Moral Hazard in Games of Miners (Short Paper)

Jingchang Sun
sunjc16@mails.tsinghua.edu.cn
Tsinghua University

Yulong Zeng
yulong.zeng@asresearch.io
ASResearch

ABSTRACT

Cryptocurrency mining, which has attracted substantial attention recently, is a game where miners cost mining power and compete for an amount of digital token. In this paper, we revisit this game under new settings that miners' maximal mining powers, i.e. capacities, are disparate. We show it has a unique pure Nash-equilibrium and derive the closed-form. In the PNE, miners fall into two types: half-hearted and all-out, the former of which owns more capacity than the latter. An all-out miner mines with her full capacity while a half-hearted miner does not. Compared with the desired equilibrium that every miner does her best, our result reveals that the disparity of capacity leads to less total mining power, compromising the security of cryptocurrency systems.

CCS CONCEPTS

• **Computing methodologies** → **Multi-agent systems**; • **Theory of computation** → *Exact and approximate computation of equilibria*; • **Applied computing** → Digital cash.

KEYWORDS

Cournot game, mining, proof-of-work, Blockchain, Bitcoin

ACM Reference Format:
Jingchang Sun and Yulong Zeng. 2019. Moral Hazard in Games of Miners (Short Paper). In *First International Conference on Distributed Artificial Intelligence (DAI '19), October 13–15, 2019, Beijing, China.* ACM, New York, NY, USA, 2 pages. https://doi.org/10.1145/3356464.3358747

1 INTRODUCTION

Since the birth of Bitcoin [18] in 2008, the blockchain-based cryptocurrency has emerged as a popular class of asset.

Most cryptocurrencies relies on the Proof-of-Work (PoW) protocol, which demands the participants, i.e. miners, consume mining power, i.e. hashrate, and allocates some digital token to them as reward. For all miners, the total reward is fixed, e.g. 12.5 for Bitcoin in practice. For each miner, the expected reward is proportional to her hashrate out of all miners', due to the nature of mining process [4], while the cost is proportional only to her own hashrate, since an amount of electricity must be burned for each unit of hashrate.

However, PoW faces severe inequality problem — miners' hashrate distribution has become increasingly disparate over the past decade [3, 7, 15, 20], which reflects that the maximal hashrates, i.e. capacities, of miners, meanwhile, are also significantly unequal. This challenges conventional models where all miners have sufficiently high capacities and invest same hashrate [4]. As a consequence, it is worth revisiting the following questions: 1) should a miner mine with full capacity or leave some capacity idle? and 2) should miners behave in the same way, despite their difference in capacity?

In order to deal with the above concern, we propose a proportional allocation game (PAG) [10] and assume every miner owns different capacity. We analyze its pure Nash-equilibrium (PNE) and compare it with other models'.

Our main contribution is to show the game has a unique PNE as well as deriving its closed-form, which suggests not all miners need to exhaust the capacity, and not all miners act in the same way. There are two kinds of miners: half-hearted and all-out, the former of which has more capacity than the latter. Only all-out miners use their capacities up, and only half-hearted miners invest the same hashrate. Not desired by conventional models, this PNE reduces the total hashrate and leads to a less secure cryptocurrency.

2 RELATED WORK

There are quite a few game-theoretic topics on cryptocurrency mining (see [1, 8, 12, 13, 16, 17, 22]) , a most basic of which is how much hashrate a miner should invest. Chiu et al. [4] and Pagnotta [19] use a simple symmetric Cournot game to study this problem. They assert each miner invests same hashrate in the equilibrium. With similar setting, Dimitri [5] and Arnosti and Weinberg [2] introduce different marginal cost of miners. However, both models rely on non-binding capacity. We, instead, take asymmetrically binding capacity into consideration.

Our model is a variation of PAG, whose basic model comes from Kelly [11]. As seminal works, Johari and Tsitsiklis [10] and Johari [9] study the price of anarchy [14]. Then Tang et al. [21] provide the closed-form PNE with a reserved price. Note they take the valuation of resource as users' type, while we take capacity as type and all miners have same valuation, since they can sell the token reward at the same price in exchanges. Feldman et al. [6] assume users have limited capacity but must spend every penny. On the contrary, our model does not force them to use the capacity up. To the best of our knowledge, we are the first to analyze PAG with retainable capacity and derive its closed-form PNE.

3 MODEL

We formalize *mining game* as a proportional allocation game with complete information, where n self-interested price-anticipating miners compete for reward R.

