Selfish Mining Attacks Exacerbated by Elastic Hash Supply

Yoko Shibuya[1], Go Yamamoto[1], Fuhito Kojima[1], Elaine Shi[2],

Sin'ichiro Matsuo[13] Aron Laszka[4]

1 NTT Research Inc.

2 Cornell University

3 Georgetown University

4 University of Houston

Summary

- **Selfish mining** strategy, originally proposed by Eyal and Sirer (2013), shows that deviant mining could be more profitable than following the Bitcoin protocol

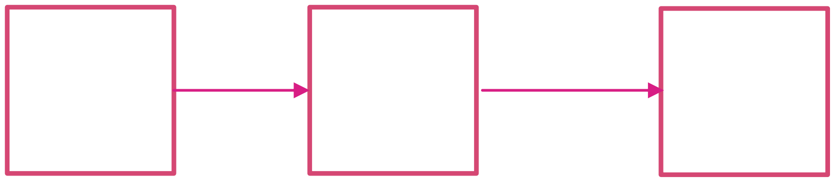
- **An important limitation of prior work**: they do not consider how honest miners react to changes in profitability when attacks occur

- In this paper, we
  - empirically show that miners react to profitability of the system (= hash supply is elastic)
  - extend the model of Eyal and Sirer (2013) with an assumption of **elastic hash supply**

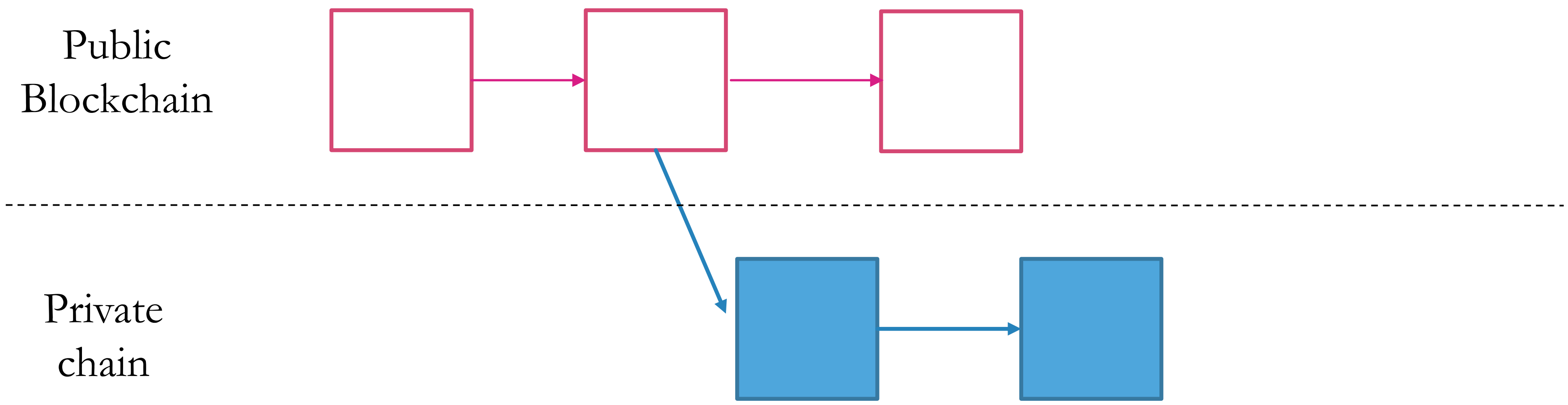
- Result: the effect of selfish mining attack is **exacerbated** under elastic hash supply

What is selfish mining?

