Motivation: Solving the double-spneding problem from the perspective of game-theory – solving the problem by adjusting the transaction price and transaction cost;

Background: the double-spneding problem refers to the situation that the same digital asset is repeatedly used due to improper operation in the digital currency system due to the replicability of data. In essence, double-spneding 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.

Decision making of participants: participants can obtain decision-making information not only through their own experience, but also by observing and imitating the decisions of other participants. In the blockchain system, all nodes form a node group, and each node has an initial strategy about whether to choose 51% double-spneding attack or not. After that, nodes repeatedly randomly select other nodes from the group to play games. In this process, nodes with low revenue will change their strategy and turn to imitate strategies with high revenue, After such continuous learning and adjustment, the node group will eventually reach a balanced state, that is, all nodes in the group choose evolutionary stable strategy.

The simplest case: the double-spneding problem in the case of two people – two nodes play the game based on whether to carry out 51% double flower attack. The strategy combination includes the following four cases: Si = attack, SJ = attack; Si = attack, SJ = no attack; Si = no attack, SJ = attack; Si does not attack, SJ = does not attack.

Simple scenario description: when I and j choose to attack, the price of an I commodity purchased from a third-party merchant is p, and the transaction fee f is broadcast to the network, and the transaction will be recorded by the mining node on the public chain; Then I send the coin P from the previous transaction (I1) to myself repeatedly, and invest a higher computational cost h to mine in another side chain, and record this transaction (i2) in the side chain. I, as a miner, gets the corresponding transaction cost and new coin reward; After that, I continued to mine on this side chain and got corresponding rewards; J also chooses attack, and chooses the same side chain as I, and the attack process is exactly the same as I. Due to the advantages of I and j in computing power, the length of the side chain eventually exceeds that of the public chain through cooperative mining. The amount P consumed in the first transaction of both sides returns to their own account, and the goods are also in their own hands. Therefore, I and j complete the double flower attack respectively. The income of node i consists of the following parts: the price P obtained in transaction I1, the transaction cost f paid; Transaction fee f paid in transaction I2, transaction fee reward F and new currency reward B obtained through mining, and computing cost h consumed; For other transactions in the network, the reward F + B is obtained by mining, and the computing cost h is consumed.

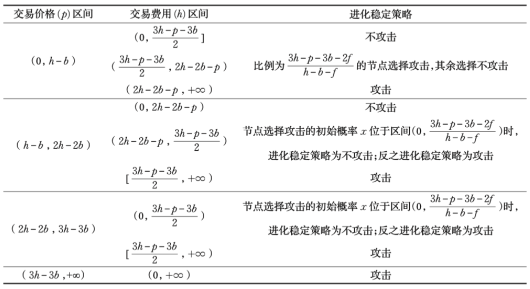
(1) : all attacks: the profit of node I: UI (attack, attack) = P + 2B − 2h, the profit of node j is exactly the same as that of I: UJ (attack, attack) = P + 2B − 2H.

(2) : I attack, J do not attack: UI (attack, do not attack) = P + F + 3B − 3h, the income of node j: UJ (attack, do not attack) = − F.

(3) : I do not attack, J attack: when I choose not to attack, J choose to attack, the situation is just opposite to (2). The profit of node I: UI (no attack, attack) = − F, the profit of node j: UJ (no attack, attack) = P + F + 3B − 3H.

(4) : when I and j choose not to attack, I and j each pay p to buy goods, and after paying the transaction cost F, they are recorded on the public chain. The income of node I: UI (not attack, not attack) = − F, the income of node j: UJ (not attack, not attack) = − F.

表2　节点的进化稳定策略分类情况



交易价格(p)区间	交易费用(h)区间	进化稳定策略
$(0, h-b)$	$(0, \frac{3h-p-3b}{2}]$	不攻击
	$(\frac{3h-p-3b}{2}, 2h-2b-p)$	比例为 $\frac{3h-p-3b-2f}{h-b-f}$ 的节点选择攻击,其余选择不攻击
	$(2h-2b-p, +\infty)$	攻击
$(h-b, 2h-2b)$	$(0, 2h-2b-p)$	不攻击
	$(2h-2b-p, \frac{3h-p-3b}{2})$	节点选择攻击的初始概率 x 位于区间$(0, \frac{3h-p-3b-2f}{h-b-f})$时,进化稳定策略为不攻击;反之进化稳定策略为攻击
	$[\frac{3h-p-3b}{2}, +\infty)$	攻击
$(2h-2b, 3h-3b)$	$(0, \frac{3h-p-3b}{2})$	节点选择攻击的初始概率 x 位于区间$(0, \frac{3h-p-3b-2f}{h-b-f})$时,进化稳定策略为不攻击;反之进化稳定策略为攻击
	$[\frac{3h-p-3b}{2}, +\infty)$	攻击
$(3h-3b, +\infty)$	$(0, +\infty)$	攻击