For miner i the capacity is c_i. Without losing generality, miners indices are sorted descendingly by capacity, i.e. $c_1 \geq c_2 \geq \cdots \geq c_n$.

Generally, $n \geq 2, R > 0$ and $c_n > 0$.

DAI '19, October 13–15, 2019, Beijing, China

ACM ISBN 978-1-4503-7656-3/19/10…$15.00
https://doi.org/10.1145/3356464.3358747

The hashrate of miner i is h_i, with $h_i \in [0, c_i]$. If $h_i = c_i$, the miner is called *all-out*, otherwise she is called *half-hearted*. The total hashrate except miner i is denoted by h_{-i}.

The utility of miner i is $u_i(h_i, h_{-i}) = \frac{h_i}{h_i+h_{-i}}R - \alpha h_i$, where the first term is the reward and the second is the cost, while α is a constant coefficient representing the electricity fee.

A hashrate profile $(h_1^*, \ldots, h_n^*)$ is a PNE, if and only if for each miner i and any $h_i' \in [0, c_i]$, it holds $u_i(h_i^*, h_{-i}^*) \geq u_i(h_i', h_{-i}^*)$, where $h_{-i}^* = \sum_{j\in[n]\wedge j\neq i} h_j^*$.

4 CLOSED FORM PURE NASH-EQUILIBRIUM

4.1 PNE with Non-binding Capacity

We introduce a symmetric result which has been widely desired as follows. Recall the conventional models where miners' capacities are sufficiently high, every miner's hashrate is $\frac{n-1}{n^2}\frac{R}{\alpha}$ (see formula 5 of [4]). Note we can assume the capacity is exactly $\frac{n-1}{n^2}\frac{R}{\alpha}$, and then all miners are deemed to do their best, contributing $\frac{n-1}{n}\frac{R}{\alpha}$ as the total hashrate.

4.2 PNE with Binding Capacity

Now we analyze the game when the capacity is not as high as it can be. By Theorem 1, we show the game has a unique pure Nash-equilibrium and derive its closed form. In the PNE, miners with the smallest capacities are all-out, while the remaining richest miners are half-hearted investing the same hashrate, which is more than any all-out miner's.

Theorem 1. *The mining game has a unique PNE, the total hashrate is* S^* *and* $h_i^* = min\{S^* - \frac{\alpha}{R}(S^*)^2, c_i\}$, *where* $S^* = min_{k\in[0,n]}S_k$ *and*

$$S_k = \frac{(k-1)R + \sqrt{4\alpha kR\sum_{j\in[k+1,n]} c_j + (k-1)^2R^2}}{2\alpha k^2}.$$

Specially, $S_0 = \sum_{j\in[n]} c_j$.

Proof. First we figure out the best response of a miner, and then we show the structure of PNE. Given h_{-i}, the best response of miner i should satisfy the first and second order conditions on utility $\frac{du_i}{dh_i} = 0$ and $\frac{d^2u_i}{dh_i^2} < 0$, which yields $h_i = (h_i + h_{-i}) - \frac{\alpha}{R}(h_i + h_{-i})^2$. Consider all miners take their best response and the total hashrate is S^* and since h_i is bounded by c_i, we have $h_i^* = min\{S^* - \frac{\alpha}{R}(S^*)^2, c_i\}$. Suppose the PNE structure is miners $[k]$ invest $S^* - \frac{\alpha}{R}(S^*)^2$ and miners $[k+1, n]$ invest their capacities, it holds that $k(S^* - \frac{\alpha}{R}(S^*)^2) + \sum_{j\in[k+1,n]} c_j = S^*$. Solving that we have $S^* = S_k$. By proving $c_{i+1} \geq (S_{i+1} - \frac{\alpha}{R}S_{i+1}^2) \Leftrightarrow c_{i+1} \geq (S_i - \frac{\alpha}{R}S_i^2) \Leftrightarrow S_i \geq S_{i+1}$ (and the "$\leq$" case)[1], we can show $S_i = min_{k\in[n]}S_k$ is the only S_i such that $S_i - \frac{\alpha}{R}S_i^2 <\in [c_{i+1}, c_i]$, which supports the PNE structure. □

Next we compare the above closed-form PNE with the symmetric result in § 4.1. Suppose $S^* = S_k$, it holds $S_k \leq S_n = \frac{n-1}{n}\frac{R}{\alpha}$, the rightmost side of which is precisely the total hashrate of the symmetric equilibrium. Thus it can be concluded that due to the binding capacity, the total hashrate is reduced, and it is easier for an adversary to control the majority of hashrate, which makes the cryptocurrency system less secure.

[1]For the interest of space, we omit the proof here.