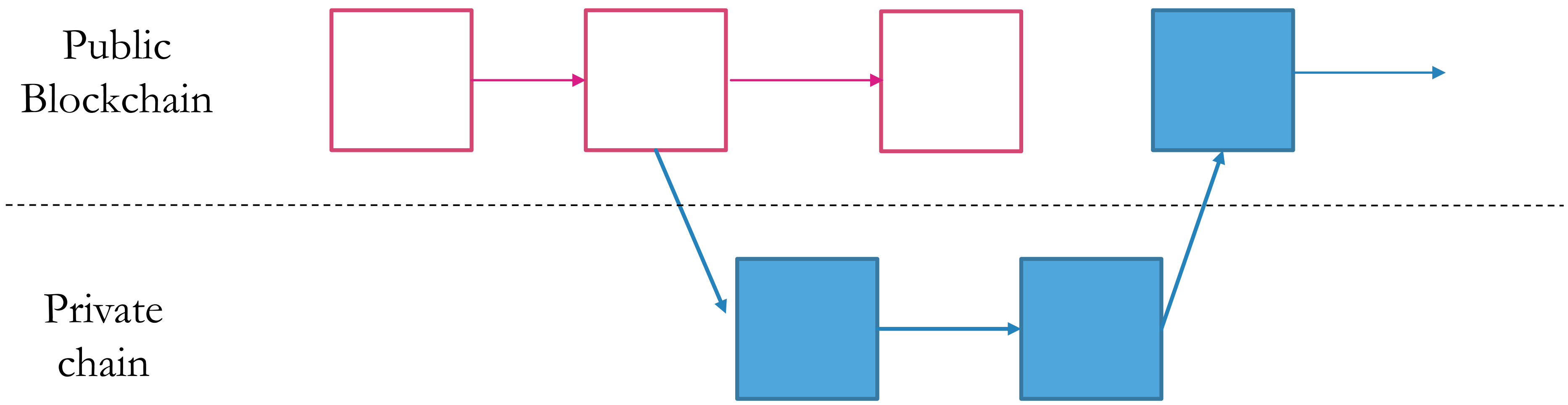
Public blockchain



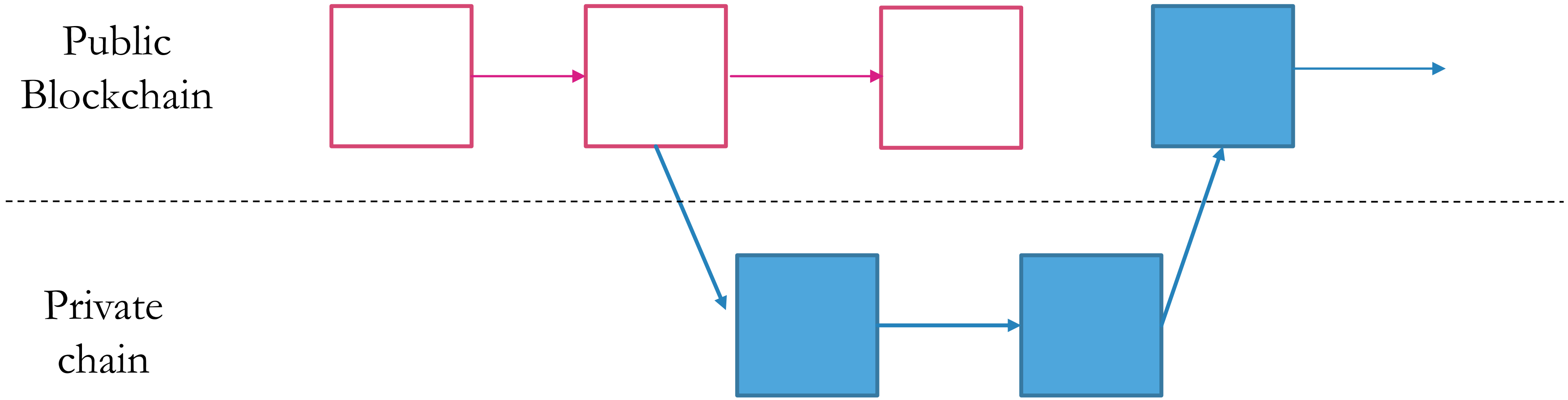
What is selfish mining?



What is selfish mining?



What is selfish mining?



- Selfish mining increases the attacker's share of the mining rewards by reducing other miners' effective mining power
- The analysis assumes that total hash power in the system is **fixed**

