Probabilistic Approach towards Mining Pool Selection in Blockchain Networks

Umer Majeed and Choong Seon Hong

Department of Computer Engineering, Kyung Hee University, Yongin, 446-701 Korea
{umermajeed, cshong }@khu.ac.kr

Abstract

Pool mining is the solution to the highly variant reward incentive in solo-mining for blockchain networks. In pool mining, miners collaborate to form mining pools and distribute the earned rewards in accordance with pool policies to reap steady income. In this paper, we consider a paradigm for a new mining enterprise which is seeking amalgamation with one of the existing mining pools. We set the criteria of the highest winning probability with respect to other mining pools after consolidation for such a merger. We formulated our problem, did simulation for a case scenario and selected the optimal mining pool for consolidation.

1. Introduction

Most of public blockchain such as cryptocurrency based blockchain networks rely on PoW-mining for the secure, irreversible and non-temperable recording of transactional data [1]. The ever-growing mining difficulty [2] in bitcoin and ethereum has made PC-mining absurd. Specialized designed hardware such as GPUs and ASICs have been engaged for efficient mining based on their significantly higher hash rate [3]. However, solo-mining using specially designed hardware is also becoming infeasible. Pool mining is a solution to overcome these challenges and thus a source of steady income for miners.

Miners in mining pool coalesce to generate valid proof-of-work before other mining pools. The mining reward is distributed to miners based upon pool policies. Fig.1 shows that the top five mining pools of bitcoin aggregately (As of April 2019) contribute 65% of total bitcoin network hash-rate.

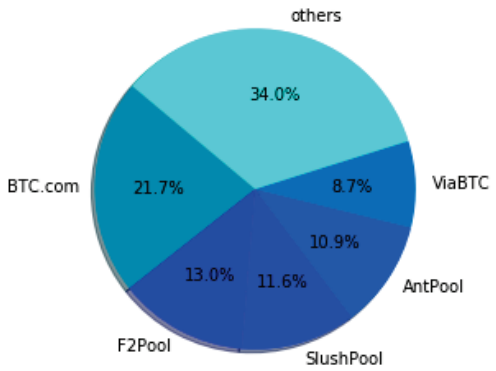

Figure 1: Bitcoin Pool distribution [4]

In this paper, we consider a scenario in which a new mining enterprise having significant hash rate want to enter the blockchain mining economy for a particular cryptocurrency e.g. bitcoin. It is foreseen that the mining enterprise alone cannot make enough profit. So, the mining enterprise has to select one of the existing mining pools for consolidation. We intercept the impact of a new mining enterprise on consequential reward anticipation of current mining pools. Finally, based on the probabilistic analysis the mining enterprise selects the mining pool to unify with.

The rest of the document is formulated as follows: In section 2 we have investigated the recent research work directed towards pool mining selection and maximizing the reward earned, in section 3 we have formulated our problem, section 4 gives simulation results, whereas we have concluded our research work in section 5.

2. Recent Advances

With the rising difficulty of solo-mining, pool mining has become popular. In this section, we concisely explored the recent work conducted regarding mining pool selection.

Liu et al. in [5] studied the concerns related to the selection of mining pool for individual miner when the computational power required to join a mining pool is pre-fixed in the policy of mining pools. The study used an evolutionary game to calculate anticipated earnings and based on them the selection of the optimum mining pool is made.

Qin et al. in [6] investigated the challenges faced by

miners while choosing the mining pool. They studied the pool selection based on the reward mechanism of mining pools such as pay-per-share and pay-per-last-N share. They modeled the pool espousing problem as a risk decision problem and explored associated risks.

