A Hashing Power Allocation Game in Cryptocurrencies

Yukun Cheng[1], Donglei Du[2], and Qiaoming Han[3(✉)]

[1] School of Business, Suzhou University of Science and Technology, Suzhou, People's Republic of China
ykcheng@amss.ac.cn

[2] Faculty of Business Administration, University of New Brunswick, Fredericton, NB, Canada
ddu@unb.ca

[3] School of Data Science, Zhejiang University of Finance and Economics, Hangzhou, People's Republic of China
qmhan@zufe.edu.cn

Abstract. Various crypto-currencies backed by Blockchain technology are now springing up like mushrooms. Miners in these peer-to-peer networks compete to maintain the validity of the underlying ledgers to earn the bootstrapped crypto-currencies. With limited hashing power, each miner needs to decide how to allocate their resource to different crypto-currencies so as to achieve the best overall payoff. Together all the miners form a hashing power allocation game. We consider the setting of the game in which the miners are risk-neutral. We show that a unique pure Nash Equilibrium exists and can be computed efficiently in this settings.

1 Introduction

With the advancement of the blockchain technologies (a.k.a., distributed ledger technology), distributed applications (DApps) are burgeoning. Starting from the bitcoin, many altcoins have been proposed to achieve different goals. At the time of this writing, there are almost 1,600 cryptocurrencies with market capitalization totalling approximate $456 billion[1], and among them Bitcoin [5], Ethereum [9] and Ripple [26] are the top three market-caped crypto-currencies.

Miners in these peer-to-peer networks play the important role of maintaining the integrity of the underlying blockchains, incentivized to earn digital currencies and transaction fees. Mining involves executing a distributed consensus protocol on how to achieve agreement of the underlying ledger when there is no central authority in presence. Among them, proof-of-work (PoW) [20], proof-of-stake (PoS) [30] and proof-of-burn (PoB) [23] are the widely adopted consensus protocols by existing crypto-currencies.

For example, in the PoW framework, during a given average time period (e.g., every 10 min for Bitcoin), miners participate in a winner-take-all competition to

[1] According to https://coinmarketcap.com/.

X. Deng (Ed.): SAGT 2018, LNCS 11059, pp. 226–238, 2018.
https://doi.org/10.1007/978-3-319-99660-8_20

extend the next block on the longest block chain by solving some cryptographic hashing proof-of-work, a mathematical puzzle. As a concrete case, in Bitcoin network, the puzzle goes as follows [33]: given a difficulty $d > 0$, a challenge c and a nonce x (usually bit-strings), a function

$$F_d(c, x) \to \{\text{TRUE,FALSE}\}$$

is called a Proof-of-Work (PoW) function if it has the following two properties: (i) $F_d(c, x)$ is fast to compute, given d, c, and x; and (ii) for fixed parameters d and c, finding x such that $F_d(c; x) = \text{TRUE}$ is computationally difficult but feasible. The difficulty d is used to adjust the time to find such an x.

With miners equipped with certain computing power (a.k.a., hashing power in Bitcoin network) and a large number of different cryptocurrencies to mine, they are facing the challenge on how to allocate their computing power to compete in mining each cryptocurrency to maximize their expected payoffs. Due to the competitive nature of the mining protocol, all miners together form a non-cooperative allocation game. This work aims to answer the following questions associated with the aforementioned game: 1. Does Nash Equilibrium (NE) exist? 2. Is NE unique? 3. Can the NE be computed efficiently? We offer affirmative answers to all three questions for the risk-neutral miners.

For the game with risk-neutral miners, we show that the Nash Equilibrium allocation is unique and follows a proportional rule (Theorems 1 and 2) where each miner will allocate his total computing power to a given crypto-currency proportional to the percentage of the award among all currencies, while his expected revenue is proportional to the percentage of the hashing power possessed and the total award.

The equilibrium analysis of the allocation game is of both theoretical and practical relevance. On the theoretical side, we set up a succinct backbone model which admits a closed-form solution via non-trivial technical analysis. On the practical side, we provide insights which can help mining pool managers (such as BTC.com [7], AntPool [3], Slush Pool [25], ViaBTC [32] and BTC.TOP [8], etc.) or individual miners in making the most important operational/tactical decisions, namely how to allocate the hashing power when facing under reward and peer competition.

To filter out the most salient factors that are of managerial relevance, we made some simplifications in the modelling, such as the the assumption that the cost to purchase certain hashing power is independent from the price of the currencies. However, this type of deviations from the realism on one hand may be a good approximation to reality and on the other hand is to be expected in an early attempt to apprehend an otherwise complex problem. Also, this work focuses on static games, and leave the discussion of dynamic games to future research.

Several blockchain games (mainly non-cooperative in nature) are proposed in the recent literature to address and improve upon the limitations of existing distributed consensus mechanism in various crypt-currencies [4,11,14,17,21,30], while some other games (mainly non-cooperative in nature) focus on the application layer without invoking any protocol technicality, such as the mining

pool games [10,13,14,24,29]. Our computing power allocation game is non-cooperative and focuses on the application layer; namely the allocation of mining resource. Furthermore, these games all deal with a single currency, which is a major difference from the game investigated in this work.

Our computing power allocation game is similar to the extensively-studied general blotto game in the game theory literature [1,2,15,16,27], but the two models have completely different utility functions to suit different applications in mind.

Our game can be considered as a special case of the games investigated in [12,31] in the context of P2P computing and post trading. However, our game possesses special structure that are lacking in the latter and hence admits stronger results. As a matter of fact, the games in [12,31] are so general that they only guarantees the existence of Nash equilibrium, while our game admits a unique pure Nash equilibrium with a closed-form solution.

