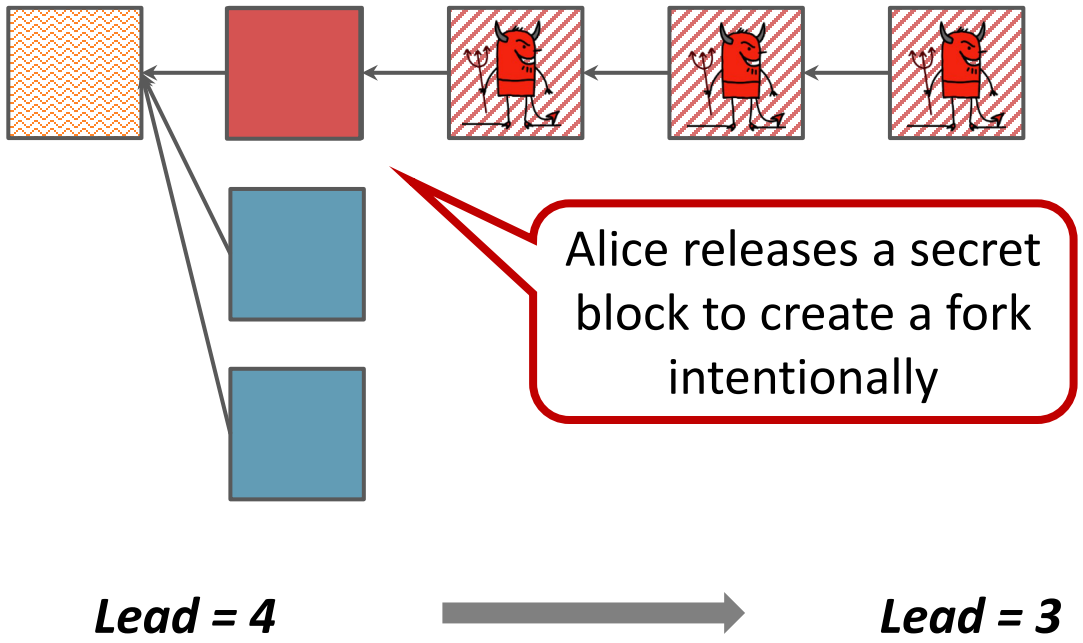
Selfish mining in GHOST

- RQ1: How does GHOST perform in selfish mining?

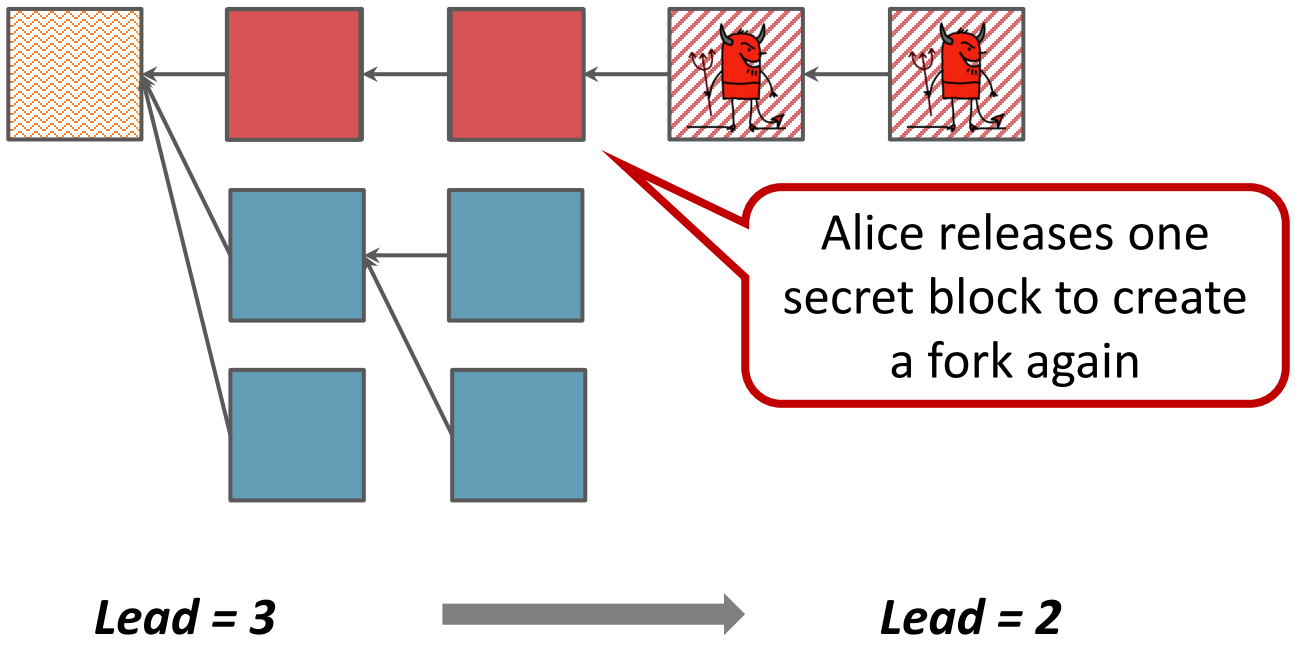
- RQ2: Does GHOST have better security than the longest chain rule under selfish mining?