3. Problem Formulation

We ruminate a blockchain network which employs Proof-of-work as its consensus algorithm. The miners in the blockchain network associate themselves with $\boldsymbol{k}$ mining pools such that the mining capacity profile (hash rate) of mining pools is given by $\boldsymbol{c} = (\boldsymbol{c_1}, \boldsymbol{c_2}, \dots, \boldsymbol{c_k})$. The probability for mining pool $\boldsymbol{i}$ to solve PoW computational puzzle foremostly and winning mining competition is [7]

$$\boldsymbol{P_i^{mine}(c)} = \frac{\boldsymbol{c_i}}{\sum_{j=1}^{k} \boldsymbol{c_j}} \quad (1)$$

The average time it takes to verify and propagate a mined block of size $\boldsymbol{s_i}$ over blockchain network is [5]

$$\boldsymbol{t(s_i)} = \boldsymbol{t_p(s_i)} + \boldsymbol{t_v(s_i)} = \frac{\boldsymbol{s_i}}{\eta \boldsymbol{c}} + \mu \boldsymbol{s_i} = \left(\frac{1}{\eta \boldsymbol{c}} + \mu\right) \boldsymbol{s_i} \quad (2)$$

Where $\boldsymbol{s_i}$ is also referred as mining strategy of pool $\boldsymbol{i}$. The probability of orphaning a valid contestant block on the grounds of propagation delay has Poisson distribution with mean rate $\frac{1}{\tau}$ and is devised as

$$\boldsymbol{P_i^{orphan}(s_i)} = \boldsymbol{1 - e^{-t(s_i)/T} = 1 - e^{-\left(\frac{1}{\eta c} + \mu\right) s_i / T}} \quad (3)$$

The probability of mining pool $\boldsymbol{i}$ to overarch the mining contest with blocksize $\boldsymbol{s_i}$ without orphaning the block is

$$\boldsymbol{P_i^{win}(c, s_i)} = \boldsymbol{1 - P_i^{orphan}(s_i)} \quad (4)$$

$$\boldsymbol{P_i^{win}(c, s_i)} = \frac{\boldsymbol{c_i}}{\sum_{j=1}^{k} \boldsymbol{c_j}} \boldsymbol{e^{-\left(\frac{1}{\eta c} + \mu\right) s_i / T}} \quad (5)$$

Let the new mining enterprise has hash rate $\boldsymbol{x}$. Since, the nodes associated with the afresh mining facility will not only mine new blocks but also take part in the entire consensus process of blockchain network. By inducing the afresh mining enterprise, the network-scale parameter η, average effective channel capacity $\boldsymbol{c}$, the network scale & average verification speed parameter μ changes to $(\eta_o, \boldsymbol{c_o}, \mu_o)$. Now, if the new mining enterprise with hash rate $\boldsymbol{x}$ collaborate with mining pool q, its wining probability becomes

$$\boldsymbol{P_{q,post}^{win}(c, s_i)} = \frac{\boldsymbol{c_q + x}}{\sum_{j=1}^{k} \boldsymbol{c_j + x}} \boldsymbol{e^{-\left(\frac{1}{\eta_o c_o} + \mu_o\right) s_i / T}} \quad (6)$$

For other mining pools $\boldsymbol{q'}$ the winning probability is

$$\boldsymbol{P_{q',post}^{win}(c, s_i)} = \frac{\boldsymbol{c_{q'}}}{\sum_{j=1}^{k} \boldsymbol{c_j + x}} \boldsymbol{e^{-\left(\frac{1}{\eta_o c_o} + \mu_o\right) s_i / T}} \quad (7)$$

Let $\boldsymbol{y_k}$ be the association variable such that

$$\boldsymbol{y_q} = \begin{cases} 1, & if\ x\ consolidate\ with\ mining\ pool\ q \\ 0, & otherwise \end{cases} \quad (8)$$

Then,

$$\boldsymbol{P_{q,post}^{win}(c, s_i) > P_{q',post}^{win}(c, s_i), \forall q' \varepsilon (c - q) \Leftrightarrow y_q = 1} \quad (9)$$

This means that new mining enterprise should only associate it with mining pool **q** if and only if the probability of mining pool **q** winning the competition after the association is greater than winning probability of its opponents. This criteria is rational based on the fact that reward revenue is correlated with numbers of blocks won by a mining pool and hence the winning probability.