The resource allocation nature is also relevant to the large literature on portfolio management [18], and the market equilibrium model, in particular the Fisher market [19,22]. However, the portfolio management literature usually assume that the supply of assets is independent from the allocation decision. And the Fisher market models focus on finding market-clearing prices and the allocation rule at market equilibrium.

The readers are referred to the survey by [6] for research perspectives and challenges for Bitcoin and cryptocurrencies.

2 The Computing Power Allocation Game

There are n miners $N = \{1, \ldots, n\}$ with computing powers $\mathbf{h} = (h_1, \ldots, h_n)$ (the cost to possess such a computing power, expressed in fiat currency such as US dollar). There are m cryptocurrencies $M = \{1, \ldots, m\}$ available for mining. Miner $i \in N$ allocates $x_{ij} \geq 0$ of his computing power to mine cryptocurrency j. Evidently $\sum_{j \in M} x_{ij} = h_i, i \in N$.

For each cryptocurrency j, the n miners play a winner-take-all game and the winner is rewarded with uncertain reward $\mathbf{R} = (R_1, \ldots, R_m)$ (expressed in fiat currency such as US dollar) with mean vector $\mathbb{E}[\mathbf{R}] = \mu^T = (\mu_1, \ldots, \mu_m)^T$. Miner $i \in N$ wins cryptocurrency $j \in M$ with probability proportional to its allocated computing power

$$p_{ij} = \frac{x_{ij}}{\sum_{\ell \in N} x_{\ell j}} \tag{1}$$

and his payoff for cryptocurrency $j \in M$ is given by

$$\pi_{ij}(x) = \begin{cases} R_j - x_{ij}, & \text{w.p. } p_{ij} \\ -x_{ij}, & \text{w.p. } 1 - p_{ij} \end{cases}$$

Therefore miner i's total payoff is given by

$$\pi_i(x) = \sum_{j \in M} \pi_{ij}(x) = \sum_{j \in M} R_j p_{ij} - \sum_{j \in M} x_{ij} = \sum_{j \in M} R_j \frac{x_{ij}}{\sum_{\ell \in N} x_{\ell j}} - h_i = R^T y_i(\mathbf{x}) - h_i$$

where $\mathbf{x} = (x_{ij})_{n\times m} \in \mathbb{R}_+^{n\times m}$ and

$$y_i(\mathbf{x}) = \begin{pmatrix} \frac{x_{i1}}{x_{11}+\ldots+x_{n1}} \\ \vdots \\ \frac{x_{im}}{x_{1m}+\ldots+x_{nm}} \end{pmatrix}, i \in N. \tag{2}$$

The mean of miner i's payoff is given as follows

$$\mathbb{E}_R[\pi_i(\mathbf{x})] = \mu^T y_i(\mathbf{x}) - h_i. \tag{3}$$

3 Main Result

The Nash Equilibrium for risk-neutral miners can be obtained by solving the following n optimization problems based on (3): for any given $i \in N$,

$$\begin{aligned} \max_{x_{i\cdot}\in\mathbb{R}_+^m} \quad & \mu^T y_i(\mathbf{x}) = \sum_{j\in M} \frac{x_{ij}}{\sum_{h=1}^n x_{hj}}\mu_j \\ \text{s.t.} \quad & \sum_{j\in M} x_{ij} = h_i \\ & x_{ij} \geq 0. \end{aligned} \tag{4}$$

Let $\mathbf{x}_i = (x_{ij})$ be the allocation of miner i and $\mathbf{x}_{-i}$ be the profile without miner i's allocation. For each risk-neutral miner, his object is to maximize the expected utility from all of cryptocurrencies. So given an allocation profile $\mathbf{x} = (x_{ij}) = (\mathbf{x}_1, \mathbf{x}_2, \cdots, \mathbf{x}_n)$, define $U_{ij}(\mathbf{x})$ to be the expected utility of miner i from cryptocurrency j, i.e. $U_{ij}(\mathbf{x}) = \frac{x_{ij}}{\sum_{h=1}^n x_{hj}}\mu_j$. Therefore the utility of miner i is $U_i(\mathbf{x}) = \sum_{j\in M} U_{ij}(\mathbf{x})$.

A power allocation profile $\mathbf{x}$ is a Nash equilibrium, if and only if no miner benefits by changing his strategy unilaterally. However, there is one difficulty, that is at the point where for some cryptocurrency $j \in M$, $x_{ij} = 0$ for each $i \in N$, U_i is discontinuous. So we cannot apply the standard method in [28] to study Nash equilibrium. We first propose the following lemma to show that Nash equilibrium could not be at the discontinuous point.

Lemma 1. *Given an allocation profile* $\mathbf{x}$*. If there is at least a cryptocurrency* $j \in M$ *with* $x_{ij} = 0$ *for each* $i \in N$*, then allocation* $\mathbf{x}$ *cannot be a Nash equilibrium.*

Proof. W.l.o.g. we assume that $x_{i1} = 0$ for each $i \in N$. Then there must exist another cryptocurrency, say $j = 2$, with $x_{i2} > 0$. Therefore, the allocation of miner i is $\mathbf{x}_i = (0, x_{i2}, x_{i3}, \cdots, x_{im})$. Let us consider another allocation $\mathbf{x}'_i$, with $x'_{i1} = \epsilon$, $x'_{i2} = x_{i2} - \epsilon$ and $x'_{ij} = x_{ij}$ for each $j = 3, \cdots, m$, in which

$$0 < \epsilon < \min\{x_{i2}, \frac{\mu_1(\sum_{h\in N} x_{h2})^2}{\mu_1 \sum_{h\in N} x_{h2} + \mu_2 \sum_{h\neq i} x_{h2}}\}.$$