“Match the height” in the longest chain rule

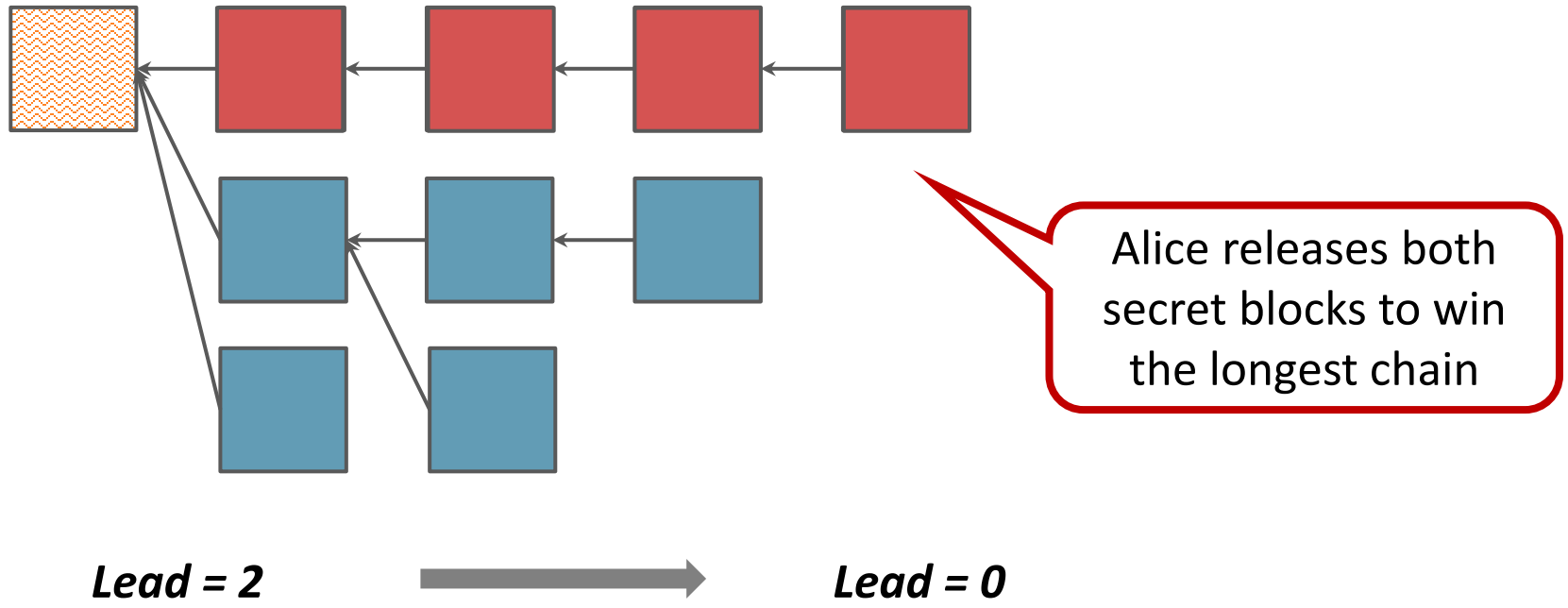
- Existing selfish mining strategies follow the idea of “match the height”.



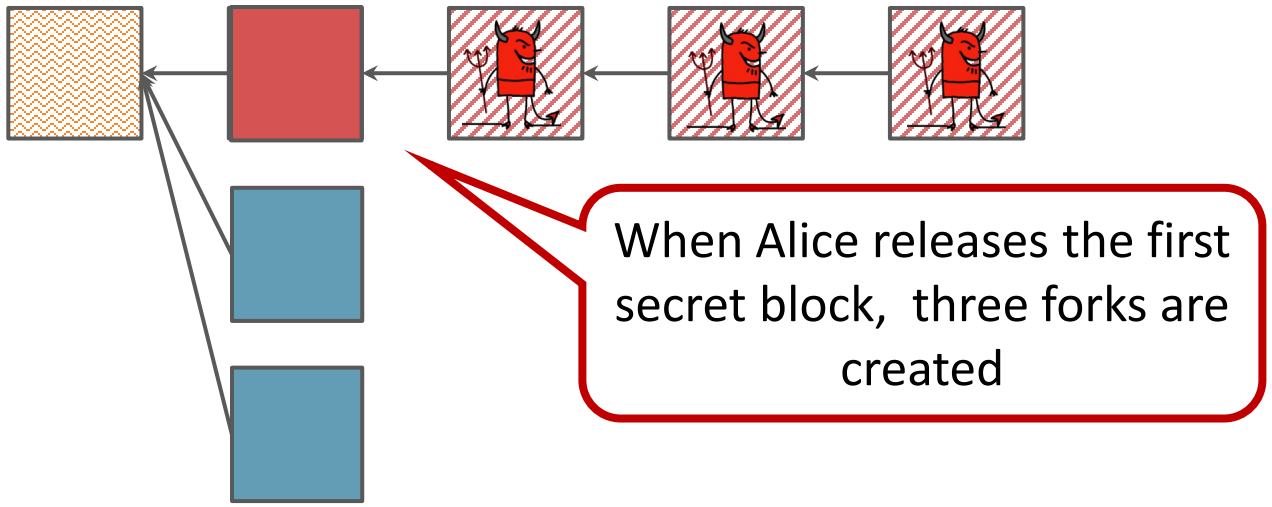
“Match the height” in the longest chain rule



