If You Can't Beat Them, Pay Them: Bitcoin Protection Racket is Profitable

Zheng Yang[1], **Chao Yin[2]**, Junming Ke[3], Tien Tuan Anh Dinh[4], Jianying Zhou[4]

[1]Southwest University
[2]Vrije University Amsterdam
[3]University of Tartu
[4]Singapore University of Technology and Design

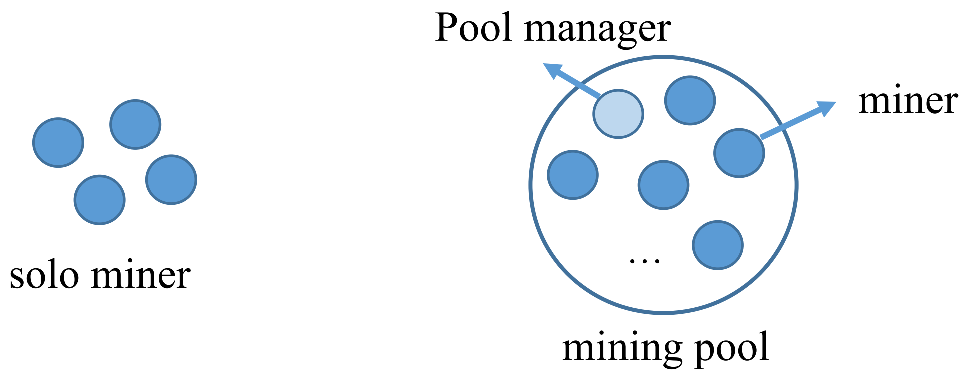
Reported by: **Chao Yin**

The Annual Computer Security Applications Conference (ACSAC 2022)
8 December 2022

- Background
- Motivation
- Theoretical analysis
- FWAP attack game
- Wining condition
- Related work
- FWAP attack
- Protection racket
- Simulation
- Future work

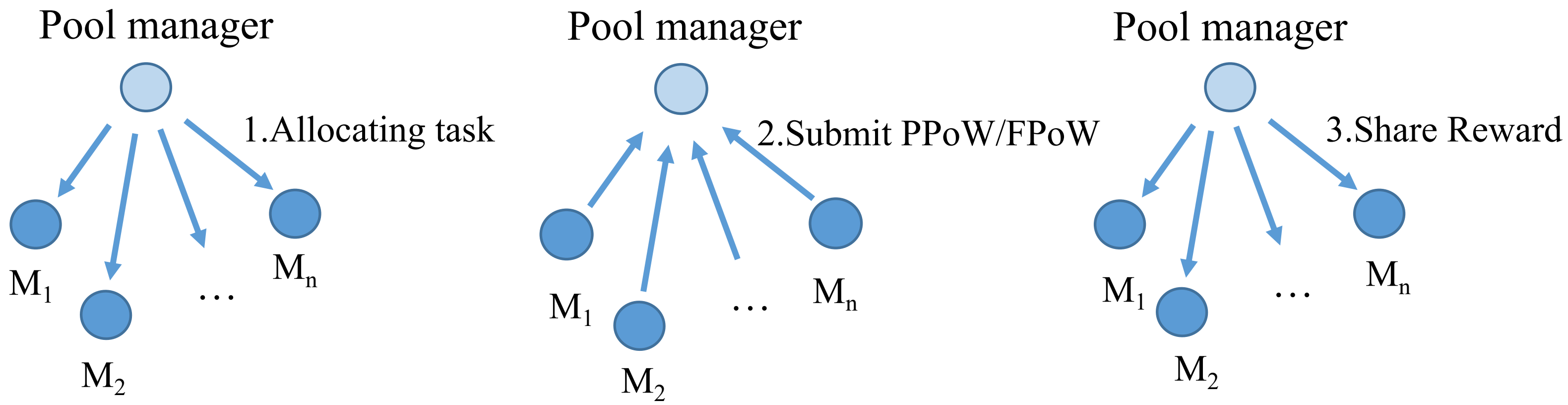
➢ Background

Mining: solve cryptographic problems



Why miners choose to mine in a mining pool?

