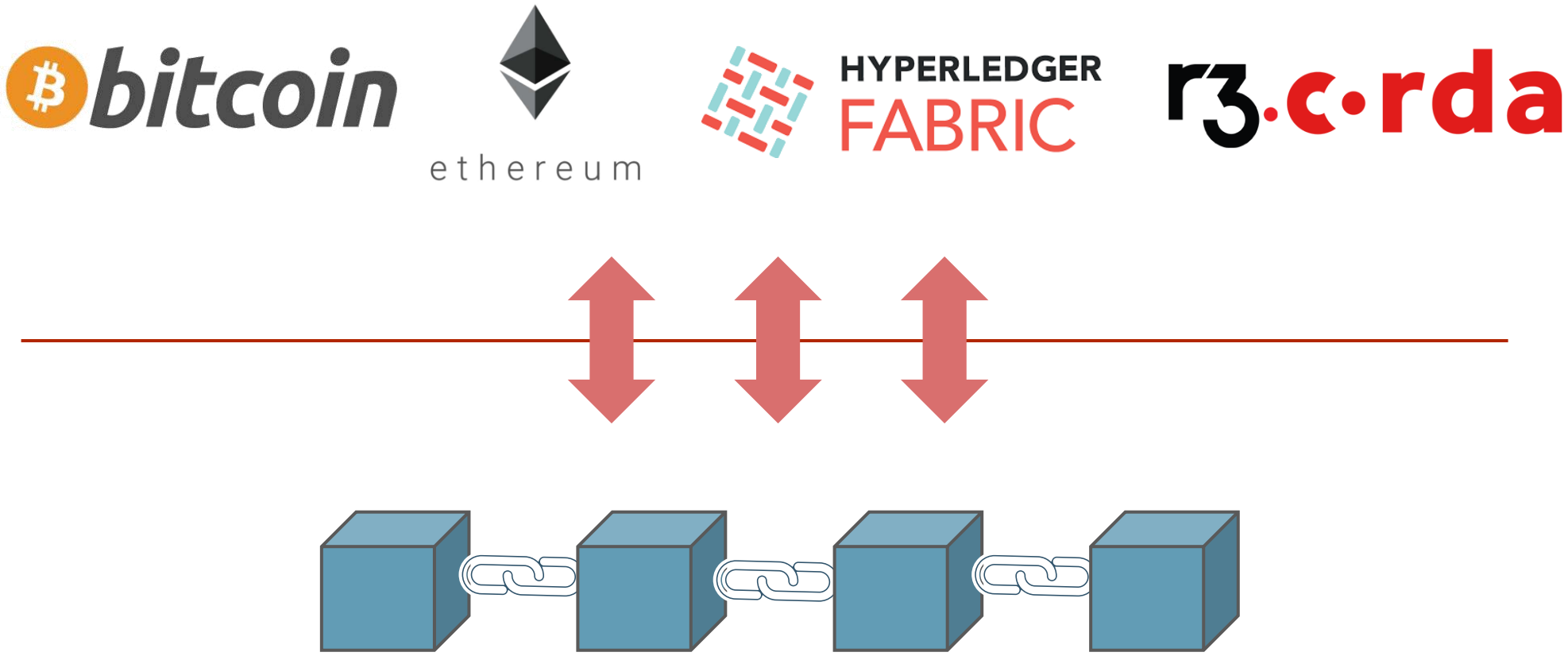
# The Impact Analysis of Multiple Miners and Propagation Delay on Selfish Mining

**Qing Xia**, Wensheng Dou, Tong Xi, Jing Zeng,
Fengjun Zhang, Jun Wei, Geng Liang

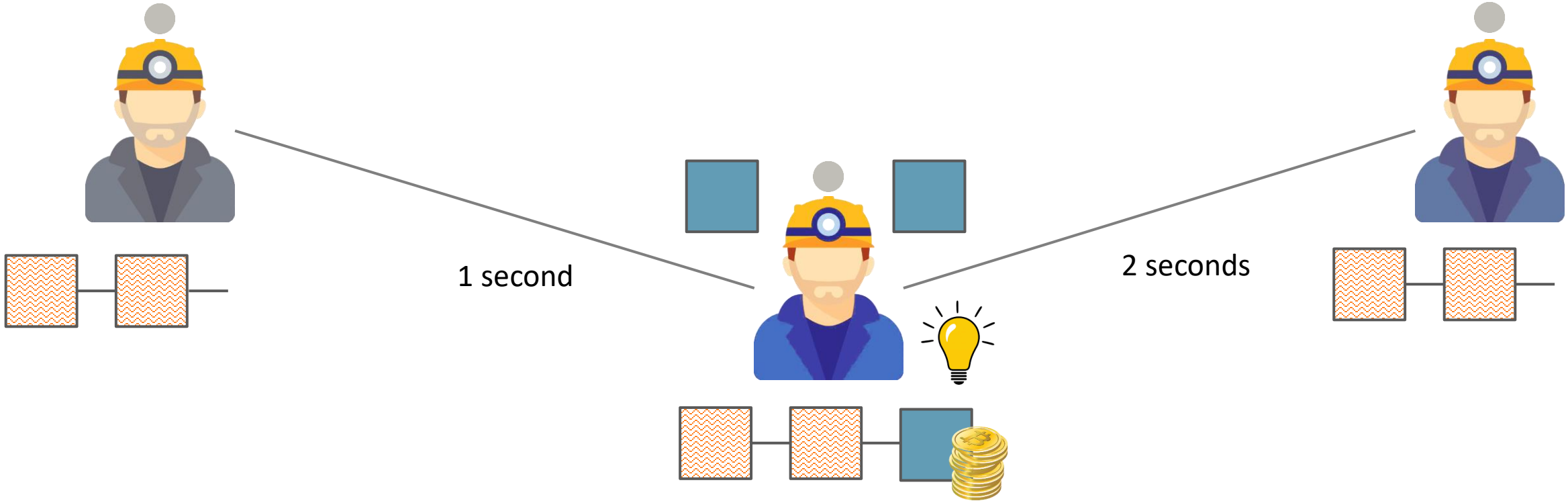
*Institute of Software, Chinese Academy of Sciences*


# Blockchain has been widely adopted



# Nakamoto Consensus

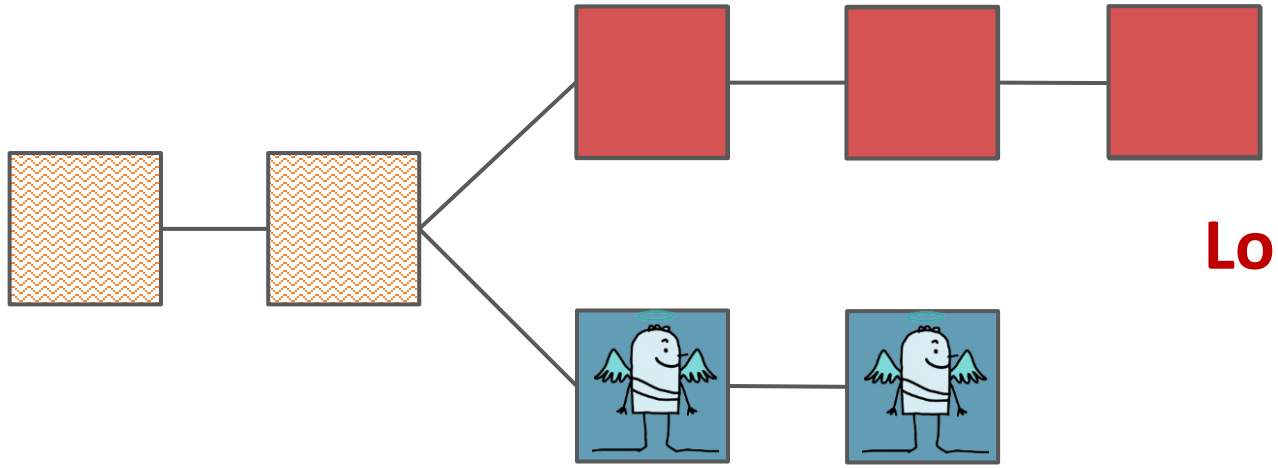
- One of the most widely-used consensus protocols proposed by Nakamoto Satoshi