On one hand, allocation $\mathbf{x}'_i$ is feasible as $0 < \epsilon < x_{i2}$. On the other hand, if other miners remain their allocations unchanged and miner i reallocate his

computing power as $\mathbf{x}'_i$ unilaterally, then miner i will obtain the whole reward from cryptocurrency 1 and his utility shall be

$$U'_i = \mu_1 + \frac{x_{i2} - \epsilon}{\sum_{h\in N} x_{h2} - \epsilon}\mu_2 + \sum_{j=3} \frac{x_{ij}}{\sum_{h\in N} x_{hj}}\mu_j.$$

The difference of utility is

$$\begin{aligned}
\Delta U_i = U'_i - U_i &= \mu_1 + \frac{x_{i2} - \epsilon}{\sum_{h\in N} x_{h2} - \epsilon}\mu_2 - \frac{x_{i2}}{\sum_{h\in N} x_{h2}}\mu_2 \\
&= \mu_1 - \frac{\sum_{h\in N, h\neq i} x_{h2}\mu_2\epsilon}{\sum_{h\in N} x_{h2}(\sum_{h\in N} x_{h2} - \epsilon)} \\
&= \frac{\mu_1(\sum_{h\in N} x_{h2})^2 - (\mu_1 \sum_{h\in N} x_{h2} + \mu_2 \sum_{h\neq i} x_{h2})\epsilon}{\sum_{h\in N} x_{h2}(\sum_{h\in N} x_{h2} - \epsilon)} \\
&> \frac{\mu_1(\sum_{h\in N} x_{h2})^2 - (\mu_1 \sum_{h\in N} x_{h2} + \mu_2 \sum_{h\neq i} x_{h2})\epsilon}{(\sum_{h\in N} x_{h2})^2} > 0.
\end{aligned}$$

The last inequality is from the definition of ϵ. Thus we can conclude that the allocation $\mathbf{x}$ in which for some $j \in M$, $x_{ij} = 0$ for each $i \in N$, is not a Nash equilibrium. □

Conveniently, we define the following condition of an allocation $\mathbf{x}$,

Condition 1 For each cryptocurrency $j \in M$, $\sum_{i\in N} x_{ij} > 0$.

Based on Lemma 1, it is sufficient for us to study the Nash equilibrium at such allocations satisfying Condition 1. From (4), we know the utility function of miner i is linear and the domain $\{(x_{i1}, x_{i2}, \cdots, x_{im}) | \sum_{j\in M} x_{ij} = h_i,\ x_{ij} \geq 0\}$ is convex. Then by the first-order optimality condition, there exists Lagrange multiplier $\alpha_i > 0$, such that

$$\frac{\partial U_i}{\partial x_{ij}} = \frac{\sum_{h\neq i} x_{hj}}{(\sum_{h=1}^{n} x_{hj})^2} \cdot \mu_j \begin{cases} = \alpha_i & \text{if } x_{ij} > 0, \\ \leq \alpha_i & \text{if } x_{ij} = 0. \end{cases}$$

From another perspective, at an equilibrium, if miner i allocates positive computing power for some cryptocurrencies, then he shall has the same marginal value on these cryptocurrencies. Otherwise, he may have lower marginal value. Therefore, we face another difficulty that how to characterize Nash equilibrium at $\mathbf{x}$ satisfying Condition 1, but $x_{ij} = 0$ for some $j \in M$ and $i \in N$. For this purpose, we consider a kind of restricted strategy at first, that is for miner i, he only changes his allocation between two cryptocurrencies j and k with

$$x'_{ij} = x_{ij} - \epsilon, \quad x'_{ik} = x_{ik} + \epsilon, \quad x'_{i\ell} = x_{i\ell},\ l \neq j, k, \tag{5}$$

where $x_{ij} > 0$ and $\epsilon > 0$. For convenience, we call such a kind of strategy as a *restricted strategy on cryptocurrencies j and k.*

Lemma 2. *In the hash power allocation game, if all miners are only permitted to play the restricted strategy, then an allocation $\mathbf{x}$ is a Nash equilibrium, if*

and only if for each miner $i \in N$, there is a constant α_i such that for each cryptocurrency j,

$$\frac{\sum_{h\neq i} x_{hj}}{(\sum_{h=1}^{n} x_{hj})^2} \cdot \mu_j = \alpha_i. \tag{6}$$

Proof. Obviously, allocation $\mathbf{x}$ must satisfy Condition 1. W.l.o.g., assume miner i plays the restricted strategy on cryptocurrencies j and k and his new allocation $\mathbf{x}'$ is shown as (5). It is possible that $x_{ik} = 0$. Clearly,

$$U_{ij}(\mathbf{x}'_i, \mathbf{x}_{-i}) = \frac{x_{ij} - \epsilon}{\sum_{h=1}^{n} x_{hj} - \epsilon}\mu_j, \quad U_{ik}(\mathbf{x}'_i, \mathbf{x}_{-i}) = \frac{x_{ik} + \epsilon}{\sum_{h=1}^{n} x_{hk} + \epsilon}\mu_k.$$