- ✓ To get a steady reward other than pure luck
- **PPoW**: partial proof-of-work (**less difficult**)
- **FPoW**: full proof-of-work (building block)
- A miner can share a block reward in terms of its contribution



➢ Background

Incentive compatible?

- Miners can get reward proportional to their contribution

Honest mining?

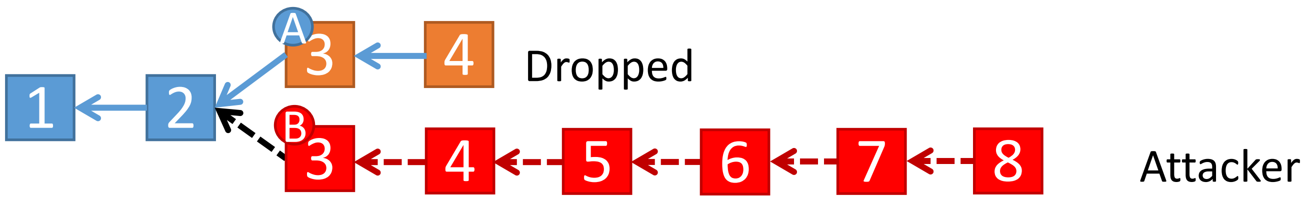
- Submit/Broadcast block once find it
- Get reward proportional to their contribution

Being rational?

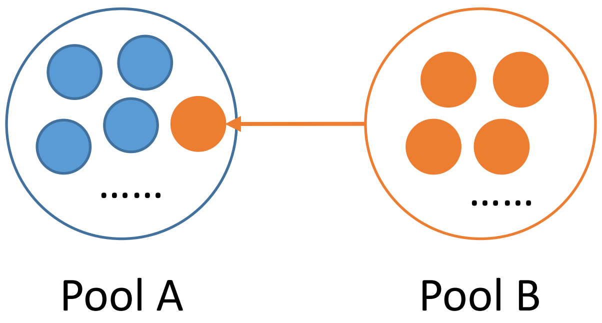
- Choose a more profitable blockchain branch when forks occur
- Obey mining rules

➢ Background

What is a fork in the Bitcoin system?



What is infiltration miner?



➢ Related work

FC '14, CCS '16, S&P 16, …
Selfish mining (SM)

CCS '19
Fork after withholding+power adjusting (PAW)

arXiv '11, arXiv '14, TIFS '17
Block withholding (BWH)

CCS '17
Fork after withholding (FAW)

ACSAC '22 Our work
Fork Withholding Attack under a Protection Racket (FWAP)

Other attacks:
Bribery attack (FC '16), Routing Attacks (S&P '17), Stealthier Partitioning Attack (S&P '20) …

