Journal of Systems Science and Information
Jun., 2021, Vol. 9, No. 3, pp. 255–265
DOI: 10.21078/JSSI-2021-255-11

A Hashing Power Allocation Game with and without Risk-free Asset

Yukun CHENG
School of Business, Suzhou University of Science and Technology, Suzhou 215009*, China*
E-mail: ykcheng@amss.ac.cn

Donglei DU
Faculty of Management, University of New Brunswick, NB Canada, Fredericton E3B 9Y2, Canada
E-mail: ddu@unb.ca

Qiaoming HAN*
School of Economics & Management, Nanjing Tech University, Nanjing 211800*, China*
E-mail: qmhan@zufe.edu.cn

Abstract Miners in various blockchain-backed cryptocurrency networks compete to maintain the validity of the underlying distributed ledgers to earn the bootstrapped cryptocurrencies. With limited hashing power, each miner needs to decide how to allocate their resource to different cryptocurrencies so as to achieve the best overall payoff. Together all the miners form a hashing power allocation game. We consider two settings of the game, depending on whether each miner can allocate their fund to a risk-free asset or not. We show that this game admits unique pure Nash equilibrium in closed-form for both settings.

Keywords game and Nash equilibrium; blockchain; cryptocurrency; mining; risk-neutral; risk-averse

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 totaling approximate $456 billion[1], and among them Bitcoin, Ethereum and Ripple 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

Received August 12, 2020, accepted January 18, 2021
The first author's research is supported by the National Nature Science Foundation of China (11871366), USTS Think Tank for Urban Development, Qin Lan Project for Young Academic Leaders and Qin Lan Project for Key Teachers. The second author's research is supported by the Natural Sciences and Engineering Research Council of Canada (NSERC) (06446), and NSFC (11771386 and 11728104). The third author's research is supported by NSFC (11771386 and 11728104)
*Corresponding author
[1]According to https://coinmarketcap.com/.

(PoW)[1] and proof-of-stake (PoS)[2] 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 minutes for Bitcoin), miners participate in a winner-take-all competition to 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[3]: 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 our game. We show that the NE allocation is unique and follows a proportional rule (Theorem 1) where each miner allocates 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 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 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.

2 Relevant Literature

Our computing power allocation game is relevant to several areas, including game theory, portfolio management, and market equilibrium models.

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[4–8], 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[7, 9–12]. 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. Dimitri[13] studied a special case of our game where there is only one currency available for mining. [14] is a survey on this line of research.

Our computing power allocation game is similar to the extensively-studied general blotto game in the game theory literature[15–18], but the two models have completely different utility functions to suit different applications in mind.

The resource allocation nature is also relevant to the large literature on portfolio management[19], and the market equilibrium model, in particular the Fisher market[20, 21]. 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[22] for research perspectives and challenges for Bitcoin and cryptocurrencies.

We describe the the hashing power allocation game in Section 3. We consider games without and with a risk-free asset in Sections 4 and 5, respectively.

3 The Hashing Power Allocation Game

There are n miners $N = \{1, 2, \cdots, n\}$ with computing powers $h = (h_1, h_2, \cdots, h_n)^{\mathrm{T}} \in \mathbb{R}^n_+$ (the cost to possess such a computing power, expressed in fiat currency such as US dollar) and there are m cryptocurrencies $M = \{1, 2, \cdots, m\}$ available for mining. When there is a risk-free asset with return r, we introduce a dummy labeled as currency 0.