Since others' allocations are unchanged and $x'_{i\ell} = x_{i\ell}$, $\ell \neq j, k$, we have $U_{i\ell}(\mathbf{x}'_i, \mathbf{x}_{-i}) = U_{i\ell}(\mathbf{x})$, $\ell \neq j, k$. Therefore

$$\begin{aligned}
\Delta U_i &= (U_{ij}(\mathbf{x}'_i, \mathbf{x}_{-i}) - U_{ij}(\mathbf{x})) + (U_{ik}(\mathbf{x}'_i, \mathbf{x}_{-i}) - U_{ik}(\mathbf{x})) \\
&= \left[\frac{x_{ij} - \epsilon}{\sum_{h=1}^{n} x_{hj} - \epsilon} - \frac{x_{ij}}{\sum_{h=1}^{n} x_{hj}}\right] \cdot \mu_j + \left[\frac{x_{ik} + \epsilon}{\sum_{h=1}^{n} x_{hk} + \epsilon} - \frac{x_{ik}}{\sum_{h=1}^{n} x_{hk}}\right] \cdot \mu_k \\
&= \frac{-\sum_{h\neq i} x_{hj}\mu_j\epsilon}{\sum_{h=1}^{n} x_{hj}(\sum_{h=1}^{n} x_{hj} - \epsilon)} + \frac{\sum_{h\neq i} x_{hk}\mu_k\epsilon}{\sum_{h=1}^{n} x_{hk}(\sum_{h=1}^{n} x_{hk} + \epsilon)}.
\end{aligned}$$

If the result of (6) holds, which means

$$\frac{\sum_{h\neq i} x_{hj}}{(\sum_{h=1}^{n} x_{hj})^2} \cdot \mu_j = \frac{\sum_{h\neq i} x_{hk}}{(\sum_{h=1}^{n} x_{hk})^2} \cdot \mu_k,$$

then it is easy to deduce that,

$$\frac{\sum_{h\neq i} x_{hj}\mu_j\epsilon}{\sum_{h=1}^{n} x_{hj}(\sum_{h=1}^{n} x_{hj} - \epsilon)} > \frac{\sum_{h\neq i} x_{hj}\mu_j\epsilon}{(\sum_{h=1}^{n} x_{hj})^2} = \frac{\sum_{h\neq i} x_{hk}\mu_k\epsilon}{(\sum_{h=1}^{n} x_{hk})^2} > \frac{\sum_{h\neq i} x_{hk}\mu_k\epsilon}{\sum_{h=1}^{n} x_{hk}(\sum_{h=1}^{n} x_{hk} + \epsilon)},$$

implying $\Delta U_i \leq 0$.

On the other hand, we shall prove (6) is the necessary condition for a Nash equilibrium allocation if each miner is only allowed to play the restricted strategy. For this purpose, we try to prove that once the result of (6) does not hold, miner i can get more utility by playing a restricted strategy.

W.l.o.g., suppose

$$\frac{\sum_{h\neq i} x_{hj}}{(\sum_{h=1}^{n} x_{hj})^2} \cdot \mu_j < \frac{\sum_{h\neq i} x_{hk}}{(\sum_{h=1}^{n} x_{hk})^2} \cdot \mu_k,$$

There must exist an arbitrarily small constant $\epsilon > 0$ such that

$$\frac{\sum_{h\neq i} x_{hj}\mu_j}{\sum_{h=1}^{n} x_{hj}(\sum_{h=1}^{n} x_{hj} - \epsilon)} < \frac{\sum_{h\neq i} x_{hk}\mu_k}{\sum_{h=1}^{n} x_{hk}(\sum_{h=1}^{n} x_{hk} + \epsilon)}.$$

So

$$\Delta U_i = \frac{-\sum_{h\neq i} x_{hj}\mu_j\epsilon}{\sum_{h=1}^{n} x_{hj}(\sum_{h=1}^{n} x_{hj} - \epsilon)} + \frac{\sum_{h\neq i} x_{hk}\mu_k\epsilon}{\sum_{h=1}^{n} x_{hk}(\sum_{h=1}^{n} x_{hk} + \epsilon)} > 0$$

It means that miner i can benefit by playing the restricted strategy on cryptocurrencies j and k and the current allocation $\mathbf{x}$ is not a Nash equilibrium.

In addition, because of the arbitrariness of j and k (even though $x_{ik} = 0$), we have the sufficient and necessary condition of any pure Nash equilibrium for the restricted strategy that there is a constant α_i for each miner $i \in N$ and

$$\frac{\sum_{h \neq i} x_{hj}}{(\sum_{h=1}^{n} x_{hj})^2} \cdot \mu_j = \alpha_i, \quad \forall j \in M.$$

is satisfied. □

Next let us turn to the characterization of any pure Nash equilibrium for more general strategy. W.l.o.g., suppose the new allocation $\mathbf{x}'_i$ after manipulation is

$$\begin{aligned} &x'_{i1} = x_{i1} + \epsilon_1,\ x'_{i2} = x_{i2} + \epsilon_2,\ \cdots,\ x'_{ik} = x_{ik} + \epsilon_k, \\ &x'_{i(k+1)} = x_{i(k+1)} - \epsilon_{k+1},\ \cdots,\ x'_{i(k+h)} = x_{i(k+h)} - \epsilon_{k+h}, \\ &x'_{i(k+h+1)} = x_{i(k+h+1)}, \cdots, x'_{im} = x_{im}, \end{aligned} \tag{7}$$

where each $\epsilon_\ell > 0$, $x'_{ij} \geq 0$ for each $j \in M$, and $\sum_{\ell=1}^{k} \epsilon_\ell = \sum_{\ell=1}^{h} \epsilon_{k+\ell}$.

Algorithm A is proposed in Table 1, which constructs a series of intermediate allocations from $\mathbf{x}_i$ to $\mathbf{x}'_i$. For the sake of convenience, let $\mathbf{x}_i^0 = \mathbf{x}_i$, $\mathbf{x}_i^p = \mathbf{x}'_i$ and the intermediate allocations are denoted by $\mathbf{x}_i^1, \cdots, \mathbf{x}_i^{p-1}$.

