Games of Miners*

Jingchang Sun
Tsinghua University
Beijing, China
sunjc16@mails.tsinghua.edu.cn

Pingzhong Tang
Tsinghua University
Beijing, China
kenshinping@gmail.com

Yulong Zeng
ASResearch
Beijing, China
yulong.zeng@asresearch.io

ABSTRACT

Conventional wisdom believes cryptocurrency miners should always work on particular token at their full power. In this paper, however, we show that miners' equilibrium strategy deviates from it, which affects the system security and energy-efficiency. Specifically, we model mining as a game where each miner has limited mining power and compete for multiple tokens. We analyze both pure Nash-equilibrium and Stackelberg-equilibrium of this game, deriving their closed-forms. It is suggested that miners might not exert full power, which, compared with fully-powered mining, provides less mining power for a token and thus makes it more vulnerable to attacks, while it helps to reduce energy consumption. Simulation results show that with more disparate capacity, this effect is more significant. Our results also show that miners should disperse power among all compatible tokens instead of only one, which matches realistic statistics well.

KEYWORDS

Blockchain, Bitcoin Mining, Game Theory, Nash Equilibrium

ACM Reference Format:
Jingchang Sun, Pingzhong Tang, and Yulong Zeng. 2020. Games of Miners. In *Proc. of the 19th International Conference on Autonomous Agents and Multiagent Systems (AAMAS 2020), Auckland, New Zealand, May 9–13, 2020,* IFAAMAS, 9 pages.

1 INTRODUCTION

The last decade has witnessed the emergence of blockchain-based cryptocurrency, which has grown from the experimental Bitcoin [31] into a new asset class with a market capitalization of about $240B as of Nov, 2019 [6].

The backbone of most cryptocurrencies is the Proof-of-Work (PoW) protocol, which keeps transactions of *tokens* (digital money) in a public ledgers. PoW demands every *miner* (ledger maintainer) exert *hashrate* (computational power) to solve a cryptographic puzzle, and only thefi rst solution-finder can commit a new block of transactions. Usually a miner's hashrate is bounded by her *capacity* (resource).

The vitality of PoW is provided by monetary incentives. On one hand, in order to generate hashrate, all miners must consume proportional electricity at a *mining price* (electricity fare). On the other hand, PoW allocates the block committer some token as *reward*.

Since any miner can become a block committer, with the chance which is proportional to her hashrate out of all miners' hashrate [3], she is constantly motivated to invest hashrate for more reward, maintaining the protocol.

The security of PoW stems from a widespread belief that honest miners control the majority of mining resource and will use it up to prevent a malicious adversary from taking over the majority of hashrate[1].

Yet, this belief is misleading. First, miners' collective hashrate could be over-estimated, since they might not mine with full capacity. Chiu et al. [5] suggest that, provided with sufficient (non-binding) capacity, each miner invests the same optimal hashrate, which is less than capacity. However, according to [18], the realistic hashrate is far from symmetric[2], and for many miners, the capacity is probably binding. Thus the following problem is still open. Given some capacity, should a miner exhaust it, i.e. being *all-out*, or leave some of it idle, i.e. being *half-hearted*? Besides, hashrate of a token could be taken by other tokens, since nowadays, miners can mine multiple tokens simultaneously, as long as these tokens are compatible with the same mining hardware, an example of which is Multipool[3]. Therefore another key question is, how should a miner distribute hashrate optimally among all compatible tokens?

In this paper, we incorporate the above concerns and propose a proportional allocation game (PAG) [21], where miners with different mining prices and capacities compete for multiple tokens (see § 2). Our analysis includes both the pure Nash-equilibrium (PNE) (see § 3) and Stackelberg Equilibrium (SE) (see § 4). In addition, we evaluate the security and energy-efficiency (see § 5), as well as comparing our result with real data (see § 6).

Our main contributions are as follows:

- We consider binding capacity, varying mining price, and multiple tokens in a comprehensive model of mining game, which is non-trivial in the sense that multiple factors collectively influence miners' behavior.
- We show this game has a unique PNE (Theorem 3.10) and propose a general algorithm to compute it efficiently (Algorithm 1). When miners have uniform mining price, we derive the closed-form PNE (Theorem 3.6), with single-token environment we show there is a unique SE and derive its closed-form (Theorem 4.1).
- We show the risk brought by binding capacity and multiple tokens in PNE. If the capacities are more disparate or the token allocates less valuable reward, the total hashrate is lower, making the blockchain more vulnerable to attacks. Yet, there is a balance: while low hashrate compromises the

*An extended abstract of this paper titled *Moral hazard in games of miners* appeared in Proceedings of DAI-19.

Proc. of the 19th International Conference on Autonomous Agents and Multiagent Systems (AAMAS 2020), B. An, N. Yorke-Smith, A. El Fallah Seghrouchni, G. Sukthankar (eds.), May 9–13, 2020, Auckland, New Zealand.

[1] "The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes." (Satoshi Nakamoto, Bitcoin whitepaper)
[2] They show the hashrate follows an exponential distribution.
[3] https://en.bitcoin.it/wiki/Multipool

security, it saves more electricity and makes mining more energy-efficient.
- Our theoretical model matches realistic statistics well. We assert the total hashrate in one token is proportional to its reward value, which effectively appears in real world.

1.1 Related Work

PoW, or cryptocurrency mining, which was invented by Nakamoto [31], provides vast topics on game theory, including the miner's dilemma [1, 9], selfish mining [10, 29] the gap game [44], reward sharing in mining pools [27], timing and mechanism design on block releasing [24, 25], the gap between mining power and reward [47] etc. See survey by Liu et al. [28] for an overview.

Security is PoW'sfi rst priority, and as analyzed by Garay et al. [16], the ratio of hashrate of an individual miner, who may be an adversary, should be less than 50% to prevent "majority attack". In practice, to launch an attack, the adversary needs to control a necessary amount of capacity, the ratio of which is crucial to security. Conventional wisdom believes the above ratio of hashrate equals to that of capacity, since miners always mine with full capacity and only focus on one token.

Literatures have disproved the optimality of mining at full power. With symmetric models, Chiu et al. [5] and Pagnotta [33] suggest all miners invest the same hashrate. Adopting similar setting, Dimitri [8] and Arnosti and Weinberg [3] endow miners with different mining prices and induce asymmetric equilibria. Nevertheless, their models all assume non-binding capacity, while our model supposes both mining price and capacity are heterogeneously binding. By exploiting a special mechanism, Goren and Spiegelman [20] and Fiat et al. [14] suggest miners can disable some capacity periodically to increase utility. However, they directly assume miners exert full power periodically, instead of using the optimal portion of capacity.

Recently, miners are motivated to mine multiple tokens. Spiegelman et al. [40] and Altman et al. [2] discuss multi-token games, except that they require each miner to mine only one token. In contrast, we mostly allow free distribution of hashrate among all compatible tokens. Bissias et al. [4] discuss the game between two tokens, who provide dual perspective to our model.

Our model is a variation of PAG, which characterizes allocating goods to players in proportion to their bids. The basic design comes from Kelly [22]. As seminal works, Johari and Tsitsiklis [21] analyze PoA [26] of PAG. Then Tang et al. [43] provide the closed-formed Nash-equilibrium with a reserved price. Note they take the valuation of resource as type of players, while we also include the capacity. A classic paper [15] also discusses PAG with multiple resources, with a background of advertising. Moreover Feige et al. [12] introduce asymmetry to resource allocators. In the model of [13], bidders have limited capacity but must spend every penny. On the contrary, we bring asymmetry to bidders, by assuming everyone has a capacity, but do not force anyone to use up.

When agents act simultaneously, PAG is equivalent with a famous economic model called Cournot competition [7]. The sequential PAG is modeled by Stackelberg competition [45], where the *leader* first commits an action that *followers* observe, and then followers respond to it. Puu and Norin [35] and Puu and Marín [34] study a kind of Cournot model for duopoly and tripoly respectively, where the price and capacity are the same as ours, except that the cost is of log function. They show the closed-formed equilibrium and prove the stability. Osborne and Pitchik [32] analyze a special duopoly with capacity and characterize the set of Nash-equilibria. Recently, the effect of unequal capacity (wealth) is also studied in congestion games [17].