Miner $i \in N$ allocates $x_{ij} \geq 0$ of his computing power to mine cryptocurrency $j \in M$. Let x_{i0} be the hashing power allocated to the dummy risk-free asset whose return is known as r for any amount allocated. Evidently, we have

$$\sum_{j \in M} x_{ij} + x_{i0} = h_i, \quad \forall i \in N.$$

For each cryptocurrency $j \in M$, the n miners play a winner-take-all game and the winner is rewarded with uncertain reward vector $R = (R_1, R_2, \cdots, R_m)^{\mathrm{T}}$ (expressed in fiat currency such as US dollar) with mean vector $\mathbb{E}[R] = \mu^{\mathrm{T}} = (\mu_1, \mu_2, \cdots, \mu_m)^{\mathrm{T}}$. 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 profit for mining cryptocurrency $j \in M$ is given by

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

Moreover the profit obtained with the risk-free asset is given by

$$\pi_{i0} = r x_{i0}.$$

Therefore miner i's total profit is given by

$$\begin{aligned} \pi_i(x) &= \sum_{j\in M} \pi_{ij}(x) + \pi_{i0} = \sum_{j\in M} R_j p_{ij} - \sum_{j\in M} x_{ij} + r x_{i0} \\ &= \sum_{j\in M} R_j \frac{x_{ij}}{\sum_{\ell\in N} x_{\ell j}} - h_i + (1+r)x_{i0} = R^{\mathrm{T}} y_i(x) - h_i + (1+r)x_{i0}, \end{aligned}$$

where $x = (x_1\ x_2\ \cdots\ x_n)^{\mathrm{T}} = (x_{ij})_{n\times m} \in \mathbb{R}_+^{n\times m}$ and

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

The mean profit of miner i is given by

$$\mathbb{E}_R[\pi_i(x)] = \mu^{\mathrm{T}} y_i(x) - h_i + (1+r)x_{i0}. \tag{3}$$

4 Game without Risk-free Asset

We recall the result without a risk-free asset. When miners allocate all their funds to mining, the NE for the miners game can be obtained by solving the following n optimization problems based on (3): For any given $i \in N$,

$$\max_{x_{i\cdot}\in\mathbb{R}_+^m} \left[\mu^{\mathrm{T}} y_i(x) : \sum_{j\in M} x_{ij} = h_i \right]. \tag{4}$$

Theorem 1 (see [23]) *Assume that $\sum_1^m \mu_\ell \geq \sum_1^n h_\ell$. The hashing power game with risk-neutral miners* (4) *admits the following unique NE*

$$x_{ij}^* = \frac{\mu_j}{\sum_1^m \mu_\ell} \cdot h_i, \quad \forall i \in N,\ \forall j \in M,$$

along with each miner i's expected profit

$$\mathbb{E}_R[\pi_i(x^*)] = \frac{h_i}{\sum_1^n h_\ell} \cdot \sum_1^m \mu_\ell - h_i = h_i \frac{\sum_1^m \mu_\ell - \sum_1^n h_\ell}{\sum_1^n h_\ell}, \quad \forall i \in N.$$

This result was obtained in our conference proceedings[23]. However the proof therein contains some errors. In this journal version we corrected all errors and include the full proof of Theorem 1 in the appendix.

5 Game with a Risk-free Asset

The main contribution of this work is to include a risk-free asset. When miners have the option to allocate their funds to both mining and the risk-free asset, the NE for the miners game can be obtained by solving the following n optimization problems based on (3): For any given $i \in N$,

$$\max_{x_{i\cdot}\in\mathbb{R}^m_+} \left[\mu^{\mathrm{T}} y_i(x) - h_i + (1+r)x_{i0} : \sum_{j\in M} x_{ij} + x_{i0} = h_i \right]. \tag{5}$$

Let $\bar{h}_i = h_i - x_{i0}$. This problem is equivalent to the following parametric problem:

$$\max_{0\le\bar{h}_i\le h_i} \max_{x_{i\cdot}\in\mathbb{R}^m_+} \left[\mu^{\mathrm{T}} y_i(x) - (1+r)\bar{h}_i + rh_i : \sum_{j\in M} x_{ij} = \bar{h}_i \right]. \tag{6}$$

Using Theorem 1, the last problem is reduced to the following optimization problem

$$\max_{0\le\bar{h}_i\le h_i} \left[\bar{h}_i \frac{\sum_1^m \mu_\ell}{\sum_1^n \bar{h}_\ell} - (1+r)\bar{h}_i \right]. \tag{7}$$