Miner's reward is proportional to its mining power

# Selfish Mining

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

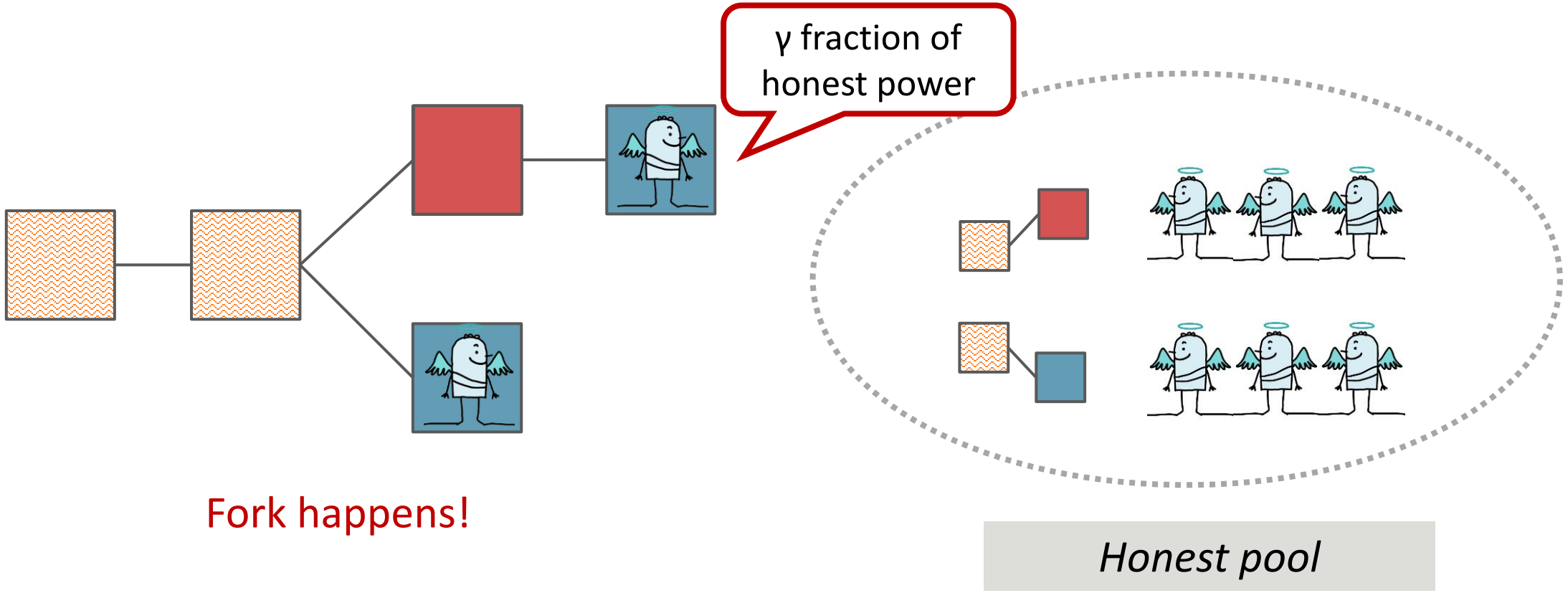


**Longest chain wins!**

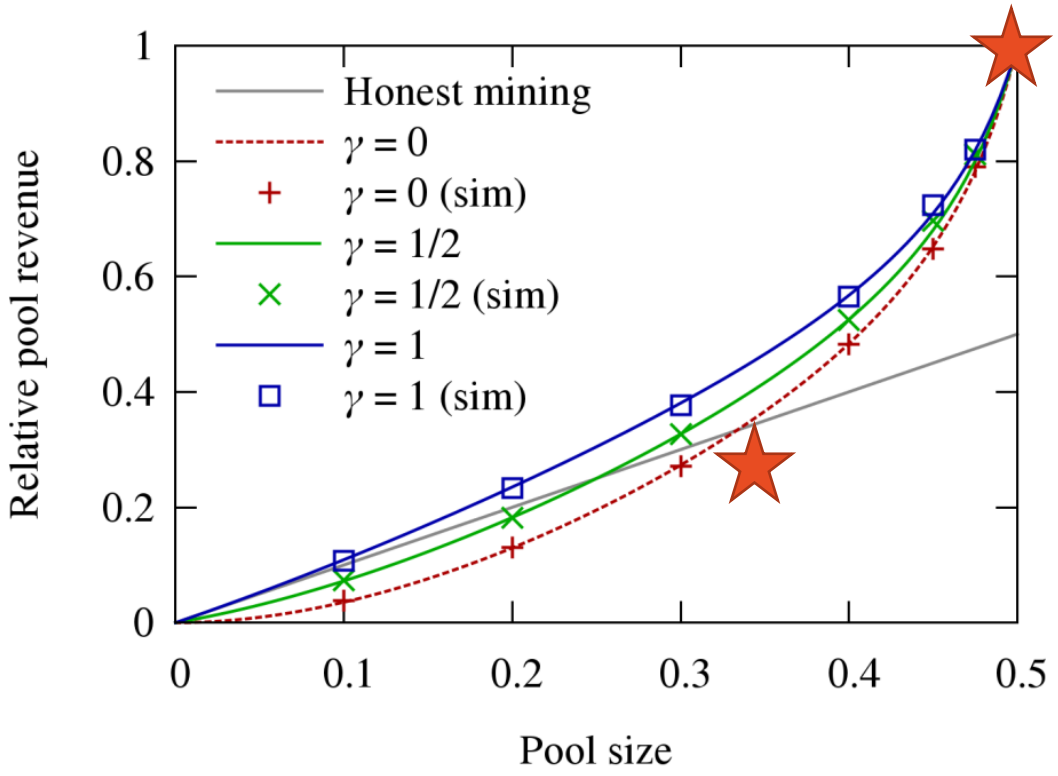
**Bob wastes its power on orphan blocks!**

# Selfish Mining

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



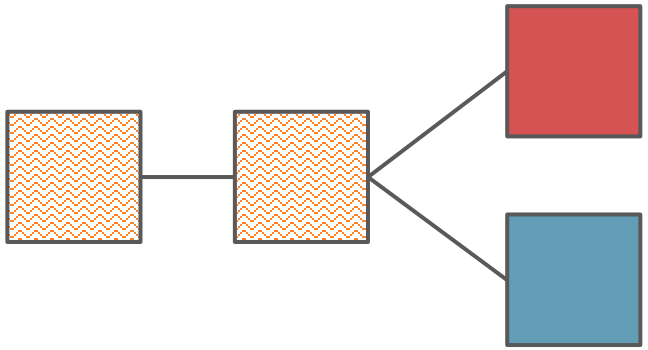
# Selfish Mining

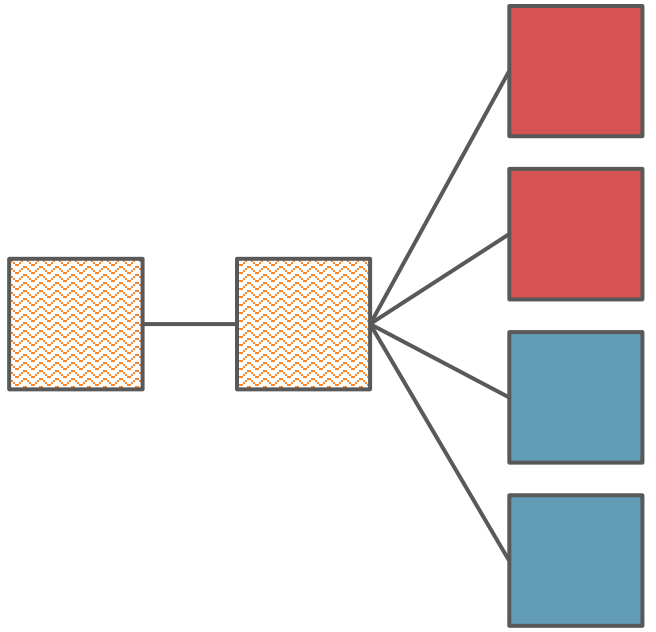



- When γ = 0, Alice with ≥ 33% mining power can gain more profit
- With half of the mining power, no matter what γ is, Alice can gain almost all profit