2 MODEL

We model cryptocurrency mining game as a PAG. Contrary to literatures assuming Bayesian settings [30, 36–39, 41, 42], we analyze the model with complete information, as is widely adopted by most mining games [5, 33] and other similar models [11]. In this game, N self-interested players compete for allocation of T token rewards. Generally, $N \geq 2$ and $T \geq 1$.

Players. Each miner i is a player, with a capacity c_i, and invests hashrate at a *mining price* of p_i, where $p_i > 0$ and $c_i > 0$. Without losing generality, miners' indices are sorted by descending order of capacity, i.e. $c_1 \geq c_2 \geq \cdots \geq c_N$. A special setting is that every miner's mining price is the same, and without losing generality[4], let it be 1. We call this case *uniform-price*.

Rewards. Each token t has a reward, which can be exchanged into fiat money of value r_t[5] The total reward of all compatible tokens is denoted by $R \triangleq \sum_{t\in[T]} r_t$.

Actions. Miner i invests hashrate $h_{i,t}$ into token t. Let $H_i \triangleq (h_{i,1}, \ldots, h_{i,T})$ be the hashrate profile of miner i, and denote the total hashrate of miner i by $h_i \triangleq \sum_{t\in[T]} h_{i,t}$. A *valid* profile should satisfy $h_i \in [0, c_i]$. When $h_i = 0$, the miner is called *inactivated*. Once *activated*, we call the miner *half-hearted* if $h_i < c_i$, otherwise *all-out*. Additionally, let $h_{-i,t}$ ($H_{-i,t}$) and h_{-i} (H_{-i}) be the total hashrate (hashrate profile) of all miners except i in token t and in whole, respectively. Token t's total hashrate in the whole network is called *nethash*, denoted by $\Gamma_t \triangleq \sum_{i\in[N]} h_{i,t}$. The nethash of all compatible tokens is $\Gamma \triangleq \sum_{t\in[T]} \Gamma_t = \sum_{i\in[N]} h_i$.

Utilities. For each token t, the utility of any miner i is $u_{i,t} \triangleq \frac{h_{i,t}}{\Gamma_t} r_t - p_i h_{i,t}$, where the former term is the expected token reward and the latter term is mining cost. Combining together, the total utility that miner i tries to maximize is $u_i(H_i, H_{-i}) \triangleq \sum_{t\in[T]} u_{i,t}$.

Equilibrium. One typical solution concept of Cournot competition is *pure Nash-equilibrium* (PNE). A hashrate profile $(H_1^*, \ldots, H_N^*)$ is a PNE, if for any miner i and any valid H_i', it holds $u_i(H_i', H_{-i}^*) \leq u_i(H_i^*, H_{-i}^*)$. Stackelberg competition's solution concept is *Stackelberg equilibrium* (SE), where the leader plays the best commitment while followers play best response to that commitment. Denote the leader by miner x. Given commitment H_x, similar to PNE, followers' hashrate profile is a best response, denoted by $\mathcal{H}^*(H_x)$, if for any follower, any deviation cannot improve the utility. The leader's hashrate H_x^* is a best commitment, if for any valid H_x' it holds $u_x(H_x', \mathcal{H}^*(h_x')) \leq u_x(H_x^*, \mathcal{H}^*(H_x^*))$. Note that unless specially mentioned, we always focus on PNE except in § 4 and § 5.2.

Security and Energy-Efficiency. When an equilibrium is reached, we measure the security as the conversion ratio of miners' capacity into nethash, denoted by $Safety \triangleq \Gamma^* / \sum_{i\in[N]} c_i$. Typically, higher

[4] Any game can be rescaled to allow any mining prices. Like the change of currency rate, it does not alter the essential of game.
[5] The exchange rate for everyone is the same, since it usually occurs in a public market.

Safety requires attackers have higher capacity and thus makes the system safer. We denote α-ATK by an attack which needs to control more than α of nethash to accomplish. The energy-efficiency is measured by the collective mining cost, i.e. $Energy = \sum_{i\in[N]} p_i h_i^*$.

3 PURE NASH-EQUILIBRIUM

In this section, we show the game has a unique PNE and derive its closed-form. Miners are layered into 3 groups according to their mining price and capacity, and each token's nethash is proportional to the reward. See Example 3.1 for a PNE with 4 miners and 2 tokens. Before revealing the whole picture (§ 3.3), we begin with the basic structure of PNE and miners' best response (§ 3.1). After that, we study the game with uniform price (§ 3.2).

Example 3.1. Consider 2 tokens, A and B, with $r_A = 100$ and $r_B = 50$, and 4 miners with $c_1 = 200$, $c_2 = 100$, $c_3 = 50$, $c_4 = 1$ and $p_1 = 2$, $p_2 = p_3 = p_4 = 1$.

They play with a PNE, which is shown in Fig 1. We explain it more throughout this section.

Miners			Token A $r_A = 100$	Token B $r_B = 50$	Idle	Status
No.	Capacity	Mining Price				
#1	200	2	0	0	200	inactivated
#2	100	1	25	12.5	62.5	half-hearted
#3	50	1			12.5	half-hearted
#4	1	1	0.67	0.33	0	all-out
Gross Hashrate (76)			**50.67**	**25.33**		
Ratio			2:1			

Figure 1: The PNE of Example 3.1

3.1 Basic Structure of PNE

In this section, we show the basic structure of PNE from two perspectives. First, the following theorem reveals miners' distribution of their hashrate among tokens.

Theorem 3.2 (Distribution amongC ryptocurrencies). *In PNE, for any activated miner i, $h_{i,t}^* > 0$ for any token t. Furthermore, for any two tokens $t, t' \in [T]$ (if $T \geq 2$), it holds $\frac{h_{i,t}^*}{h_{i,t'}^*} = \frac{r_t}{r_{t'}}$.*

For an activated miner, she invests in all compatible tokens and the hashrate in each token is proportional to the reward. Recall in Example 3.1, token A's reward is twice of B's, and for each activated miner, the hashrate in token A is also twice of that in B.

Next we try to determine the total hashrate of each miner by the following theorem.

Theorem 3.3 (Layering). *In PNE, for any miner i, if and only if $p_i \geq \frac{R}{\Gamma^*}$, she is inactivated and $h_i^* = 0$. Otherwise if and only if $c_i \leq \Gamma^* - \frac{p_i}{R}(\Gamma^*)^2$, miner i is all-out and $h_i^* = c_i$. Or with $c_i > \Gamma^* - \frac{p_i}{R}(\Gamma^*)^2$, miner i is all-out and $h_i^* = \Gamma^* - \frac{p_i}{R}(\Gamma^*)^2$.*

Essentially, miners' behaviors are jointly decided by their capacities and mining prices, which forms 3 groups (layers) in PNE. In order to illustrate this structure, we take a game with 1000 miners ($R = 100$) for example and plot each miner's PNE hashrate level in Fig 2. In detail, miner i falls into 1) inactivated group (top area), if her mining price is higher than $\frac{R}{\Gamma^*}$, 2) all-out group (bottom-left area), if her capacity is less than $\Gamma^* - \frac{p_i}{R}(\Gamma^*)^2$, or otherwise 3) half-hearted group (bottom-right area) with hashrate $\Gamma^* - \frac{p_i}{R}(\Gamma^*)^2$. Take Example 3.1 again, since only miner 1's p_1 is higher than $\frac{R}{\Gamma^*} = \frac{150}{76} = 1.97$, it falls into the inactivated group alone, while the others are either half-hearted or all-out.

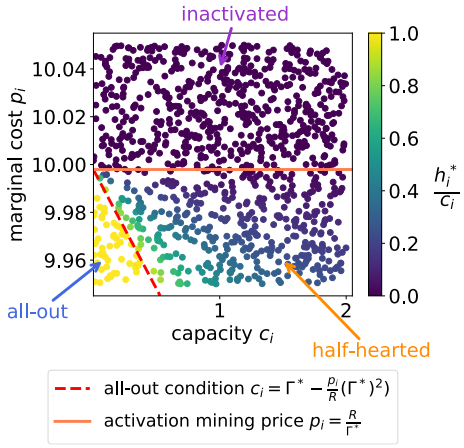


Figure 2: Layering of miners' hashrate level in PNE (Each point reflects one miner.)

