# Game Theory in Mining

# 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.

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 attacking miners or mining pools would implement to obtain more profit for themselves.

1. **P+Epsilon Attack**

However, Vitalik Buterin, the founder of Ethereum, proposed an idea call **P+epsilon Attack.** 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 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)**

1. **Block Interception Attack（区块截留攻击）**

There two main reasons for this attack:

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.

**Our goal is to simulate the attack situation 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.**