ISSN 2383-6318(Print) / ISSN 2383-6326(Online)
KIISE Transactions on Computing Practices, Vol. 26, No. 6, pp. 280-285, 2020. 6
https://doi.org/10.5626/KTCP.2020.26.6.280

블록체인 네트워크에서 마이닝 풀 선택에 대한 확률적 접근

(Mining Pool Selection Strategy in Blockchain Networks: A Probabilistic Approach)

우머 마지드 † 김 기 태 † 홍 충 선 ††
(Umer Majeed) (Kitae Kim) (Choong Seon Hong)

요 약 풀 마이닝은 블록 체인 네트워크에 대한 솔로 마이닝에서 매우 다양한 보상에 대한 솔루션이며 풀 마이닝 에서 채굴자들은 마이닝 풀을 형성하고 꾸준한 보상 획득을 위하여 얻은 보상을 풀 정책에 따라 분배한다. 본 논문에서는 기존의 채굴 풀 중 하나와의 합동을 추구하는 새로운 마이닝 패러다임을 제안한다. 이러한 마이닝 풀 간 합병을 위하여 후보 마이닝 풀 중 가장 높은 승리 확률에 대한 기준을 설정하였으며 새로운 마이닝 엔터프라이즈와 통합하기 위한 마이닝 풀 선택에 대한 문제를 공식화하였다. 시나리오를 설정을 통한 시뮬레이션 결과 전파 지연 및 승리 확률에 대해 블록의 크기가 영향을 미치는 것을 확인하였으며 승리 확률과 경험적 분석을 기반으로 새로운 통합을 위한 최적의 마이닝 풀을 선택하였다.

키워드: 블록체인, 마이닝 풀 선택, 풀 마이닝, 확률적 접근, 승리 확률

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 earn a steady income. In this paper, we considered a paradigm for a new mining enterprise seeking amalgamation with one of the existing mining pools. We set the criteria of the highest winning probability with respect to other mining pools for such a merger. We formulated our problem for the selection of a mining pool for consolidation with the new mining enterprise. The simulation for a case scenario shows the influence of block size on propagation delay and winning probability. Finally, we selected the optimal mining pool for consolidation with the new mining enterprise based on winning probability and empirical analysis.

Keywords: blockchain, mining pool selection, pool mining, probabilistic approach, winning probability

· This research was supported by the MSIT(Ministry of Science and ICT), Korea, under the Grand Information Technology Research Center support program(IITP-2020-1711103234) supervised by the IITP(Institute for Information & communications Technology Planning & Evaluation)
· 이 논문은 2019 한국컴퓨터종합학술대회에서 'Probabilistic Approach towards Mining Pool Selection in Blockchain Networks'의 제목으로 발표된 논문을 확장한 것임

† 학생회원 : 경희대학교 컴퓨터공학과 학생
umermajeed@khu.ac.kr
glideslope@khu.ac.kr
†† 종신회원 : 경희대학교 컴퓨터공학과 교수(Kyung Hee Univ.)
cshong@khu.ac.kr
(Corresponding author임)

논문접수 : 2019년 9월 16일
(Received 16 September 2019)
논문수정 : 2020년 3월 25일
(Revised 25 March 2020)
심사완료 : 2020년 3월 25일
(Accepted 25 March 2020)

정보과학회 컴퓨팅의 실제 논문지 제26권 제6호(2020. 6)

1. Introduction

Most of the public blockchain network (PBN) such as cryptocurrency-based blockchain networks rely on Proof-of-Work (PoW) based mining as underlying consensus algorithm for the secure, immutable, irreversible and non-forgeable transactional records as well as meta-data [1]. The computational expensiveness of proof of work algorithm is indicated by the mining difficulty metric. With the increase of the global hash rate within a blockchain network, the mining difficulty is increased to maintain network stability [2]. The ever-growing mining difficulty [3] in bitcoin and Ethereum has made PC mining absurd. Specialized designed dedicated hardware such as GPUs and ASICs have been engaged for efficient mining based on their significantly higher hash rate [4]. Solo mining [5] refers to mining alone to compute the target hash by finding suitable nonce value, whereby mining reward for the block is entirely paid to the solo miner. However, solo mining using specially designed hardware is also becoming infeasible and non-profitable due to low winning probability. Pool mining is a solution to overcome these challenges and thus a source of steady income for miners.