4. Simulation Results

In this section, we did numerical calculation to find the mining pool q with which the new mining enterprise will consolidate. We consider 4 mining pools with mining capacity profile (hash rate) of $c = (10,20,15,20)$ With mining strategy profile $s = (60,120,140,100)$. While, the hash rate of new enterprise is x=5. We set $\left(\frac{1}{\eta c} + \mu\right) = 0.05$ and $\left(\frac{1}{\eta_o c_o} + \mu_o\right) = 0.09$. The block generation time is set as T=60.

In Fig.2 (a) the mining probability of pool 2 and 4 are same because of equal mining capacity. However, Fig.2 (b) shows that pool 4 has greater winning probability than pool 2 despite same capacity. This is because of different mining strategy. Fig.2 (c) forbids to consolidate with mining pool 1 as constraint (9) is not satisfied. Fig.2 (e) dismiss amalgamation with mining pool 3 on behalf of constraint (9) again. Both Fig.2 (d) and Fig.2 (f) permit affiliation with mining pool 2 and mining pool 4 respectively as L.H.S of constraint (9) is slaked. However, the empirical analysis shows that winning probability of pool 4 after consolidation is greater than winning probability of pool 2 after consolidation. Thus, according to probabilistic approach, the new mining enterprise should blend with pool 4 to maximize its revenue.

