The Tight Bound for Pure Price of Anarchy in an Extended Miner's Dilemma Game

Extended Abstract

Qian Wang
CFCS, Computer Science Dept.
Peking University
Beijing
charlie@pku.edu.cn

Yurong Chen
CFCS, Computer Science Dept.
Peking University
Beijing
chenyur911@pku.edu.cn

ABSTRACT

Pool block withholding attack, which reduces the effective mining power in the system and leads to potential systemic instability in the blockchain, can be modeled as a non-cooperative game called "the miner's dilemma". However, existing literature on the game-theoretic properties of this attack only gives a preliminary analysis. In this paper, we establish the existence and uniqueness of pure Nash equilibrium for the two-player miner's dilemma. Then we give a tight upper bound 2 for PPoA, which measures how much mining power is wasted in the game. Moreover, we show the uniqueness and the tight bound holds in a more general setting with betrayal assumption. Inspired by the experiments on the games among three mining pools, we conjecture that similar results should hold for the N-player miner's dilemma game ($N \geq 2$).

KEYWORDS

Block Withholding Attack; Nash Equilibrium Analysis; Pure Price of Anarchy

ACM Reference Format:
Qian Wang and Yurong Chen. 2021. The Tight Bound for Pure Price of Anarchy in an Extended Miner's Dilemma Game: Extended Abstract. In *Proc. of the 20th International Conference on Autonomous Agents and Multiagent Systems (AAMAS 2021), Online, May 3–7, 2021*, IFAAMAS, 3 pages.

1 INTRODUCTION

Bitcoin, assumed to be one of the most successful applications of blockchain, has gained considerable attention since its inception in 2008 [5]. Miners in Bitcoin blockchain can get considerable block rewards for being the first one to successfully find the next valid block and broadcast it. Due to fierce competition in Bitcoin system, miners tend to form mining pools to reduce the high variance of mining rewards, with each miner getting the reward proportional to his mining power. To evaluate how much power miners spend, a pool manager will accept blocks with lower difficulty from miners, called "share" or partial solution, as their proof of work. For example, a full solution requires a hash value containing 80 leading '0' bits, which can only be obtained with a very low probability. To estimate miners' contributions, the pool sets a lower threshold—might as well accept values with 60 leading '0' bits as partial solutions.

Proc. of the 20th International Conference on Autonomous Agents and Multiagent Systems (AAMAS 2021), U. Endriss, A. Nowé, F. Dignum, A. Lomuscio (eds.), May 3–7, 2021, Online.

Such open pools are susceptible to the pool block withholding attack [3]. Eyal [3] demonstrated that mining pools have the incentive to infiltrate their own miners into other opponent pools. These infiltrators only submit partial solutions while throw away valid blocks, thus they can share block rewards but make no contribution to block mining. The attack among mining pools can be modeled as a non-cooperative game, where two open mining pools choose the number of mining power to attack each other. Eyal [3] referred this game with two players as "the 2-player miner's dilemma". Alkalay-Houlihan and Shah [1] gave a detailed analysis based on this model. It calculated the pure Nash equilibrium in some special cases and proved that the pure price of anarchy (PPoA), which measures how much mining power is wasted due to the attack, is at most 3 in the general case.

In this paper, we advance this game analysis further by proving the conjecture proposed in Alkalay-Houlihan and Shah [1]. That is, we prove the existence and uniqueness of the Nash equilibrium, and show the tight upper bound of PPoA is 2. Moreover, we actually prove the above results in an extended model, which includes previous model as a special case. Instead of assuming the loyalty of miners as in Eyal [3] and Alkalay-Houlihan and Shah [1], we allow infiltrators to betray for their own interests. Finally, we conduct experiments on the game among three pools, which provide convincing evidence for our conjecture that N-player ($N \geq 2$) miner's dilemma game with betrayal assumption still admits a unique pure Nash equilibrium and PPoA is within $(1, 2]$.