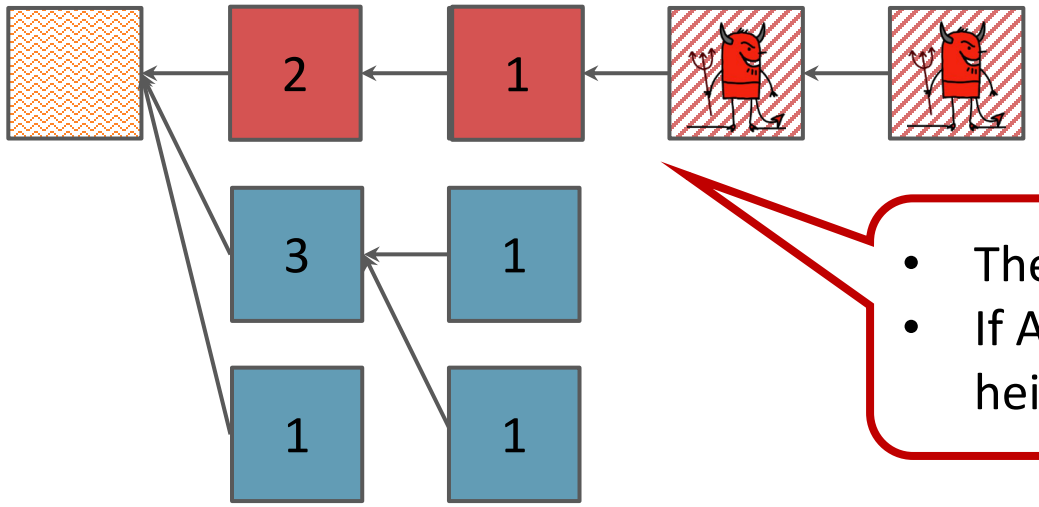
“Match the height” in the longest chain rule



“Match the height” in GHOST



“Match the height” in GHOST

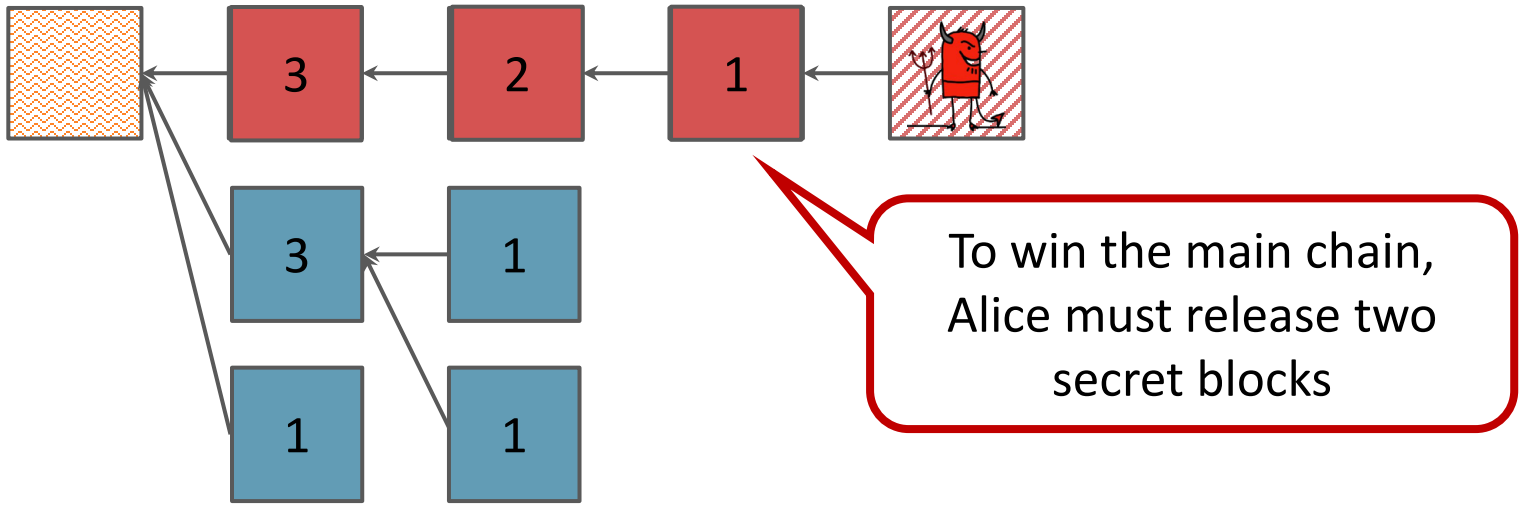


- There is only one heaviest chain.
- If Alice follows the idea of “match the height”, it can not win the main chain.