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

# Limitation 1

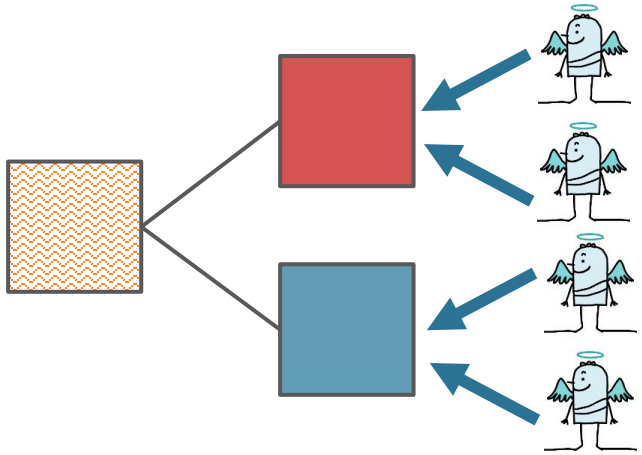


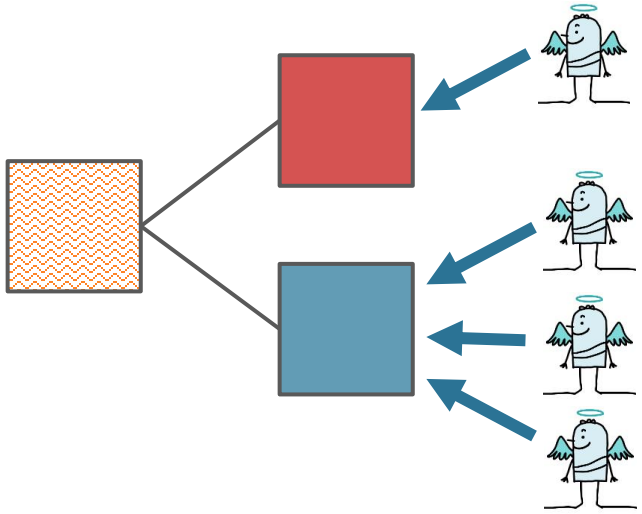


***Previous work:*** Fork can only happen between the honest pool and selfish pool

***Real-world scenario***: Fork can happen inside the honest pool or the selfish pool

# Limitation 2

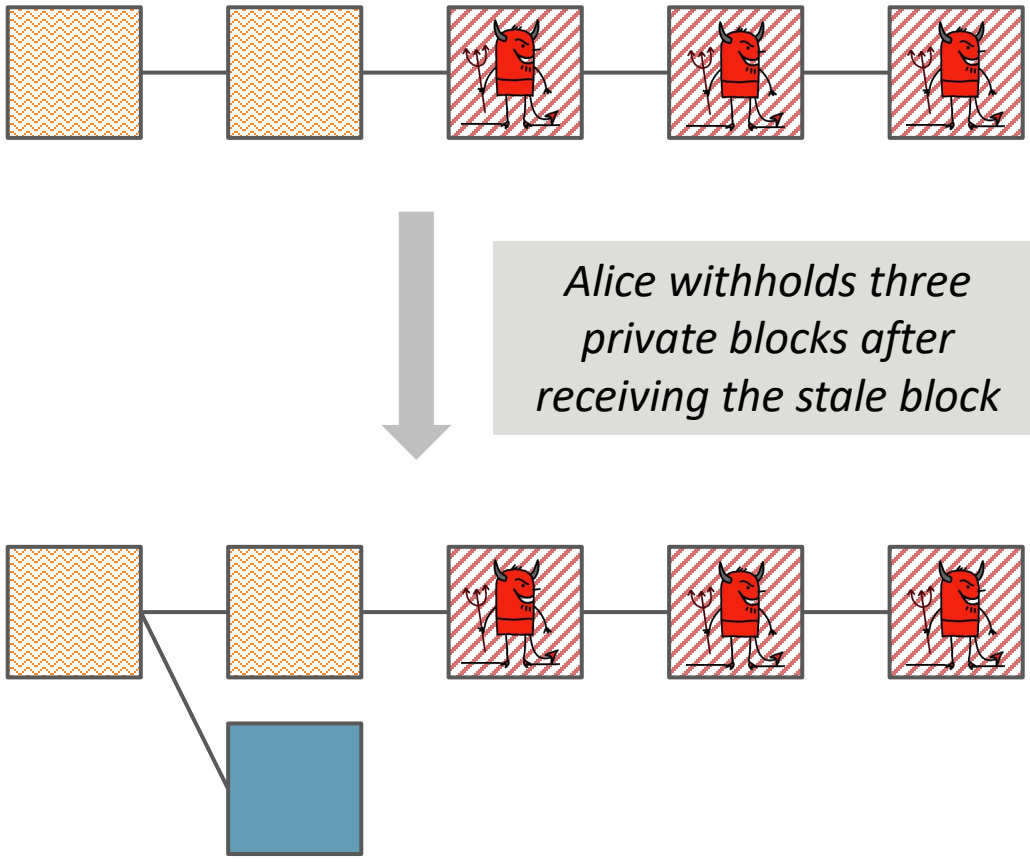




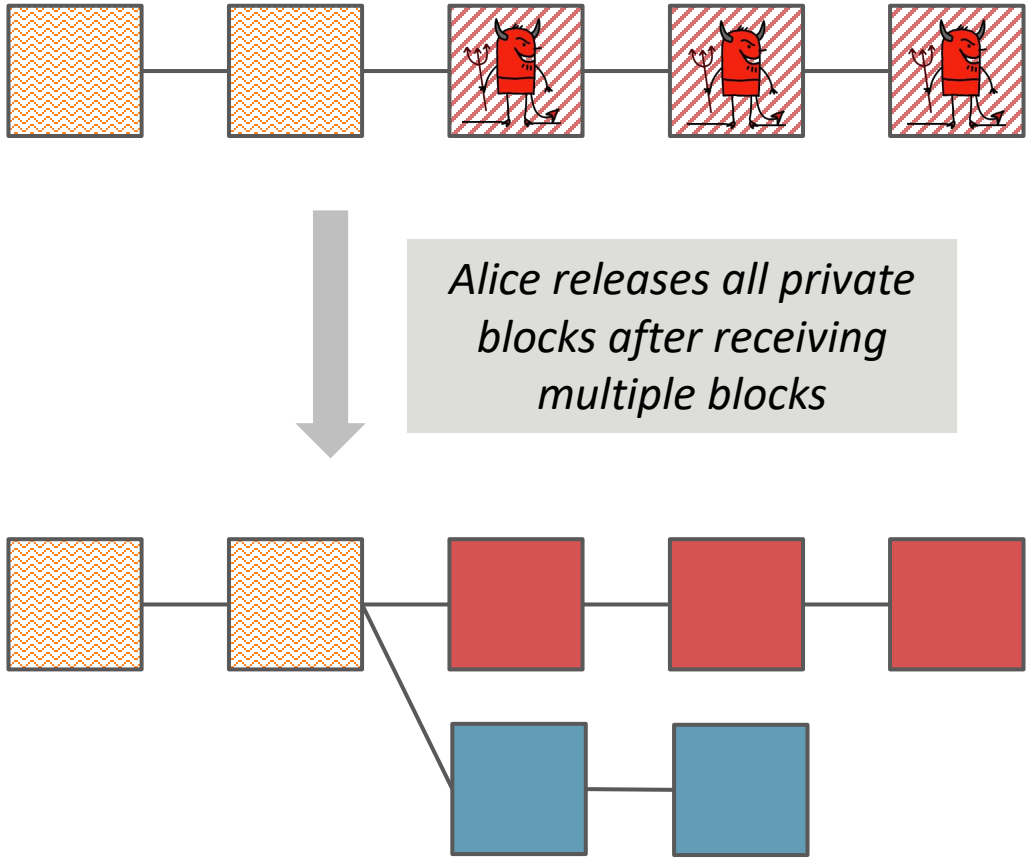
***Previous work:*** A fixed fraction of honest power always works after the selfish branch

***Real-world scenario***: γ is dynamically-changing and unknown due to varied delay

# Practical Selfish Mining Strategy



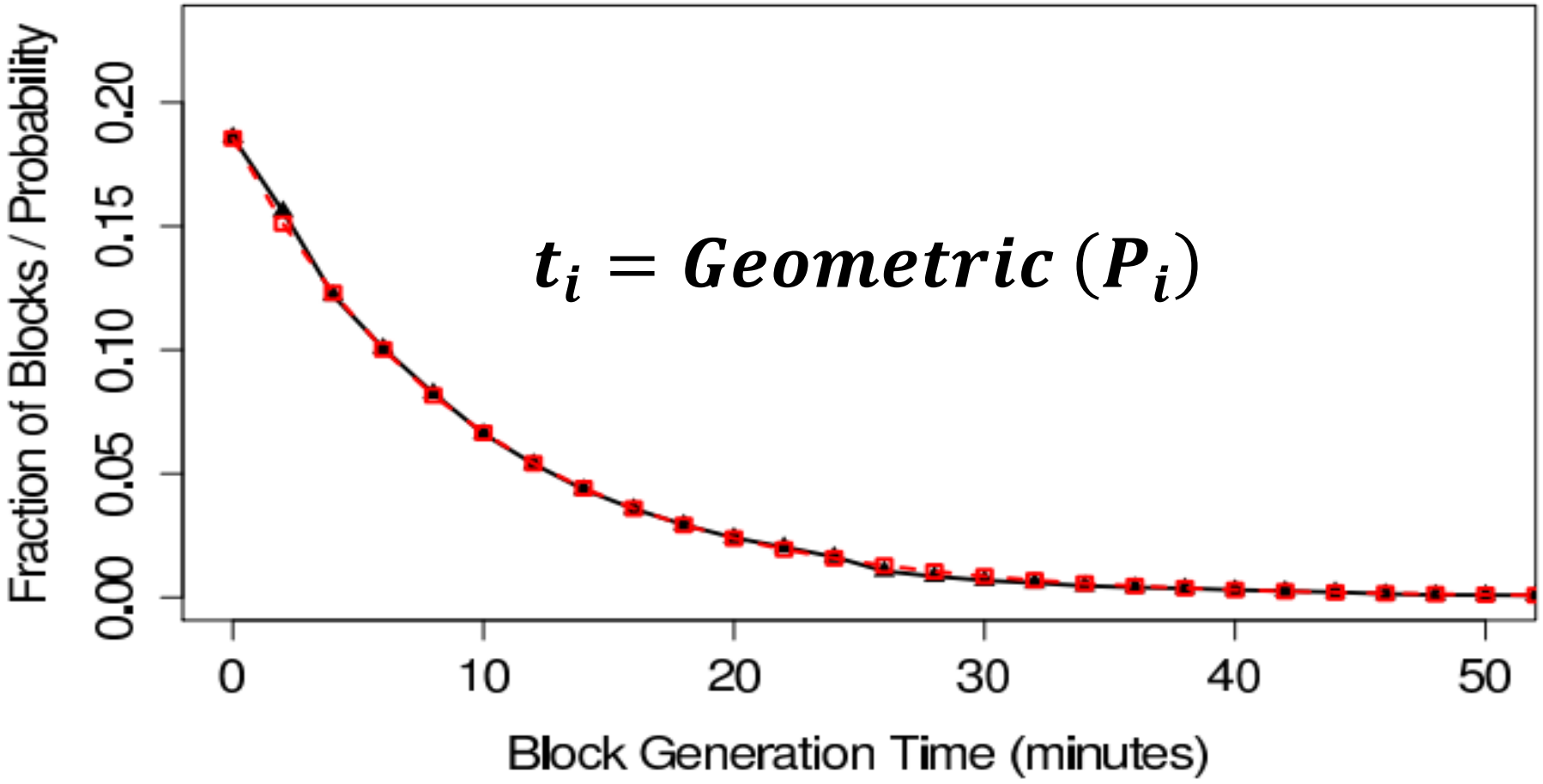
*Alice withholds three private blocks after receiving the stale block*