Miners in a mining pool coalesce to generate valid proof-of-work before other mining pools. This is done by dividing the task of searching for target hash into smaller sub-task. The sub-tasks are assigned to the miners in proportion to their reported individual hash-rate. The detailed pool mining process in a blockchain network is described in [6]. The mining reward is distributed to miners within a mining pool based upon pool policies by the pool manager. Fig. 1 shows that the top five mining pools of bitcoin aggregately (as of April 2019) contribute 65% of the total bitcoin network hash-rate.

The primary considerations for miners in the mining ecosystem are selection of blockchain-based cryptocurrency network, selection of mining pool, switching between mining pools, leaving a mining pool and even leaving the cryptocurrency network. These decisions are made based on criteria defined by potential reward incentives in terms of mining reward and cryptocurrency market value.

Most of the published work consider revenue maximization from the perspective of individual miner. However, in this study, we consider revenue maximization from the perspective of a mining enterprise that has a significant hash rate, using the probabilistic approach. The contributions of this paper are as follows:

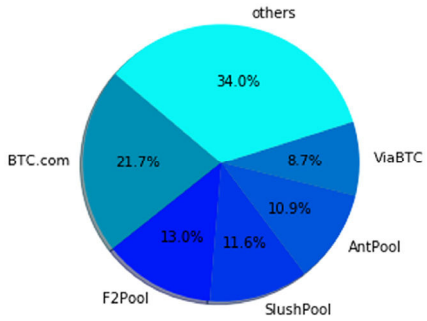

Fig. 1 Bitcoin Pool distribution [7]

- we consider a novel scenario in which a new mining enterprise having a significant hash rate wants to enter the blockchain mining economy for a cryptocurrency e.g. bitcoin. The new mining enterprise will join one of the existing mining pools to maximize its profit.
- We determine the impact of the consolidation of the new mining enterprise on consequential reward anticipation of current mining pools in terms of winning probability.
- Finally, based on the probabilistic and empirical analysis, we selected one of the existing mining pools for the mining enterprise to consolidate 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. Section 3 gives the system model. In section 4 we have formulated our problem, section 5 gives simulation results, whereas we have concluded our research work in section 6.

2. Recent Advances

With the rising difficulty of solo-mining, pool mining has become popular. The joining policy, mining rewards mechanism is divergent among different mining pools. Thus, the fundamental question of which mining pool to choose is faced by the miners within the mining ecosystem of a blockchain

network. In this section, we concisely explored the recent work conducted regarding mining pool selection.

Liu et al. in [8] studied the concerns related to the selection of mining pool for an individual miner when the computational power required to join a mining pool is pre-fixed in the policy of mining pools. The N miners in the network organize to join M mining pools. The study used an evolutionary game for payoff maximization and the final selection of the optimum mining pool is made for each miner through achieved Nash equilibrium. The propagation delay, block size, and hash rate are key parameters affecting the outcome of such mining pool selection.

Qin et al. in [9] 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 proportional mechanism, pay-per-share and pay-per-last-N-shares (PPLNS). They modeled the pool espousing problem as a risk decision problem with maximum-likelihood criterion for optimal mining pool selection and explored associated risks with different reward mechanisms. Finally, the results of computational experiments endorsed that the proposed pool selection strategies perform better than baseline strategies. The results indicate that the value of N for PPLNS has a significant impact on the mining pool selection decision.

Liu et al. in [10] discussed the scenarios for miners to join, switch or leave a mining pool. Authors emphasized that the mining pool's rewards are non-linear due to network delay in the blockchain network, the miners in the pool are incentivized to non-cooperation and may leave a mining pool and join another one for a better payoff. The extensive-form game can model the distribution of miners over time among mining pools.

3. System Model

We ruminate a blockchain network that employs Proof-of-work as its consensus algorithm. The miners in the blockchain network associate themselves with k mining pools such that the mining capacity profile (hash rate) of mining pools is given by $c=(c_1,c_2,\ldots,c_k)$. A new mining enterprise with hash rate x wants to join the blockchain network. It is foreseen that the mining enterprise alone cannot make enough profit. So, the mining enterprise must select one of the existing mining pools for consolidation. In section 4, we will formulate a problem for the selection of one of the existing mining pools based on the maximum winning probability.