Next we prove the above theorems. Wefi rst derive the form of miners' best response by the following lemma. From it we can get that, for each miner t, $h_{i,t}^* = \Gamma_t - \frac{p_i+\beta_i-\alpha_{i,t}}{r_t}\Gamma_t^2$, where β_i is a constant indicating whether to be all-out or half-hearted and $\alpha_{i,t}$ is a constant indicating whether to invest token t.

Lemma 3.4 (Best response). *Given H_{-i}, the best response of miner i is $h_{i,t}^* = \sqrt{\frac{r_t}{p_i+\beta_i-\alpha_{i,t}}h_{-i,t}} - h_{-i,t}$, where $\beta_i \geq 0$ and $\alpha_{i,t} \geq 0$ for each $t \in [T]$. It holds that $\alpha_{i,t} = 0$ if and only if $h_{i,t}^* > 0$; $\beta_i = 0$ if and only if $\sum_{t\in[T]} h_{i,t}^* < c_i$.*

Proof ofL emma3.4. Miner i's best response is the solution of the following convex optimization problem:

$$\max_{h_{i,t},\forall t\in[T]} \quad u_i = \sum_{t\in[T]} \frac{h_{i,t}}{h_{i,t}+h_{-i,t}} r_t - p_i \sum_{t\in[T]} h_{i,t} \tag{1}$$

$$\text{s.t.} \quad h_{i,t} \geq 0, \forall t \in [T] \tag{2}$$

$$\sum_{t\in[T]} h_{i,t} \leq c_i \tag{3}$$

Introduce non-negative multipliers $\alpha_{i,t}$ for each of (2) and β_i for (3). We can derive $h_{i,t}^* = \frac{1}{\sqrt{p_i-\alpha_{i,t}+\beta_i}}\sqrt{r_t h_{-i,t}} - h_{-i,t}$ from the KKT stationarity condition $\frac{\partial u_i}{\partial h_{i,t}} + \alpha_{i,t}\frac{\partial h_{i,t}}{\partial h_{i,t}} - \beta_i \frac{\partial h_{i,t}}{\partial h_{i,t}} = 0$. According to the KKT complementary slackness condition, $\alpha_{i,t} = 0$ if and only if $h_{i,t}^* > 0$; $\beta_i = 0$ if and only if $\sum_{t\in[T]} h_{i,t}^* = c_i$. □

Then the following lemma depicts the most basic structure of PNE: all compatible tokens is invested by all activated miners.

Lemma3.5. *In PNE, each token is invested by each activated miner.*

Proof ofL emma3.5. First, every token is invested, otherwise anyone can earn the reward with infinitesimal hashrate.

Then, before proving the whole lemma, we show the following preliminary result: if miner i's best response is to invest in token a but not token b, it holds $\frac{r_a}{\Gamma_a} > \frac{r_b}{\Gamma_b}$. To prove it, from i's hashrate in token a, $h^*_{i,a} = \sqrt{\frac{r_a}{p_i+\beta_i}h_{-i,a}} - h_{-i,a}$, we derive $\Gamma_a = \sqrt{\frac{r_a}{p_i+\beta_i}(\Gamma_a - h^*_{i,a})}$, and thus $h^*_{i,a} = \Gamma_a(1 - \frac{p_i+\beta_i}{r_a}\Gamma_a) > 0$, i.e. $\frac{r_a}{\Gamma_a} > p_i + \beta_i$. From j's hashrate in token b, $h^*_{i,b} = \sqrt{\frac{r_b}{p_i+\beta_i-\alpha_{i,b}}h_{-i,b}} - h_{-i,b} = 0$, we derive $\frac{r_b}{\Gamma_b} = \frac{r_b}{h_{-i,b}} = p_i + \beta_i - \alpha_{i,b} \le p_i + \beta_i < \frac{r_a}{\Gamma_a}$.

Therefore using the above conclusion, it is easy to show that at least one token is invested by all activated miners.

Now we prove that each token is invested by all miners. Suppose token a is invested by all miners, while b is not invested by miners in set M, we have $\frac{\Gamma^*_a}{r_a} < \frac{\Gamma^*_b}{r_b}$. For any miner $i \in [N]/M$, it holds $\frac{h^*_{i,a}}{\Gamma^*_a} = 1 - \frac{\Gamma^*_a}{r_a}(p_i + \beta_i)$, and $\frac{h^*_{i,b}}{\Gamma^*_b} = 1 - \frac{\Gamma^*_b}{r_b}(p_i + \beta_i)$. Therefore $\frac{h^*_{i,a}}{\Gamma^*_a} > \frac{h^*_{i,b}}{\Gamma^*_b}$. Then it leads to the following contradiction:

$$1 = \sum_{i\in[N]/M}\frac{h^*_{i,a}}{\Gamma^*_a} + \sum_{j\in M}\frac{h^*_{j,a}}{\Gamma^*_a} = \sum_{i\in[N]/M}\frac{h^*_{i,b}}{\Gamma^*_b}.$$

□

Finally, we prove the basic PNE structure as follows.

Proof ofT heorem3.2. Denote the activated miners by set M_A, for any token t, we can obtain

$$\Gamma^*_t = \sum_{i\in M_A} = \Gamma^*_t(|M_A| - \frac{\Gamma^*_t}{r_t}\sum_{i\in M_A}(p_i + \beta_i)),$$

i.e. $\Gamma^*_t = \frac{|M_A|-1}{\sum_{i\in M_A}(p_i+\beta_i)}r_t$. So we have

$$\frac{h^*_{i,t}}{r_t} = \frac{|M_A| - 1}{\sum_{i\in M_A}(p_i + \beta_i)}(1 - \frac{(|M_A| - 1)(p_i + \beta_i)}{\sum_{j\in M_A}(p_j + \beta_j)}),$$

which is irrelevant with token t. □

Proof ofT heorem3.3. For any miner i in PNE, being inactivated is equivalent with $\alpha_{i,t} \ge 0$. Since $h^*_{i,t} = \sqrt{\frac{r_t}{p_i-\alpha_{i,t}}\Gamma^*_t} - \Gamma^*_t = 0$, we have $\alpha_{i,t} = p_i - \frac{r_t}{\Gamma^*_t} \ge 0$, i.e. $p_i \ge \frac{r_t}{\Gamma^*_t} = \frac{R}{\Gamma^*}$. Being half-hearted is equivalent with $\beta_i = 0$ and $\alpha_{i,t} = 0$. Therefore $h^*_i = \sum_{t\in[T]} h_{i,t} = \sum_{t\in[T]}\Gamma^*_t - p_i\sum_{t\in[T]}\frac{(\Gamma^*_t)^2}{r_t} = \Gamma^* - \frac{p_i}{R}(\Gamma^*)^2$. Being all-out is equivalent with $\beta_i \ge 0$ and $\alpha_{i,t} = 0$. Therefore $c_i = h_i = \Gamma^* - \frac{p_i+\beta_i}{R}(\Gamma^*)^2 \le \Gamma^* - \frac{p_i}{R}(\Gamma^*)^2$. □

3.2 PNE with Uniform Price

Before discussing general cases, we analyze games with uniform price and show the closed-form PNE by the following theorem.

Theorem 3.6 (PNE with uniform price). *With uniform price, the mining game has a PNE, with nethash $\Gamma^* = Q_k$. Miners $[k]$ are half-hearted, with hashrate $h^*_i = Q_k - \frac{Q_k^2}{R}$, while the remaining are all-out, where k is the smallest integer such that $Q_k = min_{i\in[N]}Q_i$ and*

$$Q_i \triangleq \frac{(i-1)R + \sqrt{4iR\sum_{j\in[i+1,N]}c_j + (i-1)^2R^2}}{2i}.$$

Specially, $Q_0 \triangleq \sum_{i\in[N]} c_i$ and $Q_N \triangleq \frac{N-1}{N}R$.