Theorem 2 *Assume that $h_1 \le h_2 \le \cdots \le h_n$. The solution to problem (7) is as follows.*

(i) *If $\frac{\sum_1^{n-1} h_\ell \cdot \sum_1^m u_j}{\left(\sum_1^n h_\ell\right)^2} \ge 1+r$, then $\bar{h}_i = h_i$ for $i = 1, 2, \cdots, n$. This case includes all those miners who spend their entire cash.*

(ii) *If $\frac{n-1}{n^2} \cdot \sum_1^m u_j < (1+r)h_1$, then $\bar{h}_i = \hat{h} = \frac{n-1}{(1+r)n^2}\sum_1^m u_j, i = 1, 2, \cdots, n$. This case includes all those miners who invest the same amount on the cryptocurrencies and invest the remaining amounts into the bond, earning an interest of r, respectively.*

(iii) *Otherwise, there exists an index $1 \le k \le n-1$ such that*

$$\frac{1+r}{\sum_1^m u_j} > \frac{\sum_1^k h_\ell + (n-k-1)h_{k+1}}{\left(\sum_1^k h_\ell + (n-k)h_{k+1}\right)^2} \ge \frac{\sum_1^{k-1} h_\ell + (n-k)h_k}{\left(\sum_1^{k-1} h_\ell + (n-k+1)h_k\right)^2} \ge \frac{1+r}{\sum_1^m u_j}.$$

Find $h_k \le \hat{h} < h_{k+1}$ such that

$$\frac{\sum_1^k h_\ell + (n-k-1)\hat{h}}{\left(\sum_1^k h_\ell + (n-k)\hat{h}\right)^2} = \frac{1+r}{\sum_1^m u_j},$$

then

$$\bar{h}_i = \begin{cases} h_i, & i = 1, 2, \cdots, k, \\ \hat{h}, & i = k+1, k+2, \cdots, n. \end{cases}$$

In this case, miners are divided into two classes: The first class $\{1, 2, \cdots, k\}$ contain those miners who spend their entire cash; and the second class $\{k+1, k+2, \cdots, n\}$ contains all those miners who invest the same amount on the cryptocurrencies and invest the remaining amounts into the bond, earning an interest of r, respectively.

The hashing power game with a risk-free asset (5) *admits the following unique NE*

$$x_{ij}^* = \begin{cases} \dfrac{\mu_j}{\sum_1^m \mu_\ell} \cdot \bar{h}_i, & \forall i \in N, \quad \forall j \in M, \\ h_i - \bar{h}_i, & \forall i \in N, \quad j = 0. \end{cases}$$

along with each miner i's expected payoff

$$\mathbb{E}_R[\pi_i(x^*)] = \frac{\bar{h}_i}{\sum_1^n \bar{h}_\ell} \cdot \sum_1^m \mu_\ell - (1+r)\bar{h}_i + rh_i = \bar{h}_i \frac{\sum_1^m \mu_\ell - (1+r)\sum_1^n \bar{h}_\ell}{\sum_1^n \bar{h}_\ell} + rh_i, \quad \forall i \in N.$$

Proof Let $f_i(\bar{h}_i) = \bar{h}_i \frac{\sum_1^m \mu_\ell}{\sum_1^n \bar{h}_\ell} - (1+r)\bar{h}_i$, then $f_i'(\bar{h}_i) = \frac{(\sum_1^n \bar{h}_\ell - \bar{h}_i)}{(\sum_1^n \bar{h}_\ell)^2} \cdot \sum_1^m \mu_\ell - (1+r)$. If $\frac{\sum_1^{n-1} h_\ell \cdot \sum_1^m u_j}{\left(\sum_1^n h_\ell\right)^2} \geq 1+r$, then $f_i'(\bar{h}_i) \geq 0$ at $\bar{h}_i = h_i$ for $i = 1, 2, \cdots, n$, so the solution to (7) is $\bar{h}_i = h_i$ for $i = 1, 2, \cdots, n$. Otherwise, some or all $\bar{h}_i = \hat{h}$ at the solution (7) so that $f_i'(\bar{h}_i) \geq 0$ for $i = 1, 2, \cdots, n$. The conclusion is obtained.