4. Problem Formulation

The probability for a mining pool to solve PoW computational puzzle foremostly is called mining probability. The mining probability is proportional to the mining capacity of the mining pool and is given by [11]

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

Once the block is mined, it is broadcasted by the pool manager to the entire blockchain network. The block is then validated by other nodes in the block-chain network. The transmission delay is defined as

$$t_p(s_i)=\frac{s_i}{\eta \hat{c}}, \quad (2)$$

whereby s_i is the block size as per policy of mining pool i, η is the network-scale parameter and $\hat{c}$ is average effective channel capacity.

Once, the broadcasted block is received at relaying nodes, the transactions in the block are validated and the block is verified. The block size is linearly related to the number of transactions within the block. The block verification time for a block is directly pro-portional to the block size and computed as

$$t_v(s_i)=\mu s_i, \quad (3)$$

Where μ is parameter delineated by the verification rate of relaying nodes, and network scale measured in terms of hop counts within the blockchain network.

The propagation delay includes transmission delay and block verification time. The propagation time for a mined block of size s_i over the blockchain network is [8]

$$t(s_i)=t_p(s_i)+t_v(s_i)=\frac{s_i}{\eta \hat{c}}+\mu s_i=\left(\frac{1}{\eta \hat{c}}+\mu\right)s_i. \quad (4)$$

A mined block may not first be able to reach consensus in the blockchain network because of propagation delay. Such a block is discarded and

considered as an orphan. The probability of orphaning [12] a valid contestant block on the grounds of propagation delay has Poisson distribution with mean rate $\frac{1}{T}$ and is devised as

$$P_i^{orphan}(s_i) = 1 - e^{-\frac{t(s_i)}{T}} = 1 - e^{-\left(\frac{(\frac{1}{\hat{\eta c}}+\mu)s_i}{T}\right)}. \quad (5)$$

The probability of mining pool i to overarch the mining contest with block size s_i without subsequently orphaning the block is called winning probability and given as [13]

$$P_i^{win}(c,\ s_i) = P_i^{min\,e}(c)(1 - P_i^{orphan}(s_i)), \quad (6)$$

$$P_i^{win}(c,\ s_i) = \frac{c_i}{\sum_{j=1}^{k} c_j} e^{-\left(\frac{(\frac{1}{\hat{\eta c}}+\mu)s_i}{T}\right)}. \quad (7)$$

Since the block size has a direct effect on winning probability. Each mining pool i makes a policy that it will mine blocks of size s_i and all associated miners comply with the policy. So, s_i is also referred as the mining strategy of pool i. From Eq. 7, only s_i and c_i are different for each mining pool, the rest of the parameters are network defined parameters. So, mining strategy has a significant role in the winning probability of a mining pool.

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

$$P_{q,post}^{win}(c,\ s_i) = \frac{c_q + x}{\sum_{j=1}^{k} c_j + x} e^{-\left(\frac{(\frac{1}{\hat{\eta c}}+\mu)s_i}{T}\right)}. \quad (8)$$

For other mining pools $\acute{q}$, the winning probability is

$$P_{q,post}^{win}(c,\ s_i) = \frac{c_{\acute{q}}}{\sum_{j=1}^{k} c_j + x} e^{-\left(\frac{(\frac{1}{\hat{\eta c}}+\mu)s_i}{T}\right)}. \quad (9)$$

Let y_k be the association variable such that

$$y_q = \begin{cases} 1, \text{if } x \ consolidate \ with mining \ pool \ q \\ 0, otherwise \end{cases} \quad (10)$$

Then,

$$P_{q,post}^{win}(c,\ s_i) > P_{\acute{q},post}^{win}(c,\ s_i), \forall \acute{q} \in (c-q) \Leftrightarrow y_q = 1 \quad (11)$$

This means that the 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 the winning probability of its opponents. This criterion is rational since reward revenue is correlated with the number of blocks won by a mining pool. Further, the number of blocks won by a mining pool is directly proportional to the winning probability of the mining pool.

5. 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 the new enterprise is $x = 5$. We set $\left(\frac{1}{\hat{\eta c}} + \mu\right) = 0.05$ and $\left(\frac{1}{\eta_o \hat{c}_o} + \mu_o\right) = 0.09$. The block generation time is set as $T = 60$.

We compare the propagation delay for the four mining pools before and after the amalgamation of the new mining enterprise. Fig. 2 and Eq. 4 show that the propagation delay is directly correlated with block size but independent of the hash rate of a mining pool.