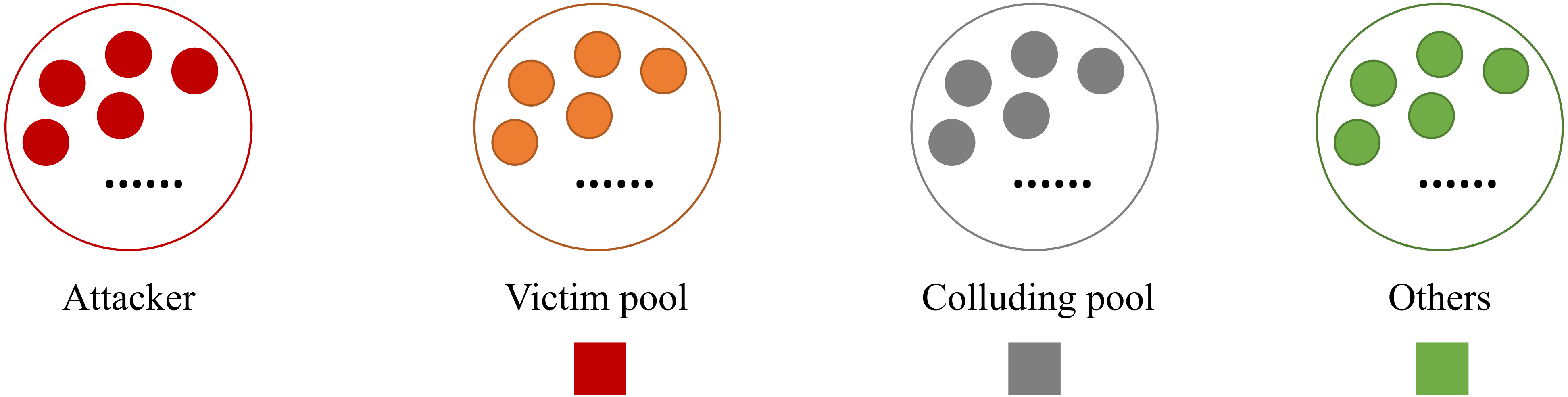
➢ Motivation

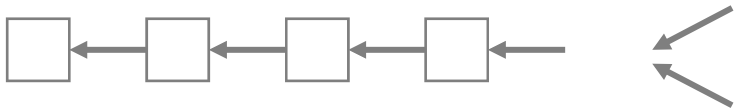
- This kind of attacks also work for other PoW based cryptocurrencies
- Still no efficient countermeasures without modifying the Bitcoin protocol
- Increase attacker’s reward

Why analyze the Bitcoin system rather than other systems?

- Highest cryptocurrency by market share to date
- Bitcoin can be seen as the first application of blockchain
- Informing further improvements to the Bitcoin system

➢ **FWAP attack** Fork Withholding Attack under a Protection Racket





Infiltration miners:

- withhold FPoWs
- protect colluding pool
- wait opportunities to generate forks

➢ Theoretical analysis

Reward of attacker:

$$R_a^{PM} = R_{inno} + R_{infi} + R_m$$

$$R_a^{PM}(\tau_1, \tau_2) = \beta \frac{\tau_1\alpha}{\beta + \tau_1\alpha} + \tau_1\alpha\left(\frac{(1-\tau_2)\alpha}{1-\tau_2\alpha} + \left(\frac{\beta}{1-\tau_2\alpha} + c\frac{\xi}{1-\tau_2\alpha}\right)\frac{\bar{\tau}\alpha}{\beta + \bar{\tau}\alpha}\right) + \mu\left(\tau_1\alpha\frac{\eta}{1-\tau_2\alpha} - (1-c)\tau'_1\alpha\frac{\eta}{1-\tau'_2\alpha}\right) + (1-\tau_1)\alpha$$

Protection money settings:

- The colluding pool can get more reward in FWAP than in PAW

$$R_{cp}^{PM} > R_{cp}^{P}$$

- Colluding pool must be able to afford protection money

$$R_{cp}^{Df} > R_m$$

➢ Protection racket

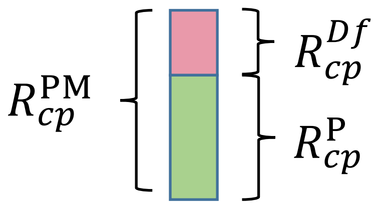
$R_m = \mu \cdot R_{cp}^{Df} \geq loss$

$\rho \cdot R_{cp}^{Df} = loss$

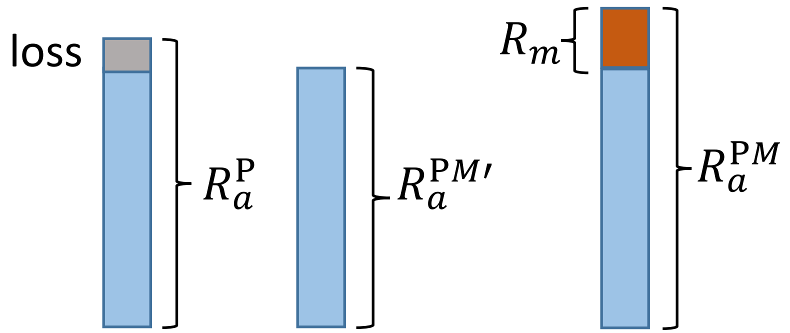
R_{cp}^{Df}: Colluding reward $R_{cp}^{Df} = R_{cp}^{PM} - R_{cp}^{P}$;