We make the following observations based on Theorem 2:

1) At the NE, the return keeps the same for all miners, that is, $\frac{\sum_1^m \mu_\ell}{\sum_1^n h_\ell} - (1+r)$.

2) At the NE, the marginal profit $f_i'(\bar{h}_i) = \frac{(\sum_1^n \bar{h}_\ell - \bar{h}_i)}{(\sum_1^n \bar{h}_\ell)^2} \cdot \sum_1^m \mu_\ell - (1+r)$ is larger for miner i with smaller $\bar{h}_i$.

3) Miner i's expected profit $\frac{\bar{h}_i}{\sum_1^n \bar{h}_\ell} \cdot \sum_1^m \mu_\ell - (1+r)\bar{h}_i + rh_i$ includes two parts. Part rh_i is the risk-free return for h_i. Part $\frac{\bar{h}_i}{\sum_1^n \bar{h}_\ell} \cdot \sum_1^m \mu_\ell - (1+r)\bar{h}_i$ is the excess return.

4) The total social welfare is increasing. The rate of increasing is larger than r.

6 Conclusion

Many future research problems are worth pursuing, such as the risk-averse miners and dynamic versions of the game.

References

[1] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system, 2008.

[2] Saleh F. Blockchain without waste: Proof-of-stake, 2017.

[3] Roger W. The Science of the Blockchain. Inverted Forest Publishing, 2016.

[4] Biais B, Bisiere C, Bouvard M, et al. The blockchain folk theorem. The Review of Financial Studies, 2019, 32(5): 1662–1715.

[5] Carlsten M, Kalodner H, Weinberg S M, et al. On the instability of bitcoin without the block reward. Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, 2016: 154–167.

[6] Eyal I, Sirer E G. Majority is not enough: Bitcoin mining is vulnerable. Christin N, Safavi-Naini R. Financial Cryptography and Data Security. Berlin, Heidelberg: Springer, 2014: 436–454.

[7] Göbel J, Keeler H P, Krzesinski A E, et al. Bitcoin blockchain dynamics: The selfish-mine strategy in the presence of propagation delay. Performance Evaluation, 2016, 104: 23–41.

[8] Kiayias A, Koutsoupias E, Kyropoulou M, et al. Blockchain mining games. Proceedings of the 2016 ACM Conference on Economics and Computation, 2016: 365–382.

[9] Eyal I. The miner's dilemma. 2015 IEEE Symposium on Security and Privacy (SP), 2015: 89–103.

[10] Fisch B A, Pass R, Shelat A. Socially optimal mining pools. arXiv preprint arXiv: 1703.03846, 2017.