Table 1. The Algorithm to Construct Intermediate Allocations

Algorithm A
Input: Allocations $\mathbf{x}_i^0 = \mathbf{x}_i$ and $\mathbf{x}_i^p = \mathbf{x}'_i$
Output: The intermediate allocations $\mathbf{x}_i^1, \mathbf{x}_i^2, \cdots, \mathbf{x}_i^{p-1}$.
1: **Set** $t := 1$, $r := 1$ and $q := 1$;
2: **While** $t \leq k$ and $r \leq h$;
3: **Set** $\eta_q = \min\{\epsilon_t, \epsilon_{k+r}\}$;
4: **Set** $x_{i\ell}^q = \begin{cases} x_{i\ell}^{q-1} + \eta_q, & \ell = t \\ x_{i\ell}^{q-1} - \eta_q, & \ell = k+r \\ x_{i\ell}^{q-1}, & \ell \neq t, k+r. \end{cases}$ and **Output** allocation $\mathbf{x}_i^q = (x_{i\ell}^q)$;
5: **If** $\eta_q = \epsilon_t = \epsilon_{k+r}$;
Set $t := t+1$, $r := r+1$, $q := q+1$ and go to line 2;
6: **Else**
7: **If** $\eta_q = \epsilon_t$
Set $\epsilon_{k+r} := \epsilon_{k+r} - \eta_q$, $t := t+1$, $q := q+1$ and go to line 2;
8: **If** $\eta_q = \epsilon_{k+r}$
Set $\epsilon_t := \epsilon_t - \eta_q$, $r := r+1$, $q := q+1$ and go to line 2.

Here we give an example to show how Algorithm A works.

Example 1. Suppose the strategic miner i changes his allocation to $\mathbf{x}'_i = (x_{i1} + 5, x_{i2} + 3, x_{i3} + 1, x_{i4} - 6, x_{i5} - 3, x_{i6})$. Then the intermediate allocations are

$$\begin{aligned}
\mathbf{x}_i^0 &= (x_{i1}, x_{i2}, x_{i3}, x_{i4}, x_{i5}, x_{i6});\\
\mathbf{x}_i^1 &= (x_{i1} + 5, x_{i2}, x_{i3}, x_{i4} - 5, x_{i5}, x_{i6});\\
\mathbf{x}_i^2 &= (x_{i1} + 5, x_{i2} + 1, x_{i3}, x_{i4} - 5 - 1, x_{i5}, x_{i6});\\
\mathbf{x}_i^3 &= (x_{i1} + 5, x_{i2} + 1 + 2, x_{i3}, x_{i4} - 5 - 1, x_{i5} - 2, x_{i6});\\
\mathbf{x}_i^4 &= (x_{i1} + 5, x_{i2} + 1 + 2, x_{i3} + 1, x_{i4} - 5 - 1, x_{i5} - 2 - 1, x_{i6}).
\end{aligned}$$

Obviously, at least one of indices t and r is increased by 1 at each step in Algorithm A. Because $\sum_{\ell=1}^{k} \epsilon_\ell = \sum_{\ell=1}^{h} \epsilon_{k+\ell}$, then Algorithm A must terminate at the case that $\eta_q = \epsilon_t = \epsilon_{k+r}$ and obtain the last allocation $\mathbf{x}'$. Thus Algorithm A can be finished in at most $k + h - 1$ steps, which implies the time complexity of Algorithm A is $O(n)$. Furthermore these intermediate allocations have several nice properties, which are necessary for us to obtain the result on Nash equilibrium.

Lemma 3. *Given the series of allocations* $\mathbf{x}_i^0, \mathbf{x}_i^1, \cdots, \mathbf{x}_i^p$ *from Algorithm A. For any two adjacent allocations* $\mathbf{x}_i^{q-1}$ *and* $\mathbf{x}_i^q$

1. $x_{it}^q = x_{it}^{q-1} + \eta_q$, $x_{i(j+r)}^q = x_{i(j+r)}^{q-1} - \eta_q$, *and* $x_{i\ell}^q = x_{i\ell}^{q-1}$, $\ell \neq t, k+r$;
2. *For any allocation* $\mathbf{x}_i^q$, $q = 1, 2, \cdots, p$, *there exist three cases:*
   - *Case 1.* $x_{it}^{q-1} = x_{it} + \omega$ *and* $x_{i(k+r)}^{q-1} = x_{i(k+r)}$, $\omega > 0$;
   - *Case 2.* $x_{it}^{q-1} = x_{it}$ *and* $x_{i(k+r)}^{q-1} = x_{i(k+r)} - \omega$, $\omega > 0$;
   - *Case 3.* $x_{it}^{q-1} = x_{it}$ *and* $x_{i(k+r)}^{q-1} = x_{i(k+r)}$.

Proof. The first claim is from line 4 in Algorithm A directly. The three cases in the second claim are right from line 5-8 in Algorithm A. □

Based on the previous analysis for the changing processes from $\mathbf{x}_i$ to $\mathbf{x}'_i$, the following theorem shows the sufficient and necessary condition for the existence of Nash equilibrium in Lemma 2 also holds, even though the miners are allowed to play more general strategy.

Theorem 1. *An allocation* $\mathbf{x}$ *in the hash power allocation game is a Nash equilibrium, if and only if for each miner* $i \in N$ *and any cryptocurrency* j, *there is a constant* α_i *satisfying*

$$\frac{\sum_{h \neq i} x_{hj}}{(\sum_{h=1}^{n} x_{hj})^2} \cdot \mu_j = \alpha_i. \tag{8}$$

Proof. Of course, $\mathbf{x}$ satisfies Condition 1. Let us suppose $\mathbf{x}$ to be a Nash equilibrium allocation, but Eq. (8) does not hold. By the proof in Lemma 2, miner i can change his allocation to a new one $\mathbf{x}'_i$ shown as (5), to improve his utility. It is a contradiction to the assumption that $\mathbf{x}$ is a Nash equilibrium.

