International Core Journal of Engineering Volume 6 Issue 1, 2020
ISSN: 2414-1895 DOI: 10.6919/ICJE.202001_6(1).0022

Method for Defending Block Withholding Attack

Di jian[1, a], Weihua Lin[1, b]

[1] School of Department of Control and Computer Engineering, North China Electric Power University, Baoding 071003, China;

[a]dijian6880@163.com, [b]linwh01@126.com

Abstract

Block interception is a typical attack method in the blockchain. It enters the mine pool through computational power, but never sends the full workload proof, only the revenue of the mine pool is shared. In response to this problem, this paper first summarizes the typical attacks of blockchains, and analyzes the principle of block interception attacks and the impact on the mine pool. In order to improve the safety of the mine, a special reward for miners that provides a complete proof of work is provided to reduce the expected profit of the attacker. Finally, the relationship between the size of the special reward and the additional income when the attack is launched is analyzed through experiments.

Keywords

Proof of Work, Block withholding attack, Mining pool income.

1. Introduction

A blockchain is a distributed chained data structure in which a complete copy is stored on each node in the network and the entire network information is unified through a consensus algorithm [1-2]. As the most typical application of blockchain technology, Bitcoin uses Proof of Work algorithm to make nodes reach consensus[3]. The main characteristics of the blockchain are decentralization, trust, collective maintenance, safety and non-defective modification[4]. In the Bitcoin system, the node obtains the accounting rights and the corresponding benefits by competing to solve a mathematical problem that can be dynamically adjusted with difficulty. This process is called mining[5]. With the popularity and value of Bitcoin, more and more nodes have joined the Bitcoin network to become miners. In the current Bitcoin system, due to the excessively large computing power, the probability of successful mining of a single node is basically zero, so the miners Usually choose to join the pool to improve the stability of the income[6].

The pool is usually composed of an administrator and a number of miners. The members of the pool cooperate with each other, share the proof of the workload, and receive rewards according to the contribution calculation. Since most of the mines are open, allowing any nodes to join, the mine is vulnerable to attack. Attacks against blockchain can be broadly divided into double-flower attacks, selfish mining, witch attacks, solar eclipse attacks, and block intercept attacks. The block withholding attack was first proposed by Rosenfeld[7]. Eyal researched a mining game in which the attack pool initiated a block interception attack by infiltrating some of its power into other mines[8]. Laszka uses game theory to analyze block interception attacks and demonstrates the long-term viability of attack-to-pool Nash equilibrium in the Bitcoin system[9]. Luu et al studied the benefits that an attacker can gain by initiating a block interception attack in different situations[10]. The above research shows that if two pools or more pools attack each other, the actual income of the honest miners in the pool will be lower than expected.

ISSN: 2414-1895 DOI: 10.6919/ICJE.202001_6(1).0022

In order to improve the safety of the mining pool, this paper reduces the attacker's expected return by giving special rewards to the miners who submit the complete workload proof, thereby reducing their desire to attack and promoting all miners in the mine to adopt honest mining strategies. Through the calculation, the relationship between the special reward size and the attacker's income is obtained, and the threshold for ensuring the safe and stable operation of the mining pool is given.

2. Related work

2.1 Bitcoin mining

With the appreciation of Bitcoin, more and more nodes joined the Bitcoin network to become miners. In order to improve the stability of revenue, miners spontaneously organized to form a mining pool. As shown in Figure 1, Pool1 and Pool2 are two mines in the Bitcoin system. The miners in the pool cooperate with each other to share the proof of workload and earn revenue according to the contribution calculation ratio. Miners can choose to join the mining pool or independently mine in the Bitcoin system.