[11] Parham R. The predictable cost of bitcoin. SSRN Electronic Journal, 2017.
[12] Rosenfeld M. Analysis of bitcoin pooled mining reward systems. arXiv preprint arXiv: 1112.4980, 2011.
[13] Dimitri N. Bitcoin mining as a contest. Ledger, 2017, 2(1): 31–37.
[14] Liu Z, Luong N C, Wang W, et al. A survey on applications of game theory in blockchain. arXiv preprint arXiv: 1902.10865, 2019.
[15] Alpern S, Howard J. Winner-take-all games: The strategic optimisation of rank. Operations Research, 2017, 65(5): 1165–1176.
[16] Hart S. Discrete colonel blotto and general lotto games. Int J Game Theory, 2008, 36: 441–460.
[17] Goldberg L A, Goldberg P W, Krysta P, et al. Ranking games that have competitiveness-based strategies. Theoret. Comput. Sci., 2013, 476: 24–37.
[18] Roberson B. The colonel blotto game. Economic Theory, 2006, 29: 1–24.
[19] Markowitz H. Portfolio selection: Efficient diversification of investments. Cowles Foundation monograph NO. 16. New York: John Wiley & Sons, Inc, 1959.
[20] Mas-Colell A, Whinston M D, Green J R, et al. Microeconomic Theory, volume 1. Oxford University Press, New York, 1995.
[21] Nisan N, Roughgarden T, Tardos E, et al. Algorithmic Game Theory Cambridge University Press. Cambridge, UK: Cambridge University Press, 2007.
[22] Bonneau J, Miller A, Clark J, et al. Sok: Research perspectives and challenges for bitcoin and cryptocurrencies. 2015 IEEE Symposium on Security and Privacy (SP), 2015: 104–121.
[23] Cheng Y, Du D, Han Q. A hashing power allocation game in cryptocurrencies. International Symposium on Algorithmic Game Theory, 2018: 226–238.
[24] Rosen J. Existence and uniqueness of equilibrium points for concave n-person games. Econometrica, 1965, 3(3): 520–534.

Appendix

Proof of Theorem 1

By the definition of Nash equilibrium, the computing power allocation profile $\boldsymbol{x} = (x_1, x_2, \cdots, x_n)$ is an NE if and only if each miner's allocation is the best response to the others. Let us denote $y^j_{-i} = \sum_{l \neq i} x_{lj}$. Then the best response of miner i is just the solution of the following optimization problem:

$$\begin{aligned} \max \ & U_i(x_{i1}, x_{i2}, \cdots, x_{im}) = \sum_{j \in M} \frac{x_{ij}}{x_{ij} + y^j_{-i}} \mu_j \\ \text{s.t.} \ & \sum_{j \in M} x_{ij} = h_i, \\ & x_{ij} \geq 0. \end{aligned} \tag{8}$$

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 directly in [24] to study Nash equilibrium. We first propose the following lemma to characterize an Nash equilibrium by pointing out that any Nash equilibrium could not be the discontinuous points.

Lemma 1 *If allocation $\boldsymbol{x}$ is an NE, then $\sum_{i \in N} x_{ij} > 0$ for each cryptocurrency $j \in M$.*

Proof To obtain this characterization of NE, it is sufficient for us to prove that any allocation profile $\boldsymbol{x}$, in which there is a cryptocurrency $j \in M$ such that $x_{ij} = 0$ for each $i \in N$, cannot be a Nash equilibrium.

W.l.o.g. we assume that $x_{k1} = 0$ for each $k \in N$. Then there must exist another cryptocurrency, say $j = 2$, with $x_{i2} > 0$ for miner i. That is, the allocation of miner i is

$\boldsymbol{x}_i = (0, x_{i2}, x_{i3}, \cdots, x_{im})$. Let us consider another allocation $\boldsymbol{x}'_i$, with $x'_{i1} = \epsilon$, $x'_{i2} = x_{i2} - \epsilon$ and $x'_{ij} = x_{ij}$ for each $j = 3, 4, \cdots, m$, in which

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

On one hand, allocation $\boldsymbol{x}'_i$ is feasible if $0 < \epsilon < x_{i2}$. On the other hand, if other miners remain their allocations unchanged and miner i reallocate his computing power as $\boldsymbol{x}'_i$ 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 $\boldsymbol{x}$ in which for some $j \in M$, $x_{ij} = 0$ for each $i \in N$, is not a Nash equilibrium.