*Alice releases all private blocks after receiving multiple blocks*

# Blockchain Simulation Approach

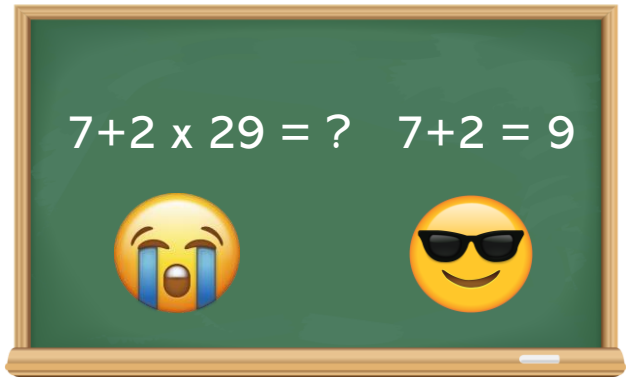
- Block generation with Proof-of-Work (PoW)




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

# Blockchain Simulation Approach

Big miner can generate blocks faster




A lower difficulty can make block generation faster

$r_i$: the fraction of mining power owned by miner i

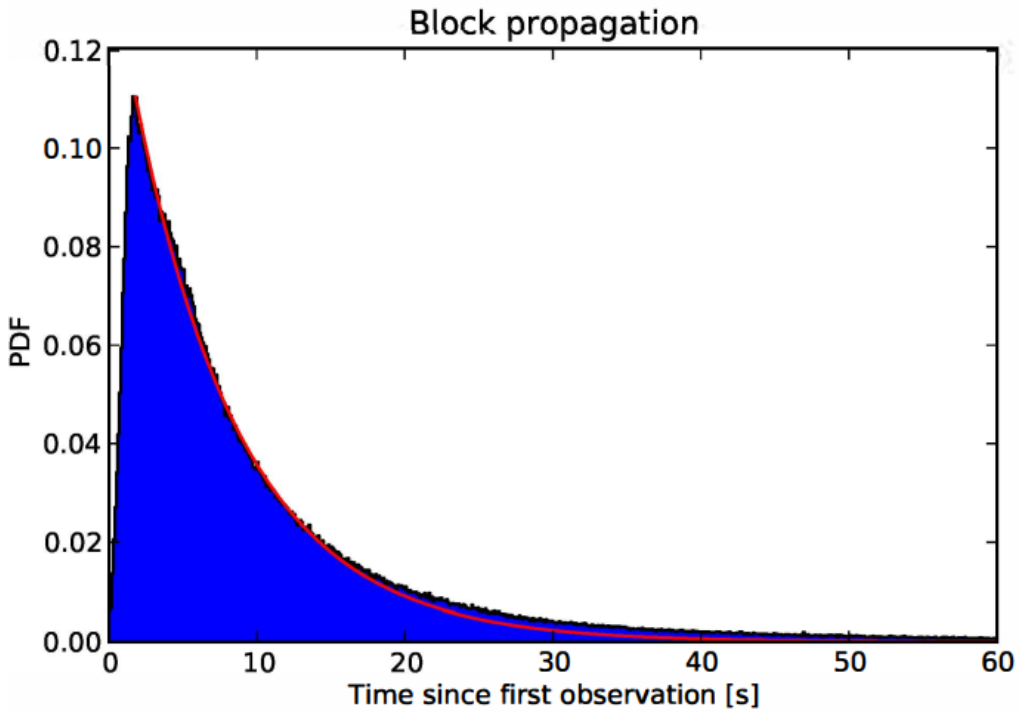
$$P_i = \frac{r_i}{G}$$

$G$: block generation interval of the system

**Flexible parameters for simulation!**

# Blockchain Simulation Approach

- Block propagation in the Peer-to-Peer (P2P) network



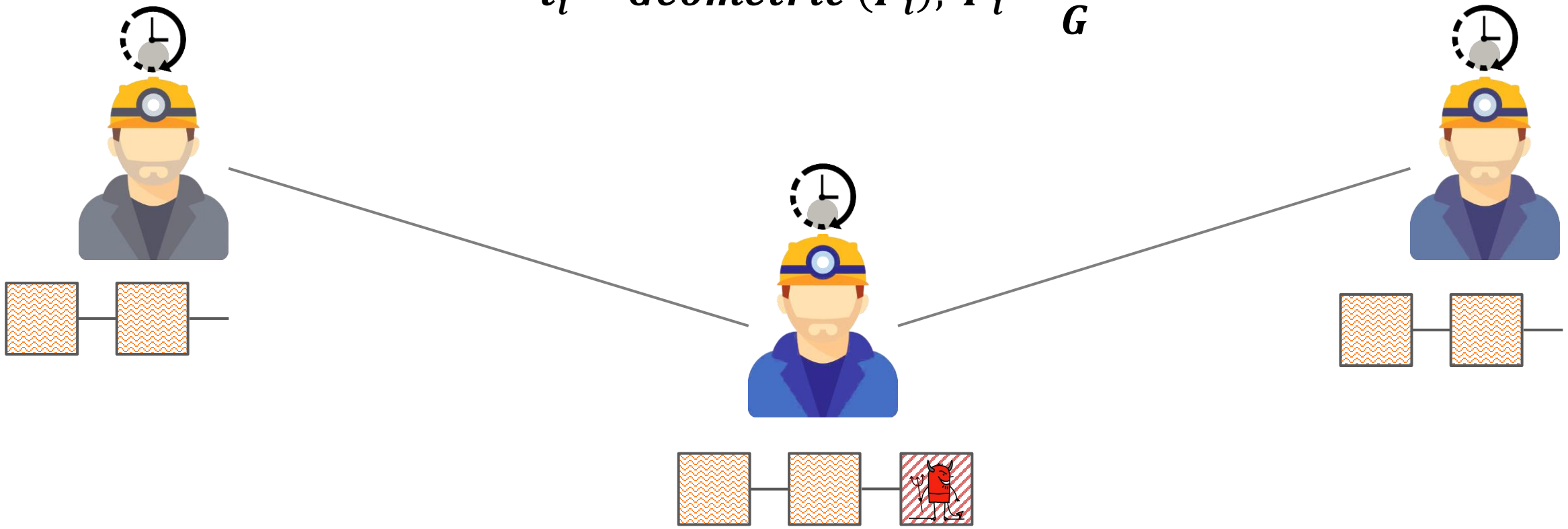

- Propagation delay in Bitcoin fits the exponential curve with meantime of 12.6s [1]
- The meantime becomes larger with a larger block size

$$\boldsymbol{Delay = Geometric\,(meantime)}$$

[1] C. Decker and R. Wattenhofer, Information propagation in the bitcoin network, P2P 2013.