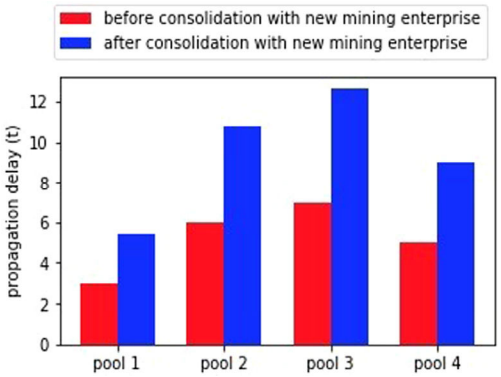

Fig. 2 Propagation delay before and after consolidation with new mining enterprise

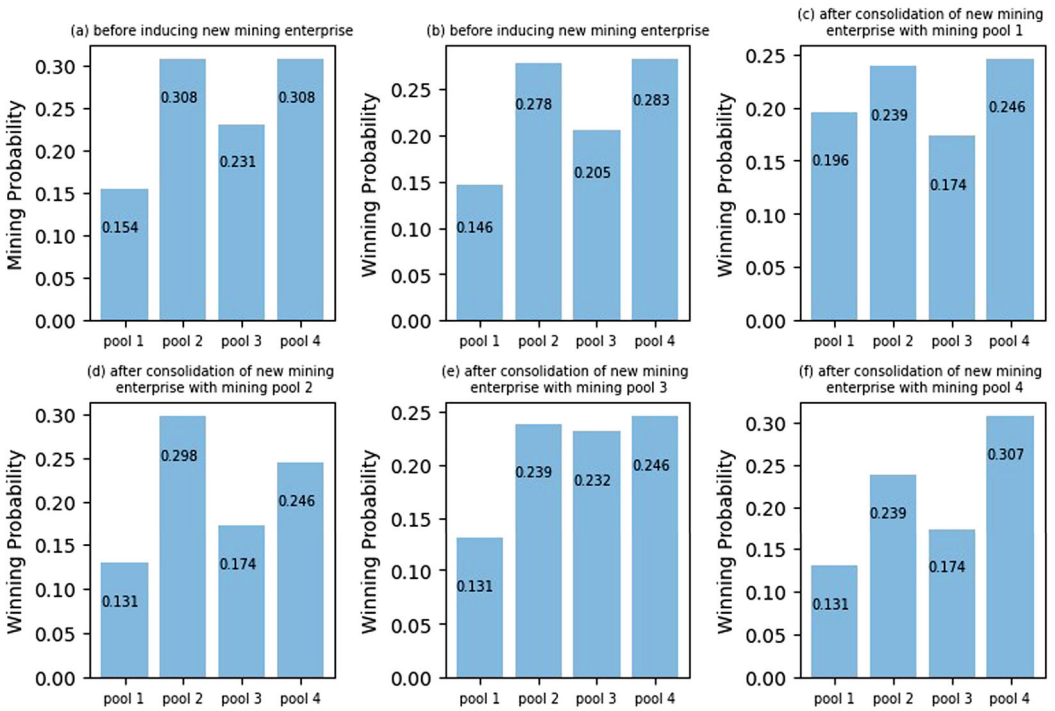

Fig. 3 (a) Mining probability before inducing new mining enterprise, (b) Winning probability before inducing new mining enterprise, (c-f) Winning probability after consolidation of new mining enterprise with mining pools 1, 2, 3, 4 respectively

In Fig. 3(a) the mining probability of pool 2 and 4 are same because of equal mining capacity. However, Fig. 3(b) shows that pool 4 has greater winning probability than pool 2 despite the same mining capacity. This is because of different mining strategies and consequently different propagation delay as indicated in Fig. 2. Fig. 3(c) forbids to consolidate with mining pool 1 as the constraint (11) is not satisfied. Fig. 3(e) dismiss amalgamation with mining pool 3 on behalf of constraint (11) again. Both Fig. 3(d) and Fig. 3 (f) permit affiliation with mining pool 2 and mining pool 4 respectively as L.H.S of constraint (11) is satisfied. However, the comparison and empirical analysis of Fig. 3(d) and Fig. 3(f) shows that the winning probability of pool 4 (after its consolidation with new mining enterprise) is greater than the winning probability of pool 2 (after its consolidation with new mining enterprise). Thus, according to the probabilistic approach, the new mining enterprise should blend with pool 4 to maximize its revenue.