µ: Protection money ratio, i.e., $R_m = \mu \cdot R_{cp}^{Df}, \mu \in (0,1)$

$$\mu = \rho + c \cdot (1 - \rho - \epsilon)$$



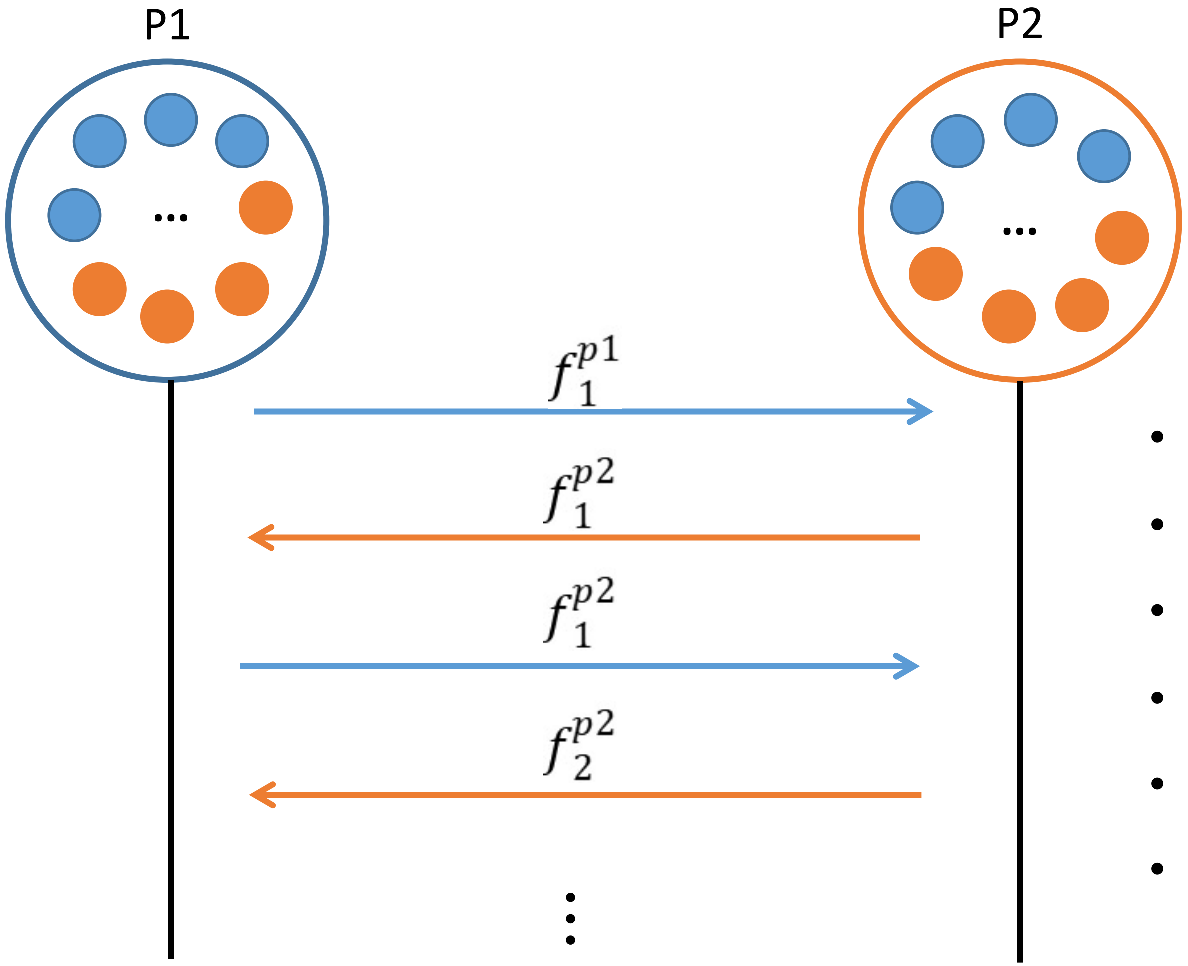
Colluding pool



Attacker

ρ: the value of the lower bound of μ;
c: Probability of the attacker's FPoW is selected as the main chain in a fork;
$\epsilon \in (0, 1)$ be a small constant that is used to guarantee the minimum colluding reward reserved;
for the colluding pool, e.g., $\epsilon = 0.01$.

➢ FWAP attack game



- Each attacker is also a victim;
- Each attacker has a colluding pool ;
- We assume P1 first infiltrate P2;
- The game will reach a Nash equilibrium;
- Pool manager’s goal is to maximize the pool reward;
- Pool reward is not equal to pure reward.