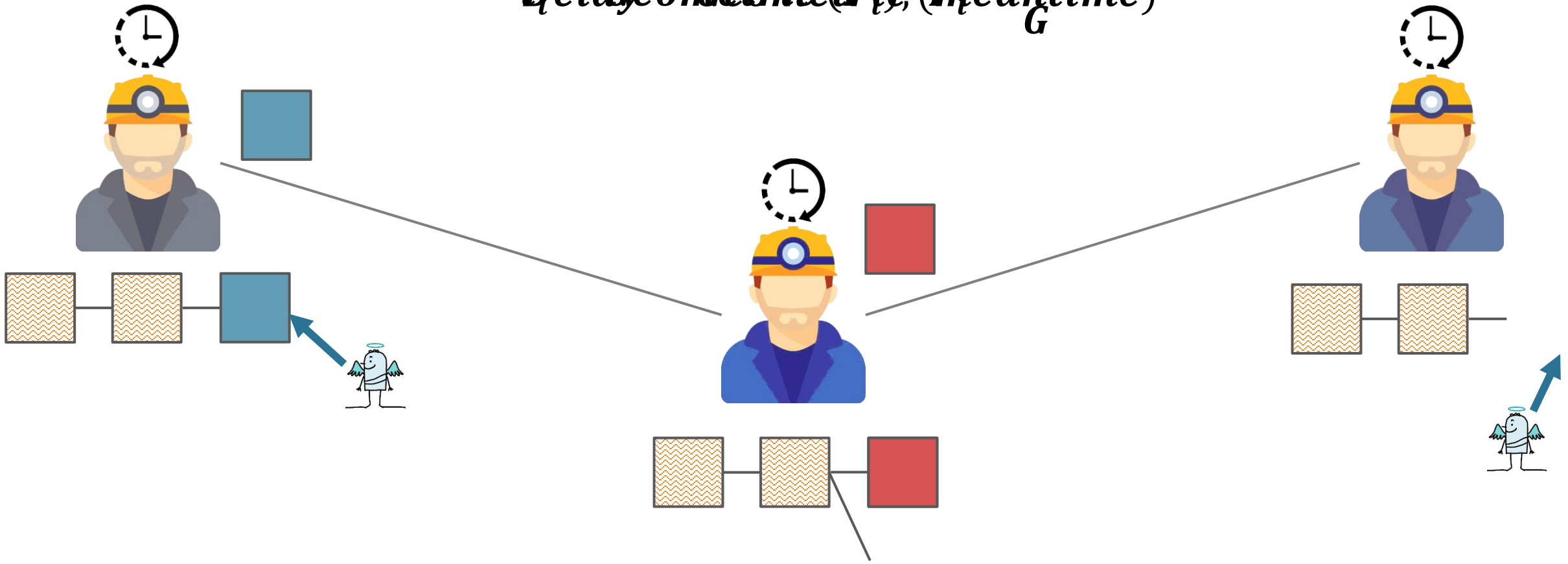
# Blockchain Simulation Approach

$$t_i = Geometric\,(P_i);\ P_i = \frac{r_i}{G}$$



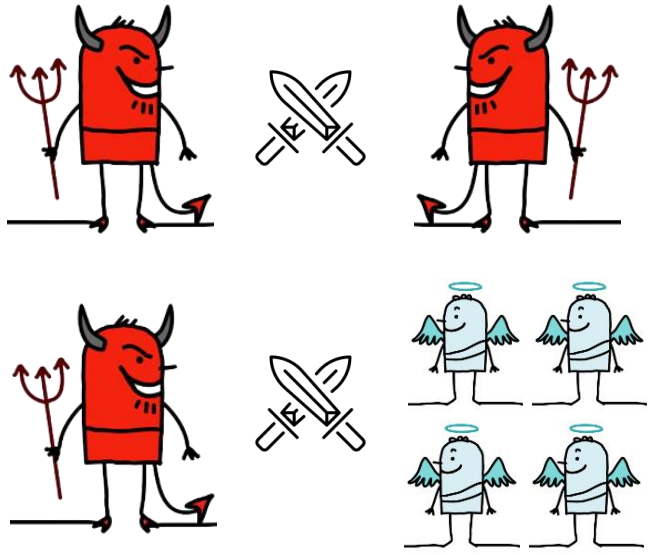
# Blockchain Simulation Approach

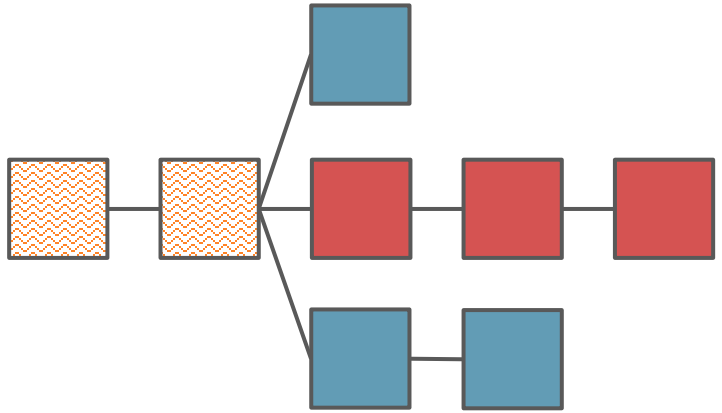
$$Delay = GetMeanTime(P_i, \frac{r_i}{G}, MeanTime)$$



# Research Questions

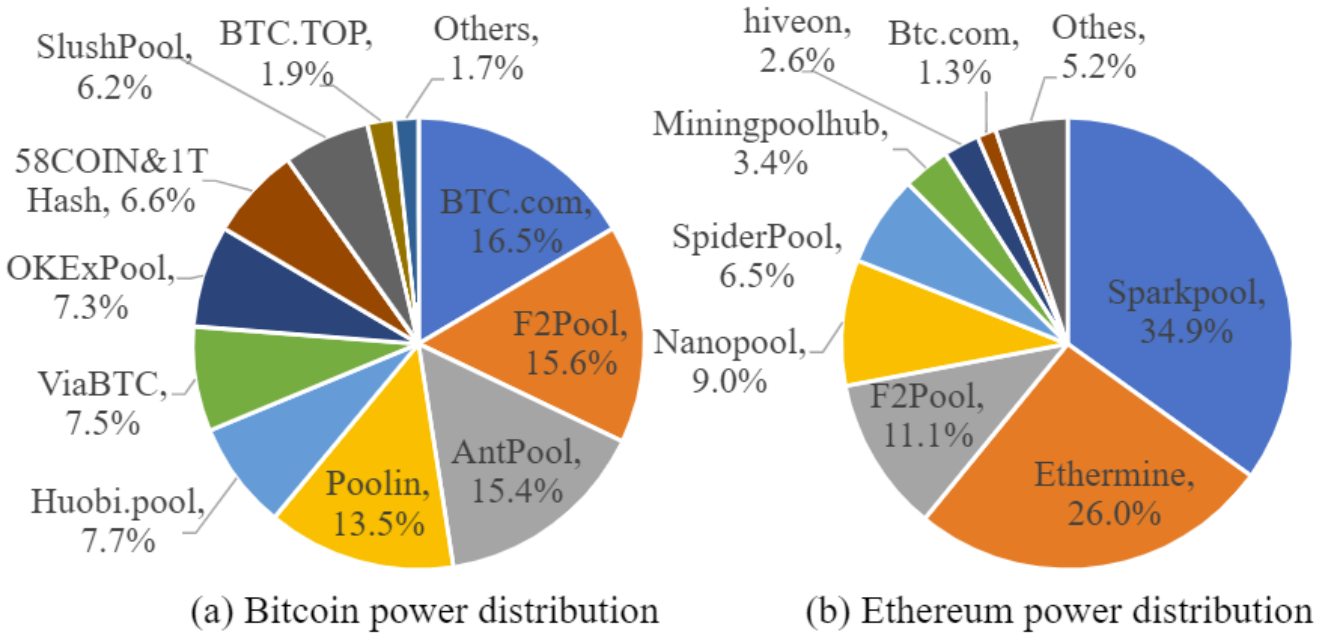
- RQ1:How can multiple mining pools affect selfish mining?
- RQ2:How can propagation delay affect selfish mining?
- RQ3:How can orphan rate affect selfish mining?



# Experiment Settings

- The number of multiple miners




(a) Bitcoin power distribution

(b) Ethereum power distribution

TOP 5 pools: 69%
TOP 10 pools: 98%

TOP 5 pools: 88%
TOP 10 pools: 96%

- Three cases
  - General case: 10 pools
  - More centralized case: 5 pools
  - More decentralized case: 20, 100 pools
- Alice has 1% ~ 50% mining power, rest pools equally share the rest mining power

# Experiment Settings

- Relative propagation delay (RPD)
  - The ratio of propagation delay to block interval
  - Measures the blockchain system's synchronization speed

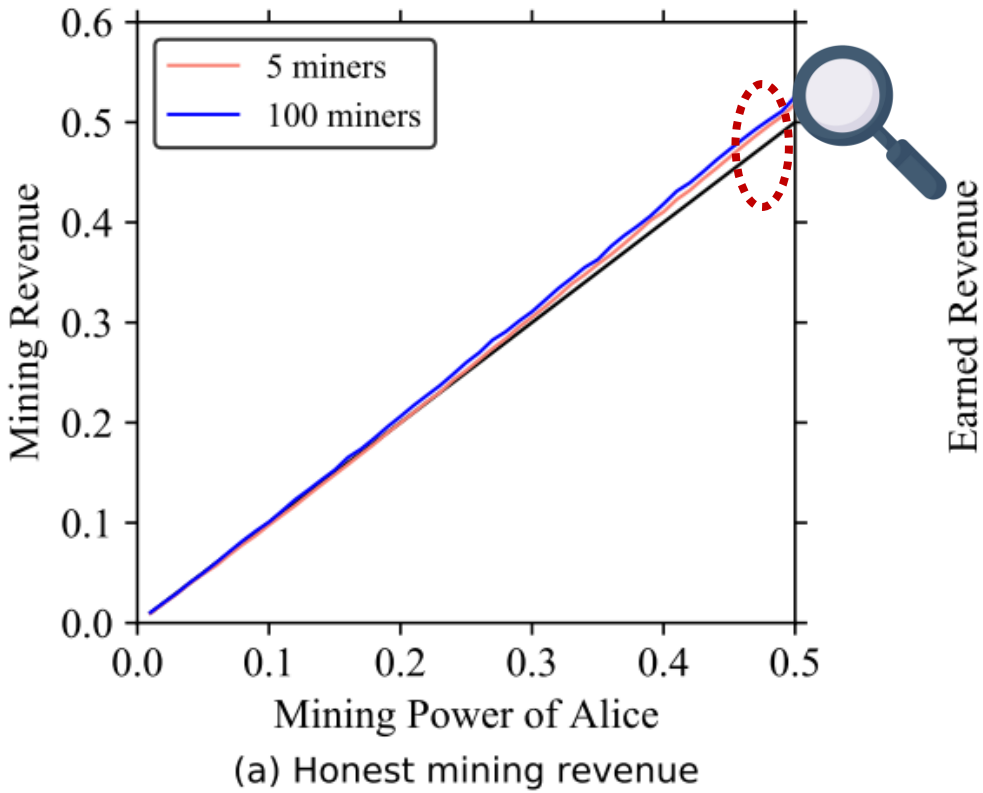
| | Bitcoin | Other systems | |
|---|---|---|---|
| Propagation delay | 12.6s | 15s | 6s |
| Block interval | 600s | 300s | 60s |
| Relative propagation delay (RPD) | **1/48** | **1/20** | **1/10** |