2 MODEL

We consider the game between two mining pools. Each mining pool, as a player, can choose how much mining power will be sent to the other pool as its strategy. We assume the total mining power of the system and the mining power of each pool are fixed. Let m denote the total mining power of the system and let m_i denote the mining power of pool i, $i \in \{1, 2\}$. The values of m, m_1, m_2 should all be positive. We assume other mining power, solo miners or other mining pools, has no interaction with these two pools. We denote this left part of mining power as t and $t = m - m_1 - m_2 \geq 0$. At some steps of analysis, we shall replace m with $m_1 + m_2 + t$ without notice. Let x_i denote the amount of the mining power used by pool i to attack the other, $x_i \in [0, m_i]$. Thus, a pure strategy profile is (x_1, x_2). We only focus on the pure Nash Equilibrium in this work.

The total effective mining power of the system is $m - x_1 - x_2$. The effective mining power of mining pool i is $m_i - x_i$, and the direct reward of pool i from the Bitcoin system, denoted as

$R_i(x_1, x_2)$, is proportional to the fraction of the effective mining power contributed to the system by the pool.

$$R_1(x_1, x_2) = \frac{m_1 - x_1}{m - x_1 - x_2},\ R_2(x_1, x_2) = \frac{m_2 - x_2}{m - x_1 - x_2}.$$

Since Neither pool will infiltrate all the mining power into the opponent pool, we can always assume $m - x_1 - x_2 > 0$ and the above functions are well defined [1, 7].

In addition to direct rewards, each pool will get reward from infiltrating the other pool, which should be the product of the average reward of the other pool and the amount of infiltrating mining power. Let $r_i(x_1, x_2)$ denote the average reward of pool i, $i \in \{1, 2\}$, we have

$$r_1(x_1, x_2) = \frac{R_1(x_1, x_2) + x_1 r_2(x_1, x_2)}{m_1 + x_2},$$
$$r_2(x_1, x_2) = \frac{R_2(x_1, x_2) + x_2 r_1(x_1, x_2)}{m_2 + x_1}.$$

As the mining power of each pool m_i is fixed, maximizing the total reward $m_i r_i(x_1, x_2)$ and maximizing the average reward $r_i(x_1, x_2)$ are equivalent.

Lemma 2.1. *$r_i(x_1, x_2)$ is concave with respect to x_i, $i \in \{1, 2\}$.*

3 UNIQUENESS OF NASH EQUILIBRIUM

By Lemma 2.1 and Glicksberg's Existence Theorem [4], we can prove the existence of pure NE as in Theorem 3.1.

Theorem 3.1 (Existence of Nash equilibrium). *Every two-player miner's dilemma game admits at least one pure Nash equilibrium.*

Now, we distinguish two types of pure NE. One is the non-extreme pure NE with $(x_1^*, x_2^*) \in (0, m_1) \times (0, m_2)$, and the other is the extreme pure NE with $x_1^* \in \{0, m_1\}$ or $x_2^* \in \{0, m_2\}$. For the former, we show there is at most one non-extreme pure NE. For the latter, we show there is at most one extreme pure NE, and if it does, there cannot exist any extreme pure Nash equilibrium [7]. Then, the uniqueness comes naturally as in Theorem 3.2.

Theorem 3.2 (Uniqueness of Nash equilibrium). *Every two-player miner's dilemma game admits a unique pure Nash equilibrium.*

Alkalay-Houlihan and Shah [1] points out another direction for establishing the uniqueness of pure Nash equilibrium, i.e., to leverage the result by Rosen [6], and show that the sufficient conditions they provide are satisfied. Unfortunately, we find counterexamples by numerical experiments.

4 PURE PRICE OF ANARCHY

Pure price of anarchy (PPoA) is a measure of the ratio between the optimal social welfare and the worst social welfare in any pure NE. Following the analysis in Alkalay-Houlihan and Shah [1], we define the social welfare to be effective mining power of these two pools. The optimal mining power is $m_1 + m_2$ when no one attacks and the effective mining power is $m_1 + m_2 - x_1^* - x_2^*$. Note the pure NE is unique, so the pure price of anarchy is

$$\text{PPoA} = \frac{m_1 + m_2}{m_1 + m_2 - x_1^* - x_2^*}.$$

The following theorem gives the tight upper bound of PPoA.

