Cournot Games with Capacity: Moral Hazard of Miners

Paper #6614 [*]

Abstract

We analyze a variant of Cournot game, where self-interested agents compete on the quantity of product they produce. It is known that the equilibrium price is inversely proportional to the total quantities. Such games model the prevalent mining games of Proof-of-Work blockchain systems: how much computational power a self-interested miner should invest given a budget capacity? We show that there is a unique pure Nash-equilibrium in the mining game and derive its closed-form, which suggests the most powerful miners do not invest all of its capacity budget, while others exhaust their capacity. We propose the Stackelberg mining game and derive the closed-form of Stackelberg equilibrium, which suggests that miners pool their computational power together is not always their best choice. Perhaps surprisingly, practical distributions of mining pools of computational power in BTC, ETH and other famous crypto-coin systems match our theoretical result well.

1 Introduction

Blockchain is a decentralized ledger recording ownerships and transactions of cryptocoins, wherein one of the most common consensus algorithms is called the Proof-of-Work (PoW) system, proposed in Bitcoin by Nakamoto and others [2008]. In a PoW system, the reward for finding a new block belongs to the user that first solves a cryptography puzzle. Therefore, there is a computation competition among users who utilize their computational powers for the new-block reward. This process is called mining and users are known as miners. Generally, due to the property of a hash function, the most efficient way for finding solutions is by brute force searching. As a result, it is believed that the probability of a miner wining the mining game equals to the ratio of his computational power, known as the hash rate, to the total hash rates of all miners.

In practice, the hash rate of a miner depends on his budget for mining, ranging from the biggest mining pool, usually contains more than 15% of total hash rate, to an individual miner with a laptop. Meanwhile, it is shown that the cost for electricity and device maintenance is also a key factor in mining process, which is consider to be proportional to the mining power that the miner utilizes. A nature question about miners' strategy is that, is it optimal for miners to invest all their capacities, i.e. utilize all hash rates? In this paper, we give a game theoretical model to show that it is not always optimal for miners to invest all their budgets. Here is a simple example:

Suppose miner A and B's hash rates are 1 and 100 respectively. In standard model, both miners utilize all their hash rates and buyer B's wining probability to the new-block reward is $100/101$. Now suppose miner B only utilizes a half of his hash rate, then his win probability becomes $50/51$, still almost 100% winning the reward, while the cost caused by hash rate significantly decreases. As a result, miner two's utility, the expected profit minus the cost, increases. In the following section we prove that miner B does not do his best in the optimal strategy.

1.1 Motivation and our contribution

Our model is both theoretical and practical significant. First, it is equivalent to a typical generation of the famous economic model known as Cournot competition which is not previously studied. Cournot competition is introduced by Cournot [1897], which capture the process where self-interested firms compete on the quantity of outputs they produce. The unit price of a product is determined by the total quantity and a decreasing function. In a basic model, each firm's marginal cost for producing a product is constant. As shown in [Chiu *et al.*, 2018], if the price function is a inverse proportion function, the Cournot competition is equivalent to the mining game.

However both Chiu *et al.* [2018] and traditional Cournot competition do not take the practical fact that each firm/miner has a capacity of his hash rate/product into consideration. In this paper, we assume that each miner has a capacity, regarded as the total hash rate he has, though the miner does not necessary to utilize all of them. We give a closed-form of Nash-equilibrium of mining game with capacities, as a typical generation of Cournot competition, which provides guidelines for practical miners' strategies and helps to predict miners' behaviors.

[*] Please find the supplementary material including all missing proofs at https://github.com/BW5V0/p/blob/master/main.pdf.

Second, our results commendably explain the distribution of computational powers in practical digital currency systems. As the expanding of miners group, the distribution of their computational powers attracts more attentions. Meanwhile, understanding the profound causes of the distribution is important to analyze digital currency markets. According to the records[1], the distribution has the following characteristic: the hash rates of top 1-t miners are roughly the same (difference within 20%), while the top t+1 miner is obviously smaller than them. However, there is still lack of an intuitively explanation. Chiu *et al.* [2018] suppose that each miner has infinite capacity, which results in a symmetric Nash-equilibrium and is far from practice. In this paper, we give a game theoretical explanation from to aspect: Nash-equilibrium and Stackelberg Equilibrium with the introduction of capacities. Simulation results show that our analysis match current distribution of computational powers well.

1.2 Related Work

Cournot competition is introduced by Cournot [1897] and has a significant effect on industry and economics. Two important components of Cournot competition are the price function and cost function. A series of literature analyze the properties of Cournot competition based on variant assumptions of the two functions. [Novshek, 1985; Gaudet and Salant, 1991; Droste *et al.*, 2002] analyze the existence, uniqueness and stability of the equilibrium of Cournot competition respectively. A survey by Daughety [2008] introduces detailed reference about Cournot competition.

Most related to our work, Puu and Marin [Puu and Norin, 2003; Puu and Marín, 2006] analyze a special kind of Cournot competition for the two agents and three agents cases respectively, where the price function is the same as our model as well as the product capacity, except that their cost function is a log function. Puu and Marin give the closed-form of the equilibrium and prove the stability. Kreps and Scheinkman; Moreno and Ubeda; Herk [1983; 2006; 1993] study a kind of Bertrand competition where agents can commit his capacity in the first stage. They prove that the Bertrand competition with capacity results in an Cournot outcome. Boccard and Wauthy [2000] extend the results by allowing firms to produce beyond capacities with an additional cost. Osborne and Pitchik [1986] analyze a price competition in a duopoly with capacity constrains and characterize the set of Nash-equilibrium. To the best our knowledge, we are the first to give the closed-form of Nash-equilibrium of cournot game with capacity, for any number of agents, which can fully model the mining process in blockchain.

It is also notable that if the marginal costs are the types of agents, the model is equivalent to an all-pay auction with proportional allocation, which is introduced in [Nisan *et al.*, 2007] (Chapter 21) and Tang *et al.* [2017]. It is proved that unique Nash-equilibrium also exists in this model. In comparison, we take the capacities as agents' types and assume constant marginal cost.

2 Cournot Game for Cryptocoin Mining

In this section, we first introduce the Cournot game for cryptocoin mining, with more than 2 miners and finite computational power (Section 2.1) . Then we derive the pure Nash equilibrium and show it exists uniquely (Section 2.2).

For clarity, we omit "Cournot" and "cryptocoin" by default in the rest of this paper: the Cournot for cryptocoin mining is called *mining game*.

2.1 Cournot Mining Game

The mining game is a Cournot competition on quantity with complete information.

Players

In this game, n *miners*, numbered from 1 to n, compete with each other for an amount of block reward. Note that generally, a miner refers to either a solo mining individual or a mining pool, and $n \geq 2$.

Each miner i owns an amount of mining power (computational power) *capacity*, denoted by c_i with $c_i \in \mathbb{R}_+$. In this model, without losing generality, miners' indices are sorted in a non-increasing order according to their capacities, i.e. $c_1 \geq c_2 \geq \dots c_n > 0$. We assume the capacities are open to every miner, due to the complete information setting.

Actions

Simultaneously, each miner puts a portion of capacity into use as *hash rate*. Let the hash rate paid by miner i be b_i, with $b_i \in [0, c_i]$, and let b_{-i} be all miners' hash rates other than i's, i.e. $b_{-i} = \sum_{j \in [n] \wedge j \neq i} b_j$.

Utilities

The utility of a miner consists of two parts: 1) the expected *block reward* it earns and 2) the *mining cost* it spends.

As most cryptocoin systems specify, the total amount of block reward that miners compete for is fixed. For convenience of discussion and without losing generality, assign the total block reward with value 1. And as widely adopted, the expected reward of miner i is proportional to its hash rate compared with all miners' [Chiu *et al.*, 2018], i.e. $\frac{b_i}{\sum_{i' \in [n]} b_{i'}}$.

Besides, we assume the mining cost for one unit of hash rate is constant, denoted by α. [2] In other words, the cost of miner i is αb_i.

Combining the above, the utility of miner i is as follows:

$$u_i(b_i, b_{-i}) = \frac{b_i}{\sum_{i' \in [n]} b_{i'}} - \alpha b_i \tag{UT}$$

Pure Nash Equilibrium Definition

A hash rate profile $(b_1^*, b_2^*, \dots, b_n^*)$ is a pure Nash equilibrium (PNE) of the game, if

$$\forall i \in [n], b_i' \in [0, c_i], u_i(b_i^*, b_{-i}^*) \geq u_i(b_i', b_{-i}^*). \tag{PNE}$$

[1] For example, 12-16, Nov. 2018. https://www.blockchain.com/en/pools?timespan=4days

[2] Generally, the actual mining time of one block depends on total computational power in the network, which leads to a changing α. However, the difficulty for mining a mew block is adjusted so that the average mining time equals to a constant due to the Proof of Work consensus. Concentrating on the long-run outcome, we take the steady state into consideration and regard the mining time as a constant.

Some Useful Symbols

In order to present the closed form of PNE more concisely, here we define some symbols which are used later.

W_i is the sum of capacities of miner $[i+1, n]$: $W_i = \sum_{j\in[i+1,n]} c_i, \forall i \in [n-1]$, Specially, $W_n = 0$.