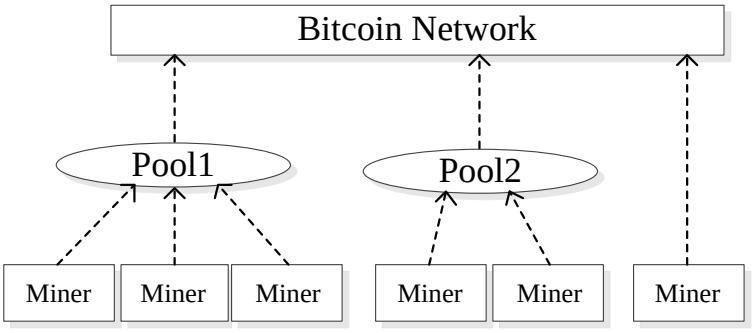

Fig.1 Mining paradigms in bitcoin system

Generally speaking, the total calculation power of the mining pool is far greater than that of the independent miners. Therefore, the probability of successful mining of the mining pool is much greater than the probability of successful mining alone, which can improve the stability of the miners' income. The mining mechanism of the mining pool is: the mining pool contains a centralized control administrator. The administrator generates the task and sends it to the miner. The miner executes the workload proof algorithm and sends the entire workload proof to the administrator. The administrator generates a new block and distributes the income of the mine pool to the member according to the contribution calculation.

2.2 Block withholding attack

A block interception attack is an attack between a miner and a miner in an open mine. The attacker only submits a partial workload certificate to the mine manager and discards it when a full workload proof is found. The workload proof can only be used by the creator of the task. The attacker cannot use the computing power of the block interception attack for other purposes, nor can it obtain any other benefit from this part of the computing power. Therefore, this kind of attack will cause waste of computing power on the one hand, and reduce the income of the mining pool on the other hand. In addition, a small part of the work proves that it will not affect the effective calculation and effective income of the mining pool to a large extent. However, after the miners attack, the effective calculation and effective income of the entire mining pool will be lower than that of all miners during normal mining. The gains earned. The miners who initiated this attack will not make any contribution to the mine, but still get the proceeds[11].

3. Block withholding model

This paper studies a method of defensive block interception attacks, which gives special rewards to miners who submit complete workload proofs, so the gains of the attackers in the mine pool will be reduced. The reward for setting a block is R, and the special reward for miners who successfully

ISSN: 2414-1895 DOI: 10.6919/ICJE.202001_6(1).0022

submits a full workload proof is $tR(0<t<1)$, and the $(1-t)R$ reward is given to the miners in the pool according to the contribution calculation. In order to ensure the stability of the income of the miners, this paper gives the critical value that the attacker can not get more benefits.

Assume that there is only one mine P and one miner A in the current bitcoin network, and their powers are p, α, with $p+\alpha=1$. Miner A infiltrated part $\beta(0<\beta<1)$ of his computing power into the mining pool P.Initiated block interception attack, and the remaining computing power mined alone. When the miners honestly mine, the gains obtained are the proportion of the entire bitcoin network, which is $R_h=\alpha$. When the miners join the mine pool, the honesty mining power in the pool is still $1-\alpha$, but the income is equally distributed to$1-\alpha(1-\beta)$. Therefore, the effective power in the Bitcoin network is $1-\alpha\beta$, so the income earned by miners in independent mining is.

$$R_0=\frac{\alpha(1-\beta)}{1-\alpha\beta} \tag{1}$$

For the mine pool, after the special reward is removed, the income is $\frac{1-\alpha}{1-\alpha\beta}(1-t)R$, and the expected income of the miner in the mine pool is

$$R_1=\frac{1-\alpha}{1-\alpha\beta}(1-t)\times\frac{\alpha\beta}{1-\alpha(1-\beta)} \tag{2}$$

Therefore, the total income of miner A is

$$R=R_0+R_1=\frac{\alpha(1-\beta)(1-\alpha+\alpha\beta)+\alpha\beta(1-t)(1-\alpha)}{(1-\alpha\beta)(1-\alpha+\alpha\beta)} \tag{3}$$

Compare this income with the benefits of honest mining, you can get,

$$\frac{R}{R_h}=\frac{(1-\alpha)(1+\alpha\beta-\alpha)+(1-\alpha)(1-t)\beta}{(1-\alpha\beta)(1+\alpha\beta-\alpha)} \tag{4}$$

Let $\frac{R}{R_h}=1$, get $t=\alpha(1-\beta)$.

When $t>\alpha(1-\beta)$, $\frac{R}{R_h}<1$, there is $R<R_h$.

When $t<\alpha(1-\beta)$, $\frac{R}{R_h}>1$, there is $R>R_h$.