Lead = 3

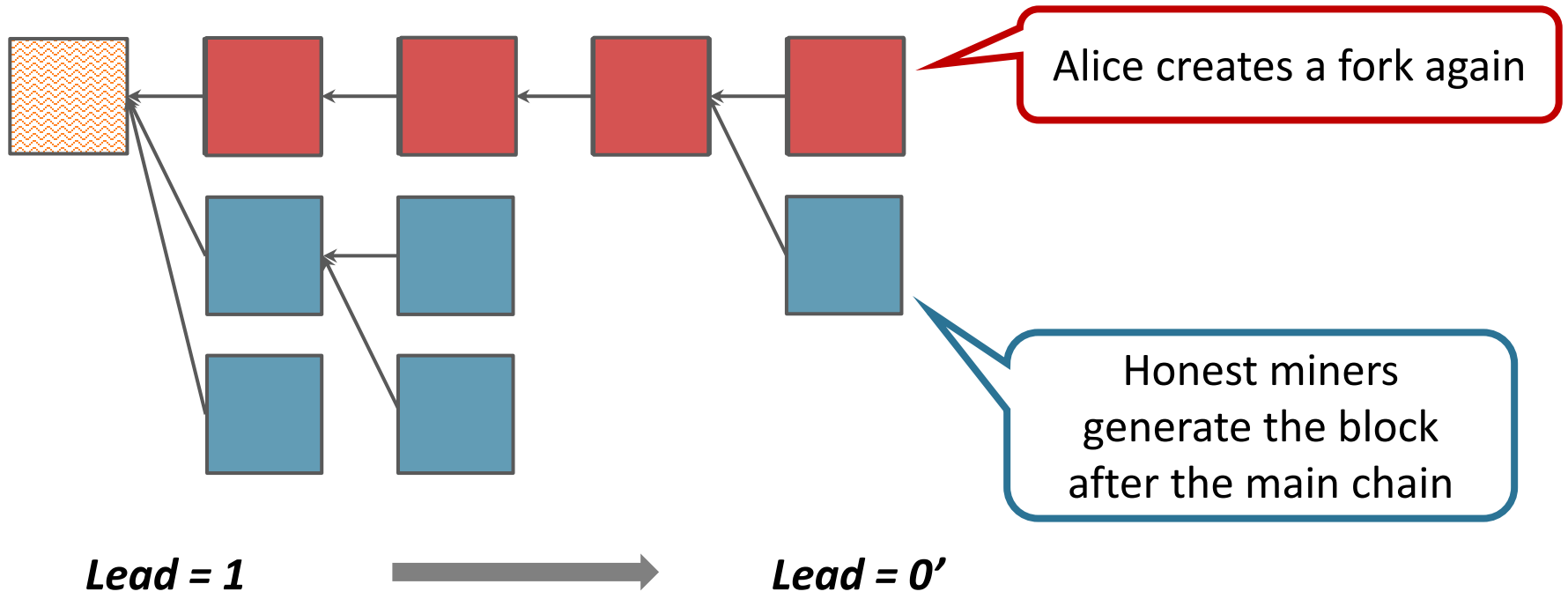
The idea of “match the height” can not be applied to GHOST.

“Match the weight” in GHOST

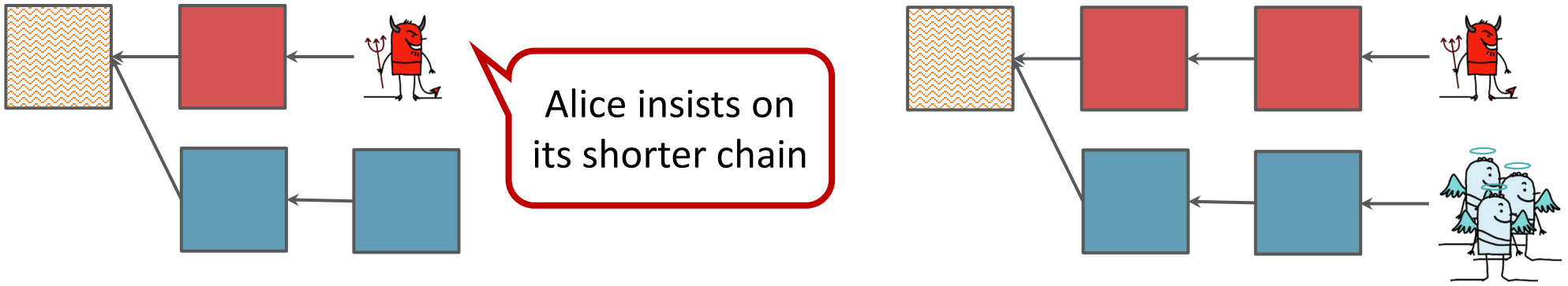


The selfish miner in GHOST follows the idea of “match the weight”.

“Match the weight” in GHOST



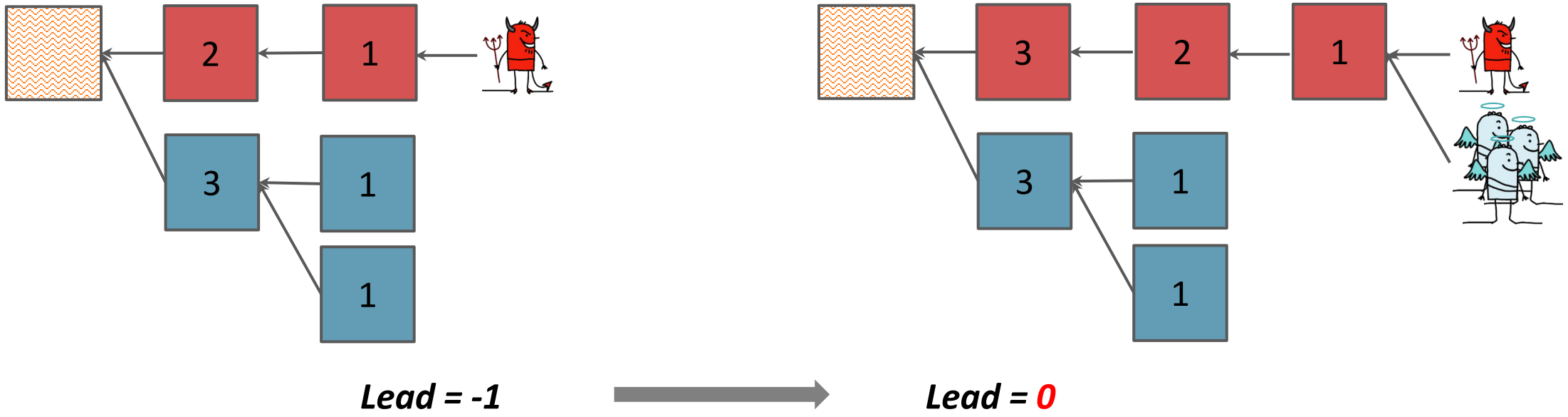
Stubborn mining in the longest chain rule



Lead = -1 ⟶ ***Lead = 0'***

Note: even if Alice succeed to generate a new block and create a fork, no honest power mines on Alice's branch since it just catches up.