In PNE with uniform price, the 3-layer structure degenerates into 2 layers: no miner is inactivated and, as miners are ordered by capacity, thefirst k (last $N-k$) of them are half-hearted (all-out). As an example, suppose the original miner 1 is removed from Example 3.1 and the remaining 3 miners are reindexed. Then $Q_0 = 151, Q_1 = \frac{(1-1)\times150+\sqrt{4\times1\times(50+1)+(1-1)^2\times150^2}}{2\times1} = 87.5$. Similarly, $Q_2 = 76$ and $Q_3 = 100$. Thus $\Gamma^* = Q_2 = 76$ and the largest 2 miners, 1 and 2, are half-hearted miners, both investing $76 - 76^2/150 = 37.5$. The smallest miner is all-out. Although doing her best, she still invests the least hashrate.

To prove the theorem, wefi rstfi gure out the structure of PNE. Among these miners, due to the same $\Gamma^* - \frac{(\Gamma^*)^2}{R}$, their behaviors only depend on capacity: those with higher capacities are half-hearted, while the remaining are all-out. Besides, all half-hearted miners invest the same hashrate, i.e. $\Gamma^* - \frac{(\Gamma^*)^2}{R}$, which is higher than any all-out miner.

Then denote $S_i = Q_i - \frac{Q_i^2}{R}$ and $W_i = \sum_{j\in[i+1,N]} c_j$. The following lemma explains the meaning of S_i and Q_i.

Lemma3.7. *With uniform price, if there are i half-hearted miners in PNE, their hashrate is S_i, and the total hashrate is Q_i.*

Proof. Let the hashrate of a half-hearted miner be x, the nethash is $\Gamma^* = ix + W_i$, and it holds $x = \Gamma^* - \frac{(\Gamma^*)^2}{R}$. Solving the equation[6], we get $x = \frac{(i-1)R+\sqrt{4iW_iR+(i-1)^2R^2}}{2i} = S_i$ and $\Gamma^* = Q_i$. □

Then Theorem 3.6 can be easily proved with the following two lemmas.

Lemma3.8. *For $i \in [N]$, $Q_i \ge \frac{i-1}{i}R$, the equality only holds for $W_i = 0$;*

For $i \in [N-1]$, if $S_i \ge c_{i+1}$, $Q_i \le \frac{N-1}{N}R$, the equality only holds for $c_{i+1} = \cdots = c_N = S_i$.

Proof ofL emma3.8. Wefi rst prove the lower bound of Q_i. Because $W_i \ge 0$,

$$Q_i = \frac{(i-1)R + \sqrt{4iW_i + (i-1)^2R^2}}{2i} \ge \frac{(i-1)R + \sqrt{(i-1)^2R^2}}{2i} = \frac{i-1}{i}R$$

The equality only holds with $W_i = 0$.

Then we prove the upper bound. Note that for any $t \in [T]$,

$$S_i = Q_i - \frac{Q_i^2}{R}.$$

Since $S_i \ge c_{i+1} \ge \cdots \ge c_N$, it holds

$$S_i \ge \frac{\sum_{i\in[i,N]} c_i}{N-i} = \frac{W_i}{N-i} \quad \Rightarrow \quad W_i \le (N-i)S_i,$$

[6]The other solution is always negative and thus is ruled out.

and

$$Q_i = iS_i + W_i \le NS_i = N(Q_i - \frac{Q_i^2}{R}).$$

Therefore

$$Q_i \le \frac{N-1}{N}R.$$

The equality only holds for $W_i = (N-i)S_i$, i.e. $c_{i+1} = \cdots = c_N = S_i$. □

Lemma3.9. *For any $i \in [N-1]$, the following 3 propositions are equivalent:*

1) $c_{i+1} \ge S_{i+1}$
2) $c_{i+1} \ge S_i$
3) $Q_i \ge Q_{i+1}$

It also holds if the above "$\ge$"s are all changed into "$\le$"s.

Proof. We denote the inverse of 1), 2), and 3) as 1)', 2)', and 3)'. First we prove 3) $\Leftrightarrow$ 1). Suppose $Q_i \ge Q_{i+1}$, it holds

$$\begin{aligned}
Q_{i+1} \le & \frac{(i-1)R + \sqrt{R}\sqrt{(i-1)^2R + 4i(W_{i+1}+c_{i+1})}}{2i} \\
\Leftrightarrow & \\
c_{i+1} \ge & \frac{\frac{(2iQ_{i+1}-(i-1)R)^2}{R} - (i-1)^2R}{4i} - W_{i+1} \\
= & \frac{(2iQ_{i+1}-(i-1)R)^2 - (i-1)^2R^2}{4iR} - W_{i+1} \\
= & \frac{(2iQ_{i+1})^2 - 2(i-1)R(2iQ_{i+1})}{4iR} - W_{i+1} \\
= & \frac{iQ_{i+1}^2}{R} - (i-1)Q_{i+1} - W_{i+1} \\
= & \frac{i}{R}\frac{\begin{array}{r} i^2R^2 + 2iR\sqrt{R}\sqrt{i^2R+4(i+1)W_{i+1}} \\ + R(i^2R+4(i+1)W_{i+1}) \end{array}}{4(i+1)^2} \\
& - (i-1)\frac{iR + 2\sqrt{R}\sqrt{i^2R+4(i+1)W_{i+1}}}{2(i+1)} - W_{i+1} \\
= & i\frac{\begin{array}{r} i^2R + 2i\sqrt{R}\sqrt{i^2R+4(i+1)W_{i+1}} \\ + i^2R + 4(i+1)W_{i+1} \end{array}}{4(i+1)^2} \\
& - (i-1)\frac{iR + \sqrt{R}\sqrt{i^2R+4(i+1)W_{i+1}}}{2(i+1)} - W_{i+1} \\
= & \frac{i^3R + i^2\sqrt{R}\sqrt{i^2R+4(i+1)W_{i+1}} + 2i(i+1)W_{i+1}}{2(i+1)^2} \\
& - (i^2-1)\frac{iR + \sqrt{R}\sqrt{i^2R+4(i+1)W_{i+1}}}{2(i+1)^2} - W_{i+1} \\
= & \frac{iR - 2(i+1)W_{i+1} + \sqrt{R}\sqrt{i^2R+4(i+1)W_{i+1}}}{2(i+1)^2} \\
= & S_{i+1}
\end{aligned}$$

Similarly, if $Q_i \le Q_{i+1}$, it also holds $c_{i+1} \le S_{i+1}$, i.e. 3)' $\Leftrightarrow$ 1)'.

Then we show 1) $\Leftrightarrow$ 2) and 1)' $\Leftrightarrow$ 2)' by disproving 1) $\wedge$ 2)' and 1)' $\wedge$ 2).

When $i \ge 2$, 1) $\wedge$ 2)' $\Leftrightarrow S_{i+1} \le c_{i+1} \le S_i \Rightarrow S_{i+1} \le S_i$. Since $S_{i+1} = Q_{i+1} - \frac{1}{R}Q_{i+1}^2$ and $S_i = Q_i - \frac{1}{R}Q_i^2$, it holds

$$\begin{aligned}
& Q_{i+1} - \frac{1}{R}Q_{i+1}^2 \le Q_i - \frac{1}{R}Q_i^2 \\
\Leftrightarrow & \\
& (Q_{i+1} - Q_i)(\frac{Q_{i+1}+Q_i}{R} - 1) \ge 0.
\end{aligned}$$

According to Lemma 3.8, it holds

$$Q_{i+1} + Q_i \ge \frac{i-1}{i}R + \frac{i}{i+1}R = \frac{2i^2-1}{i^2+i}R \ge \frac{7}{6}R \ge R.$$

Thus $Q_{i+1} \ge Q_i$ and 3)' $\Rightarrow$ 1)', which leads to contradiction. Similarly, 1)' $\wedge$ 2) $\Leftrightarrow S_{i+1} \ge c_{i+1} \ge S_i \Rightarrow S_{i+1} \ge S_i$, and then we can obtain 3) $\Rightarrow$ 1), which is also contradiction.