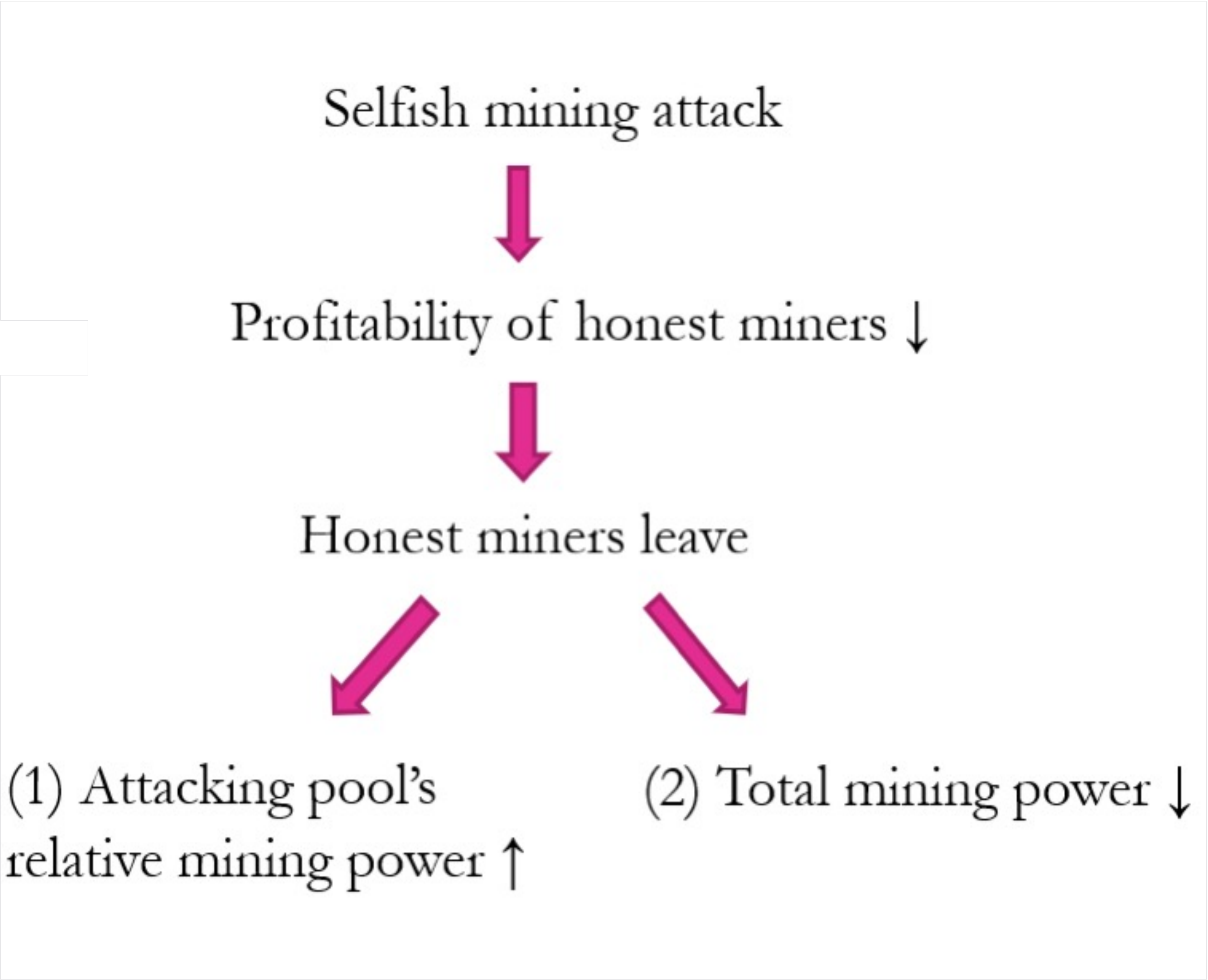
Q: What if honest miners respond to the reduction in profitability?

Elastic hash supply

1. If effect (1) dominates, all honest miners leave the system

2. If effect (2) dominates, honest miners stay in the system, where profitability = 0

- When honest miners leave/enter the system in response to the change in profitability, we say hash supply is "**elastic**"