Stubborn mining in GHOST



Different from the longest chain rule, sometimes Alice can even win the main chain after mining on the lagged chain.

Experiment setup

- Monte Carlo simulator is used to simulate the blockchain system, involving 3 variables.
- We simulate 1,000 miners equally sharing the total mining power as in [1], and fix γ as 0.5.

Meaning	Value
Block generation interval	1~15s
Selfish pool's mining power	1%~40%
honest pool's mining power	1-selfish power

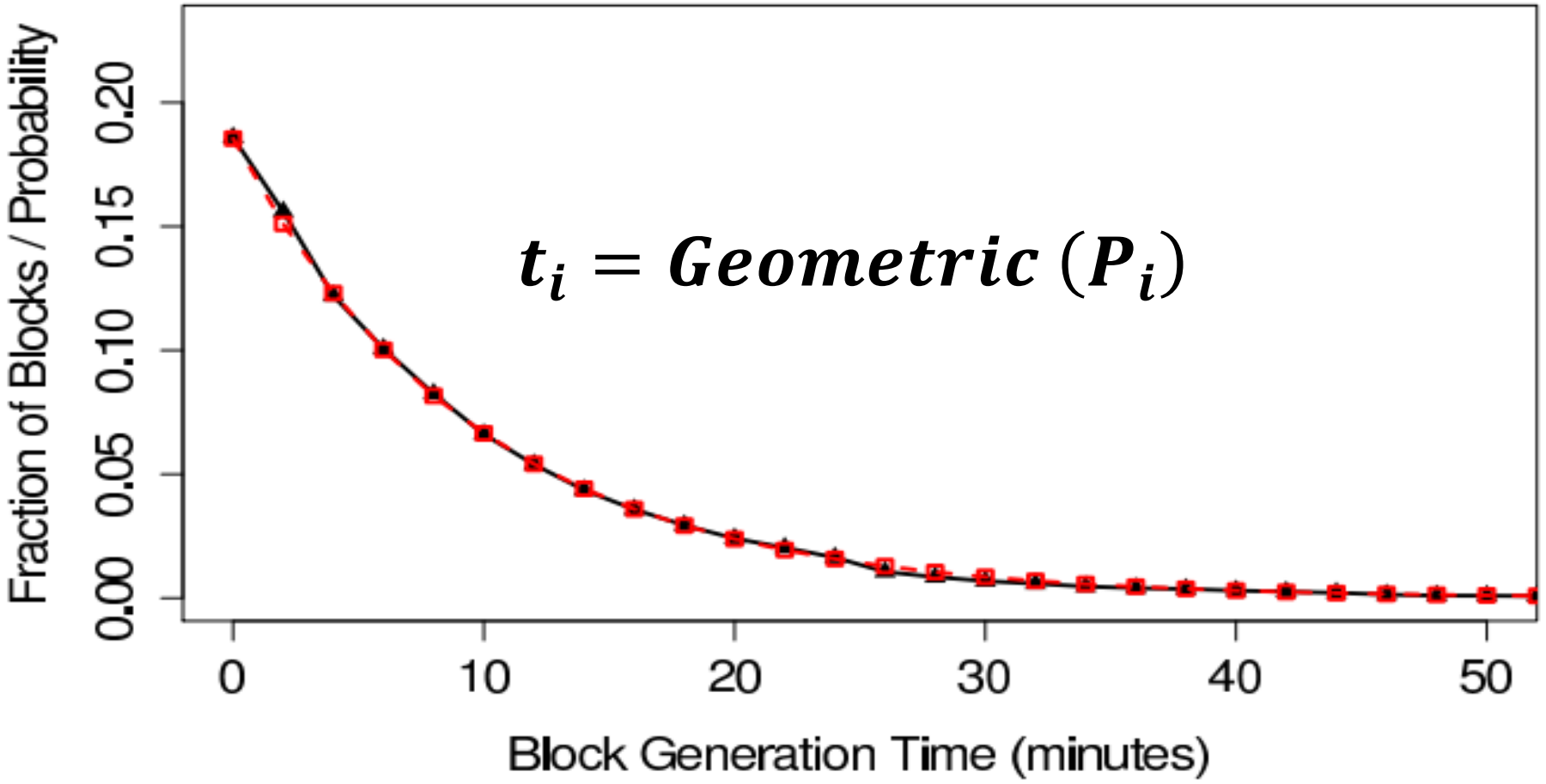
A shorter interval means a faster block generation speed

E.g., when selfish power is 10%, selfish pool consists of 1000*10% miners

[1] I. Eyal and E. G. Sirer, Majority is not enough: Bitcoin mining is vulnerable, FC 2014.

Block generation simulation

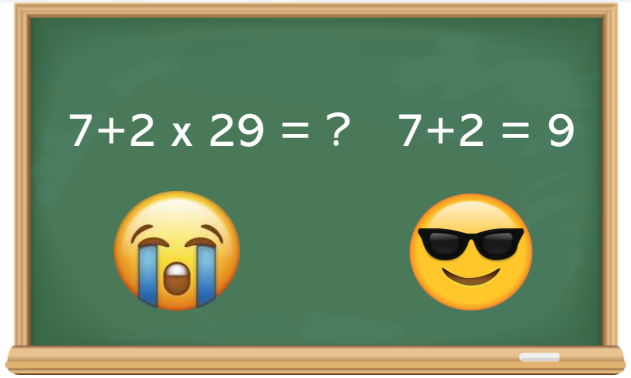
- Block generation with Proof-of-Work (PoW)



[1] G. O. Karame, E. Androulaki, and S. Capkun, Double-spending fastpayments in bitcoin, CCS 2012.