For each $i \in [n]$, denote S_i:

$$S_i = \frac{(i-1) - 2\alpha i W_i + \sqrt{(i-1)^2 + 4\alpha i W_i}}{2\alpha i^2} \tag{1}$$

The meaning of S_i is given in Section 2.2 before it is actually used.

Let k be the largest integer such that

$$S_k = max_{i\in[n]} S_i.$$

2.2 Closed Form Pure Nash Equilibrium

The mining game has a unique pure Nash equilibrium, where the biggest t miners utilize just a part of the capacities, while the rest smallest $n-t$ miners do their best ($t \in [n]$). The biggest t miners' hash rate are the same, which is larger than any of the smallest $n-t$ miners'. The example below shows the PNE of a game with 4 miners. The closed form of PNE is presented at the end of this section by Theorem 5.

Example 1. *Consider a game with* 4 *miners and* $\alpha = 1/36$. *The capacities are:* $c_w = 14, c_x = 10, c_y = 6, c_z = 2$. *We could find a PNE with* $t = 2$*: miner* w*'s and* x*'s hash rate are both* 8*, while miner* y *and* z *pay all of their capacities, i.e.* 6 *and* 2*, which is smaller than* 8. *The profile could be verified to be a PNE by analyzing the first and second order condition.*

In this subsection, to figure out the PNE of cryptocoin mining game, we first reveal the best response of a miner (Lemma 2). Then we illustrate the necessary structure of a PNE (Lemma 3). Finally, with an assistive lemma, we give out the closed form of PNE and prove it is unique (Lemma 4 and Theorem 5).

The following lemma shows the best response of a miner. The intuition is that given other miners hash rate b_{-i}, by first and second order condition, miner i could maximize its utility with $b_i = \sqrt{\frac{b_{-i}}{\alpha}} - b_{-i}$. Meanwhile, the hash rate is constrained by $b_i \in [0, c_i]$.

Lemma 2 (Best Response)**.** $\forall i \in [n]$*, given* b_{-i}*, the unique best response is*

$$b_i = max\{min\{c_i, \sqrt{\frac{b_{-i}}{\alpha}} - b_{-i}\}, 0\} \tag{2}$$

Lemma 3 implies the necessary form of a PNE: with integer $t = 0, \ldots, n$, the PNE consists of two roles of miners: 1) the *dominant* miners, who own the top t capacities, and 2) the *weak* miners, who own the bottom $n-t$ capacities. Dominant miners pay the same hash rate, which is less than their capacities. On the contrary, all weak miners pay different hash rate, and they would use up all of their capacities. However, a dominant miner still pays more hash rate than any weak miner.

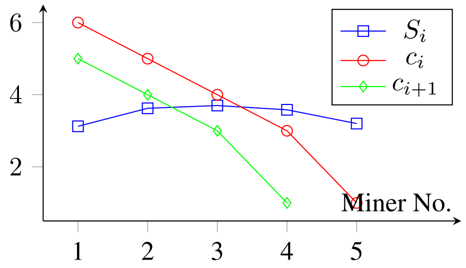


Figure 1: An example of Lemma 4 on the monotonicity of S_i and the relation between S_i and capacity c_i, with $\alpha = 0.05$, and $(c_1, c_2, c_3, c_4, c_5) = (6, 5, 4, 3, 1)$.

Lemma 3 (Necessary Form of PNE)**.** *If* $(b_1, \ldots, b_n)$ *is a PNE. Then there must be some* $t = 0, 1, \ldots, n$*, such that*

$$\begin{aligned} &\forall i \in [t], b_i = \sqrt{\frac{b_{-i}}{\alpha}} - b_{-i} = S_t; \\ &\forall i \in [t+1, n], b_i = c_i \end{aligned} \tag{3}$$

It holds $b_t \geq c_{t+1}$ *if* $t \leq n-1$.

As a helpful tool to find the PNE, the Lemma 4 below shows S_i's monotonicity and its ordering relation with c_i. Fig 1 gives an example when $S_1 \leq c_2$. It could be observed that S_i first increases and then decreases with i. Only when S_i reaches its peak, it holds $c_{i+1} \leq S_i \leq c_i$. Otherwise before that point, $S_i \leq c_{i+1}$ and after that $S_i \geq c_i$. In the case of $S_1 > c_2$, for any miner i, if its capacity is less than c_1, it is also less than the corresponding S_i. Formally, let k be the largest integer such that $S_k = max_{i\in[n]} S_i$, we have the following lemma.

Lemma 4. *When* $S_1 \leq c_2$*, it holds*

$$S_1 \leq \cdots \leq S_{k-1} \leq S_k \geq S_{k+1} \geq \ldots S_n \tag{4}$$

$$\begin{aligned} &\forall i \in [k-1], S_i \leq c_{i+1}; \\ &\forall i \in [k+1, n], S_i \geq c_i; \\ &c_{k+1} \leq S_k \leq c_k \end{aligned} \tag{5}$$

If $S_1 > c_2$*, for each* $i \in [2, n]$*,* $S_i \geq c_i$.

Now we are ready to give the closed form PNE of cryptomining game. As Lemma 3 indicates, the dominant miner with least capacity, i.e. miner t, must satisfy two necessary conditions: 1) $S_t \leq c_t \leq \cdots \leq c_1$ and 2) $S_t \geq c_{t+1}$. According to Lemma 4, when $S_1 \leq c_2$, k is the only miner satisfying both conditions; otherwise if $c_1 \geq S_1 > c_2$, only miner 1 is qualified; or if $S_1 > c_1 \geq c_2$, no miner could fulfill the first condition and thus $t = 0$. Actually, the above choice of t is not only necessary but also sufficient — the PNE of cryptocoin mining game exists and is unique, as the following theorem shows.

Theorem 5 (PNE Closed Form)**.** *Given* n*,* $(c_1, \ldots, c_n)$ *and* α*, the cryptocoin mining game has a unique pure Nash equilibrium* $(b_1^*, b_2^*, \ldots, b_n^*)$ *with* $b_i^* = min\{c_i, S^*\}$*, where*

$$S^* = \begin{cases} S_1, & when \quad S_1 > c_2 \\ S_k, & otherwise \end{cases} \tag{6}$$

3 Insights on the Equilibrium

In this section, we present some interesting insights based on the equilibrium of mining game. First we discover that $\frac{1}{\alpha}$ is the maximum "designed mining capacity" for the cryptocoin system. Then we map our result to the security requirement of blockchain PoW consensus: to avoid the famous "51% attacking" (or "selfish mining"), it only needs more than 2 (or 4) dominant miners in the PNE. (Section 3.1). Then, we study the special case when the number of dominant miner is not k and infer this case is rare in reality (Section 3.3). Finally, we show the impact of capacity distribution on the equilibrium by simulation and find that unequal distribution of capacity leads to waste of computational power budget.(Section 3.4)

3.1 System Capacity and Social Quantity

We compute the bounds of total hash rate (aka social quantity) in the PNE as follows.

Corollary 6 (Social Quantity Bounds). *In PNE* $(b_1^*, \ldots, b_n^*)$*,*

$$\frac{t-1}{t\alpha} \le \sum_{i\in[n]} b_i^* \le \frac{n-1}{n\alpha} < \frac{1}{\alpha},$$

both equalities only hold for $t = n$*, where* t *is the number of dominant miners.*

As the first observation, we suppose $\frac{1}{\alpha}$ is actually the "designed mining capacity" of a blockchain system. Since in the PNE, with the number of miners $n \to \infty$, the upper bound of total hash rate will approach to $\frac{1}{\alpha}$ but would never exceed $\frac{1}{\alpha}$. Intuitively, $\frac{1}{\alpha}$ is how much hash rate one can buy with the block reward 1. Therefore the cryptocoin system does not allow more than $\frac{1}{\alpha}$ hash rate, otherwise mining is not profitable anymore. Besides, the lower bound of total hash rate gets higher with more dominant miners in the PNE.

3.2 System Security and Social Welfare

The Proof-of-Work consensus, for example Bitcoin protocol, assumes the maximum hash rate of a miner must be less than 50% to prevent "double spending" [Nakamoto and others, 2008], whereas [Eyal and Sirer, 2018] points out the safety threshold of Bitcoin is actually 25% to defense against "selfish mining". In our model, we also study the maximum hash rate ratio of miners, i.e. $max_{i\in[n]}\{\frac{b_i}{\sum_{j\in[n]} b_j}\}$, which is defined as the *unsafeness*. A smaller unsafeness means more decentralization and reliability of the cryptocoin system. The upper bound of it is as Corollary 7 shows.

Corollary 7 (Social Welfare and Unsafeness Upper Bound). *In PNE* $(b_1^*, \ldots, b_n^*)$*,*

$$\sum_{j\in[n]} u_j^* = max_{i\in[n]}\{\frac{b_i^*}{\sum_{j\in[n]} b_j^*}\} = 1 - \alpha \sum_{i\in[n]} b_i^* \le \frac{1}{t}$$

the equality only holds for $t = n$*, where* t *is the number of dominant miners.*

Inspiringly, according to Corollary 7, the 50% threshold is easily guaranteed with 2 or more dominant miners in the PNE. However the 25% threshold needs either more than 4 dominant miners or the total hash rate is more than $\frac{3}{4\alpha}$.