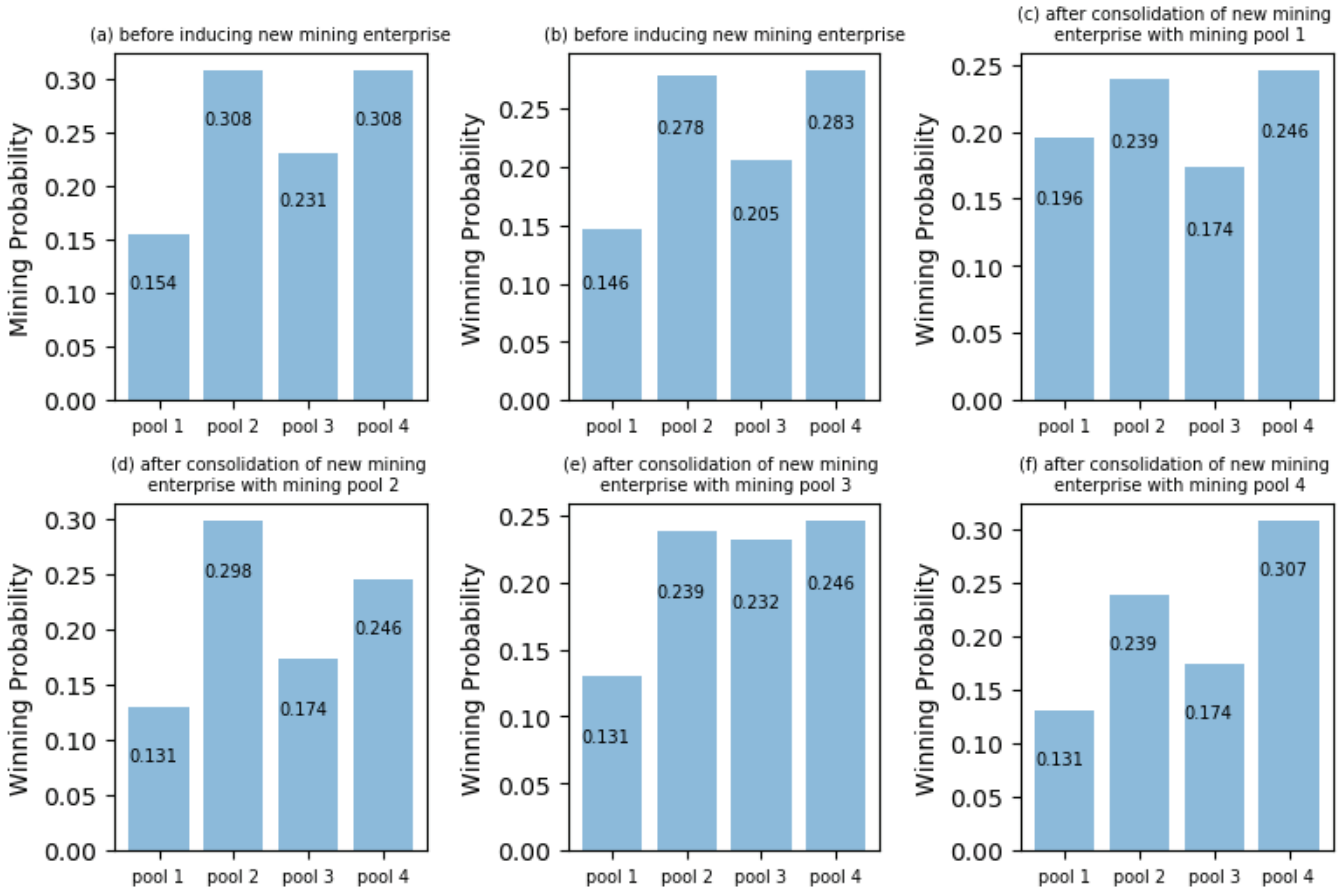

Figure 2: (a) Mining Probability before inducing new mining enterprise, (b) Winning Probability before inducing new mining enterprise, (c-f) Winning Probability after consolidation of new mining enterprise with mining pool 1, 2, 3, 4 respectively

5. Conclusion

Pool mining is the source of invariant income for participating miners. In this paper, we consider the probabilistic approach towards selection of mining pool for new mining enterprise. The limitation of this paper is that it only considers the winning probability for choosing the pool to consolidate with. However, the revenue of pools not only depend upon no of blocks mined but pools also collect revenue from transaction fees which is directly correlated with block size (or mining strategy). In our future work, we will propose more dynamic model for such selection paradigm accommodating aforementioned limitations.

Acknowledgment:

This work was supported by Institute for Information & communications Technology Promotion(IITP) grant funded by the Korea government(MSIT) (No.2015-0-00557, Resilient/Fault-Tolerant Autonomic Networking Based on Physicality, Relationship and Service Semantic of IoT Devices) *Dr. CS Hong is the corresponding author.

[REFERENCES]

[1] Jiao, Yutao, et al. "Auction mechanisms in cloud/fog computing resource allocation for public blockchain networks." *IEEE Transactions on Parallel and Distributed Systems* (2019).

[2] Majeed, Umer, and Choong Seon Hong. "On the Proof-of-Work Puzzle Hardness in Bitcoin Blockchain." Proc. of the Korean Information Science Society (2018): 1348-1350.

[3] Cho, Hyungmin. "ASIC-resistance of multi-hash proof-of-work mechanisms for blockchain consensus protocols." *IEEE Access* 6 (2018): 66210-66222.

[4] Data collected from “Bitcoin Pool distribution” (accessed on 18 April 2019). [Online]. Available: https://btc.com/stats/pool?pool_mode=day.

[5] Liu, Xiaojun, et al. "Evolutionary game for mining pool selection in blockchain networks." *IEEE Wireless Communications Letters* 7.5 (2018): 760-763.

[6] Qin, Rui, Yong Yuan, and Fei-Yue Wang. "Research on the selection strategies of blockchain mining pools." *IEEE Transactions on Computational Social Systems* 99 (2018): 1-10.

[7] Tschorsch, Florian, and Björn Scheuermann. "Bitcoin and beyond: A technical survey on decentralized digital currencies." *IEEE Communications Surveys & Tutorials* 18.3 (2016): 2084-2123.