Obviously, given the other miners' allocation profile $\boldsymbol{x}_{-i}$, utility function U_i is concave and the domain $\{(x_{i1}, x_{i2}, \cdots, x_{im}) | \sum_1^m x_{ij} = h_i, x_{ij} \geq 0\}$ is convex and compact. Therefore, the optimal solution of (8) is the KKT point. By the first-order optimality condition, there exists a Lagrange multiplier α_i such that

$$\frac{\partial U_i}{\partial x_{ij}} = \frac{\sum_{h\neq i} x_{hj}}{(\sum_{h=1}^n x_{hj})^2} \cdot \mu_j \begin{cases} = \alpha_i, & \text{if } x_{ij} > 0, \\ \leq \alpha_i, & \text{if } x_{ij} = 0. \end{cases} \tag{9}$$

Intuitively, at an equilibrium, each miner has the same marginal value on cryptocurrencies which they place positive allocation to and has lower marginal values on those cryptocurrencies that they do not assign computing power.

We first prove that each element of the Nash equilibrium solution which satisfies KKT condition (9) is positive. Given an allocation, let $Y_j = \sum_{i=1}^n x_{ij}$, $1, 2, \cdots, m$, for convenience.

Lemma 2 *If $\boldsymbol{x}$ is the NE solution of* (8) *which satisfies KKT condition* (9)*, then $x_{ij} > 0$ for each $i \in N$ and $j \in M$.*

Proof We will prove the correctness of this lemma by supposing to the contrary that there is at least one zero element in $\boldsymbol{x}$. Then we try to drive the contradiction by distinguishing following two cases.

Case 1 There is only one miner, say miner 1, whose allocation profile has at least one element equal to zero.

Without loss of generality, assume $x_{11} = 0$. Of course, his allocation profile must has at least one positive element, say $x_{12} > 0$. At this time, the number of miners must be greater than or equal to 3. Otherwise, if there are only two miners, then miner 2 can obtain the whole reward of cryptocurrency 1, even though he only allocates arbitrarily small and positive computing power. Therefore the fact of no lower limit to his allocation, results in the nonexistence of the NE. So there are at least 3 miners in the game.

Based on the condition that there is only one miner having zero element, it is obvious that $x_{i1} > 0$ and $x_{i2} > 0$ for each $i = 2, 3 \cdots, n$. Obviously, $Y_1 = \sum_{i=2}^{n} x_{i1}$ and $Y_2 = \sum_{i=1}^{n} x_{i2}$. Since $x_{11} = 0$ and $x_{12} > 0$, the KKT condition (9) promises

$$\frac{\mu_1}{Y_1} = \frac{\partial U_1}{\partial x_{11}}\bigg|_{\boldsymbol{x}} \leq \frac{\partial U_1}{\partial x_{12}}\bigg|_{\boldsymbol{x}} = \frac{\mu_2(Y_2 - x_{12})}{Y_2^2}. \tag{10}$$

For each miner $i = 2, 3, \cdots, n$, the following equations are right by the conditions of $x_{i1} > 0$ and $x_{i2} > 0$ and the KKT condition (9),

$$\frac{\mu_1(Y_1 - x_{i1})}{Y_1^2} = \frac{\partial U_i}{\partial x_{i1}}\bigg|_{\boldsymbol{x}} = \frac{\partial U_i}{\partial x_{i2}}\bigg|_{\boldsymbol{x}} = \frac{\mu_2(Y_2 - x_{i2})}{Y_2^2}. \tag{11}$$

From (10) and (11), we have

$$\frac{\mu_1}{\mu_2} \leq \frac{Y_2 - x_{12}}{Y_1} \cdot \left(\frac{Y_1}{Y_2}\right)^2, \tag{12}$$

$$\frac{\mu_1}{\mu_2} = \frac{Y_2 - x_{i2}}{Y_1 - x_{i1}} \cdot \left(\frac{Y_1}{Y_2}\right)^2. \tag{13}$$

By combining (12) and (13),

$$\frac{\mu_1}{\mu_2} = \frac{(n-1)Y_2 - \sum_{i=2}^{n} x_{i2}}{(n-1)Y_1 - \sum_{i=2}^{n} x_{i1}} \cdot \left(\frac{Y_1}{Y_2}\right)^2 \leq \frac{Y_2 - x_{12}}{Y_1} \cdot \left(\frac{Y_1}{Y_2}\right)^2. \tag{14}$$