**Increase the block size and decrease the block interval**

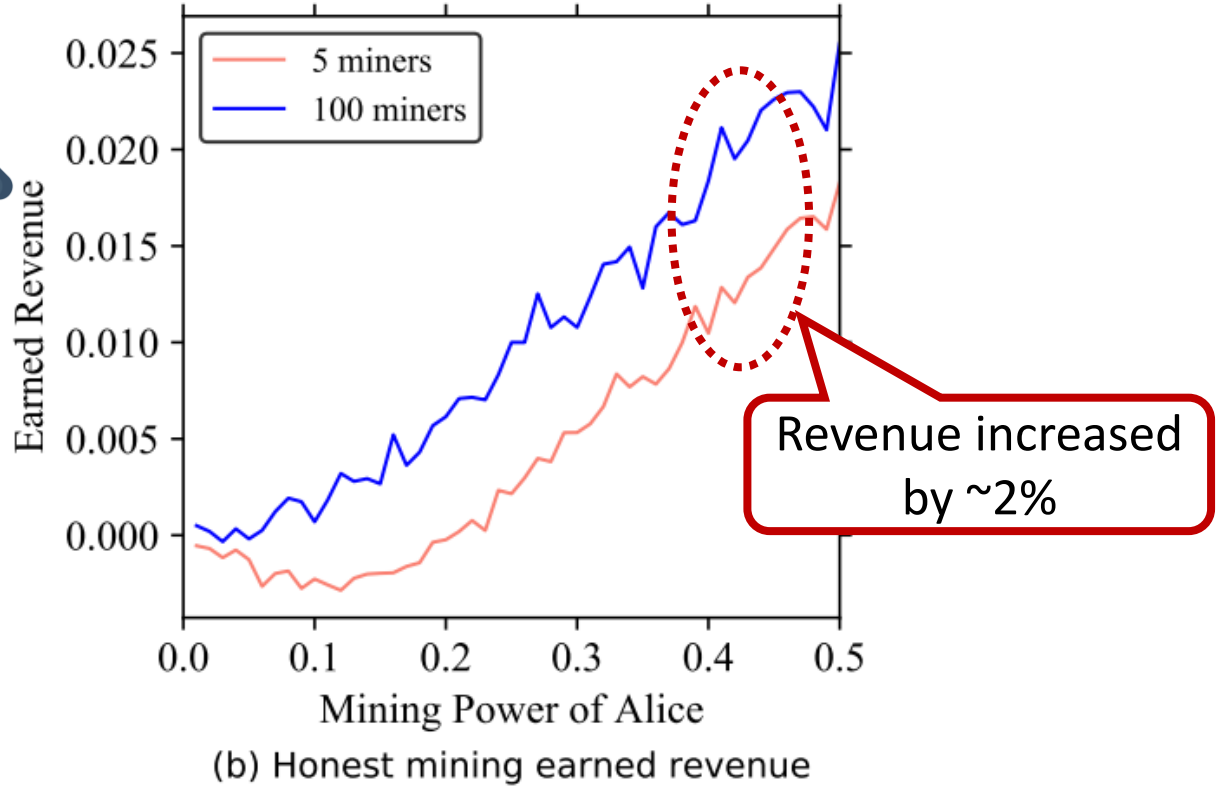
We focus on the system with a larger relative propagation delay

# RQ1: Multiple Miners

- A miner with sufficient mining power has an ***inherent advantage*** in the honest mode, especially in a more decentralized system.




(a) Honest mining revenue

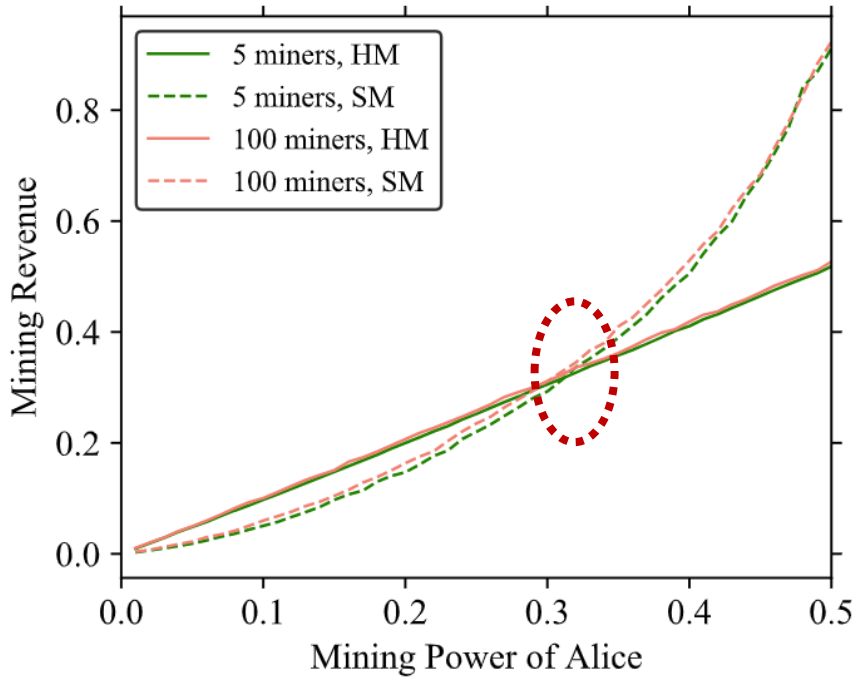



(b) Honest mining earned revenue

*Alice's **honest revenue** with different honest miners*

# RQ1: Multiple Miners

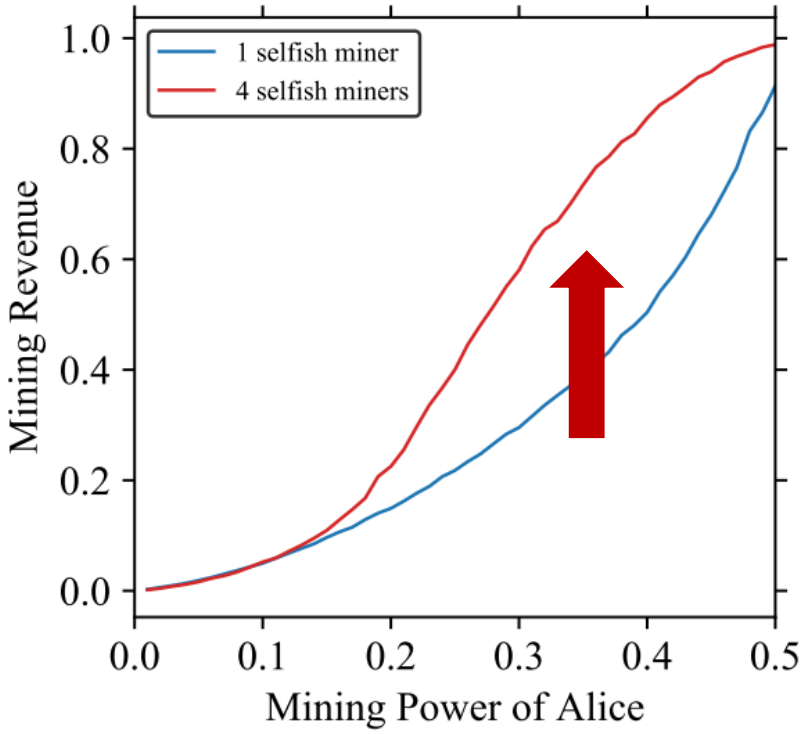
- Selfish mining performs better in the more decentralized system with more honest miners.
  - E.g., Alice's ***profit threshold*** is 31% and 29% with 5 and 100 miners



