Game Theory in Mining Block

Bo Sun 2001212291

Mengjie Ye 2001212409

Yifan Jiang 2001212347

Yinjie Jiang 1901212596

Yanjie Zong 1901212689

Motivation

The PoW (proof of work) consensus algorithm in the blockchain guarantees the security and reliability of the blockchain system. However, apart from the **cooperative** relationship, **miners can attack each other**, and thus increase their profits. When miners choose to attack, the total profits of the mining pool would decrease. In this case, there is a need for **incentive compatible**, a mechanism that every participant can achieve the best outcome to themselves just by acting according to their true preferences. How to form a consensus among "unorganized" groups (mining pool in block chain) is the classic "**Byzantine Generals Problem**". The following tables show the payoff matrix of three cases. (See reference 1&2)

When there is no reward or penalty:

	Cooperate	Attack
Cooperate	(8,8)	(-2,6)
Attack	(6,-2)	(-1,-1)

Nash Equilibrium: (Cooperate, Cooperate) or (Attack, Attack)

When there is reward (block reward, transaction fee, right to package the block):

	Cooperate	Attack
Cooperate	(11,11)	(1,6)
Attack	(6,1)	(-1,-1)

Nash Equilibrium: (Cooperate, Cooperate)

When there is penalty (cost of mining)

	Cooperate	Attack
Cooperate	(8,8)	(-2,3)
Attack	(3,-2)	(-4,-4)

Nash Equilibrium: (Cooperate, Cooperate)

Undoubtedly, if appropriate incentives and punishment mechanisms are applied at the same time, the security of the system can be more guaranteed. However, there are still some kinds of attack miners or mining pools would implement to obtain more profit for themselves.

1. P + Epsilon Attack

Vitalik Buterin, the founder of Ethereum, proposed an idea call **P + Epsilon Attack** (see reference 1). The idea relies on the assumption that the attacker can credibly commit to something quite crazy. The crazy thing is this: paying out 25.01 (epsilon = 0.01) BTC to all the people who help him in his attack to steal 25 BTC from everyone, but only if the attack fails. This leads to a weird payoff matrix where the dominant strategy is to **help him in the attack. The attack succeeds, and no payoff is made.**

	Cooperate	Attack
Cooperate	(8,8)	(-2, 8+epsilon)

Attack	(8+epsilon,-2)	(-1,-1)

Nash Equilibrium: (Attack, Attack)

2. Block Interception Attack（区块截留攻击）

There two main reasons for this attack (see reference 3):

1) The block chain can adjust the difficulty level to keep one block generating speed. Some miners would like to attack the mining pool, reducing its effective computing power. Then, the block chain would reduce the difficulty level and certain miners can get more profit unit time.
2) The rewards are distributed to each miner according to the proportion of their proof of work. However, it is difficult to generate a full proof of work. Miners who are sneaky and slippery can choose to send partial proof of work to the mining pool to get rewards that can only be obtained by contributing actual computing power.

There are many strategies to face this attack, details can be seen from the reference.

3. Double Spending Attack

In essence, double-spending attack in blockchain is an economic problem. Nodes play a game on **whether to attack or not, and choose the strategy** based on their own revenue maximization. The strategy choice of nodes will also have an impact on each other. Participants can obtain decision-making information not only through their own experience, but also by observing and imitating the decisions of other participants. After continuous learning and adjustment, the node group will eventually reach a balanced state, that is, all nodes in the group choose evolutionary stable strategy. Reference 4 provides a simple scenario to illustrate how to solve the problem by **adjusting the transaction price and transaction cost**.

Objective

Our project aims to simulate different situations during the mining process, and then implement different strategies to see how these mining polices can affect the final reward of the whole system and each mining pool.

3 kinds of game in Bitcoin mining:

1. Forming a mining pool or be an individual miner

There are two cases:

1.1 There is no limit to the size of a mining pool

1.2 There cannot exist a mining pool that has a mining power of more than 50% of the total power.

In each case we will simulate the activity of 10 miners. A miner can choose to form a mining pool with anther miner, or joining an existing mining pool, or just mining by itself. We want to see in the long run, what is the state of the whole system. Is there going to have mining pools? What is the size of mining pools? Will individual miners be forced to quit the game? Besides, we will examine two key factors: the total productivity of the system, and the payoff to each strategy carrying out by miners.

2. Selfish mining

Selfish mining is a strategy for mining bitcoin or other cryptocurrencies in which groups of miners collude to increase their revenue and exert power over a blockchain. "Mining" is the process by which nodes in the blockchains network validate and confirm transacti ons, with miners earning newly minted tokens in return for their computational effort. With selfish mining, the cartel obscures newly created blocks from the main chain, revealing them at a later point in time.

We will simulate the activity of selfish mining in two cases

2.1 There are 10 miners with no mining pools

2.2 There exists a mining pool that has 5 miners, and other 5 miners are mining individually.

We will track the activity of miners in the long run, and see what the state of the whole system is. Is there going to have selfish mining in these two cases? Are mining pools be more likely to do selfish mining than individual miners? We will examine two key factors: the total productivity of the system, and the payoff to each strategy carrying out by miners.

3. Block withholding attack between two mining pools

Block withholding attack 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.

We will simulate the activity of two mining pools, each has 5 miners. Both of them can choose to send some miners to the “competing pool” to do withholding attack. We will examine three things: Is there an equilibrium of the system? What will be the total productivity of the system? And what is the payoff to each mining pools?

References

1. 姚前. 区块链技术的激励相容:基于博弈论的经济分析[J]. 清华金融评论,2018(09):95-100.
2. 宋丽华,李涛,王伊蕾. 博弈论在区块链中的应用研究[J]. 密码学报,2019,6(01):100-111.
3. 杨天,薛质. 区块链系统中矿池间的博弈问题及优化[J]. 通信技术,2019,52(05):1189-1195.
4. 王雷,任南,李保珍. 区块链 51%双花攻击的进化博弈及防控策略研究[J]. 计算机工程与应用,2020,56(03):28-34.

For your better understanding, we provide our reading note here.