Finally we disprove $S_2 \le c_2 \le S_1$ and $S_2 \ge c_2 \ge S_1$. On one hand,

$$\begin{aligned}
S_1 \ge c_2 & \Leftrightarrow \sqrt{R}\sqrt{c_2+W_2} - c_2 - W_2 \ge c_2 \\
& \Leftrightarrow R \ge \frac{(W_2+2c_2)^2}{W_2+c_2}
\end{aligned}$$

On the other hand,

$$\begin{aligned}
S_2 \le c_2 & \Leftrightarrow \frac{1}{8}(\sqrt{R}\sqrt{R+8W_2} + R - 4W_2) \le c_2 \\
& \Leftrightarrow R(R+8W_2) \le (4(W_2+2c_2) - R)^2 \\
& \Leftrightarrow 16RW_2 \le 16(W_2+2c_2)^2 - 16Rc_2 \\
& \Leftrightarrow RW_2 \le (W_2+2c_2)^2 - Rc_2) \\
& \Leftrightarrow R \le \frac{(W_2+2c_2)^2}{W_2+c_2}.
\end{aligned}$$

They contradicts with each other and it cannot be $S_2 \le c_2 \le S_1$. Similarly, $S_2 \ge c_2 \ge S_1$ does not hold, either. □

3.3 PNE in General Cases

Finally we discuss the PNE in general cases. Combining the total hashrate and its distribution, which are uncovered in § 3.1, Theorem 3.10 discloses the overall form of general PNE while declaring its existence and uniqueness. Along with that, we propose Algorithm 1 to compute nethash efficiently, which is equivalent with a complicated closed-form expression.

Theorem 3.10 (GeneralPNE). *The mining game has a unique PNE, the nethash of which, Γ^*, can be computed within $O(NlogN)$ time by Algorithm 1. Miner i's hashrate in token t is $h_{i,t}^* = \frac{r_t}{R}h_i^*$, where $h_i^* = max\{0, min\{c_i, \Gamma^* - \frac{p_i}{r_t}(\Gamma^*)^2\}\}$.*

Proof. Let miners of set $\mathcal{M}_I$, $\mathcal{M}_H$, $\mathcal{M}_A$ be inactivated, half-hearted, and all-out, respectively. The total hashrate in PNE is the solution[7] of equation $\Gamma = f(\Gamma)$, where $f(\Gamma) = \sum_{i\in\mathcal{M}_H}(\Gamma - \frac{p_i}{R}\Gamma^2) + \sum_{i\in\mathcal{M}_A} c_i$. Thus we have

$$\Gamma = \frac{(B-1) + \sqrt{(B-1)^2 + 4AC}}{2A} \text{ if } A > 0 \text{ or } \Gamma = C,$$

where $A = \sum_{i\in\mathcal{M}_H}\frac{p_i}{R}$, $B = |\mathcal{M}_H|$, $C = \sum_{i\in\mathcal{M}_A} c_i$.

[7]The other solution is always negative and thus is ruled out.

Algorithm 1: Compute total hashrate in PNE

Result: Total hashrate in PNE, Γ^*.

1 Build a empty list $\mathbf{L}$;
2 **for** *miner* $i \leftarrow 1$ **to** N **do**
3 Add the following 3 tuples into $\mathbf{L}$:
$(\frac{1-\sqrt{max\{0,1-4c_ip_i/R\}}}{2p_i/R}, -\frac{p_i}{R}, -1, c_i)$,
$(\frac{1+\sqrt{max\{0,1-4c_ip_i/R\}}}{2p_i/R}, \frac{p_i}{R}, 1, -c_i)$, $(\frac{R}{p_i}, -\frac{p_i}{R}, -1, 0)$;
4 **end**
5 Sort $\mathbf{L}$ in ascending order of tuples'fi rst elements ;
6 $\Gamma_- \leftarrow 0$;
7 **for** $i \leftarrow 1$ **to** $3N$ **do**
8 $\Gamma_+ \leftarrow \mathbf{L}[i][1]$;
9 $A, B, C \leftarrow \sum_{j\in[i]} \mathbf{L}[j][2], \sum_{j\in[i]} \mathbf{L}[j][3], \sum_{j\in[i]} \mathbf{L}[j][4]$;
10 $\Gamma' \leftarrow \frac{(B-1)+\sqrt{(B-1)^2+4AC}}{2A}$ **if** $A > 0$ **else** C ;
11 **if** $\Gamma_- \le \Gamma' \le \Gamma_+$ **then**
12 return Γ' as Γ^*;
13 **end**
14 $\Gamma_- \leftarrow \Gamma_+$;
15 **end**

For miner i, starting from 0, when Γ exceeds 0, $\frac{1-\sqrt{max\{0,1-4c_ip_i/R\}}}{2p_i/R}$, $\frac{1+\sqrt{max\{0,1-4c_ip_i/R\}}}{2p_i/R}$, $\frac{R}{p_i}$, it holds $c_i > \Gamma - \frac{p_i\Gamma^2}{R}$, $c_i \le \Gamma - \frac{p_i\Gamma^2}{R}$, $c_i > \Gamma - \frac{p_i\Gamma^2}{R}$, $p_i \ge \frac{R}{\Gamma}$, and equivalently, miner $i \in \mathcal{M}_H$, $\mathcal{M}_A$, $\mathcal{M}_H$, $\mathcal{M}_I$, respectively. Thefi rst elements of list $\mathbf{L}$ in Algorithm 1 reflect the above thresholds of Γ, and the remaining elements of $\mathbf{L}$ represent the addition operation on A, B, and C when a miners enters (or leaves) the sets (Line 3). After sorting $\mathbf{L}$ (Line 5), we can simulate Γ increases from 0 to a segment $[\mathbf{L}[i-1][0], \mathbf{L}[i][0]]$, denoted by $[\Gamma_-, \Gamma_+]$ (Line 8, 14), and the corresponding A, B, and C are the sum of 2nd, 3rd, and 4th elements of thefirst i tuples (Line 9). Then we can compute a solution Γ' (Line 10), which is qualified if it is inside the segment (Line 11 - 12).

For the equation $\Gamma = f(\Gamma)$, the existence of solution can be proved by showing $f(x)$ is continuously concave with $f(0) = 0$, $f(\frac{R}{min_{i\in[N]}\{p_i\}}) = 0$, and $f'(0) = N > 1$.

Now we prove the solution of $\Gamma = f(\Gamma)$ is unique. Suppose x is the smallest solution, when $\Gamma = x$, the hashrate of miner i is h_i, and miners sets are still denoted by $\mathcal{M}_H$, $\mathcal{M}_A$, $\mathcal{M}_I$, with A, B, and C correspondingly induced from them. Assume $x' > x$ is also a solution, when $\Gamma = x'$, the hashrate of miner i is h'_i. Then it can be proved that $h'_i \le h_i$ for each $i \in [N]/\mathcal{M}_H$ and $h'_i \le x' - \frac{p_i}{R}(x')^2$ for each $i \in \mathcal{M}_H$. Thus it holds

$$\begin{aligned} x &= \sum_{i\in\mathcal{M}_H}(x - \frac{p_i}{R}x^2) + \sum_{i\in[N]/\mathcal{M}_A} h_i \\ &< x' \le \sum_{i\in\mathcal{M}_H}(x' - \frac{p_i}{R}(x')^2) + \sum_{i\in[N]/\mathcal{M}_A} h'_i \\ &\le \sum_{i\in\mathcal{M}_H}(x' - \frac{p_i}{R}(x')^2) + \sum_{i\in[N]/\mathcal{M}_A} h_i, \end{aligned}$$

which leads to $x + x' \le \frac{B}{A} \rightarrow x < \frac{B}{2A}$. Since $x = \frac{(B-1)+\sqrt{(B-1)^2+4AC}}{2A}$, if $B \ge 2$, it holds $x > \frac{B+B-2}{2A} \ge \frac{B}{2A}$, which contradicts with the above result. If $B = 0$, it holds $x' < 0$, which also causes contradiction. If $B = 1$, there is only one miner in $\mathcal{M}_H$ and suppose this miner's mining price is p. Then it can be proved that $x' \le \sqrt{\frac{C}{A}} = x$, also contradicts with assumption. □

4 STACKELBERG EQUILIBRIUM

In this section we discuss SE. Thefi rst motivation is that SE can characterize the competition between big miners and small miners in reality. As a preliminary knowledge, a Cournot miner always has the incentive to become the Stackelberg leader, since being the leader, at least she can get the PNE utility by committing PNE best response. However, the leader must be wealthy to tolerate the risk that others do not follow SE, and she also needs to be well-known to effectively publish a commitment. In practice, such powerful miners indeed exist and is public. For example, there was a time that Bitmain is known for holding nearly 51% of Bitcoin mining market [46]. Therefore, if a miner is notably bigger than others, she probably plays SE. Our second motivation is that SE can better capture the "benevolent" miners in some new tokens. Usually, in order to prevent a new token from losing mining power, as well as reserving some rewards, its supporters will invest some "benevolent" hashrate in this token. No matter how other miners act, the benevolent miners keep unchanged, which is similar with the behavior of Stackelberg leader. In order to maximize the reserved reward, the benevolent miners might play SE.