We also compute the total utility (aka social welfare) in Corollary 7. It equals to the maximum hash rate ratio. This could be interpreted as a trade-off between security and social welfare: to make the system more reliable (less unsafeness), the miners should endure less social welfare.

3.3 The Rare Case with $t \neq k$

We notice in Theorem 5, as (6) shows, sometimes the number of dominant miner is not k. In this case, $k \ge 2$, but there is less than 1 dominant miner, i.e. $S_2 \ge S_1 \ge c_2$. Solving this, Corollary 8 shows the detail of condition on c_2 and W_2 of this case: the capacity of miner 2 should be less than $1/4$ of $\frac{1}{\alpha}$, i.e. system capacity and the total capacities from miner 3 to n is upper bounded by c_2.

Corollary 8. *Precisely, if and only if*

$$c_2 \le \frac{1}{4\alpha} \text{ and } W_2 \le \frac{7 - 4\alpha c_2 - 3\sqrt{5 - 4\alpha c_2}}{2\alpha} (\le \frac{1}{4\alpha}),$$

it holds $S_2 \ge S_1 \ge c_2$*.*

Notably, in this case, the total hash rate except miner 1 is less than $1/4$ of the system capacity $\frac{1}{\alpha}$, which is too small. Therefore we remark it is very unlikely in the real world — commonly, the number of dominant miners is k.

3.4 Capacity Distribution vs. Budget Waste

In this subsection, we simulate with different distributions of capacity and evaluate the consequential PNE.

We pick inequality as the feature of capacity distribution. Specifically, the inequality is measured by Gini coefficient []:

$$G = 1 - \frac{1}{n} - \frac{2}{W_0} \sum_{i\in[n]} W_i \tag{7}$$

With smaller Gini coefficient, the capacity is more equally distributed, i.e. every miner has more similar computational power capacity.

To quantify a PNE, we compute how much capacity is being used as hash rate, i.e. utilization of budget:

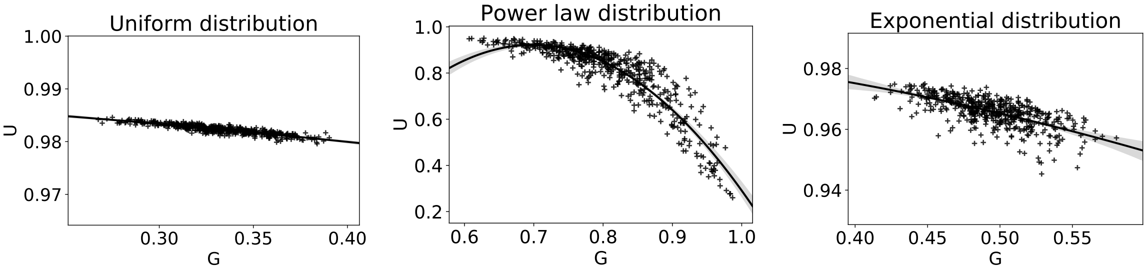
$$U = \frac{\sum_{i\in[n]} b_i^*}{\sum_{i\in[n]} W_i} \tag{8}$$

In the simulation, we set $n = 100$, $\alpha = 0.01$ and fix the total capacity as 100. We try 3 kinds of distribution and for each kind generate $1,000$ games randomly. For each game, we collect the Gini coefficient of capacity distribution and the utiliztion of budget in PNE.

As the simulation result shown in Fig 2, data with all three kinds of distribution indicate the same trend: if the capacity is distributed more unequally, there is less mining power capacity utilized, i.e. miners are not doing their best with more leftover budget wasted.

4 Stackelberg Game and Pooled Mining

In this section, we propose a natural extension of Cournot setting — the *Stackelberg mining game*.First, we define the Stackelberg model and reveal its significance (Section 4.1 and Section 4.2). After that, we give out the closed form Stackelberg equilibrium (Section 4.3). Finally, we discuss its application in the popular pooled mining (Section 4.4).



(a) Uniform distribution (b) Power-law distribution(power $\alpha = 1$) (c) Exponential Distribution ($\lambda = 1$)

Figure 2: Capacity Inequality vs. Budget Utilization ($n = 100$, $\alpha = 0.1$, $\sum_{i\in[n]} c_i = 10$)

4.1 Stackelberg Mining Game

Based on the Cournot model, the Stackelberg mining game introduces an additional miner as the ”leader” and requires miners to act sequentially.

In detail, there are n followers (miner 1 to n) and 1 leader (miner x) in the game. It consists of two phases. During the 1st phase, leader x pays some of its computational power as hash rate $b_x \in [0, c_x]$. The leader's action is called *commitment*, which is public and irreversible. Then in the 2nd phase, each follower i observes the commitment and pays b_i. The utility function in Stackelberg mining game is same as in the Cournot setting:

$$u_i = \frac{b_i}{\sum_{j\in[n]} b_j + b_x} - \alpha b_i, \forall i \in [n] \cup \{x\}$$

We described the Stackelberg equilibrium backwardly as follows. First consider the second phase. Given the commitment, the second phase is actually a subgame among followers with Cournot setting. The followers reach a pure (Cournot) Nash equilibrium in the subgame. Then consider the first phase. Since with any commitment, the leader can anticipates subgame equilibrium, it chooses the best commitment to maximize its utility.

Note that without losing much generality, we assume $\sum_{i\in[2,n]} c_i \geq \frac{1}{4\alpha}$ in the Stackelberg mining game, which rules out the rare case in Section 3.3.

4.2 Significance of Stackelberg Game

Consider a “deviated” miner who refuses to follow the Cournot equilirbium, the Stackelberg game can instruct its action by taking it as the leader. It could be realized in two ways. On one hand, in reality, a sophisticated miner can use its advantage in all kinds of resources to be the leader and force other miners to follow its decision. In this case, the realistic mining game eventually falls into the Stackelberg equilibrium. On the other hand, if a miner is allowed to split into small miners, it could act like a leader by “splitting”. According to the following Lemma 9, the following strategy always works. First the miner thinks of a commitment. And then it split the capacity into multiple parts and announce each part to be a new miner. In the game with new capacity profile, each miner plays follows Nash equilibrium. Finally in the PNE, the sum of split miners' hash rate is exactly the commitment it thinks at first. By this mean, the miner can always pick the best way of splitting and reach the Cournot PNE which is actually “equivalent” with the Stackelberg equilibrium.

Lemma 9. *For any Stackelberg mining game with n followers, there is always a Cournot game with $n + m$ miners such that ($m = 1, 2, \dots$)*

- *The followers in Stackelberg game are also in the Cournot game, and their hash rates in the Stackelberg equilibrium are the same as Cournot PNE;*
- *Besides the followers, there are m more miners in the Cournot game and the total capacity of them is c_x; in the PNE their total hash rate equals to the best commitment in Stackelberg equilibrium.*

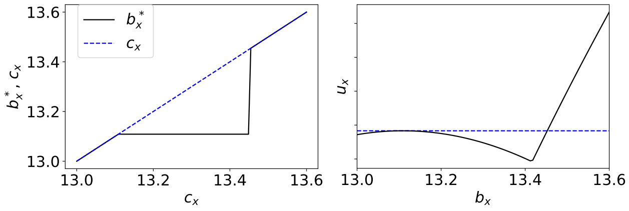
4.3 Closed Form Stackelberg Equilibrium

The Stackelberg mining game has a unique equilibrium, the key part of which is the best commitment. Given the capacity distribution of followers, the best commitment is determined by leader's capacity in an uncontinuous manner: The leader does not need to do its best if the capacity is large, but counterintuitively, when the capacity is larger, it might have to start using up all capacity again. The Example 10 shows a Stackelberg game with 5 followers. After the example, we give the closed form of Stackelberg game by Theorem 11.

Example 10. *Consider a Stackelberg mining game with 5 followers and $\alpha = 1/36$. Followers' capacities are $10, 8, 6, 4, 2$.*

Fig 3a shows the best commitment b^*_x when the leader's capacity c_x is between 13 and 13.6. The special part is when $c_x \in [13.11, 13.45]$: before $c_x = 13.11$, the leader should use all of its capacity up to gain most utility. However, when the leader owns more than 13.11 capacity, it should not continue to pay more unless its capacity is more than 13.45. That is because the leader knowns its utility with any commitment, anticipating the followers' best reaction, and as shown in Fig 3b, the leaders' utility decreases with c_x from 13.11 and starts increasing again later. In other words, $c_x = 13.11$ is a local optima for leader utility function. What is interesting, when $c_x > 13.45$, the utility beats the local optima and the miner need to pay its capacity again — the best commitment suddenly increases to c_x.

The following Theorem 11 shows the closed form of Stackelberg equilibrium. It is the extension of Theorem 5. Before



(a) b_x^* vs. c_x (b) u_x vs. c_x

Figure 3: An Example of Stackelberg Game

the explanation, we denote $\Gamma(b_x)$, Θ_i and Φ_i, all of which could be computed with $i, \{c_i\}$ and α, the detailed expression of which is leaved at supplementary material. The intuition is that suppose a commitment is made, we can construct an Cournot game equivalent with the second-phase subgame among followers. If there are i dominant miners in the constructed game PNE, the total hash rate of all miners is a function of commitment b_x, the closed form is $\Gamma(b_x)$. With that, the leader's utility is a concave function of commitment, and the first-order condition yields $b_x = \Phi_i$. Additionally, the commitment is restricted between Θ_i and Θ_{i+1}. Then the best commitment could be found by comparing Φ_i, Θ_i and Θ_{i+1}, the result of which is denoted by Ω_i. Finally, the leader picks the most proper number of dominant miners by maximizing its utility i.e. $\frac{\Omega_i}{\Gamma(\Omega_i)} - \alpha\Omega_i$.