Block generation simulation

Big miner can generate blocks faster

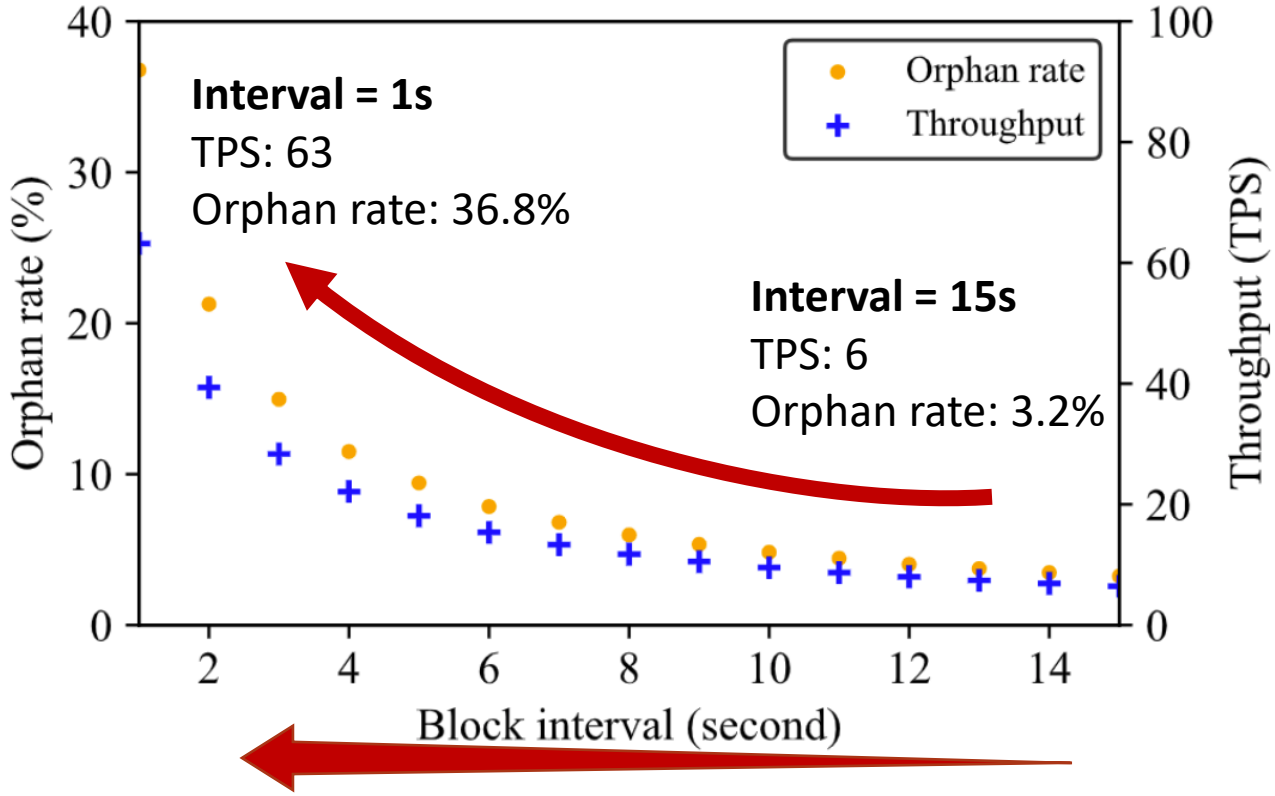


A shorter interval can make block generation faster

$$P_i = \frac{\text{the fraction of mining power owned by miner i } (0.1\%)}{\text{block generation interval}}$$

RQ1: How does GHOST perform in selfish mining?

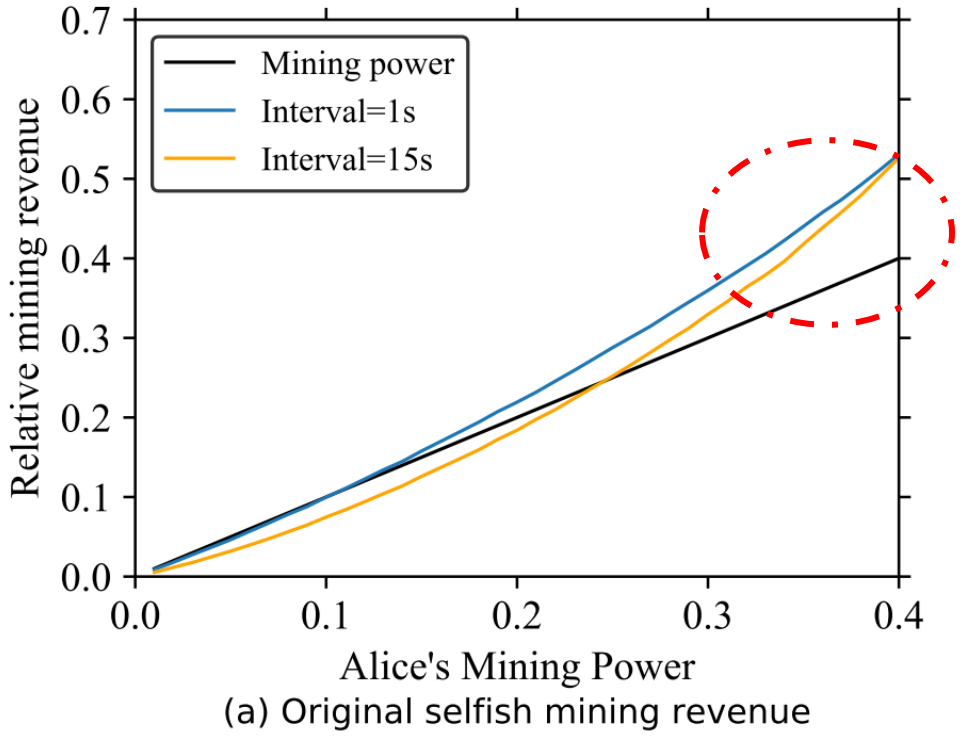
- A shorter block generation interval results in a higher throughput and an increased orphan rate.