Theorem 4.1 (tight upper bound of PPoA). *In every two-player miner's dilemma game, the pure price of anarchy is at most 2, and equal to 2 if and only if $m_1 = m_2 = \frac{m}{2}$.*

5 BETRAYAL ASSUMPTION

Previous model always assumes the loyalty of infiltrators, however infiltrators may betray the original pool for their own interests. Since full solutions are also counted as shares, if an infiltrator secretly reports full solutions to the opponent pool, he can get more reward from the opponent mining pool and hide the extra reward for himself. Although the extra reward could be negligible, even 0, it is always non-negative, and positive in expectation, so infiltrators do have motives to betray.

Considering that different miners own different moral thresholds and that some miners are not even aware he is an infiltrator [2], not all infiltrators will betray. Here we introduce a betrayal parameter, $p \in [0, 1]$, to represent the percent of betrayal. The effective mining power of pool i attacking the other pool is actually $(1-p)x_i$. Notice the model employed in previous work [1, 3] is a special case of ours when $p = 0$.

Theorem 5.1. *Every two-player miner's dilemma game with betrayal assumption admits a unique pure Nash equilibrium. The pure price of anarchy is at most 2, and equal to 2 if and only if $m_1 = m_2 = \frac{m}{2}$ and $p = 0$.*

For the two-player miner's dilemma game with betrayal assumption, we find the uniqueness of NE and the tight bound of PPoA still hold. Interestingly, the upper bound of PPoA decreases with p as PPoA $\le \frac{2}{1+p}$, but $x_1^* + x_2^* \le \frac{m_1+m_2}{2}$ holds tightly regardless of the value of p. In other words, Allowing miners to betray has no substantial impact on the macro strategy of the mining pool, but can reduce the social loss.

6 N-PLAYER GAME

Since the dimension of strategy profile space increases quadratically w.r.t. the number of players, the problem with more than two pools is much more complicated to analyze theoretically. Having thoroughly studied the case of two players, we focus on the PPoA of N-player miner's dilemma game and set $N = 3$ in our experiments. The results (illustrated in the full paper [7]) show that in most instances, PPoA $\le \frac{3}{2}$, which means $\sum_{i,j} x_{i,j} \le \frac{m_1+m_2+m_3}{3}$. PPoA will exceed $\frac{3}{2}$ only if the mining power of one pool approaches zero. In fact, the 3-player miner's dilemma game degenerates to a 2-player game in this case. Although our experiment only covers a few special settings, it can be intuitively judged that decentralization can help reduce the mining power wasted in the game. We conjecture that the following stronger result should hold.

Conjecture 6.1. *Every N-player ($N \ge 2$) miner's dilemma game with betrayal assumption admits a unique pure Nash equilibrium, and the tight upper bound of pure price of anarchy is 2.*

ACKNOWLEDGMENTS

This work is supported by Science and Technology Innovation 2030 –"The New Generation of Artificial Intelligence" Major Project No.2018AAA0100901, China.

REFERENCES

[1] Colleen Alkalay-Houlihan and Nisarg Shah. 2019. The Pure Price of Anarchy of Pool Block Withholding Attacks in Bitcoin Mining. In *Proceedings of the AAAI Conference on Artificial Intelligence*, Vol. 33. 1724–1731.

[2] Nicolas T Courtois. 2014. On the longest chain rule and programmed self-destruction of crypto currencies. *arXiv preprint arXiv:1405.0534* (2014).

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

[4] Irving L Glicksberg. 1952. A further generalization of the Kakutani fixed point theorem, with application to Nash equilibrium points. *Proc. Amer. Math. Soc.* 3, 1 (1952), 170–174.

[5] Satoshi Nakamoto. 2008. A peer-to-peer electronic cash system. *Bitcoin.–URL: https://bitcoin. org/bitcoin. pdf* (2008).

[6] J Ben Rosen. 1965. Existence and uniqueness of equilibrium points for concave n-person games. *Econometrica: Journal of the Econometric Society* (1965), 520–534.

[7] Qian Wang and Yurong Chen. 2021. The Tight Bound for Pure Price of Anarchy in an Extended Miner's Dilemma Game. *arXiv preprint arXiv:2101.11855* (2021).