➢ Simulation

	Attacker	Target pool	Colluding pool (cp)	Coefficient C	PM Ratio μ
One Target Pool	α=0.2	$\beta = 0.1$	$\eta = 0.2$	0~1	0~1
		$\beta = 0.2$			
		$\beta = 0.3$			
Two Target pool	α=0.2	$(\beta_1, \beta_2) = (0.1, 0.1)$	$\eta = 0.2$	0~1	0~1
		$(\beta_1, \beta_2) = (0.1, 0.2)$			
		$(\beta_1, \beta_2) = (0.1, 0.3)$			

	Pool1	Pool2	Colluding pool	Coefficient C	PM Ratio μ
Attack Game	$\alpha_1 = 0$~0.5	$\alpha_2 = 0$~0.5	$\eta_1 = \eta_2 = 0.1$	0~1	According to pricing function
			$\eta_1 = 0.12, \eta_2 = 0.08$		

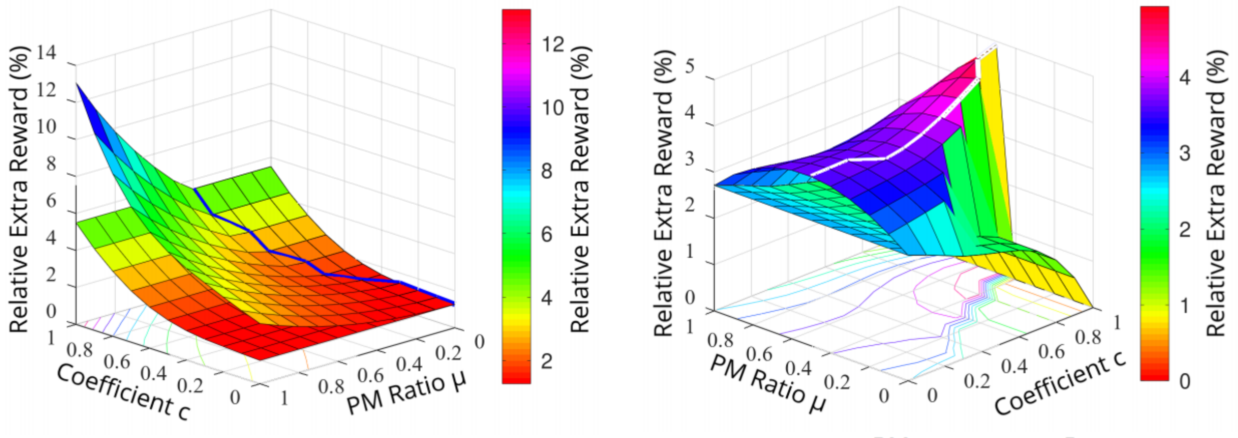
➢ Simulation

Coefficient c : the probability of attacker's block being selected as the main chain;

PM Ratio μ： protection money ratio.