Theorem 11 (Commitment in Stackelberg Equilibrium)**.** *Any Stackelberg mining game has a unique equilibrium:*

$$b_x^* = argmax_{\Omega_i \in [0,c_x]}\{\frac{\Omega_i}{\Gamma(b_x)} - \alpha\Omega_i\},$$

where

$$\Omega_i = \begin{cases} \Phi_i, & when\ \Phi_i \in [\Theta_i, \Theta_{i+1}] \\ max\{0, \Theta_i\}, & when\ \Phi_i < \Theta_i \\ min\{c_x, \Theta_{i+1}\}, & otherwise \end{cases} \tag{9}$$

With the above closed form, we could explain the counter-intuition revealed by Example 10. It is from the discontinuity of the best commitment function with capacity. When the leaders' commitment increases beyond Θ_i, the number of dominant miners in the subgame equilibrium increases from $i-1$ to i, discretely. Then the best commitment to maximize utility changes from Ω_i to Ω_{i+1}, which is also discrete.

4.4 Pooled Mining

Cooperation among miners, i.e. pooled mining, is not always good. We show it by the following example. Consider in a Cournot PNE, there are some weak miners who want to cooperate. Combine those miners into one with the capacities also summed. Take the combined miner as the leader while the others as followers, we can always construct a Stackelberg mining game. In the Stackelberg equilibrium, if the leader's best commitment is not to exhaust the capacity, then those miners could improve their utility by forming a pool and then reducing their total hash rate collectively by "splitting" as discussed in Section 4.2. Otherwise, if the Stackelberg equilibrium suggests the leader do its best, then those miners are free to stay solo in the original Cournot PNE, where they already do their best.

Remarkably, the model of [Lewenberg *et al.*, 2015] assumes pooling is always better than solo mining. That comes from the lower variance of mining income in a pool than solo mining, and has no relationship with the game model. What's more, their model does not consider the gap between computational power capacity and the realistic hash rate. On the contrary, our model based on another realistic assumption that miners can pay less than their capacities.

5 Comparing with Realistic Data

After checking the mining power distributions of realistic cryptocoins, we find the data surprisingly match the structure of equilibrium in our model and conjecture that in reality, the miners are nearly playing the equilibrium.

According to Theorem 5, the phenomenon of a pure (Cournot) Nash equilibrium should be: the hash rates of top t miners are roughly the same, where t is the number of dominant miners. With the realistic data, we try to find the "gap" between top t miner and top $t+1$ miner. If such "gap" is found with reasonable t, the data is considered to match the PNE structure. As a heuristic measurement, we estimate the "gap" by finding the smallest i such that $(R_i - R_{i+1})/R_{i+1} > 0.2$, where R_i is the realistic hash rate of top i miner. Also, based on system security discussion in Section 3.2, we consider $t \geq 2$ as reasonable number of dominant miners.

We collect the top 6 miners' hash rates for 8 most famous cryptocoins during November, 2018. As Table 1 shows, for most cryptocoins, we find the gap and observe that the top miners are paying similar hash rates, which matches our prediction. The estimated numbers of dominant miners for BTC, ETH, LTC, XMR DASH and ZEC are between 2 and 6, while there are also two exceptions: in BCH and ETC, we estimate there is only one dominant miner. The reason could be that 1) BCH faces severe centralization problem [VK, 2018] and 2) ETC lost much support from the mining community due to a famous hacking accident[Popper, 2016]. However, in the exceptional case with BCH, the hash rates from top miner 3 to top miner 5 are similar, this could be explained by the Stackelberg model: each of these miners takes itself as the leader and their best commitments are the same, although they may have different capacities.

	Top 1 Miner	Top 2 Miner	Top 3 Miner	Top 4 Miner	Top 5 Miner	Top 6 Miner
BTC	**14.6%**	**13.7%**	**12.4%**	**11.3%**	**10.5%**	**9.8%**
ETH	**26.9%**	**22.1%**	13.2%	11.5%	8.0%	2.0%
BCH	**40.9%**	15.3%	11.1%	10.8%	9.1%	4.9%
LTC	**19.8%**	**16.2%**	**14.8%**	**14.0%**	**14.0%**	**14.0%**
XMR	**22.0%**	**19.0%**	**19.0%**	**19.0%**	5.0%	5.0%
DASH	**20.0%**	**16.0%**	**14.0%**	**12.0%**	8.0%	5.0%
ETC	**38.2%**	20.8%	11.9%	5.9%	3.7%	2.8%
ZEC	**20.4%**	**18.7%**	**17.0%**	**15.5%**	8.80%	4.10%

Table 1: Top Miners' Hash Power Distribution of Famous Cryptocoins (estimated dominant miners labeled with bold font)

References

[Boccard and Wauthy, 2000] Nicolas Boccard and Xavier Wauthy. Bertrand competition and cournot outcomes: further results. *Economics Letters*, 68(3):279–285, 2000.

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

[Cournot, 1897] Antoine Augustin Cournot. *Researches into the Mathematical Principles of the Theory of Wealth*. Macmillan, 1897.

[Daughety, 2008] Andrew F Daughety. Cournot competition. 2008.

[Droste *et al.*, 2002] Edward Droste, Cars Hommes, and Jan Tuinstra. Endogenous fluctuations under evolutionary pressure in cournot competition. *Games and Economic Behavior*, 40(2):232–269, 2002.

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

[Gaudet and Salant, 1991] Gerard Gaudet and Stephen W Salant. Uniqueness of cournot equilibrium: new results from old methods. *The Review of Economic Studies*, 58(2):399–404, 1991.

[Herk, 1993] Leonard F Herk. Consumer choice and cournot behavior in capacity-constrained duopoly competition. *The RAND Journal of Economics*, pages 399–417, 1993.

[Kreps and Scheinkman, 1983] David M Kreps and Jose A Scheinkman. Quantity precommitment and bertrand competition yield cournot outcomes. *The Bell Journal of Economics*, pages 326–337, 1983.

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

[Moreno and Ubeda, 2006] Diego Moreno and Luis Ubeda. Capacity precommitment and price competition yield the cournot outcome. *Games and Economic Behavior*, 56(2):323–332, 2006.

[Nakamoto and others, 2008] Satoshi Nakamoto et al. Bitcoin: A peer-to-peer electronic cash system. 2008.

[Nisan *et al.*, 2007] Noam Nisan, Tim Roughgarden, Eva Tardos, and Vijay V Vazirani. *Algorithmic game theory*. Cambridge University Press, 2007.

[Novshek, 1985] William Novshek. On the existence of cournot equilibrium. *The Review of Economic Studies*, 52(1):85–98, 1985.

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

[Popper, 2016] Nathaniel Popper. A hacking of more than 50 million dashes hopes in the world of virtual currency, 2016.

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

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

[Tang *et al.*, 2017] Pingzhong Tang, Yulong Zeng, and Song Zuo. Fans economy and all-pay auctions with proportional allocations. In *AAAI*, pages 713–719, 2017.

[VK, 2018] Anirudh VK. Bitcoin cash [bch] chain is 70wright as bitmain prepares to deploy 90,000 new miners, 2018.

A Stackelberg Mining Game

A.1 Some Symbols in Stackelberg Game

We give out the closed form of some symbols used in Section 4.3 as follows.

In the Stackelberg game, W_i is the sum of capacities from follower 1 to n, same as the Cournot setting:

$$W_i = \sum_{j \in [i+1,n]} c_j.$$

Specially, $W_0 = \sum_{i \in [n]} c_i$ and $W_n = 0$.

Definition 12 ($S_i^{(b_x)}$). *For each $i \in [n]$,*

$$S_i^{(b_x)} = \frac{(i-1) - 2\alpha i(W_i + b_x) + \sqrt{(i-1)^2 + 4\alpha i(W_i + b_x)}}{2\alpha i^2} \tag{10}$$

Definition 13 ($k^{(b_x)}$). *Let $k^{(b_x)}$ be the largest integer such that*

$$S_{k^{(b_x)}}^{(b_x)} = max_{i \in [n]} S_i^{(b_x)}$$

Denote $\Gamma(b_x)$ as follows

$$\Gamma(b_x) = k^{(b_x)} S_{k^{(b_x)}}^{(b_x)} + W_{k^{(b_x)}} + b_x.$$

Definition 14 (Θ_i). *For each $i \in [n]$,*

$$\Theta_i = \frac{1 + \sqrt{1 - 4\alpha c_i}}{2\alpha} - (ic_i + W_i) \tag{11}$$

Specially, $\Theta_{n+1} = \frac{1}{\alpha}$ and $\Theta_0 = min\{\frac{W_1 - \alpha W_0}{\alpha - 1}, 0\}$.