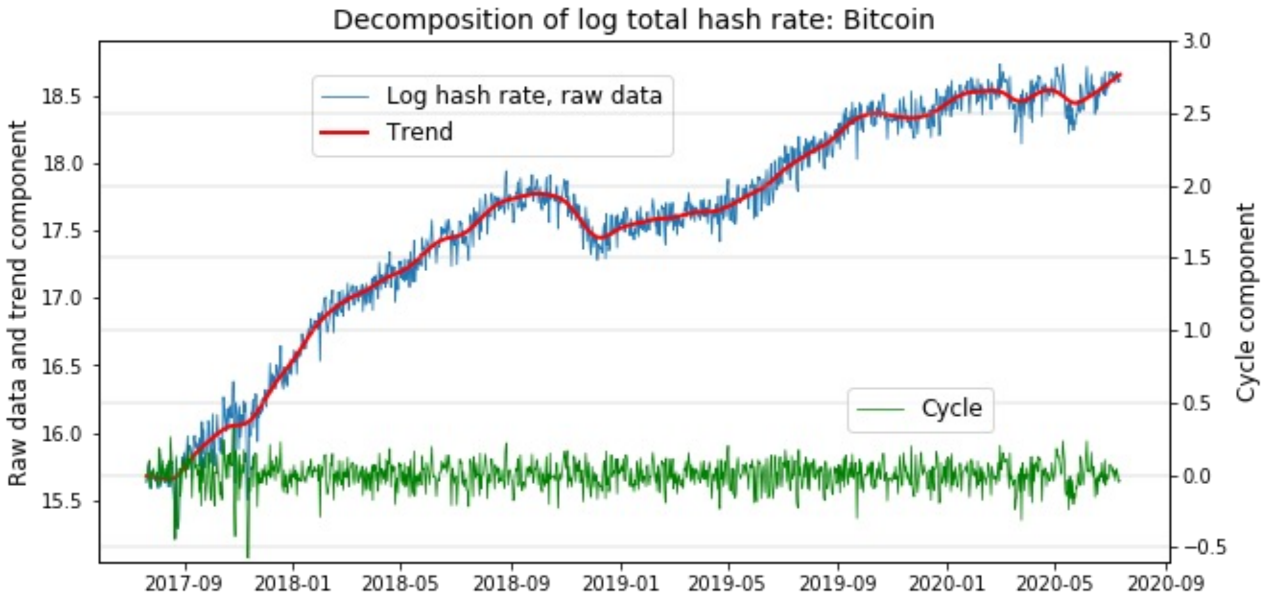


Empirical analysis

- **Objective**: Measure the correlation between total hash rate and miners' revenue in three different cryptocurrencies

- **Difficulty**: Timeseries data suffers from increasing trends in hash rate and miners' revenue due to technological advancement

- **Strategy**:
  - Apply time-detrending method to eliminate long-term trend
  - Measure correlation between short-term movements in total hash rate and revenue



<u>Three types of filters</u>

1. Hodrick-Prescott filter (HP)
2. Baxter-King filter (BK)
3. Christiano-Fitzgerald filter(CF)

Evidence for elastic hash supply

Table 1. Regression results for three currencies in sample period 2017/1/1–2020/7/31

	Bitcoin			Ethereum			Ethereum Classic		
Filters that extract the trends	HP	BK	CF	HP	BK	CF	HP	BK	CF
$\Delta \log$ MRC	0.175***	0.183***	0.181***	0.028***	0.033***	0.079***	0.041***	0.048***	0.027***
	(5.53)	(8.83)	(1.30)	(3.69)	(5.08)	(12.54)	(3.20)	(3.12)	(2.57)
No. of obs.	1308	1296	1308	1308	1296	1308	1308	1296	1308

$^{***}p < 0.01$, $^{**}p < 0.05$, $^{*}p < 0.1$, t-values in parentheses.

Coefficients on linear regression

- With any type of filter and any type of cryptocurrency, the correlation between the total hash rate and miners' revenue is **positive and statistically significant**

= **Evidence of elastic hash supply**

Model setting

- We introduce elastic hash supply to a model of selfish mining by imposing free-entry condition

- **Free-entry condition**: Miners enter/leave the system until the profitability of mining in the system converges to zero
  - Equilibrium hash power of honest miners (H^*) is determined at $u(H^*) = 0$

- Starting from zero profitability, selfish mining attack forces honest miners to leave because profitability is reduced to negative. Then,
  1. Attacking pool's relative mining power increases → profitability further decreases
  2. Total hash rate decreases → profitability increases

Q: Which effect will dominate in the equilibrium?