On the other hand, we shall prove that once an allocation $\mathbf{x}$ satisfies (8), it must be a Nash equilibrium. W.l.o.g., suppose a strategic miner i changes his allocation to $\mathbf{x}_i'$ as (7). So we can obtain a series of allocations $\mathbf{x}_i^0, \mathbf{x}_i^1, \cdots, \mathbf{x}_i^p$ from Algorithm A. The first claim in Lemma 3,

$$x_{it}^q = x_{it}^{q-1} + \eta_q,\ x_{i(k+r)}^q = x_{i(k+r)}^{q-1} - \eta_q,\ \text{and } x_{i\ell}^q = x_{i\ell}^{q-1},\ \ell \neq t, j+r,$$

shows that any two adjacent allocations $\mathbf{x}_i^q$ and $\mathbf{x}_i^{q-1}$ are the same, except for the t-th and $k+r$-th elements. It can be viewed as miner i plays a restricted strategy on two cryptocurrencies t and $k+r$ from $\mathbf{x}_i^{q-1}$ to $\mathbf{x}_i^q$. So we focus on the change between $\mathbf{x}_i^q$ and $\mathbf{x}_i^{q-1}$ by using the similar proof in Lemma 2. There are three cases for each $\mathbf{x}_i^q$, $q = 1, \cdots, p$, in the second claim of Lemma 3. Here we only concentrate on Case 1: $x_{it}^{q-1} = x_{it} + \omega$ and $x_{i(k+r)}^{q-1} = x_{i(k+r)}$, $\omega > 0$.

Suppose to the contrary that $\Delta U_i^q = U_i(\mathbf{x}_i^q, \mathbf{x}_{-i}) - U_i(\mathbf{x}_i^{q-1}, \mathbf{x}_{-i}) > 0$, then

$$0 < U_i(\mathbf{x}_i^q, \mathbf{x}_{-i}) - U_i(\mathbf{x}_i^{q-1}, \mathbf{x}_{-i}) =$$
$$\left(\frac{x_{i(k+r)} - \eta_q}{\sum_{g=1}^n x_{g(k+r)} - \eta_q} - \frac{x_{i(k+r)}}{\sum_{g=1}^n x_{g(k+r)}}\right)\mu_{k+r} + \left(\frac{x_{it} + \omega + \eta_q}{\sum_{g=1}^n x_{gt} + \omega + \eta_q} - \frac{x_{it} + \omega}{\sum_{g=1}^n x_{gt} + \omega}\right)\mu_t.$$

It is equivalent to

$$\frac{(\sum_{g\neq i} x_{gt})\mu_t}{(\sum_{g=1}^n x_{gt} + \omega)(\sum_{g=1}^n x_{gt} + \eta_q + \omega)} > \frac{(\sum_{g\neq i} x_{g(k+r)})\mu_{k+r}}{(\sum_{g=1}^n x_{g(k+r)})(\sum_{g=1}^n x_{g(k+r)} - \eta_q)}$$
$$\Leftrightarrow \eta_q < \frac{(\sum_{g\neq i} x_{gt})\mu_t(\sum_{g=1}^n x_{g(k+r)})^2 - (\sum_{g\neq i} x_{g(k+r)})\mu_{k+r}(\sum_{g=1}^n x_{gt} + \omega)^2}{(\sum_{g\neq i} x_{gt})\mu_t(\sum_{g=1}^n x_{g(k+r)}) + (\sum_{g\neq i} x_{g(k+r)})\mu_{k+r}(\sum_{g=1}^n x_{gt} + \omega)}. \quad (9)$$

Since

$$\frac{(\sum_{g\neq i} x_{gt}) \cdot \mu_t}{(\sum_{g=1}^n x_{gt} + \omega)^2} < \frac{\sum_{g\neq i} x_{gt} \cdot \mu_t}{(\sum_{g=1}^n x_{gt})^2} = \frac{\sum_{g\neq i} x_{g(k+r)} \cdot \mu_{k+r}}{(\sum_{g=1}^n x_{g(k+r)})^2},$$

where the equation is from condition (8), we can continue (9) to be

$$\eta_q < \frac{(\sum_{g\neq i} x_{gt})\mu_t(\sum_{g=1}^n x_{g(k+r)})^2 - (\sum_{g\neq i} x_{g(k+r)})\mu_{k+r}(\sum_{g=1}^n x_{gt} + \omega)^2}{(\sum_{g\neq i} x_{gt})\mu_t(\sum_{g=1}^n x_{g(k+r)}) + (\sum_{g\neq i} x_{g(k+r)})\mu_{k+r}(\sum_{g=1}^n x_{gt} + \omega)} < 0.$$

This contradicts to the condition that $\eta_q > 0$. Therefore $\Delta U_i^q \leq 0$ for Case 1.

By the similar analysis, we also can get $\Delta U_i^q \leq 0$ for other two cases. Thus each $\Delta U_i^q \leq 0$, $q = 1, \cdots, p$. It is not hard to see that the total difference ΔU_i can be partitioned as

$$\begin{aligned}\Delta U_i &= \left[U_i(\mathbf{x}_i^1, \mathbf{x}_{-i}) - U_i(\mathbf{x})\right] + \cdots + \left[U_i(\mathbf{x}_i', \mathbf{x}_{-i}) - U_i(\mathbf{x}_i^{p-1}, \mathbf{x}_{-i})\right] \\ &= \Delta U_i^1 + \cdots + \Delta U_i^p. \end{aligned} \quad (10)$$

It implies $\Delta U_i \leq 0$, since each component $\Delta U_i^q \leq 0$ in (10). So miner i can not improve his utility by changing allocation from $\mathbf{x}_i$ to $\mathbf{x}_i'$. □

Based on the sufficient and necessary condition for a Nash equilibrium, we will propose the closed-form solution of a pure Nash equilibrium and prove the the uniqueness of such a pure Nash equilibrium in following theorem.