Definition 15 (Φ_i). *For each $i \in [n]$,*

$$\Phi_i = \frac{\Psi_i^{2/3} + \alpha(2i-1)\Psi_i^{1/3} + \alpha^2(2i-1)^2 - 12\alpha^2 i W_i(\Psi_i^{1/3} + 2\alpha i(i-2))}{12\alpha^2 i \Psi_i^{1/3}} \tag{12}$$

where

$$\Psi_i = \alpha^3(2i-1)^3 + 36\alpha^4 i^2(4i^2 - 7i + 4)W_i + 216\alpha^5 i^4 W_i^2 + 12\sqrt{3}\sqrt{a^7 i^2 W_i(2\alpha i^2 W_i + i - 1)^2 \times ((2i-1)^3 + 27\alpha i^2 W_i)} \tag{13}$$

Specially, $\Phi_0 = \frac{-\alpha W_0 + \alpha\sqrt{\alpha W_0}}{\alpha}$.

A.2 Stackelberg Mining Game (Formal Definition)

As a natural extension of Cournot setting, the Stackelberg mining game is also a quantity competition with complete information, but it introduces an additional miner as the "leader" and requires miners to act sequentially.

Players

In the Stackelberg mining game, there are totally $n+1$ miners. Miner x is the leader, along with miner 1 to miner n as the followers. The capacity of the leader is $c_x > 0$, and followers' capacities are $c_1 \geq \cdots \geq c_n > 0$, which is of the same assumption as Cournot setting.

Actions and Utilities

There are two phases in the game. During the first phase, leader x pays some of its computational power as hash rate $b_x \in [0, c_x]$. This decision is called *commitment*, which is irreversible and public. Then in the second phase, after observing the leader's commitment b_x, each follower i pays hash rate $b_i \in [0, c_i]$. Let b_{-i} be the sum of followers' hash rate other than i.

The Stackelberg mining game shares utility function with Cournot setting: the leader's utility is

$$u_x(b_x, \sum_{i \in [n]} b_i^{(b_x)}) = \frac{b_x}{b_x + \sum_{i \in [n]} b_i^{(b_x)}} - \alpha b_x \tag{14}$$

while the utility of follower i is

$$u_i(b_i, b_{-i}, b_x) = \frac{b_i}{b_i + b_{-i} + b_x} - \alpha b_i. \tag{15}$$

Stackelberg equilibrium

Formally, in the second-phase subgame of followers, given commitment b_x, the profile $(b_1^{(b_x)*}, \ldots, b_n^{(b_x)*})$ is an equilibrium, if for each miner i,

$$\forall b_i' \in [0, c_i], u_i(b_i', b_{-i}^{(b_x)*}, b_x) \leq u_i(b_i^{(b_x)*}, b_{-i}^{(b_x)*}, b_x) \tag{16}$$

Let $\Gamma^{(b_x)*} = \sum_{i \in [n]} b_i^{(b_x)*}$ be the sum of followers' hash rates in the subgame with b_x.

In the Stackelberg mining game, profile $(b_x^*, b_1^*, \ldots, b_n^*)$ is a Stackelberg equilibrium, if for the leader x,

$$\forall b_x' \in [0, c_x], u_x(b_x', \Gamma^{(b_x')*}) \leq u_x(b_x^*, \Gamma^{(b_x^*)*}) \tag{17}$$

and for each follower $i \in [n]$, $b_i^* = b_i^{(b_x^*)^*}$.

B Missing Proofs of All Lemmas and Theorems

Proof of Lemma 2. Given b_{-i}, the utility of i is $u_i = \frac{b_i}{b_i+b_{-i}} - \alpha b_i$. And i tries to maximize it by choosing b_i.

By the first and second order condition, b_i should satisfy

$$\frac{du_i}{db_i} = \frac{b_{-i}}{(b_i+b_{-i})^2} - \alpha = 0 \tag{18}$$

$$\frac{d^2u_i}{db_i^2} = -\frac{2b_{-i}}{(b_{-i}+b_i)^3} \leq 0 \tag{19}$$

Solving (18) and (19) with restriction $b_i \in [0, c_i]$, we get $b_i = \sqrt{\frac{b_{-i}}{\alpha}} - b_{-i}$ when $c_i \geq \sqrt{\frac{b_{-i}}{\alpha}} - b_{-i}$. If $c_i < \sqrt{\frac{b_{-i}}{\alpha}} - b_{-i}$ (18) could not be fulfilled, however it holds

$$\frac{du_i}{db_i} = \frac{b_{-i}}{(b_i+b_{-i})^2} - \alpha \geq \frac{b_{-i}}{(c_i+b_{-i})^2} - \alpha > 0.$$

So the utility u_i is largest when $b_i = c_i$. To conclude, the best response is as follows:

$$b_i = max\{min\{c_i, \sqrt{\frac{b_{-i}}{\alpha}} - b_{-i}\}, 0\} \tag{20}$$

□

Proof of Lemma 3. According to Lemma 2, for each $i \in [n]$, b_i could be c_i, $\sqrt{\frac{b_{-i}}{\alpha}} - b_{-i}$, or 0.

First we prove $b_i \neq 0$ by contradiction. Assume $b_i = 0$, it holds $\sqrt{\frac{b_{-i}}{\alpha}} - b_{-i} \leq b_i = 0$. Thus $b_{-i} \geq \frac{1}{\alpha}$, i.e. $\sum_{x\in[n]} b_x = b_i + b_{-i} \geq \frac{1}{\alpha}$. For any $j \in [n]$, its utility is $u_j(b_j, b_{-j}) = \frac{b_j}{\sum_{x\in[n]} b_x} - \alpha b_j \leq \frac{b_j}{1/\alpha} - \alpha b_j = 0$. Thus the utility of j is 0, i.e. $u_j(b_j, b_{-j}) = b_j(\frac{1}{\sum_{x\in[n]} b_x} - \alpha) = 0$. If $b_j > 0$, it holds $\sum_{x\in[n]} b_x = b_j + b_{-j} = \frac{1}{\alpha}$. However, for any $b'_j \in (0, b_j)$, the utility of j will be higher than 0:

$$u_j(b'_j, b_{-j}) = \frac{b'_j}{b'_j + b_{-j}} - \alpha b'_j = \frac{b'_j}{1/\alpha - b_j + b'_j} - \alpha b'_j > 0$$

So b_j could only be 0. That is, the profile is every miner paying 0 hash rate. However, the "all 0" profile is not a PNE.

For two miner i and j with $i < j$, if $b_i = \sqrt{\frac{b_{-i}}{\alpha}} - b_{-i}$ and $b_j = \sqrt{\frac{b_{-j}}{\alpha}} - b_{-j}$, it holds $\sqrt{\frac{b_{-i}}{\alpha}} = b_i + b_{-i} = \sum_{x\in[n]} b_x = b_j + b_{-j} = \sqrt{\frac{b_{-j}}{\alpha}}$. Thus $b_{-i} = b_{-j}$ and $b_i = b_j$.

For two miner i and j with $i < j$, if $b_i = c_i$, b_j could only be c_j, since otherwise we assume $b_j = \sqrt{\frac{b_{-j}}{\alpha}} - b_{-j}$, it holds $\sqrt{\frac{b_{-j}}{\alpha}} = b_j + b_{-j} = \sum_{x\in[n]} b_x = b_i + b_{-i} = c_i + b_{-i} \leq \sqrt{\frac{b_{-i}}{\alpha}} - b_{-i} + b_{-i} = \sqrt{\frac{b_{-i}}{\alpha}}$. Therefore $b_{-j} \leq b_{-i}$ and $b_j \geq b_i = c_i \geq c_j$, indicating b_j is an invalid hash rate.

Therefore, suppose the miner with least capacity who pays $\sqrt{\frac{b_{-i}}{\alpha}} - b_{-i}$ is miner t, then for each $i \in [t], b_i = b_t = \sqrt{\frac{b_{-t}}{\alpha}} - b_{-t}$ and for each $i \in [t+1, n], b_i = c_i$.

Since $b_{-t} = tb_t - b_t + W_t$ and $b_t = \sqrt{\frac{b_{-t}}{\alpha}} - b_{-t}$, reducing b_{-t}, we get

$$tb_t + W_t = \sqrt{\frac{(t-1)b_t + W_t}{\alpha}} \tag{21}$$

If $t \leq n-1$, with $b_{-(t+1)} = tb_t + W_{t+1}$ and $b_{t+1} = c_{t+1} \leq \sqrt{\frac{b_{-(t+1)}}{\alpha}} - b_{-(t+1)}$, reducing $b_{-(t+1)}$, we get

$$\sqrt{\frac{tb_t + W_{t+1}}{\alpha}} \geq tb_t + W_{t+1} + c_{t+1} = tb_t + W_t$$

Therefore we get $\sqrt{\frac{tb_t+W_{t+1}}{\alpha}} \geq \sqrt{\frac{tb_t+W_{t+1}+c_{t+1}-b_t}{\alpha}}$. That is, $b_t \geq c_{t+1}$.

Finally we prove the closed form of b_t is S_t. Solving (21), we get $b_t = \frac{(t-1)-2\alpha tW_t+\sqrt{(t-1)^2+4\alpha tW_t}}{2\alpha t^2}$ or $b_t = \frac{(t-1)-2\alpha tW_t-\sqrt{(t-1)^2+4\alpha tW_t}}{2\alpha t^2}$. The latter is ruled out since it is always negative.