REFERENCES

[1] Colleen Alkalay-Houlihan and Nisarg Shah. 2019. The Pure Price of Anarchy of Pool Block Withholding Attacks in Bitcoin Mining. (2019).
[2] Nick Arnosti and S. Matthew Weinberg. 2018. Bitcoin: A Natural Oligopoly. arXiv:cs.CR/1811.08572
[3] Alireza Beikverdi and JooSeok Song. 2015. Trend of centralization in Bitcoin's distributed network. In *2015 IEEE/ACIS 16th International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD)*. IEEE, 1–6.
[4] Jonathan Chiu, Thorsten Koeppl, et al. 2018. *Incentive compatibility on the blockchain.* Technical Report. Bank of Canada.
[5] Nicola Dimitri. 2017. Bitcoin mining as a contest. *Ledger* 2 (2017), 31–37.
[6] Michal Feldman, Kevin Lai, and Li Zhang. 2005. A price-anticipating resource allocation mechanism for distributed shared clusters. In *Proceedings of the sixth ACM conference on Electronic commerce*. ACM, 127–136.
[7] Adem Efe Gencer, Soumya Basu, Ittay Eyal, Robbert Van Renesse, and Emin Gün Sirer. 2018. Decentralization in bitcoin and ethereum networks. *arXiv preprint arXiv:1801.03998* (2018).
[8] Nicolas Houy. 2016. The Bitcoin Mining Game. *Ledger* 1 (2016), 53–68.
[9] Ramesh Johari. 2007. The price of anarchy and the design of scalable resource allocation mechanisms, Noam Nisan, Tim Roughgarden, Eva Tardos, and Vijay V Vazirani (Eds.). *Algorithmic Game Theory*, 543–568.
[10] Ramesh Johari and John N Tsitsiklis. 2004. Efficiency loss in a network resource allocation game. *Mathematics of Operations Research* 29, 3 (2004), 407–435.
[11] Frank Kelly. 1997. Charging and rate control for elastic traffic. *European transactions on Telecommunications* 8, 1 (1997), 33–37.
[12] Aggelos Kiayias, Elias Koutsoupias, Maria Kyropoulou, and Yiannis Tselekounis. 2016. Blockchain Mining Games. In *Proceedings of the 2016 ACM Conference on Economics and Computation (EC '16)*. ACM, New York, NY, USA, 365–382. https://doi.org/10.1145/2940716.2940773
[13] Elias Koutsoupias, Philip Lazos, Paolo Serafino, and Foluso Ogunlana. 2019. Blockchain Mining Games with Pay Forward. *arXiv preprint arXiv:1905.07397* (2019).
[14] Elias Koutsoupias and Christos Papadimitriou. 1999. Worst-case equilibria. In *Annual Symposium on Theoretical Aspects of Computer Science*. Springer, 404–413.
[15] Yujin Kwon, Jian Liu, Minjeong Kim, Dawn Song, and Yongdae Kim. 2019. Impossibility of Full Decentralization in Permissionless Blockchains. *arXiv preprint arXiv:1905.05158* (2019).
[16] Yoad Lewenberg, Yoram Bachrach, Yonatan Sompolinsky, Aviv Zohar, and Jeffrey S Rosenschein. 2015. Bitcoin mining pools: A cooperative game theoretic analysis. In *Proceedings of the 2015 International Conference on Autonomous Agents and Multiagent Systems*. Citeseer, 919–927.
[17] Francisco J Marmolejo-Cossío, Eric Brigham, Benjamin Sela, and Jonathan Katz. 2019. Competing (Semi)-Selfish Miners in Bitcoin. *arXiv preprint arXiv:1906.04502* (2019).
[18] Satoshi Nakamoto. 2008. Bitcoin: a peer-to-peer electronic cash system.
[19] Emiliano Pagnotta. 2018. Bitcoin as Decentralized Money: Prices, Mining Rewards, and Network Security. *Mining Rewards, and Network Security (October 26, 2018)* (2018).
[20] Matteo Romiti, Aljosha Judmayer, Alexei Zamyatin, and Bernhard Haslhofer. 2019. A Deep Dive into Bitcoin Mining Pools: An Empirical Analysis of Mining Shares. *arXiv preprint arXiv:1905.05999* (2019).
[21] Pingzhong Tang, Yulong Zeng, and Song Zuo. 2017. Fans Economy and All-Pay Auctions with Proportional Allocations.. In *AAAI*. 713–719.
[22] Itay Tsabary and Ittay Eyal. 2018. The gap game. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 713–728.