Upper plain: reward in FWAP attack

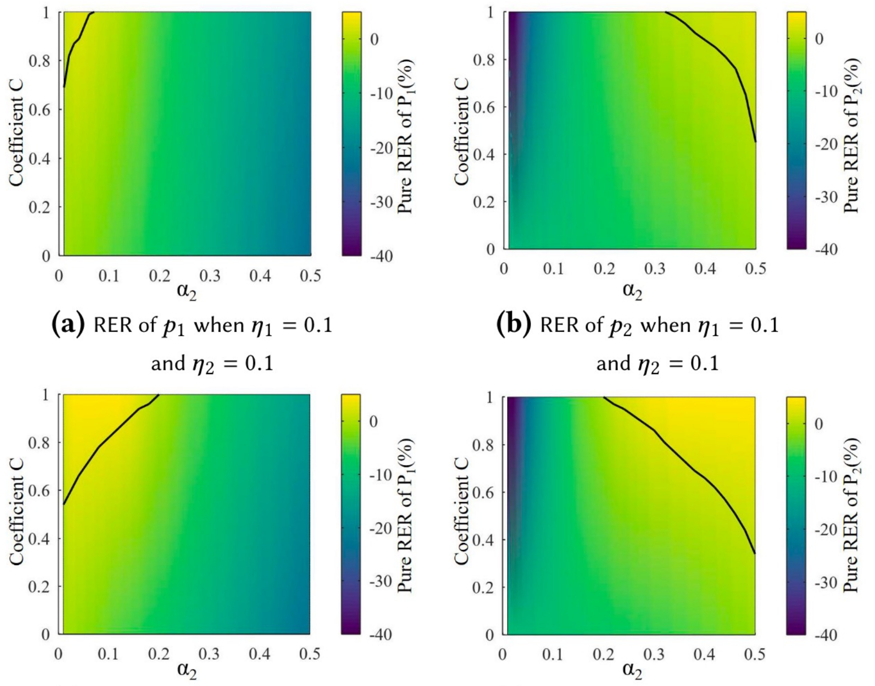
lower plain: reward in PAW attack



(a) RER_a^{PM} and RER_a^{P} (b) RER_{cp}^{PM} and RER_{cp}^{P}

Fig. 2: Quantitative analysis results against one pool. (a) and (b) show the RERs of the FWAP attacker and the colluding pool, respectively, with varying network capability c and protection money (PM) ratio μ, and constant computational power of attacker, victim pool, and colluding pool, i.e., $\alpha = 0.2$, $\beta = 0.2$, and $\eta = 0.2$.

➢ **Winning condition** —— $R_{FWAP} > R_{honest}$



(a) RER of p_1 when $\eta_1 = 0.1$ and $\eta_2 = 0.1$

(b) RER of p_2 when $\eta_1 = 0.1$ and $\eta_2 = 0.1$

(c) RER of p_1 when $\eta_1 = 0.12$ and $\eta_2 = 0.08$

(d) RER of p_2 when $\eta_1 = 0.12$ and $\eta_2 = 0.08$

Figure 6: Quantitative analysis results of a two-pool FWAP game according to pool p_2's size α_2 and coefficient c ($c_1^{(p_1)} = c_1^{(p_2)}$, $c_2^{(p_1)} = c_2^{(p_2)} = c/2$) when $\alpha_1 = 0.2$.

- Bigger pool has the chance to win the FWAP attack game.(Avoid miner's delemma)
- Attacker with bigger colluding pool is easier to win the game.
- The smaller pool will always suffer a loss despite c.

➢ Future work

- Multi-pool attack game
- Countermeasures without systematically modify the Bitcoin protocol
- Analyze the combination of FWAP and other type of attacks, e.g., bribery attack
- ……

Thanks for listening!