With single-token and uniform-price, Theorem 4.1 suggests the game has a unique SE, and given the best commitment of leader, the closed-form of followers' hashrate is also derived.

Theorem4.1. *A single-token uniform-price mining game has a unique Stackelberg-equilibrium:*

$$h_x^* = \Omega_k$$

$$\forall i \in [N], h_i^* = min\{Q_k(\Omega_k) - \frac{(Q_k(\Omega_k))^2}{R}, c_i\}$$

where

$$k \triangleq \underset{i\in[k_0,N]\wedge\Omega_i\in[0,c_x]}{\arg\max} \{\frac{\Omega_i}{Q_k(\Omega_i)+\Omega_i}R - \Omega_i\},$$

$$k_0 \triangleq \underset{i\in[0,N]}{\arg\min} Q_i(0);$$

$$\Omega_i \triangleq min\{max\{max\{0, \Theta_i\}, \Phi_i\}, min\{\Theta_{i+1}, c_x\}\};$$

$$\Theta_i \triangleq \frac{R + \sqrt{R^2 - 4c_iR}}{2} - (ic_i + W_i);$$

$$\Phi_i \triangleq \frac{\begin{array}{c}\Psi_i^2 + (2i-1)R\Psi_i + (2i-1)^2R^2 \\ - 12iW_i(\Psi_i + 2iR(i-2))\end{array}}{12i\Psi_i};$$

$$\Psi_i \triangleq \Bigg((2i-1)^3R^3 + 36i^2(4i^2-7i+4)R^2W_i + 216i^4RW_i^2 + 12\sqrt{3}\sqrt{\begin{matrix} i^2R^2W_i((i-1)R+2i^2W_i)^2 \\ ((2i-1)^3R+27i^2W_i) \end{matrix}} \Bigg)^{1/3};$$

$$Q_i(x) \triangleq \frac{(i-1)R + \sqrt{4i(W_i+x)R + (i-1)^2R^2}}{2i}; \quad (4)$$

and

$$W_i \triangleq \sum_{j\in[i+1,N]} c_j. \quad (5)$$

Specially, $\Theta_{N+1} = R$, $\Theta_0 = 0$, $\Phi_0 = \sqrt{RW_0} - W_0$, $Q_0(x) = W_0 + x$ *and* $W_N = 0$.

Comparing the form of Q_i and $Q_i(.)$, wefi nd that, followers' behavior in SE is similar with PNE, except that they take the leader as a group of all-out miners whose capacity is the best commitment. The leader's best commitment is more complicated, here we show a counter-intuitive behavior of the leader. Recall in PNE, there is a threshold such that as long as the capacity is higher (lower) than it, the miner is half-hearted (all-out). However, such threshold might not exist in SE. In other words, if we provide some extra capacity to the leader, it could make no difference to her best commitment. Interestingly, if provided with even more, the best commitment suddenly increases, like a "phase change". Example 4.2 illustrates this insight.

Example 4.2. Consider a single-token uniform-price game with $R = 100$. There are 15 miners with $c_1 = 10$ and $c_2 = \cdots = c_{15} = 5$.

First we add a miner and study her PNE behavior given different capacity. As shown at the left of Fig 3), provided with more capacity, the PNE best response also increases, until reaching 9.6, when the utility also saturates at 1.2.

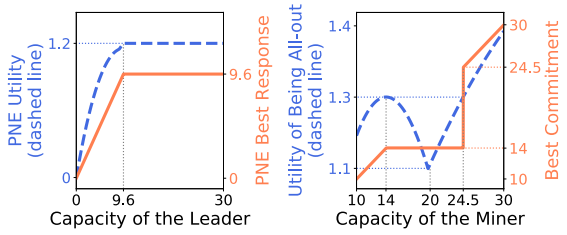


Figure 3: Behavior vs. Capacity (Example 4.2)

Then we take her as the Stackelberg leader butfi nd such saturation point does not exist. As shown at the right of Fig 3, when capacity is less than 14, the best commitment is all-out. When it exceeds 14, however, the utility of being all-out drops until it reaches 20. Meanwhile, the best commitment stays as 14, being half-hearted. Interestingly, a phase change happens when capacity is around 24.5: the best commitment increases to 24.5 abruptly (all-out again).

Finally the following corollary discloses one effect of one miner playing SE instead of PNE.

Corollary4.3. *In single-token uniform-price mining game, the nethash in SE is no less than the nethash in PNE.*

This actually matches the aim of "benevolent" forces — raising the total hashrate of specific token.

5 SECURITY AND ENERGY-EFFICIENCY

In this section, we analyze the effect of various factors on security and energy-efficiency. First we consider the attacker as an "outsider" while honest miners play PNE (see § 5.1). Then suppose the attacker is the Stackelberg leader, we study her action (see § 5.2).

5.1 Security and Energy-Efficiency in PNE

Assume honest miners are not aware of the attacker and play PNE, we show the influence of capacity distribution and multi-token. Since mining price and the total capacity are not relevant here, we assume uniform-price setting and the total capacity is C.

First we show how capacity can affect the security indirectly by the following corollary.

Corollary5.1. *In PNE with uniform-price, given* $C = \sum_{i\in[N]} c_i$, *it holds* $Energy = Safety \times C$. *If there are* k *half-hearted miners and* $k \geq 1$, *it holds* $\frac{R}{C}(1-\frac{1}{k}) \leq Safety \leq \frac{R}{C}(1-\frac{1}{N})$, *The equality only holds for* $k = N$.

Following different distribution, the capacity produces different k and a lower bound of $Safety$, i.e. $\frac{R}{C}(1-1/k)$. If the capacity of an attacker is xC, in order to prevent her from launching α-ATK, k should be at least $\lceil \alpha/(\alpha - Cx/R) \rceil$. For the two most famous attacks, 50%-ATK (majority attack [31]) and 25%-ATK (selfish mining [10]), k should be at least $\lceil 1/(1-2Cx/R) \rceil$. and $\lceil 1/(1-4Cx/R) \rceil$, respectively. With higher x, k also needs to be bigger. Note that while raising $Safety$ makes a more robust system, the value of $Energy$ also increases, which is less environmental-friendly.

Next we show the relation between capacity disparity and security by simulation. To quantify the disparity, we adopt Gini index [19]:

$$Gini \triangleq \Big(\sum_{i\in[N]} \sum_{j\in[N]} |c_i - c_j| \Big) / \Big(2N \sum_{i\in[N]} c_i \Big).$$

Note that $Gini \in [0,1]$, and a higher (or lower) value of it implies the capacity is more (or less) equally distributed.

We generate games following 3 kinds of capacity distributions[8] (500 games for each). In every game, $N = 100$, $R = 100$, and total capacity is normalized into 100.

For each game, the security ($Safety$) is evaluated, which is represented by each point in Fig 4: (a) - (c). With all distributions, if the capacity is more disparate (larger $Gini$), the blockchain is less secure (lower $Safety$). Such trend is most significant with power-law distribution, since it produces extremely unequal capacity.