Theorem 2. *A hash power allocation profile* $\mathbf{x} = (x_{ij})$ *is a Nash equilibrium, if and only if it has the form as* $x_{ij} = \frac{\mu_j}{\sum_{\ell=1}^{m} \mu_\ell} \cdot h_i$, *for any* $i \in N$ *and* $j \in M$.

Proof. It is not hard to see that once each x_{ij} has the form as $x_{ij} = \frac{\mu_j}{\sum_{\ell=1}^{m} \mu_\ell} \cdot h_i$, then for any $j \in M$,

$$\frac{\sum_{h \neq i} x_{hj}}{(\sum_{h=1}^{n} x_{hj})^2} \cdot \mu_j = \frac{\sum_{h=1}^{n} h_h - h_i}{(\sum_{h=1}^{n} h_h)^2} (\sum_{\ell=1}^{m} \mu_\ell),$$

which is irrelevant to the cyprocurrency j and such a ratio can be defined as α_i. Then the allocation $\mathbf{x} = (x_{ij})$ with $x_{ij} = \frac{\mu_j}{\sum_{\ell=1}^{m} \mu_\ell} \cdot h_i$ is a Nash equilibrium by Theorem 1.

On the other hand, Theorem 1 tells us for any $j \in M$, $\frac{\sum_{h \neq i} x_{hj}}{(\sum_{h=1}^{n} x_{hj})^2} \cdot \mu_j = \alpha_i$. It implies

$$\sum_{i=1}^{n} \alpha_i = \sum_{i=1}^{n} \frac{\sum_{h \neq i} x_{hj}}{(\sum_{h=1}^{n} x_{hj})^2} \mu_j = \frac{(n-1) \sum_{h=1}^{n} x_{hj}}{(\sum_{h=1}^{n} x_{hj})^2} \mu_j = \frac{n-1}{\sum_{h=1}^{n} x_{hj}} \mu_j. \tag{11}$$

From Eq. (11), we continue to have

$$\sum_{i=1}^{n} \alpha_i = \frac{(n-1)\mu_1}{\sum_{h=1}^{n} x_{h1}} = \cdots = \frac{(n-1)\mu_m}{\sum_{h=1}^{n} x_{hm}}.$$

Then

$$\frac{\mu_1}{\sum_{h=1}^{n} x_{h1}} = \cdots = \frac{\mu_m}{\sum_{h=1}^{n} x_{hm}} = \frac{\sum_{j=1}^{m} \mu_j}{\sum_{j=1}^{m} \sum_{i=1}^{n} x_{ij}} = \frac{\sum_{j=1}^{m} \mu_j}{\sum_{i=1}^{n} h_i}.$$

So $\sum_{i=1}^{n} \alpha_i = (n-1) \cdot \frac{\sum_{j=1}^{m} \mu_j}{\sum_{i=1}^{n} h_i}$, which is a constant. On the other hand, from Eq. (11), we can get

$$\frac{\sum_{h=1}^{n} x_{hj}}{\mu_j} = \frac{n-1}{\sum_{i=1}^{n} \alpha_i} \quad \forall j \in M; \tag{12}$$

Then for any $j \in M$,

$$\alpha_i = \frac{\sum_{h \neq i} x_{hj}}{(\sum_{h=1}^{n} x_{hj})^2} \mu_j = \frac{\sum_{h \neq i} x_{hj}}{\mu_j} \left(\frac{\mu_j}{\sum_{h=1}^{n} x_{hj}} \right)^2 = \frac{\sum_{h \neq i} x_{hj}}{\mu_j} \left(\frac{\sum_{i=1}^{n} \alpha_i}{n-1} \right)^2, \tag{13}$$

where the last equality is from (12). Also Eq. (13) guarantees

$$\frac{\sum_{h \neq i} x_{hj}}{\mu_j} = \frac{(n-1)^2 \alpha_i}{(\sum_{i=1}^{n} \alpha_i)^2}. \tag{14}$$

Furthermore, the difference between (12) and (14) is

$$\frac{x_{ij}}{\mu_j} = \frac{n-1}{\sum_{i=1}^{n} \alpha_i} - \frac{(n-1)^2 \alpha_i}{(\sum_{i=1}^{n} \alpha_i)^2}. \tag{15}$$

The right side of (15) shows $\frac{x_{ij}}{\mu_j}$ is only related to index i which can be denoted by γ_i. So $x_{ij} = \gamma_i \mu_j$. In addition, by the condition of $\sum_{j=1}^{m} x_{ij} = h_i$, we have

$$\sum_{j=1}^{n} x_{ij} = \sum_{j=1}^{n} \gamma_i \mu_j = \gamma_i \sum_{j=1}^{n} \mu_j = h_i.$$

Therefore, $\gamma_i = \frac{h_i}{\sum_{j=1}^{n} \mu_j}$ and $x_{ij} = \frac{\mu_j}{\sum_{\ell=1}^{m} \mu_\ell} \cdot h_i$. It concludes this claim. □

Based on the result of Theorem 2 and the formation of each miner's expected payoff (3), we can easily get the following corollary.

Corollary 1 *Under the pure Nash equilibrium allocation* $x_{ij} = \frac{\mu_j}{\sum_{\ell=1}^{m} \mu_\ell} \cdot h_i$ *for any* $i \in N$ *and* $j \in M$*, each miner* i*'s expected payoff is* $\frac{h_i}{\sum_{\ell=1}^{n} h_\ell}(\sum_{\ell=1}^{m} \mu_\ell)$.