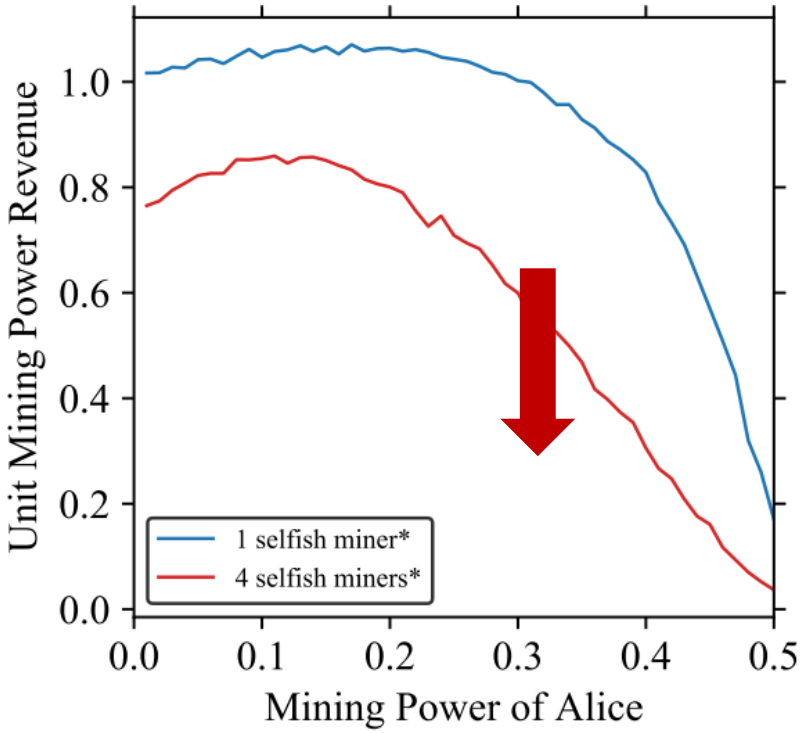

*Alice's **selfish revenue** with different honest miners*

# RQ1: Multiple Miners

- With multiple selfish miners, the large selfish miner can benefit from selfish mining, while other smaller miners cannot.




(a) Mining revenue of Alice

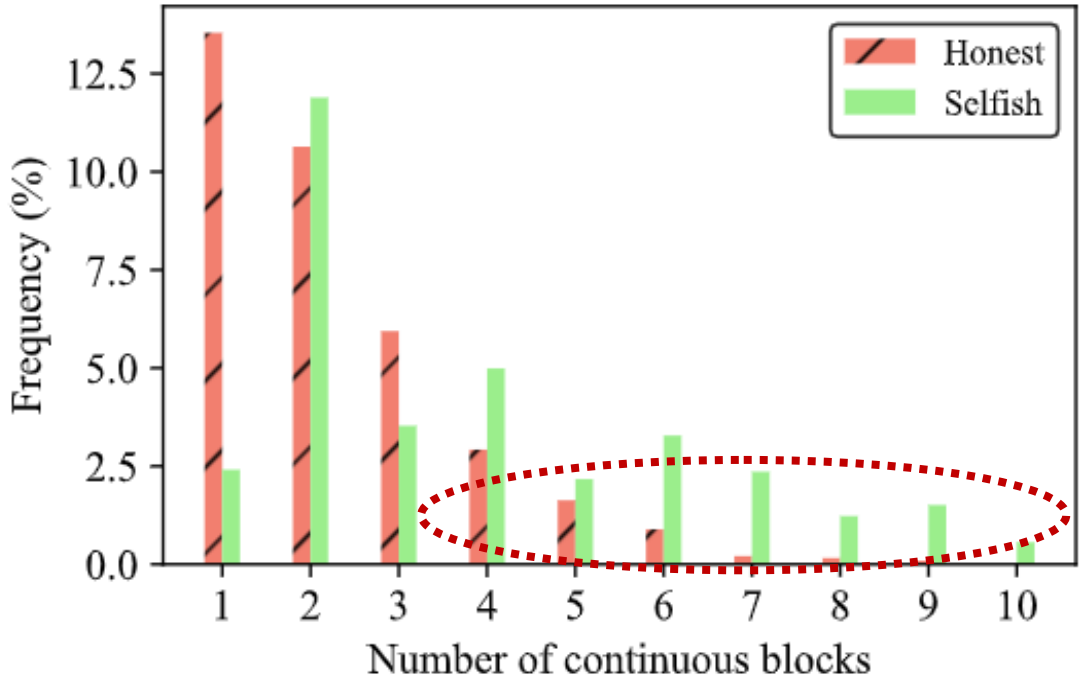



(c) Unit mining power revenue of miner5

*Alice's **selfish revenue** with different selfish miners*

# Comparison Analysis

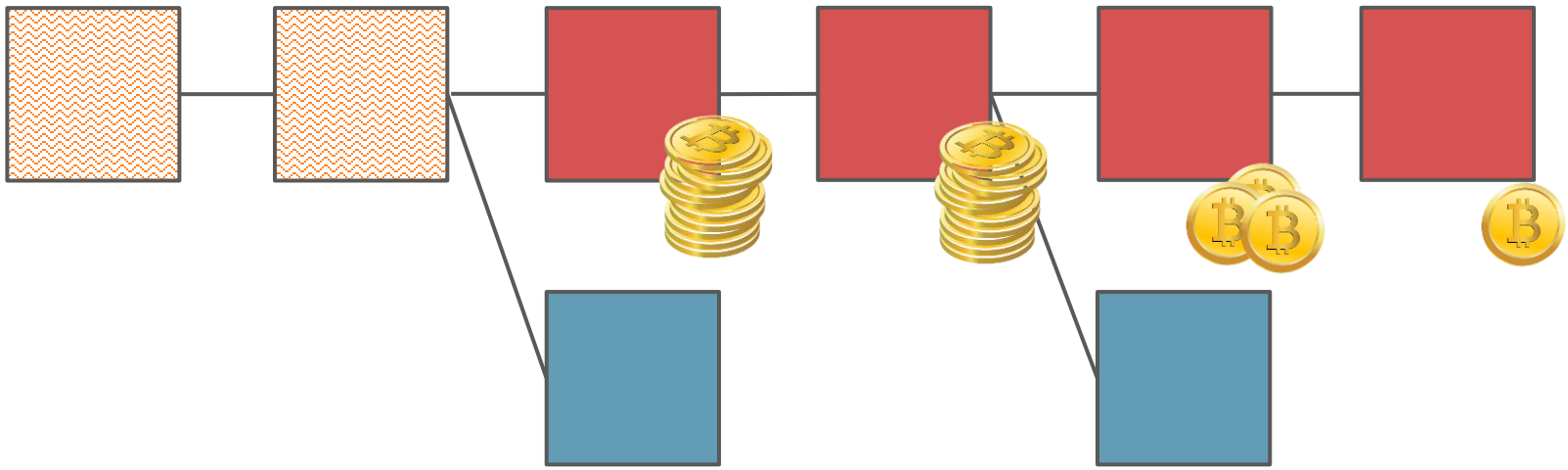
- Selfish mining results in more consecutive blocks generated by the selfish miner
  - selfish miner is more likely to succeed with a longer private chain



# Implication

- Alleviate selfish mining

**Revise the reward mechanism!**

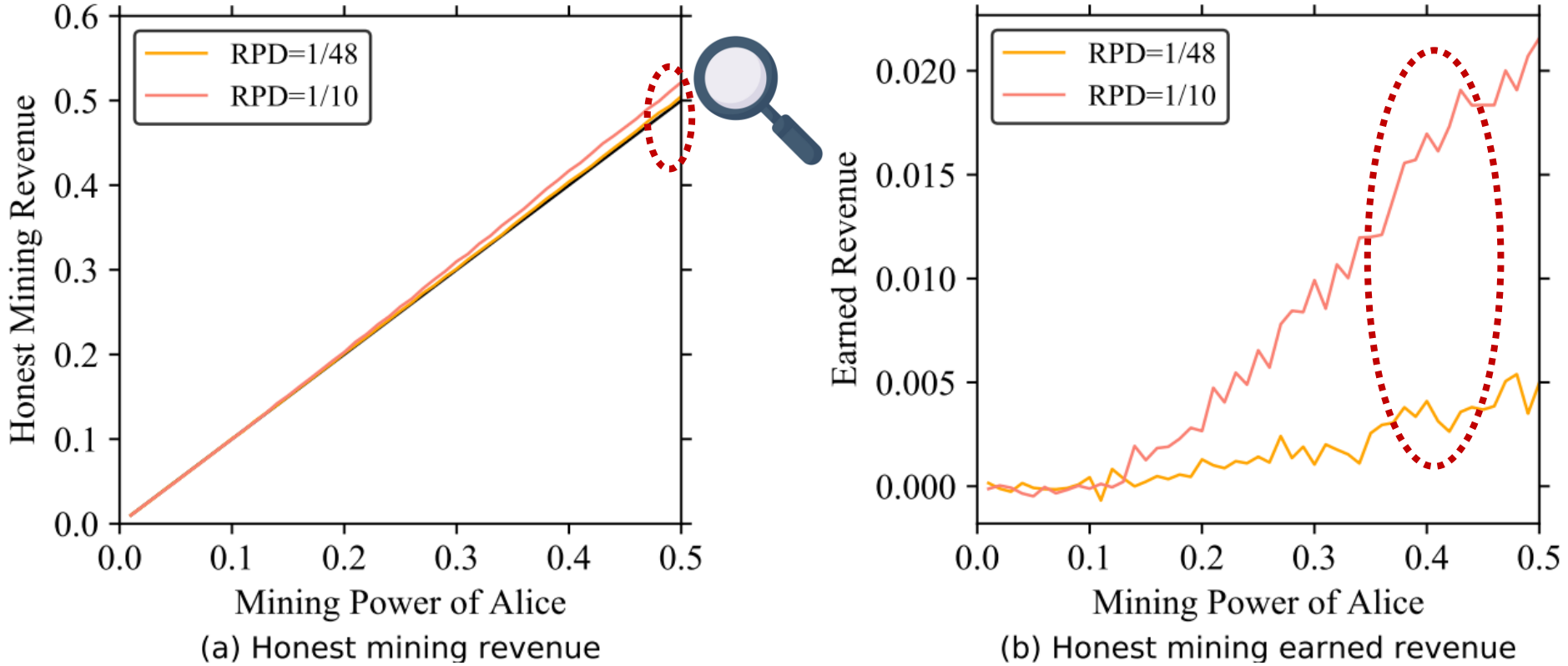


$$\begin{cases} \boldsymbol{blockReward}\ (\boldsymbol{Conti} = \mathbf{1}, \dots, \mathbf{4}) \\ \dfrac{\boldsymbol{blockReward}}{\boldsymbol{Conti}\ - \mathbf{2}}\ (\boldsymbol{Conti}\ \geq \mathbf{5}) \end{cases}$$