Finally, we discuss the effect of multiple tokens. Specifically, by raising reward value, a token can gain more hashrate. However, the gained hashrate is less than raised reward, and when the reward is higher, this effect is weaker. The intuition is that since $\frac{dQ_i}{dR} > 0$ and $\frac{d^2Q_i}{dR^2} < 0$, according to Theorem 3.6, the nethash, i.e. minimum

[8] Exponential is exponential distribution with parameter $\lambda = 2$, and power-law is Pareto type II distribution with parameter $\alpha = 1$

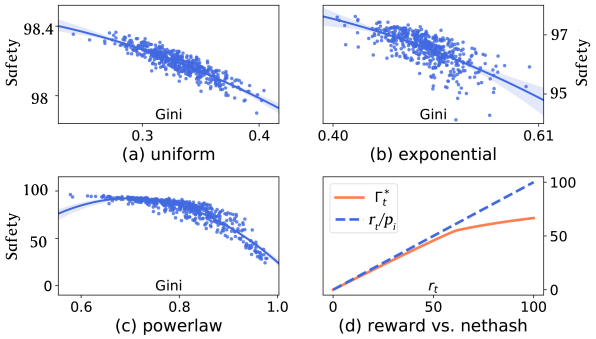


Figure 4: Simulation results in § 5 (a-c: disparity vs. security. d: token reward vs. nethash)

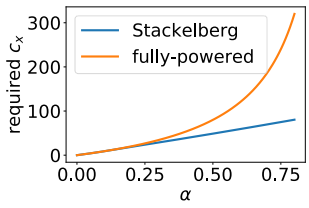
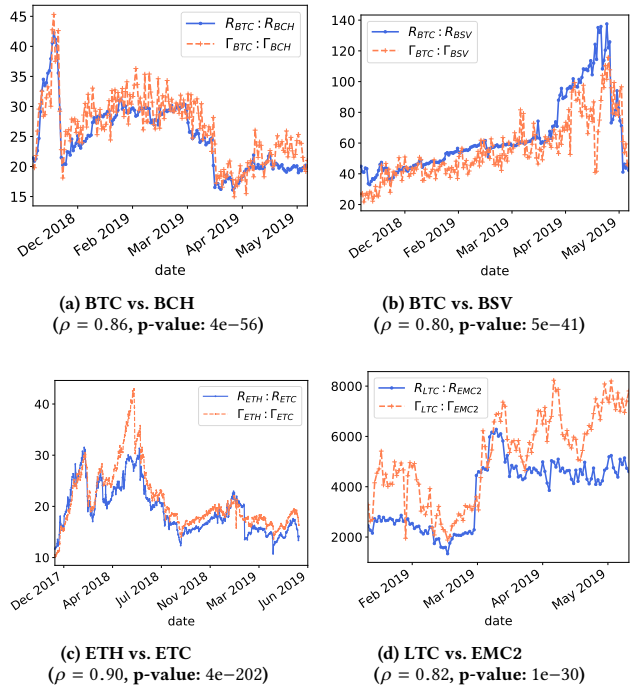


Figure 5: Capacity to attack in SE vs. fully-powered mining



(a) BTC vs. BCH ($\rho = 0.86$, **p-value:** 4e−56)

(b) BTC vs. BSV ($\rho = 0.80$, **p-value:** 5e−41)

(c) ETH vs. ETC ($\rho = 0.90$, **p-value:** 4e−202)

(d) LTC vs. EMC2 ($\rho = 0.82$, **p-value:** 1e−30)

Figure 6: History Ratio of Reward and Nethash (ρ is Pearson correlation coefficient of $\frac{R_A}{R_B}$ and $\frac{\Gamma_A}{\Gamma_B}$)

Q_i, is also concave with R. We illustrate this insight by an example with 20 randomly generated miners ($C = 100$). Suppose token t increases its reward from 0 to 100, while the total reward of other tokens remain 50. As shown in Fig 4: (d), Γ_t^* increases concavely with r_t, but is always smaller than r_t/p_i.

5.2 Security in SE

When the attacker is the Stackelberg leader, she can launch an α-ATK only if her capacity is large enough, the closed-form condition of which is given by the following corollary, using Q_i and W_i from (4) and (5) in Theorem 4.1.

Corollary5.2. *In a mining game, with single-token and uniform-price setting, the Stackelberg leader is able to launch an α-ATK if $c_x > \alpha min\{W_0 + c_x, min_{i\in[N]}Q_i(c_x)\}$.*

Compared with fully-powered mining (all miners exerting full capacity), the system in SE are more vulnerable, which is illustrated by the following simulation. With the same profile as Example 4.2, suppose the leader tries to launch an α-ATK, we compute the minimum required capacity (the values in SE can be computed by binary search.). The results are shown by Fig 5, when honest miners are fully-powered , compared with SE, it is more difficult, i.e. demands higher capacity, for the attacker to succeed, and the gap increases with α.

6 THEORY VS. REALITY

In this section, we show realistic statistics to support a key pattern of our theoretical result: Take a pair of tokens sharing the same cryptographic puzzle, say A and B, their ratio of reward and nethash should be the same, i.e. $\frac{R_A}{R_B} = \frac{\Gamma_A}{\Gamma_B}$ (by Theorem 3.10).

We collect reward and gross hashrate of 4 qualified token-pairs: BTC-BCH, BTC-BSV, ETH-ETC and LTC-EMC2.[9] Their daily $\frac{R_A}{R_B}$ and $\frac{\Gamma_A}{\Gamma_B}$ are compared in Fig 6. We observe that, indeed, the two ratios are close with each other.

For each pair, Fig 6 shows the Pearson correlation coefficient of the two ratios, all of which are significantly high, ranging from 0.8 to 0.9, with p-value less than 0.001. We also compute their average daily $\frac{R_A}{R_B}/\frac{\Gamma_A}{\Gamma_B}$, denoted by $\omega_{A,B}$, the results of which are $\omega_{BTC,BCH} = 0.95$, $\omega_{BTC,BCH} = 1.19$, $\omega_{ETH,ETC} = 0.92$, and $\omega_{LTC,EMC2} = 0.74$. Usually they should be close to 1, while two of them slightly deviates. One is BTC-BSV, with too much hashrate in BSV. We conjecture it comes from the "benevolent" hashrate during the famous "mining war" recently [23]. In order to promote BSV, its supporters invested a lot hashrate without caring about the token price. According to Corollary 4.3, this actually causes disproportionality between nethash and reward value. The other is LTC-EMC2 with too less hashrate in EMC2. It might because EMC2 is a lesser-known token, and miners would avoid mining it.

7 ACKNOWLEDGMENTS

This work is supported by Science and Technology Innovation 2030 — "New Generation Artificial Intelligence" Major Project No. 2018AAA0100904, 2018AAA0101103, Turing AI Institute of Nanjing and Beijing Academy of Artificial Intelligence (BAAI).

[9] Ranked by the market capitalization in Nov, 2019 [6], these tokens include top 1, 2, 3, 4, 5, 7 PoW cryptocurrencies.

REFERENCES

[1] Colleen Alkalay-Houlihan and Nisarg Shah. 2019. The Pure Price of Anarchy of Pool Block Withholding Attacks in Bitcoin Mining. In *AAAI 2019*.

[2] Eitan Altman, Alexandre Reiffers-Masson, Daniel Sadoc Menasché, Mandar Datar, Swapnil Dhamal, and Corinne Touati. 2018. Mining competition in a multi-cryptocurrency ecosystem at the network edge: A congestion game approach.

[3] Nick Arnosti and S. Matthew Weinberg. 2018. Bitcoin: A Natural Oligopoly. (2018). arXiv:cs.CR/1811.08572

[4] George Bissias, Brian N Levine, and David Thibodeau. 2019. Greedy but cautious: Conditions for miner convergence to resource allocation equilibrium. *arXiv preprint arXiv:1907.09883* (2019).

[5] Jonathan Chiu, Thorsten Koeppl, et al. 2018. *Incentive compatibility on the blockchain*. Technical Report. Bank of Canada.

[6] CoinMarketCap. 2019. Cryptocurrency market capitalizations. (2019). https://coinmarketcap.com/all/views/all/ [Online; accessed Nov-2019].

[7] Antoine-Augustin Cournot. 1838. *Recherches sur les principes mathématiques de la théorie des richesses par Augustin Cournot*. chez L. Hachette.

[8] Nicola Dimitri. 2017. Bitcoin mining as a contest. *Ledger* 2 (2017), 31–37.

[9] Ittay Eyal. 2015. The miner's dilemma. In *2015 IEEE Symposium on Security and Privacy*. IEEE, 89–103.