6. Conclusion

Pool mining is the source of stable income for participating miners. In this paper, we consider the probabilistic approach towards the selection of a mining pool for the new mining enterprise. We explored the influence of mining strategy on propagation delay and subsequently on winning probability of a mining pool. 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 depends upon the number 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 a more dynamic model for such a selection paradigm accommodating these limitations.

References

[1] Y. Jiao, P. Wang, D. Niyato and K. Suankaewmanee, "Auction mechanisms in cloud/fog compu-

ting resource allocation for public blockchain networks," *IEEE Transactions on Parallel and Distributed Systems*, Vol. 30, No. 9, pp. 1975-1989, Sept. 2019.
[2] D. Kraft, "Difficulty control for blockchain-based consensus systems," *Peer-to-Peer Networking and Applications*, Vol. 9, No. 2, pp. 397-413, 2016.
[3] U. Majeed, and C. S. Hong, "On the Proof-of-Work Puzzle Hardness in Bitcoin Blockchain," *Proc. of the KIISE Korea Computer Congress 2018*, pp. 1348-1350, 2018.
[4] H. Cho, "ASIC-resistance of multi-hash proof-of-work mechanisms for blockchain consensus protocols," *IEEE Access*, Vol. 6, pp. 66210-66222, 2018.
[5] N. Zhao, H. Wu and Y. Chen, "Coalition Game-based Computation Resource Allocation for Wireless Blockchain Networks," *IEEE Internet of Things Journal*, Vol. 6, No. 5, pp. 8507-8518, 2019.
[6] R. Qin, Y. Yuan, F. Wang, "A novel hybrid share reporting strategy for blockchain miners in PPLNS pools," *Decision Support Systems*, Vol. 118, pp. 91-101, 2019.
[7] "Bitcoin Pool distribution," [Online]. Available: https://btc.com/stats/pool?pool_mode=day (accessed 2019, Apr. 18)
[8] X. Liu, W. Wang, D. Niyato, N. Zhao and P. Wang, "Evolutionary Game for Mining Pool Selection in Blockchain Networks," *IEEE Wireless Communications Letters*, Vol. 7, No. 5, pp. 760-763, 2018.
[9] R. Qin, Y. Yuan and F. Wang, "Research on the Selection Strategies of Blockchain Mining Pools," *IEEE Transactions on Computational Social Systems*, Vol. 5, No. 3, pp. 748- 757, 2018.
[10] Z. Liu, N. C. Luong, W. Wang, D. Niyato, P. Wang, Y. Liang and D. I. Kim, "A Survey on Blockchain: A Game Theoretical Perspective," *IEEE Access*, Vol. 7, pp. 47615-47643, 2019.
[11] F. Tschorsch, and B. Scheuermann, "Bitcoin and beyond: A technical survey on decentralized digital currencies," *IEEE Communications Surveys & Tutorials*, Vol. 18, No. 3, pp. 2084-2123, 2016.
[12] Y. Jiao, P. Wang, D. Niyato and Z. Xiong, "Social Welfare Maximization Auction in Edge Computing Resource Allocation for Mobile Blockchain," *2018 IEEE International Conference on Communications (ICC)*, pp. 1-6, 2018.
[13] W. Wang, D. T. Hoang, P. Hu, Z. Xiong, D. Niyato, P. Wang, Y. Wen and D. I. Kim, "A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks," *IEEE Access*, Vol. 7, pp. 22328-22370, 2019.

Umer Majeed received BS (Hons.) degree in Electrical Engineering from the National University of Science & Technology (NUST), Pakistan in 2015. Since March 2017, he is working towards his Ph.D. in Computer Science and Engineering at Kyung Hee University, South Korea. His research interest includes Blockchain, Mobile Edge Computing, Internet of Things, Machine Learning, and Wireless Networks.

Kitae Kim received the B.S and M.S degrees in Computer Science and Engineering at Kyung Hee University, Seoul, Korea, in 2017 and 2019 respectively. He is currently pursuing the Ph.D degree in the Computer Science and Engineering at Kyung Hee University, Seoul, Korea. His research interest includes SDN/NFV, wireless network, unmanned aerial vehicle communications, and Machine Learning.

홍 충 선
정보과학회 컴퓨팅의 실제 논문지
제 26 권 제 1 호 참조