□

From the above proof, we know $S_t = b_t$ satisfies equation (21). As a consequence, let $t = i$, it holds

$$iS_i + W_i = \sqrt{\frac{(i-1)S_i + W_i}{\alpha}} \tag{22}$$

Based on S_i, let Γ_i be the total hash rate of all miners when there are i dominant miners, i.e.

$$\Gamma_i = iS_i + W_i = \frac{(i-1) + \sqrt{(i-1)^2 + 4\alpha iW_i}}{2\alpha i} \tag{23}$$

Γ_i has the following two properties:

Lemma 16. *For $i \in [n]$, $\Gamma_i \geq \frac{i-1}{i\alpha}$, the equality only holds for $W_i = 0$;*

For $i \in [n-1]$, if $S_i \geq c_{i+1}$, $\Gamma_i \leq \frac{n-1}{n\alpha}$, the equality only holds for $c_{i+1} = \cdots = c_n = S_i$.

Proof of Lemma 16. We first prove the lower bound of Γ_i. Because $W_i \geq 0$,

$$\begin{aligned}\Gamma_i &= \frac{(i-1) + \sqrt{(i-1)^2 + 4\alpha iW_i}}{2\alpha i} \\ &\geq \frac{(i-1) + \sqrt{(i-1)^2}}{2\alpha i} = \frac{i-1}{i\alpha}\end{aligned} \tag{24}$$

The equality only holds with $W_i = 0$.

Then we prove the upper bound of Γ_i. Note that

$$S_i = \Gamma_i - \alpha\Gamma_i^2,$$

since equation (22) could be written as

$$\Gamma_i = \sqrt{\frac{\Gamma_i - S_i}{\alpha}}.$$

With $S_i \geq c_{i+1} \geq \cdots \geq c_n$, $W_i = c_{i+1} + \cdots + c_n \leq (n-i)S_i$. So $\Gamma_i = iS_i + W_i \leq nS_i = n(\Gamma_i - \alpha\Gamma_i^2)$. And then $\Gamma_i \leq \frac{n-1}{n\alpha}$. The equality only holds for $W_i = (n-i)S_i$, i.e. $c_{i+1} = \cdots = c_n = S_i$. □

In order to prove Lemma 4, we first reveal the following relation between S_i and c_i.

Lemma 17. *Considering the following 6 statements,*

1) $c_{i+1} \ge S_{i+1}$ *1)'* $c_{i+1} \le S_{i+1}$
2) $c_{i+1} \ge S_i$ *2)'* $c_{i+1} \le S_i$
3) $S_{i+1} \ge S_i$ *3)'* $S_{i+1} \le S_i$

- $\forall i \in [n-1]$, *it holds* 1) $\Leftrightarrow$ 2) $\wedge$ 3)*,* 3)$'$ $\Rightarrow$ 2)$'$*, and* 2)$'$ $\Rightarrow$ 1)$'$
- $\forall i \in [2, n-1]$*, it holds* 3) $\Leftrightarrow$ 1) *and* 1)$'$ $\Leftrightarrow$ 2)$'$ $\Leftrightarrow$ 3)$'$
- *The ”=” case only holds when* $c_{i+1} = S_{i+1} = S_i$

Proof of Lemma 17. According to (22), S_i and S_{i+1} satisfy the following two equations.

$$iS_i + W_{i+1} + c_{i+1} = \sqrt{\frac{iS_i + W_{i+1} + c_{i+1} - S_i}{\alpha}} \tag{25}$$

$$iS_{i+1} + W_{i+1} + S_{i+1} = \sqrt{\frac{iS_{i+1} + W_{i+1}}{\alpha}} \tag{26}$$

By subtracting $(25)^2$ and $(26)^2$, we get

$$\begin{aligned}&\alpha(iS_i + W_{i+1} + c_{i+1} + iS_{i+1} + W_{i+1} + S_{i+1})\\&(i(S_i - S_{i+1}) + c_{i+1} - S_{i+1})\\=&\alpha(\Gamma_i + \Gamma_{i+1})(i(S_i - S_{i+1}) + c_{i+1} - S_{i+1})\\=&i(S_i - S_{i+1}) + c_{i+1} - S_i\end{aligned} \tag{27}$$

First we show the ”=” case: I) If $S_i = S_{i+1}$, (27) becomes $\alpha((2i+1)S_i + 2W_{i+1} + c_{i+1})(c_{i+1} - S_i) = c_{i+1} - S_i$. Because $(i+1)S_i + W_{i+1} > \frac{1}{2\alpha}$, it holds

$$(2i+1)S_i + 2W_{i+1} + c_{i+1} > \frac{1}{\alpha} - S_i + c_{i+1} > \frac{1}{\alpha},$$

otherwise $S_i > c_{i+1}$ and $S_i > S_{i+1}$. Thus it could only be $c_{i+1} = S_i$. II) If $c_{i+1} = S_i$, (27) becomes

$$(\Gamma_i + \Gamma_{i+1})(S_i - S_{i+1}) = \frac{i}{(i+1)\alpha}(S_i - S_{i+1}).$$

By Lemma 16, $\Gamma_i + \Gamma_{i+1} \ge \frac{i-1}{i\alpha} + \frac{i}{(i+1)\alpha} = \frac{2i^2-1}{i(i+1)\alpha} > \frac{i}{(i+1)\alpha}$, it could only be $S_i = S_{i+1}$. III) If $c_{i+1} = S_{i+1}$, (27) becomes

$$(\Gamma_i + \Gamma_{i+1})(S_i - S_{i-1}) = \frac{i-1}{i\alpha}(S_i - S_{i-1}).$$

Since $\Gamma_i + \Gamma_{i+1} \ge \frac{i-1}{i\alpha} + \frac{i}{(i+1)\alpha} = \frac{2i^2-1}{i(i+1)\alpha} > \frac{i-1}{i\alpha}$, it could only be $S_i = S_{i+1}$.

Then, assume $S_{i+1} \ne S_i \ne c_{i+1}$, considering $\Gamma_{i+1} = iS_{i+1} + W_{i+1} + S_{i+1} \ge \frac{1}{2\alpha}$ (by Lemma 16), it holds

$$\begin{aligned}1 \le&2\alpha(iS_{i+1} + W_{i+1} + S_{i+1})\\=&\alpha(iS_{i+1} + W_{i+1} + S_{i+1} + iS_{i+1} + W_{i+1} + S_{i+1})\\=&\alpha(iS_{i+1} + W_{i+1} + S_{i+1} + iS_i + W_{i+1} + c_{i+1})\\&+ \alpha(i(S_{i+1} - S_i) + S_{i+1} - c_{i+1})\\=&\frac{i(S_i - S_{i+1}) + c_{i+1} - S_i}{i(S_i - S_{i+1}) + c_{i+1} - S_{i+1}}\\&+ \alpha(i(S_{i+1} - S_i) + S_{i+1} - c_{i+1})\\=&1 + \frac{S_{i+1} - S_i}{i(S_i - S_{i+1}) + c_{i+1} - S_{i+1}}\\&+ \alpha(i(S_{i+1} - S_i) + S_{i+1} - c_{i+1})\end{aligned} \tag{28}$$

$\Rightarrow$

$$\alpha(i(S_{i+1} - S_i) + S_{i+1} - c_{i+1}) \ge \frac{S_{i+1} - S_i}{i(S_{i+1} - S_i) + S_{i+1} - c_{i+1}} \tag{29}$$

If both $S_{i+1} < S_i$ and $S_{i+1} < c_{i+1}$ hold, it leads to following contradiction:

$$\alpha(i(S_{i+1} - S_i) + S_{i+1} - c_{i+1})^2 \le S_{i+1} - S_i < 0 \tag{30}$$

Therefore if $S_{i+1} < S_i$, then $S_{i+1} > c_{i+1}$ and $S_i > c_{i+1}$. Besides, if $c_{i+1} < S_i$, it could only be $c_{i+1} < S_{i+1}$ otherwise $S_{i+1} < c_{i+1} < S_i$. Also if $c_{i+1} > S_{i+1}$, it holds $S_{i+1} > S_i$ and $S_i < c_{i+1}$. The above three statements show 3)$'$ $\Rightarrow$ 2)$'$, 2)$'$ $\Rightarrow$ 1)$'$ and 1) $\Rightarrow$ 2) $\wedge$ 3), respectively.

Additionally, with condition $i \ge 2$, it holds $\Gamma_i + \Gamma_{i+1} \ge \frac{1}{2\alpha} + \frac{1}{2\alpha} = \frac{1}{\alpha}$. Assume $S_{i+1} > S_i$ and $c_{i+1} < S_{i+1}$, (27) becomes

$$\begin{aligned}&i(S_i - S_{i+1}) + c_{i+1} - S_i\\&= \alpha(\Gamma_i + \Gamma_{i+1})(i(S_i - S_{i+1}) + c_{i+1} - S_{i+1})\\&\le i(S_i - S_{i+1}) + c_{i+1} - S_{i+1}\end{aligned} \tag{31}$$

This leads to contradiction: $S_i \ge S_{i+1}$, proving 3) $\Rightarrow$ 1) and 1)$'$ $\Rightarrow$ 3)$'$. Thus with $i \ge 2$, it holds 3) $\Leftrightarrow$ 1) and 1)$'$ $\Leftrightarrow$ 2)$'$ $\Leftrightarrow$ 3)$'$.