[10] Ittay Eyal and Emin Gün Sirer. 2018. Majority is not enough: Bitcoin mining is vulnerable. *Commun. ACM* 61, 7 (2018), 95–102.

[11] Wenyi Fang, Pingzhong Tang, and Song Zuo. 2016. Digital good exchange. In *Proceedings of the 2016 International Conference on Autonomous Agents & Multiagent Systems*. 1277–1278.

[12] Uriel Feige, Ron Lavi, and Moshe Tennenholtz. 2013. Competition among asymmetric sellers withfi xed supply. In *Proceedings of the fourteenth ACM conference on Electronic commerce*. ACM, 415–416.

[13] Michal Feldman, Kevin Lai, and Li Zhang. 2005. A price-anticipating resource allocation mechanism for distributed shared clusters. In *Proceedings of the sixth ACM conference on Electronic commerce*. ACM, 127–136.

[14] Amos Fiat, Anna Karlin, Elias Koutsoupias, and Christos Papadimitriou. 2019. Energy Equilibria in Proof-of-Work Mining. In *Proceedings of the 2019 ACM Conference on Economics and Computation*. ACM, 489–502.

[15] Lawrence Friedman. 1958. Game-theory models in the allocation of advertising expenditures. *Operations research* 6, 5 (1958), 699–709.

[16] Juan Garay, Aggelos Kiayias, and Nikos Leonardos. 2015. The bitcoin backbone protocol: Analysis and applications. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 281–310.

[17] Kurtuluş Gemici, Elias Koutsoupias, Barnabé Monnot, Christos Papadimitriou, and Georgios Piliouras. 2018. Wealth Inequality and the Price of Anarchy. *arXiv preprint arXiv:1802.09269* (2018).

[18] Adem Efe Gencer, Soumya Basu, Ittay Eyal, Robbert Van Renesse, and Emin Gün Sirer. 2018. Decentralization in bitcoin and ethereum networks. *arXiv preprint arXiv:1801.03998* (2018).

[19] Corrado Gini. 1997. Concentration and dependency ratios. *Rivista di politica economica* 87 (1997), 769–792.

[20] Guy Goren and Alexander Spiegelman. 2019. Mind the Mining. In *Proceedings of the 2019 ACM Conference on Economics and Computation*. ACM, 475–487.

[21] Ramesh Johari and John N Tsitsiklis. 2004. Efficiency loss in a network resource allocation game. *Mathematics of Operations Research* 29, 3 (2004), 407–435.

[22] Frank Kelly. 1997. Charging and rate control for elastic traffic. *European transactions on Telecommunications* 8, 1 (1997), 33–37.

[23] Olga Kharif. 2018. Bitcoin Cash Clash Is Costing Billions With No End in Sight. (2018). https://www.bloomberg.com/news/articles/2018-11-16/bitcoin-cash-clash-is-costing-billions-with-no-end-in-sight

[24] Aggelos Kiayias, Elias Koutsoupias, Maria Kyropoulou, and Yiannis Tselekounis. 2016. Blockchain Mining Games. In *Proceedings of the 2016 ACM Conference on Economics and Computation (EC '16)*. ACM, New York, NY, USA, 365–382. https://doi.org/10.1145/2940716.2940773

[25] Elias Koutsoupias, Philip Lazos, Paolo Serafino, and Foluso Ogunlana. 2019. Blockchain Mining Games with Pay Forward. *arXiv preprint arXiv:1905.07397* (2019).

[26] Elias Koutsoupias and Christos Papadimitriou. 1999. Worst-case equilibria. In *Annual Symposium on Theoretical Aspects of Computer Science*. Springer, 404–413.

[27] Yoad Lewenberg, Yoram Bachrach, Yonatan Sompolinsky, Aviv Zohar, and Jeffrey S Rosenschein. 2015. Bitcoin mining pools: A cooperative game theoretic analysis. In *Proceedings of the 2015 International Conference on Autonomous Agents and Multiagent Systems*. Citeseer, 919–927.

[28] Ziyao Liu, Nguyen Cong Luong, Wenbo Wang, Dusit Niyato, Ping Wang, Ying-Chang Liang, and Dong In Kim. 2019. A Survey on Applications of Game Theory in Blockchain. *arXiv preprint arXiv:1902.10865* (2019).

[29] Francisco J Marmolejo-Cossío, Eric Brigham, Benjamin Sela, and Jonathan Katz. 2019. Competing (Semi)-Selfish Miners in Bitcoin. *arXiv preprint arXiv:1906.04502* (2019).

[30] Vahab S Mirrokni, Renato Paes Leme, Pingzhong Tang, and Song Zuo. 2016. Dynamic Auctions with Bank Accounts.. In *IJCAI*, Vol. 16. 387–393.

[31] Satoshi Nakamoto. 2008. Bitcoin: a peer-to-peer electronic cash system. (2008).

[32] Martin J Osborne and Carolyn Pitchik. 1986. Price competition in a capacity-constrained duopoly. *Journal of Economic Theory* 38, 2 (1986), 238–260.

[33] Emiliano Pagnotta. 2018. Bitcoin as Decentralized Money: Prices, Mining Rewards, and Network Security. *Mining Rewards, and Network Security (October 26, 2018)* (2018).

[34] Tönu Puu and Manuel Ruíz Marín. 2006. The dynamics of a triopoly Cournot game when the competitors operate under capacity constraints. *Chaos, Solitons & Fractals* 28, 2 (2006), 403–413.

[35] Tönu Puu and Anna Norin. 2003. Cournot duopoly when the competitors operate under capacity constraints. *Chaos, Solitons & Fractals* 18, 3 (2003), 577–592.

[36] Weiran Shen and Pingzhong Tang. 2017. Practical versus optimal mechanisms. In *Proceedings of the 16th Conference on Autonomous Agents and MultiAgent Systems*. 78–86.

[37] Weiran Shen, Pingzhong Tang, and Yulong Zeng. 2018. Buyer-Optimal Distribution. In *Proceedings of the 17th International Conference on Autonomous Agents and MultiAgent Systems*. International Foundation for Autonomous Agents and Multiagent Systems, 1513–1521.

[38] Weiran Shen, Pingzhong Tang, and Yulong Zeng. 2018. A closed-form characterization of buyer signaling schemes in monopoly pricing. In *Proceedings of the 17th International Conference on Autonomous Agents and MultiAgent Systems*. International Foundation for Autonomous Agents and Multiagent Systems, 1531–1539.

[39] Weiran Shen, Pingzhong Tang, and Yulong Zeng. 2019. Buyer Signaling Games in Auctions. In *Proceedings of the 18th International Conference on Autonomous Agents and MultiAgent Systems*. International Foundation for Autonomous Agents and Multiagent Systems, 1591–1599.

[40] Alexander Spiegelman, Idit Keidar, and Moshe Tennenholtz. 2018. Game of coins. *arXiv preprint arXiv:1805.08979* (2018).

[41] Pingzhong Tang and Zihe Wang. 2017. Optimal mechanisms with simple menus. *Journal of Mathematical Economics* 69 (2017), 54–70.

[42] Pingzhong Tang, Zihe Wang, and Xiaoquan Zhang. 2016. Optimal commitments in asymmetric auctions with incomplete information. In *Proceedings of the 2016 ACM Conference on Economics and Computation*. 197–211.

[43] Pingzhong Tang, Yulong Zeng, and Song Zuo. 2017. Fans Economy and All-Pay Auctions with Proportional Allocations.. In *AAAI*. 713–719.

[44] Itay Tsabary and Ittay Eyal. 2018. The gap game. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 713–728.

[45] Heinrich Von Stackelberg. 1934. *Marktform und gleichgewicht*. J. springer.

[46] Josiah Wilmoth. 2018. Bitmain's Mining Pools Now Control Nearly 51 Percent of the Bitcoin Hashrate. (2018). https://finance.yahoo.com/news/bitmain-mining-pools-now-control-155804143.html

[47] Yulong Zeng and Song Zuo. 2019. The Matthew Effect in Computation Contests: High Difficulty May Lead to 51% Dominance?. In *The World Wide Web Conference*. 2281–2289.