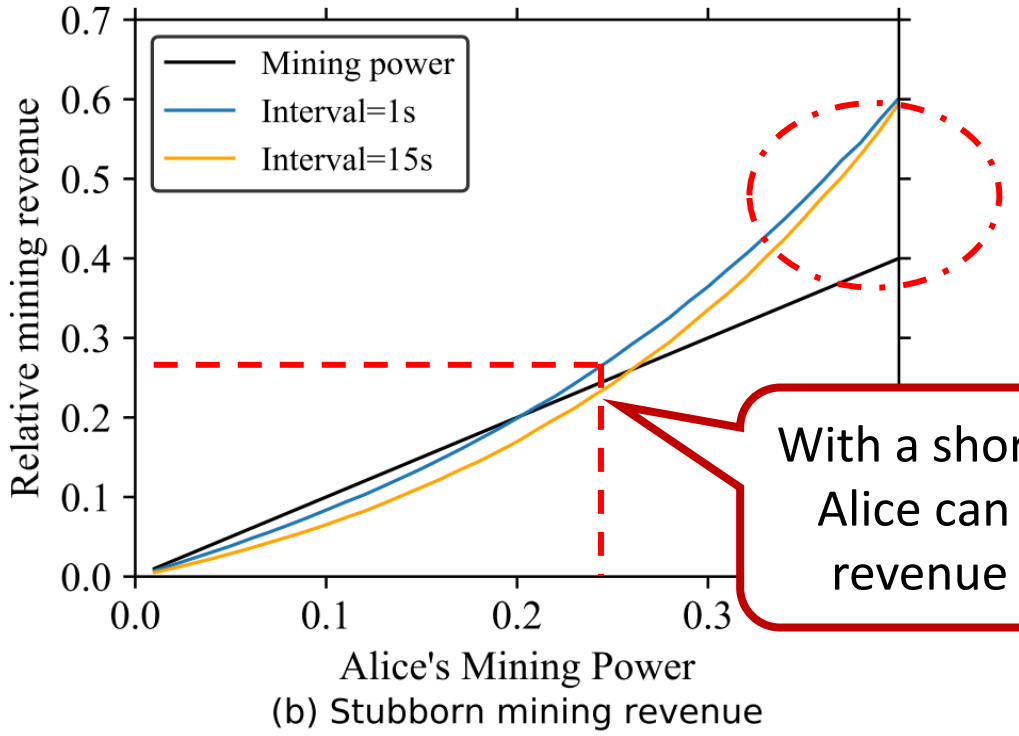
System throughput and orphan rate *with different block intervals*

RQ1: How does GHOST perform in selfish mining?

- GHOST can also suffer from selfish mining when Alice has enough mining power.