4. Experimental evaluation

This experiment assumes that the calculation power of the mine is greater than the calculation power of miner A, then the calculation power of miner A is $0<\alpha<0.5$,taking $\beta=\{0.1,0.3,0.5,0.7,0.9\}$ and $t=\alpha(1-\beta)$ respectively, and the experimental results are shown in Fig. 2.

As can be seen from the figure, the value of t increases with the increase of α, which means that the greater the power of miner A, in order to make it unable to obtain additional income when it initiates the block interception attack, it is necessary to submit a complete workload. The proof proves that the miners have more special rewards. When α is constant, as β increases, the special rewards for honest miners who need to submit a full proof of work are reduced. Therefore, most of the miners' calculations have penetrated into the pool and never submitted a full proof of work, so it is never possible to receive special rewards.

ISSN: 2414-1895 DOI: 10.6919/ICJE.202001_6(1).0022

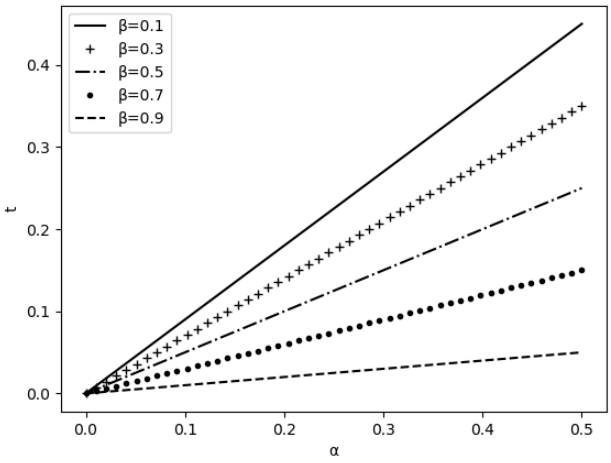

Fig.2 t with α, β change

5. Conclusion

This paper examines the need to reduce the expected benefits of non-honest miners and reduce their desire to attack by providing a special reward for honest miners who submit proof of complete workload, thus providing a guarantee for the safe and stable operation of the mine.

References

[1] Yuan Yong, Wang Feiyue. Blockchain: the state of the art and future trends[J]. Acta Automatica Sinica, 2016, 42(4): 481-494.

[2] Blockchain introduction [Online], available: http:// bravenewcoin. com/assets/Uploads /Transactoins AsProofOfStake10.pdf,December 14, 2015.

[3] Nakamoto S. Bitcoin: a peer-to-peer electronic cash system [EB/OL]. (2008)[2019-5-10]. https://bitcoin.org/bitcoin.pdf.

[4] Zheng Z, Xie S, Dai H, et al.An overview of blockchain technology: Architecture, consensus, and future trends[C]//2017 IEEE International Congress on Big Data, Honolulu, HI, 2017: 557-564.

[5] VILIM M, DUWE H, KUMAR R. Approximate bitcoin mining[C]// Proceedings of the 53rd Annual Design Automation Conference. New York: ACM, 2016: Article No. 97.

[6] LIU Y, CHEN X Y, ZHANG L, et al. An intelligent strategy to gain profit for bitcoin mining pools [C]//Proceedings of the 10th International Symposium on Computational Intelligence and Design. Piscataway, NJ: IEEE, 2017: 427–430.

[7] M. Rosenfeld, Analysis of Bitcoin pooled mining reward systems, arXivpreprint arXiv:1112.4980.

[8] EYAL I. The miner's dilemma [C]// Proceedings of the 2015 IEEE Symposium on Security and Privacy. Piscataway, NJ: IEEE, 2015: 89 – 103.

[9] A. Laszka, B. Johnson, and J. Grossklags, "When bitcoin mining pools run dry," in Financial Cryptography and Data Security: FC 2015 International Workshops, BITCOIN, WAHC, and Wearable. Berlin, Germany: Springer, 2015, pp. 63–77.

[10] L. Luu, R. Saha, I. Parameshwaran, P. Saxena, and A. Hobor, "On power splitting games in distributed computation: The case of bitcoin pooled mining," in Proc. IEEE 28th Comput. Secur. Found. Symp. (CSF), Verona, Italy, Jul. 2015, pp. 397–411.

[11] N. T. Courtois, L. Bahack, On subversive miner strategies and block withholding attack in bitcoin digital currency, arXiv preprintarXiv:1402.1718.