In addition, since $Y_1 = \sum_{i=2}^{n} x_{i1} + x_{11} = \sum_{i=2}^{n} x_{i1}$ and $Y_2 = \sum_{i=1}^{n} x_{i2}$, (14) can be rewritten as

$$\frac{(n-2)Y_2 + x_{12}}{(n-2)Y_1} \leq \frac{Y_2 - x_{12}}{Y_1}. \tag{15}$$

However, the condition of $x_{12} > 0$ shows the inequality in (15) can not hold. It is a contradiction.

Case 2 There are at least two miners in the game, whose allocations have elements equal to zero.

For this case, we first discuss the subcase that there are two miners, say miner 1 and 2, and two crptocurrencies, say crptocurrency 1 and 2, such that $x_{11} = 0$, $x_{12} > 0$ and $x_{21} > 0$, $x_{22} = 0$.

Therefore, by the KKT condition (9), we have

$$\frac{\mu_1}{Y_1} \leq \frac{\mu_2(Y_2 - x_{12})}{Y_2^2}, \tag{16}$$

$$\frac{\mu_2}{Y_2} \leq \frac{\mu_1(Y_1 - x_{21})}{Y_1^2}. \tag{17}$$

Hence, by (16) and (17),

$$\frac{\mu_2(Y_2 - x_{12})}{Y_2^2} \geq \frac{\mu_1}{Y_1} > \frac{\mu_1(Y_1 - x_{21})}{Y_1^2} \geq \frac{\mu_2}{Y_2},$$

which is not right, since $x_{12} > 0$ by assumption.

Next, we will discuss the rest case, in which there are more than be two miners whose allocations have some elements equal to zero. Without loss of generality, assume $x_{11} = 0$. At the same time, miner 1 must also have at least one positive element, say $x_{12} > 0$. Now let us define the miner set as $N' = \{i \in N | x_{i1} > 0\}$. Clearly, $x_{i2} > 0$ for each $i \in N'$. If there is one miner $i \in N'$ having $x_{i2} = 0$, then the previous subcase happens. Thus we have $Y_1 = \sum_{i \in N'} x_{i1}$. Similar to the analysis for Case 1, we can get the followings by KKT condition (9).

$$\frac{\mu_1}{Y_1} \leq \frac{\mu_2(Y_2 - x_{12})}{Y_2^2}, \tag{18}$$

$$\frac{\mu_1(Y_1 - x_{i1})}{Y_1^2} = \frac{\mu_2(Y_2 - x_{i2})}{Y_2^2}, \text{ for each } i \in N'. \tag{19}$$

Therefore,

$$\frac{Y_2 - x_{12}}{Y_1} \cdot \left(\frac{Y_1}{Y_2}\right)^2 \geq \frac{\mu_1}{\mu_2} = \frac{|N'|Y_2 - \sum_{i \in N'} x_{i2}}{|N'|Y_1 - \sum_{i \in N'} x_{i1}} \left(\frac{Y_1}{Y_2}\right)^2.$$

In addition, by the condition of $Y_1 = \sum_{i \in N'} x_{i1}$, we have

$$\frac{Y_2 - x_{12}}{Y_1} \geq \frac{(|N'| - 1)Y_2 + \sum_{i \notin N'} x_{i2}}{(|N'| - 1)Y_1}. \tag{20}$$

Obviously, (20) is not right, because $x_{12} > 0$.

Conveniently, the following corollary can be derived directly from Lemma 2.

Corollary 1 *An allocation $\boldsymbol{x}$ 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*

$$\frac{\sum_{h \neq i} x_{hj}}{(\sum_{h=1}^n x_{hj})^2} \cdot \mu_j = \alpha_i. \tag{21}$$

Proof Since each element of a Nash equilibrium solution is positive by Lemma 2, then KKT condition (9) promises (21) directly.