(a) Original selfish mining revenue



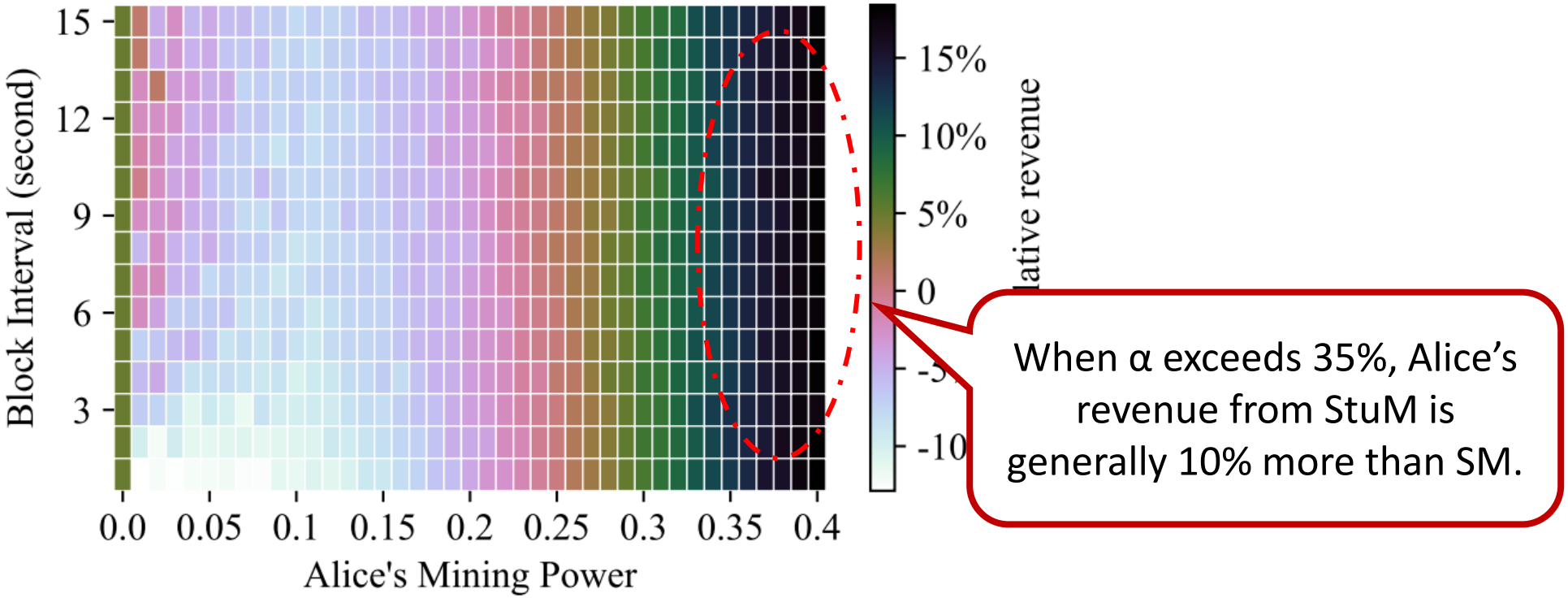
(b) Stubborn mining revenue

With a shorter interval, Alice can gain more revenue in GHOST

*Alice's **selfish revenue** with different mining power*

RQ1: How does GHOST perform in selfish mining?

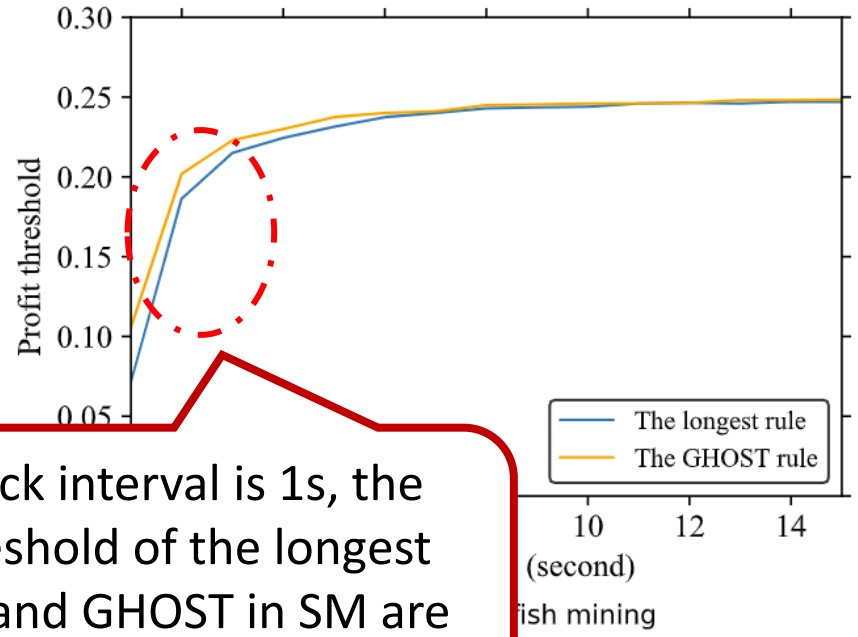
- with enough mining power, Alice can gain more revenue from StuM compared to SM.

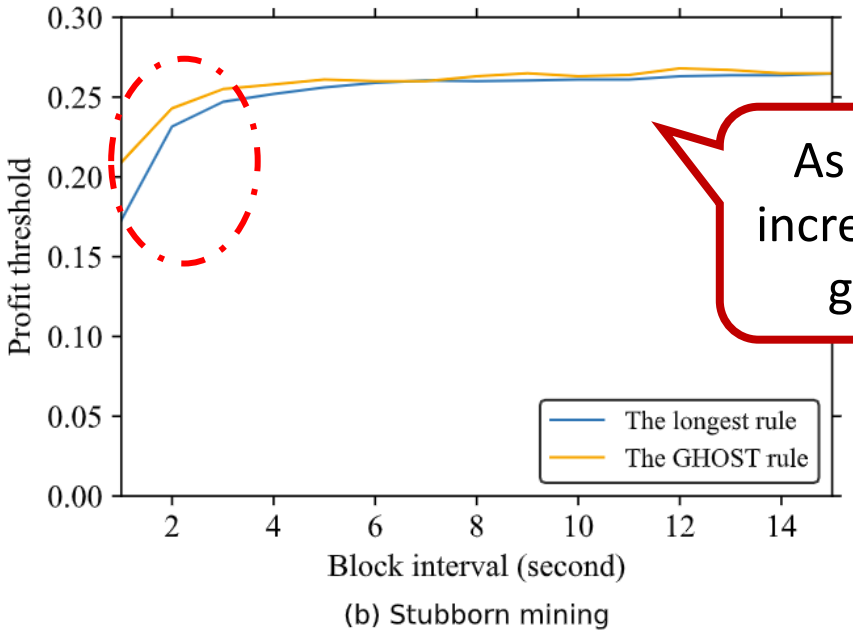


*Alice's **StuM revenue compared to SM revenue***

RQ2: GHOST vs. the longest chain rule?

- GHOST is more secure than the longest chain rule especially in the system with a short block generation interval.





When block interval is 1s, the profit threshold of the longest chain rule and GHOST in SM are 7.15% and 10.55%.

As the block interval increases, their security gap is narrowing.

Profit threshold of two protocol in SM and StuM

Conclusion

- We propose two selfish mining strategies for GHOST
- We evaluate these two selfish mining strategies on the blockchain simulation system
- We find that GHOST can still suffer from selfish mining, and its security boundary is higher than the longest chain rule with a short block interval.

Consortium blockchain open source community

Q&A

THANK YOU!