Finally we finish the proof of 2) $\wedge$ 3) $\Rightarrow$ 1). As the above paragraph already proves it with $i \ge 2$, we consider the case $i = 1$. Assume $S_2 > c_2 > S_1$. We could reduce $\frac{1 - 4\alpha W_2 + \sqrt{1 + 8\alpha W_2}}{8\alpha} = S_2 > c_2 > 0$ into $\alpha W_2 < 1$. Besides, $S_1 = \sqrt{\frac{W_2 + c_2}{\alpha}} - W_2 - c_2 < c_2$ could be reduced into $\alpha W_2 > 1$ or $c > \frac{1 - 4\alpha W_2 + \sqrt{1 + 8\alpha W_2}}{8\alpha} = S_2$. However, they contradicts with each other. As a result, $c_2 > S_2$. □

Proof of Lemma 4. If $S_1 \le c_2$, it holds $S_2 \ge S_1$ and $k \ge 2$, otherwise assume $S_2 \le S_1 \le c_2$, by 1) $\Rightarrow$ 2) of Lemma 17 ($i = 1$), $c_2 \ge S_1$, which leads to contradiction.

On one hand, we consider $[k-1]$. When $k \ge 3$, since $S_k \ge S_{k-1}$, by 3) $\Rightarrow$ 1) $\Rightarrow$ 2) of Lemma 17 ($i = k-1$), it holds $S_{k-1} \le c_k \le c_{k-1}$. According to 1) $\Rightarrow$ 2) $\wedge$ 3) of Lemma 17 ($i = k-2$), we get $c_{k-1} \ge S_{k-2}$ and $S_{k-1} \ge S_{k-2}$. Similarly, by applying 1) $\Rightarrow$ 2) $\wedge$ 3) of Lemma 17 inductively ($i = k-3, \dots, 2$), it holds $S_{i+1} \ge S_i$ and $c_{i+1} \ge S_i$ for each $i \in [2, k-3]$. Along with $S_2 \ge S_1$ and $c_2 \ge S_1$, it holds $S_k \ge \cdots \ge S_1$ and $c_{i+1} \ge S_i$ for each $i \in [k-1]$. If $k = 2$, $S_2 \ge S_1$ and $c_2 \ge S_1$ also satisfy the result above.

On the other hand, consider $[k+1, n]$. Since $S_k \ge S_{k+1}$, by 3)$'$ $\Rightarrow$ 2)$'$ $\Rightarrow$ 1)$'$ of Lemma 17 ($i = k$), it holds $S_{k+1} \ge c_{k+1} \ge c_{k+2}$. According to 2)$'$ $\Rightarrow$ 1)$'$ $\wedge$ 3)$'$ of Lemma 17 ($i = k+1$), , it holds $S_{k+2} \le S_{k+1}$ and $S_{k+2} \ge c_{k+2} \ge c_{k+3}$. Similarly, by applying 2)$'$ $\Rightarrow$ 1)$'$ $\wedge$ 3)$'$ of Lemma 17 inductively ($i = k+2, \dots, n$), it holds $S_k \ge S_{k+1} \ge \cdots \ge S_n$ and $c_i \le S_i$ for each $i \in [k+1, n]$.

Now consider S_k, it holds $c_{k+1} \le S_k \le c_k$: First, $S_k \ge S_{k+1} \ge c_{k+1}$. Second, since $S_k \ge S_{k-1}$ and $S_{k-1} \le c_k$, by 3) $\wedge$ 2) $\Rightarrow$ 1) of Lemma 17 ($i = k-1$), $S_k \le c_k$.

Finally, assume $S_1 > c_2$, by 2)$'$ $\Rightarrow$ 1)$'$ of Lemma 17 ($i = 1$), it holds $S_2 \ge c_2 \ge c_3$. Similarly, by applying 2)$'$ $\Rightarrow$ 1)$'$ of Lemma 17 inductively ($i = 2, \dots, n$), it holds $S_i \ge c_i$ for each $i \in [2, n]$. □

Proof of Theorem 5. We first prove the hash rate profile given by Theorem 5 is a PNE and then show the uniqueness.

When $S_1 > c_2$, the profile is $(min\{c_1, S_1\}, c_2, \dots, c_n)$. For miner 1, $b_{-1} = W_1$ and

$$S_1 = \sqrt{\frac{W_1}{\alpha}} - W_1 = \sqrt{\frac{b_{-1}}{\alpha}} - b_{-1} > c_2 > 0.$$

By Lemma 2, the best response is $max\{min\{c_1, \sqrt{\frac{b_{-1}}{\alpha}} - b_{-1}\}, 0\} = min\{c_1, \sqrt{\frac{b_{-1}}{\alpha}} - b_{-1}\} = min\{c_1, S_1\}$. For miner $i \in [2, n]$, $b_{-i} = min\{c_1, S_1\} + W_1 - c_i \geq W_1$ and

$$\sqrt{\frac{b_{-i}}{\alpha}} - b_{-i} \geq \sqrt{\frac{W_1}{\alpha}} - b_{-i} = \sqrt{\frac{W_1}{\alpha}} - W_1 - min\{c_1, S_1\} + c_i$$
$$= S_1 + c_i - min\{c_1, S_1\} \geq c_i > 0.$$

By Lemma 2, the best response is $max\{min\{c_i, \sqrt{\frac{b_{-i}}{\alpha}} - b_{-i}\}, 0\} = c_i$.

Now we consider $S_1 \leq c_2$. In this case the profile is $\forall i \in [k], b_i^* = S_k$ and $\forall i \in [k+1, n], b_i^* = c_i$.

For miner $i \in [k]$, $b_{-i} = (k-1)S_k + W_k$. Then it holds $S_k = \sqrt{\frac{b_{-i}}{\alpha}} - b_{-i}$ (by equation (22)). Also by Lemma 4, $0 < c_{k+1} \leq S_k \leq c_k$. According to Lemma 2, the best response is $max\{min\{c_i, \sqrt{\frac{b_{-i}}{\alpha}} - b_{-i}\}, 0\} = \sqrt{\frac{b_{-i}}{\alpha}} - b_{-i} = S_k$.

For miner $i \in [k+1, n]$, $b_{-i} = kS_k + W_k - c_i$. With $S_k \geq c_{k+1} \geq c_i$ (by Lemma 4), it holds

$$\begin{aligned}\sqrt{\frac{b_{-i}}{\alpha}} - b_{-i} &\geq \sqrt{\frac{b_{-i} + c_i - S_k}{\alpha}} - b_{-i} \\ &= \sqrt{\frac{b_{-k}}{\alpha}} - b_{-i} \\ &= S_k + b_{-k} - b_{-i} = S_k + c_i - S_k = c_i\end{aligned} \tag{32}$$

By Lemma 2, the best response is $max\{min\{c_i, \sqrt{\frac{b_{-i}}{\alpha}} - b_{-i}\}, 0\} = max\{c_i, 0\} = c_i$. So the hash rate profile given by Theorem 5 is a PNE.

Finally, we prove the uniqueness of PNE. As all PNEs must match the necessary structure in Lemma 3, we just need to prove the number of dominant miners, i.e. t, is unique. Assume there is another choice of t other than the one in Theorem 5, it would lead to contradiction: 1) When $S_1 > c_1 \geq c_2$, assume $t \neq 0$. By Lemma 4, $S_i \geq c_i$ for each $i \in [n]$, including t, indicating S_t exceeds the capacity of miner t. 2) When $c_1 \geq S_1 \geq c_2$, assume $t \neq 1$. By Lemma 4, $S_i \geq c_i$ for each $i \in [2, n]$, thus t could not be $[2, n]$. If $t = 0$, each miner pays its capacity. However, $c_1 \geq S_1 = \sqrt{\frac{W_1}{\alpha}} - W_1 = \sqrt{\frac{b_{-1}}{\alpha}} - b_{-1}$, indicating its capacity is not the best response of miner 1. 3) When $S_1 \leq c_2$, assume $t \neq k$. Note that specially, if there are more than one miner i that $S_i = S_k$, according to the "=" case in Lemma 17, letting $t = i$ is equivalent with $t = k$. So by assuming $t \neq k$, we mean $S_t \neq S_k$. By Lemma 4, for any $i \in [k-1]$, $S_i \leq c_{i+1}$, and for any $i \in [k+1, n]$, $S_i \geq c_i$, i.e. all of $1, \dots, k-1, k+1, \dots, n$ do not meet the requirement of t in Lemma 3. If $t = 0$, similar with case 2) above, miner 1 will not be making the best response since $c_1 \geq S_1 = \sqrt{\frac{b_{-1}}{\alpha}} - b_{-1}$. To summarize, the choice of t is unique, i.e. the pure Nash equilibrium is unique. □

Proof of Corollary 8. Given the closed form of S_1 and S_2 as follows:

$$S_2 = \frac{1 - 4\alpha W_2 + \sqrt{1 + 8\alpha W_2}}{8\alpha},$$

$$S_1 = \sqrt{\frac{W_2 + c_2}{\alpha}} - W_2 - c_2,$$

solving $S_2 \geq S_1 \geq c_2$, we get

$$c_2 \leq \frac{1}{4\alpha} \; \&\& \; W_2 \leq \frac{7 - 4\alpha c_2 - 3\sqrt{5 - 4\alpha c_2}}{2\alpha}.$$

□

Proof of Corollary 6. According to Lemma 16, $\sum_{i \in [n]} b_i^* = \Gamma_k \geq \frac{k-1}{k\alpha}$.