- Alice's revenue decreases by 14% in selfish mining
- Even if Alice has nearly 50% of mining power, it cannot benefit from selfish mining

# RQ2: Relative Propagation Delay (RPD)

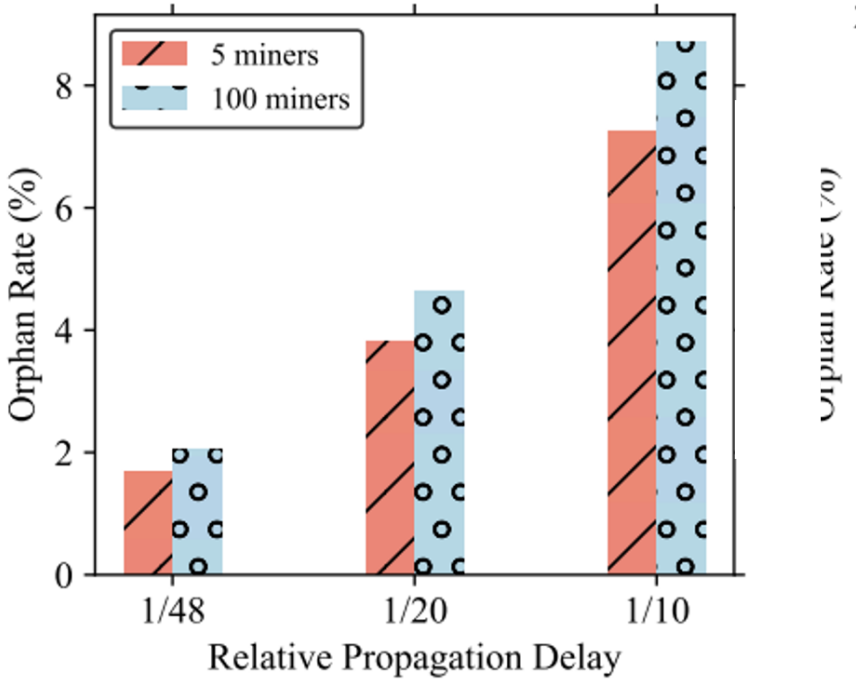
- A miner with sufficient mining power has an inherent advantage in honest mining, especially in the system with a larger delay.



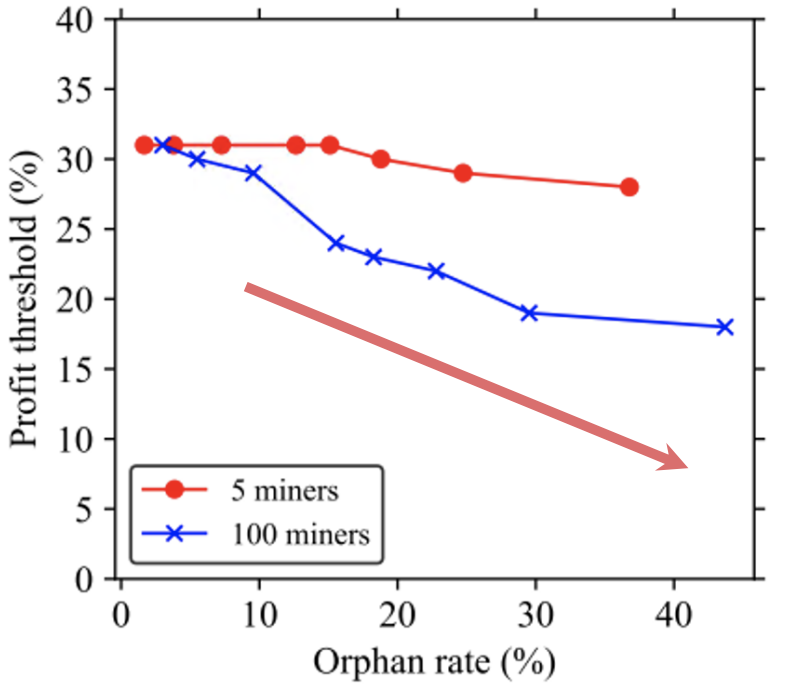

*Alice's **honest revenue** with different RPDs*

# RQ3: Orphan Rate

- The system has a higher orphan rate with more miners and a larger delay.
- ***Profit threshold*** of selfish mining decreases when the orphan rate increases.




(a) System Orphan rate of different blockchain systems



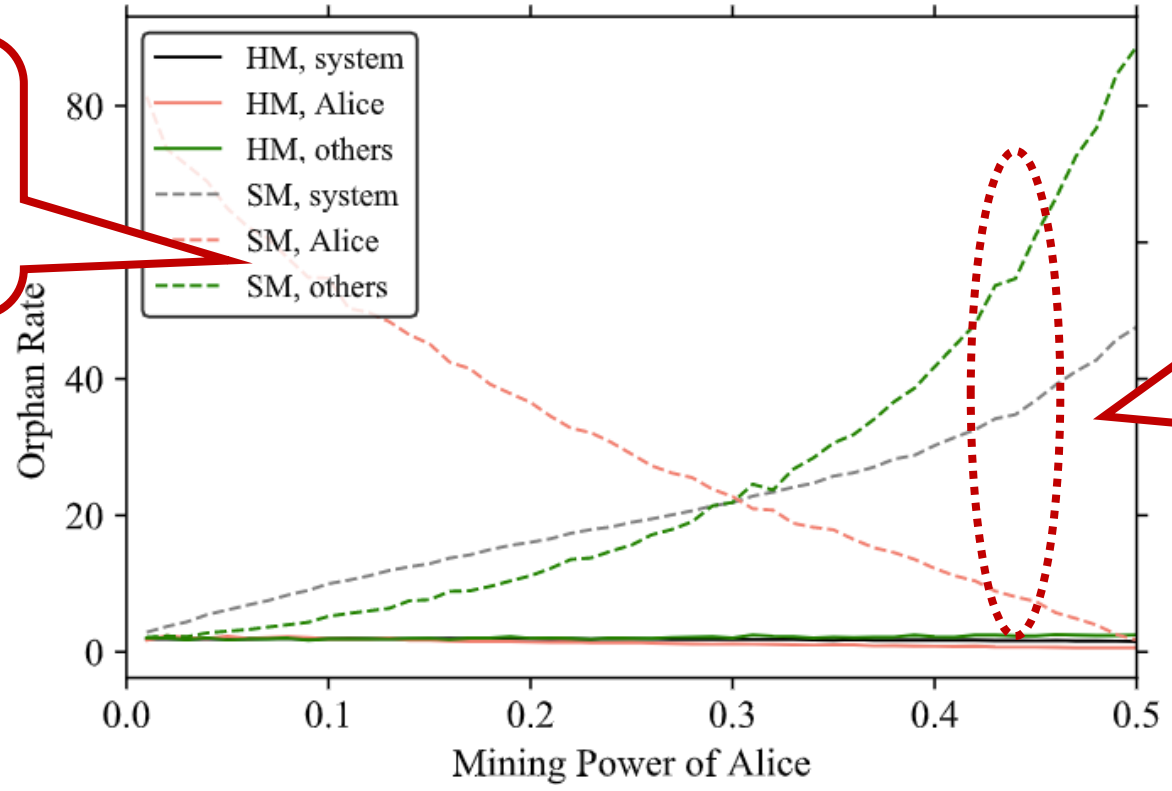

(c) Profit threshold in different blockchain system

***Profit threshold*** in different blockchain systems

# Implication

- Selfish mining has a great impact on the orphan rates

Selfish miner has a high orphan rate with less mining power




As the mining power increases, the selfish orphan rate decreases, while the honest and system increases

***Orphan rate*** in different mining modes

# Conclusion

- We propose ***a new selfish mining strategy*** to handle blockchain scenarios with multiple miners and propagation delay.
- We propose ***a simulation approach*** to simulate the real-world blockchain scenarios.
- We evaluate the performance of the selfish mining strategy on the simulation system and obtain many interesting findings from the empirical study.


# THANK YOU!