4 Conclusion

This paper discusses the issue of a hashing power allocation game in cryptocurrencies, in which there are n miners equipped with certain computing power and m different cryptocurrencies to be mined. Each miner shall allocate his computing power in mining the cryptocurrencies properly to compete with others to maximize his payoff. In this paper, we mainly consider the hashing power allocation game with the risk-neutral objective. We show that the Nash Equilibrium allocation of this game is unique and follows a proportional rule where each miner will allocate his total computing power to a given cryptocurrency proportional to the percentage of the award among all currencies, while his expected revenue is proportional to the percentage of the hashing power possessed and total award.

Besides, the risk-averse objective is also interesting for us to consider in the future. For each risk-averse miner i, he tries to minimize the uncertainty, that is to minimize the objective of $y_i(\mathbf{x})^T \Sigma y_i(\mathbf{x})$, subject to the constraint of $\sum_{j \in M} x_{ij} = h_i$. Here vector $y_i(\mathbf{x})$ is defined as (2) and $\Sigma \succ 0$ is the covariance matrix of uncertain reward $\mathbf{R}$, i.e. $\Sigma = \mathrm{Cov}[\mathbf{R}]$. For this kind of game, we are also concerned about the existence and uniqueness of a pure Nash equilibrium. In addition, how to compute a pure Nash equilibrium is our task too.

Acknowledgments. The first author's research is partially supported by the National Nature Science Foundation of China (No. 11301457). The second author's research is supported by the Natural Sciences and Engineering Research Council of Canada (NSERC) grant 06446, and NNSF of China 11771386 and 11728104. The third author's research is supported by NSFC (No. 10971187) and the NSF of 415 Zhejiang Province grant LQ12A01011.

References

1. Ahmadinejad, A.M., Dehghani, S., Hajiaghayi, M.T., Lucier, B., Mahini, H., Seddighin, S.: Computing equilibria of blotto and other games, from duels to battefields (2016)
2. Alpern, S., Howard, J.V.: Winner-take-all games: the strategic optimisation of rank. Oper. Res. **65**, 1165–1176 (2017)
3. AntPool. https://www.antpool.com/
4. Biais, B., Bisiere, C., Bouvard, M., Casamatta, C.: The Blockchain Folk Theorem. In: Social Science Electronic Publishing (2017)
5. Bitcoin. https://bitcoin.org/en/
6. Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J.A., Felten, E.W.: Research perspectives and challenges for bitcoin and cryptocurrencies to appear. pp. 104–121 (2015)
7. BTC.com. https://btc.com/
8. BTC.TOP. http://btc.top/
9. Ethereum. https://www.ethereum.org/
10. Eyal, I.: The Miner's Dilemma, pp. 89–103. Computer Science (2015)
11. Eyal, I., Sirer, E.G.: Majority is not enough: bitcoin mining is vulnerable. Eprint Arxiv **8437**, 436–454 (2013)
12. Feldman, M., Lai, K., Zhang, L.: The proportional-share allocation market for computational resources. IEEE Trans. Parallel Distrib. Syst. **20**(8), 1075–1088 (2009)
13. Fisch, B., Pass, R., Shelat, A.: Socially optimal mining pools. In: International Conference on Web and Internet Economics, pp. 205–218 (2017)
14. Göbel, J., Keeler, H.P., Krzesinski, A.E., Taylor, P.G.: Bitcoin blockchain dynamics: the selfish-mine strategy in the presence of propagation delay. Perform. Eval. **104**, 23–41 (2016)
15. Goldberg, L.A., Goldberg, P.W., Krysta, P., Ventre, C.: Ranking games that have competitiveness-based strategies. In: ACM Conference on Electronic Commerce, pp. 335–344 (2010)
16. Hart, S.: Discrete colonel blotto and general lotto games. Int. J. Game Theory **36**(3–4), 441–460 (2008)
17. Kiayias, A., Koutsoupias, E., Kyropoulou, M., Tselekounis ,Y.: Blockchain mining games. In: ACM Conference on Economics and Computation, pp. 365–382 (2016)
18. Markowitz, H.: Portfolio selection. J. Financ. **7**(1), 77–91 (1952)
19. Mas-Colell, A., Whinston, M.D., Green, J.R.: Microeconomic Theory. Oxford University Press, Oxford (1995)
20. Nakamoto, S.: Bitcoin: a peer-to-peer electronic cash system. Consulted (2008)
21. Carlsten, M., Kalodner, H., Weinberg, S.M., Narayanan, A.: On the instability of bitcoin without the block reward. In: ACM Sigsac Conference on Computer and Communications Security, pp. 154–167 (2016)
22. Nisan, N., Roughgarden, T., Tardos, E., Vazirani, V.V.: Algorithmic Game Theory. Cambridge University Press, Cambridge (2007)
23. Proof of burn. https://en.bitcoin.it/wiki/proofofburn
24. Parham, R.: The predictable cost of bitcoin. Social Science Electronic Publishing (2017)
25. Slush Pool. https://slushpool.com/home/
26. Ripple. https://ripple.com/
27. Roberson, B.: The colonel blotto game. Econ. Theory **29**(1), 1–24 (2006)

28. Rosen, J.B.: Existence and uniqueness of equilibrium points for concave n-person games. Econometrica **33**(3), 520–534 (1965)
29. Rosenfeld, M.: Analysis of bitcoin pooled mining reward systems. Computer Science, December (2011)
30. Saleh, F.: Blockchain without waste: proof-of-stake (2017)
31. Shapley, L., Shubik, M.: Trade using one commodity as a means of payment. J. Polit. Econ. **85**(5), 937–968 (1977)
32. ViaBTC. https://viabtc.com/
33. Wattenhofer, R.: The Science of the Blockchain. CreateSpace Independent Publishing Platform, Charleston (2016)