Based on the sufficient and necessary condition for a Nash equilibrium in Corollary 1, we will prove Theorem 1.

Proof of Theorem 1 We first prove that a hash power allocation profile $\boldsymbol{x} = (x_{ij})$ 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 $j \in M$.

It is not hard to see that once each x_{ij} has the form as $x_{ij} = \frac{\mu_j}{\sum_1^m \mu_\ell} \cdot h_i$, then for any $j \in M$,

$$\frac{\sum_{h \neq i} x_{hj}}{(\sum_{h=1}^n x_{hj})^2} \cdot \mu_j = \frac{\sum_{h=1}^n h_h - h_i}{(\sum_{h=1}^n h_h)^2} \Big(\sum_1^m \mu_\ell \Big),$$

which is irrelevant to the cyprocurrency j and such a ratio can be defined as α_i. Then the allocation $\boldsymbol{x} = (x_{ij})$ with $x_{ij} = \frac{\mu_j}{\sum_1^m \mu_\ell} \cdot h_i$ is a Nash equilibrium by Corollary 1.

On the other hand, Corollary 1 shows 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

$$\sum_{i=1}^{n} \alpha_i = \sum_{i=1}^{n} \frac{\sum_{h\neq i} x_{hj}}{(\sum_{h=1}^{n} x_{hj})^2}\mu_j = \frac{(n-1)\sum_{h=1}^{n} x_{hj}}{(\sum_{h=1}^{n} x_{hj})^2}\mu_j = \frac{n-1}{\sum_{h=1}^{n} x_{hj}}\mu_j. \tag{22}$$

From Equation (22), 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

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

So $\sum_{i=1}^{n} \alpha_i = (n-1) \cdot \frac{\sum_{1}^{m} \mu_j}{\sum_{i=1}^{n} h_i}$, which is a constant. In addition, from Equation (22), we can get

$$\frac{\sum_{h=1}^{n} x_{hj}}{\mu_j} = \frac{n-1}{\sum_{i=1}^{n} \alpha_i}, \quad \forall j \in M. \tag{23}$$

Then for any $j \in M$,

$$\alpha_i = \frac{\sum_{h\neq i} x_{hj}}{(\sum_{h=1}^{n} x_{hj})^2}\mu_j = \frac{\sum_{h\neq i} x_{hj}}{\mu_j}\left(\frac{\mu_j}{\sum_{h=1}^{n} x_{hj}}\right)^2 = \frac{\sum_{h\neq i} x_{hj}}{\mu_j}\left(\frac{\sum_{i=1}^{n} \alpha_i}{n-1}\right)^2, \tag{24}$$

where the last equality is from (23). Also Equation (24) guarantees

$$\frac{\sum_{h\neq i} x_{hj}}{\mu_j} = \frac{(n-1)^2\alpha_i}{(\sum_{i=1}^{n} \alpha_i)^2}. \tag{25}$$

Furthermore, the difference between (23) and (25) is

$$\frac{x_{ij}}{\mu_j} = \frac{n-1}{\sum_{i=1}^{n} \alpha_i} - \frac{(n-1)^2\alpha_i}{(\sum_{i=1}^{n} \alpha_i)^2}. \tag{26}$$

Since $\sum_{i=1}^{n} \alpha_i = (n-1) \cdot \frac{\sum_{1}^{m} \mu_j}{\sum_{i=1}^{n} h_i}$ is a constant, the right side of (26) is only related to index i, denote it by γ_i. Then $x_{ij} = \gamma_i \mu_j$. By the condition of $\sum_{j=1}^{m} x_{ij} = h_i$, we have

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

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

Based on the necessary and sufficient condition of NE, and the formation of each miner's expected payoff without a risk-free asset (3), we can get each miner i's expected payoff which is $h_i \cdot \frac{\sum_{1}^{m} \mu_\ell}{\sum_{1}^{n} h_\ell} - h_i$.