If $k \leq n-1$, according to Lemma 16, $\sum_{i \in [n]} b_i^* = \Gamma_k \leq \frac{n-1}{n\alpha}$. If $k = n$, $\sum_{i \in [n]} b_i^* = nS_n = \frac{n-1}{n\alpha}$. □

Proof of Corollary 7. Since $\sum_{i \in [n]} b_i^* \geq \frac{k-1}{k\alpha}$ and $\sum_{i \in [n]} b_i^* \leq nS_k$, it holds

$$nS_k \geq \sum_{i \in [n]} b_i^* \geq \frac{k-1}{k\alpha}.$$

That is, $S_k \geq \frac{k-1}{k\alpha}$. □

Lemma 18. *In a Stackelberg mining game with α, n and $(c_x, c_1, \dots, c_n)$, given commitment $b_x \leq \frac{1}{\alpha}$, a Cournot mining game could always be constructed, such that in the game:*

- *The marginal cost of mining α remains unchanged;*
- *There are $n + m$ miners, also ordered by their capacity, from large to small;*
- *The capacity for each miner $i \in [n]$ is c_i, same as the follower i in the Stackelberg setting;*
- *The capacities for miner $i \in [n+1, n+m]$ satisfy $\sum_{i \in [n+1, n+m]} c_i = b_x$;*
- *Miner $n+1$ is a weak miner in the PNE.*

The second-phase subgame of Stackelberg mining game is equivalent with the constructed Cournot game:

1. *The utility functions are the same, i.e. for each $i \in [n]$, $u_i(b_i, b_{-i}, b_x) = u_i(b_i, b_{-i})$, where the left (right) side is the utility function of subgame (constructed game) ;*
2. *The PNEs are the same, i.e. for each $i \in [n]$, $b_i^{(b_x)*} = b_i^*$, where $b_i^{(b_x)*}$ is the PNE of subgame (See (16)), and b_i^* is the PNE of the constructed Cournot game (See (PNE))*

Corollary 19. *In a Stackelberg mining game with α, n and $(c_x, c_1, \dots, c_n)$, given commitment $b_x \leq \frac{1}{\alpha}$, the second-phase game has a unique equilibrium where*

$$\forall i \in [k^{(b_x)}], b_i^{(b_x)*} = S_{k^{(b_x)}}^{(b_x)}$$

and

$$\forall i \in [k^{(b_x)} + 1, n], b_i^{(b_x)*} = c_i.$$

Correspondingly, $\Gamma^{(b_x)*} = k^{(b_x)} S_{k^{(b_x)}}^{(b_x)} + W_{k^{(b_x)}}$.

Proof of Lemma 18. We first construct a Cournot mining game as an example. Keep α and let $m = \lceil \frac{b_x}{min\{S_n^{(b_x)}, c_n\}} \rceil$ and $c_{n+1} = \cdots = c_{n+m} = \frac{b_x}{m}$. Such m could always be found, since $b_x \in [0, \frac{1}{\alpha}]$ and $S_n^{(b_x)} > 0$. It holds $\sum_{i \in [n+1, n+m]} c_i = b_x$ and $c_n \geq c_{n+1} = \cdots = c_{n+m}$.

Then we show that miner $n+1$ is a weak miner in the PNE. Since $c_i, \forall i \in [n]$ is the same in both games, it holds $S_i = S_i^{(b_x)}$ for each $i \in [n]$. According to Theorem 5, if $S_1 \geq c_2$, there is less than one dominant miner and $n+1$ is naturally a weak miner. When $S_1 < c_2$, the hash rate of dominant miner is $S_k \geq S_n = S_n^{(b_x)} \geq c_{n+1}$. So miner $n+1$ is a weak miner in the PNE.

Finally, since c_i in both games are the same, and W_i in the constructed game is $W_i + b_x$ in the second-phase subgame, it holds for each $i \in [n]$, $u_i(b_i, b_{-i}, b_x) = u_i(b_i, b_{-1}) = \frac{b_i}{b_{-i} + b_i + b_x}$. Since the utility function are the same, and $[n+1, n+m]$ pay their capacities, in the equilibrium of subgame, each miner $i \in [n]$ would make the same decision as in the PNE of the constructed game. That is, $b_i^* = b^{(b_x)*}, \forall i \in [n]$. □

Proof of Corollary 19. According to Lemma 18, an equivalent Cournot game could be constructed. Also due to the assumption that $W_1 \geq \frac{1}{\alpha}$, the PNE of constructed game could be found by finding the maximum S_i. That is, the PNE is

$$\forall i \in [k], b_i^* = S_k; \quad \forall i \in [k+1, n], b_i^* = c_i$$

Due to the equivalence,

$$b_i^{(b_x)*} = b_i^*, \quad S_i^{(b_x)} = S_i, \quad k^{(b_x)} = k$$

□

Lemma 20. *In a Stackelberg equilibrium, the best commitment is equal to the leader's capacity, if the best commitment is smaller than the largest followers' hash rate.*

Proof of Lemma 20. Given a commitment b_x, according to Corollary 19, the largest followers' hash rate is $max\{S_i^{(b_x)}\}$. If $b_x \leq max\{S_i^{(b_x)}\}$, we can always construct a Cournot equivalent with the second-phase game such that the leader does not need to be split and its hash rate in the constructed game is equal to b_x.

Suppose b_x decreases from c_x, by Lemma 2, if other miners stay, u_x decreases. Also by the closed form of $S_i^{(b_x)}$, other miners' hash rate do not decrease. Therefore u_x decreases further. To conclude, b_x needs to be as large as possible until $b_x = c_x$. □

Proof of Lemma 9. Let $S = S_{k^{(b_x^*)}}^{(b_x^*)}$.

If $b_x^* < S$, according to Lemma 20, $c_x = b_x^*$. Construct a Cournot where the leader does not need to be split, and the PNE is equivalent with the second-phase game PNE

When $b_x^* \geq S$, we can construct a Cournot game by splitting the leader as follows. Split the leader's capacity into m parts: one part with $c_x - (m-1)S$ and other $m-1$ parts with S, where $m = \lfloor \frac{c_x}{S} \rfloor$. Then in the constructed Cournot game PNE, one of the split miners is dominant with hash rate S while the others are all weak with dominant c_i. The total hash rate is still b^*, and the dominant miner's hash rate is also S, i.e. equivalent equilibrium with the second-phase PNE. □

Proof of Theorem 11. We find the best commitment of leader by backward induction. Before the detail, note that $b_x^* \leq \frac{1}{\alpha}$, otherwise the leader will get negative utility.

First consider the second-phase subgame of Stackelberg game, given commitment $b_x \in [0, \frac{1}{\alpha}]$, according to Lemma 18, we construct an equivalent Cournot game. In the PNE of constructed game, it holds $S_k \geq S_{k-1}$ and $S_k \geq S_{k+1}$, which is equivalent to $S_k^{b_x} \geq S_{k-1}^{b_x}$ and $S_k^{b_x} \geq S_{k+1}^{b_x}$. Solving the two inequalities we get $b_x \in [\Theta_k, \Theta_{k+1}]$. That is, if there is i dominant miners in the PNE of constructed game, it holds

$$b_x \in [\Theta_i, \Theta_{i+1}] \tag{33}$$

Then consider the first phase. The utility of leader x is

$$\begin{aligned} u_x(b_x, kS_k^{(b_x)} + W_k) &= \frac{b_x}{b_x + kS_k^{(b_x)} + W_k} - \alpha b_x \\ &= b_x\left(\frac{2\alpha k}{k - 1 + \sqrt{\begin{array}{r}4\alpha k(W_k + b_x) \\ + (k-1)^2\end{array}}} - \alpha\right) \end{aligned} \tag{34}$$

The first-order yields

$$\frac{d}{db_x} u_x(b_x, kS_k^{(b_x)} + W_k) = 0$$

Solving it we get $b_x = \Phi_k$. Besides, the function $u_x(b_x) = u_x(b_x, kS_k^{(b_x)} + W_k)$ is concave. So it is maximized at Φ_k. Along with the restriction (33), when there are i dominant miners in the PNE of subgame, the utility of leader u_x gets maximized at $b_x = \Phi_i$ if $\Phi_i \in [\Theta_i, \Theta_{i+1}]$, or $b_x = \Theta_i$ if $\Phi_i < \Theta_i$ or $b_x = \Theta_{i+1}$ otherwise. This point is Ω_i defined by (9).

Once the leader picks i as the number of dominant miners in the subgame PNE, the leader could pay Ω_i to maximize the utility. Out of all valid $\Omega_i \in [0, c_i]$, the leader chooses the best one as the solution, i.e. $b_x^* = argmax_{\Omega_i \in [0, c_x]}\{u_x(\Omega_i, \Gamma^{(\Omega_i)*})\}$.

□