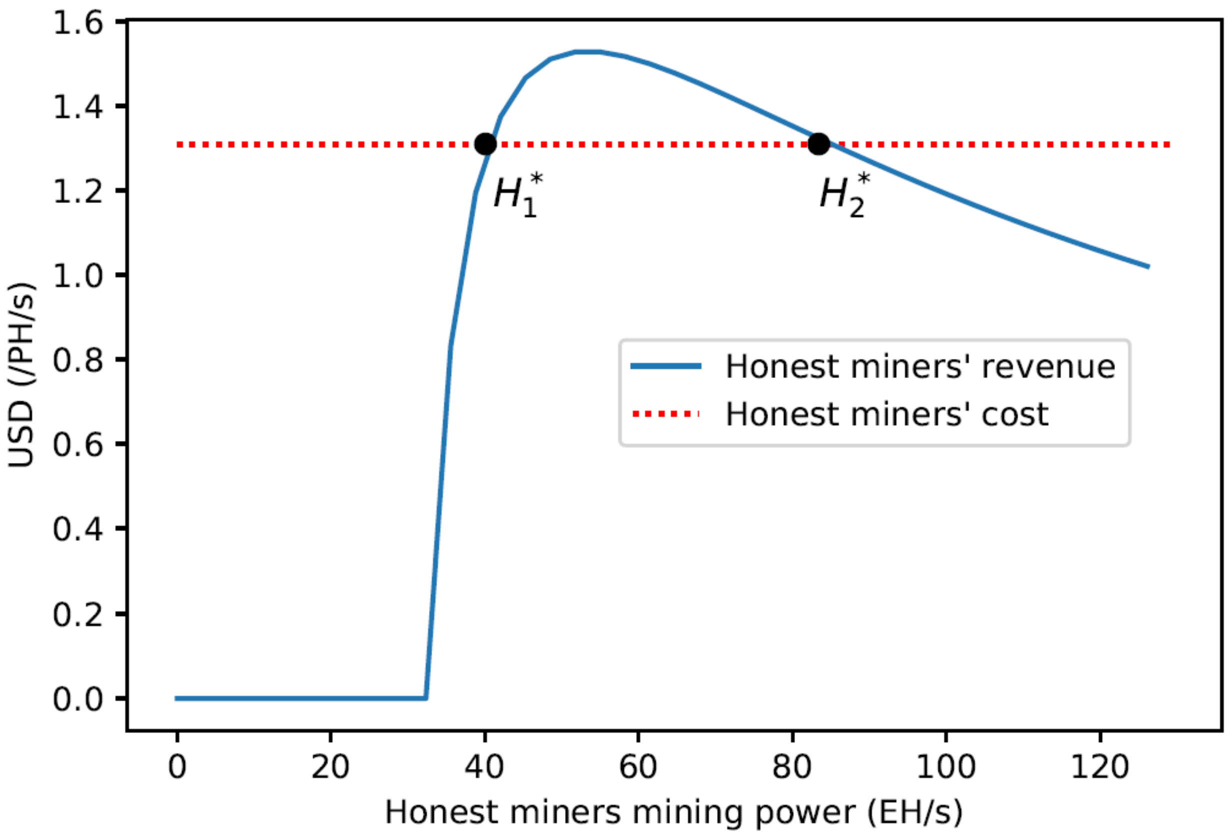
Model result

- There exists a threshold mining power for attacking pool where
  1. If initial mining power of the attacking pool is **below** the threshold, positive number of honest miners stay in the system
  2. If initial mining power of the attacking pool is **above** the threshold, **all the honest miners leave** and the system collapses

- If the attacking pool's share is large enough, the negative propagation effect forces all honest miners to leave the system

- The threshold depends on parameter $\gamma \equiv$ **the ratio of honest miners that choose to mine on the attacking pool's block**
  - $\gamma = 0$: the threshold share is about 34%
  - $\gamma = 1$: the threshold share is about 29%

Possibility of multiple equilibria



- When honest miners stay in the system, there is a possibility of multiple equilibria

1. H_1^* is an unstable equilibrium
   - A slight increase in miners' revenue would lead to H_2^*
   - A slight decrease in miners' revenue would lead to $H = 0$ (all miners leave)
2. H_2^* is a stable equilibrium

Conclusion

1. We used data from three different currencies and found that total hash rate responds to miners' revenue in short-term (elastic hash supply)
   - Time-detrending method

2. We introduced elastic hash supply into the model of selfish mining and showed that the effect of selfish mining is exacerbated

- **Future work**
  - Analyze the effect of elastic hash supply in different attacking strategies
  - Extend the model to a dynamic context