双花问题是什么：双花问题是指在数字货币系统中，由于数据的可复制性，存在同一笔数字资产因不当操作被重复使用的情况。

作者眼中的双花问题：区块链中的双花攻击在本质上是一个经济问题，节点间关于是否攻击进行博弈，**选择基于自身收益最大化的策略，**节点的策略选择相互之间也会产生影响。本文选择针对双花攻击中破坏力较强的 51%双花攻击，构建了节点群体的进化博弈模型，以揭示节点策略的动态演化趋势，并通过推导进化博弈策略，预测51%双花攻击出现的概率；同时，把交易价格和交易费用作为进化博弈模型中的两个重要变量，探讨变量在取值改变时对博弈结果产生的影响；最后，基于前面得到的结论，本文从交易费用和交易价格两个方面提出51%双花攻击的防控策略。

参与人的决策：参与人既可以通过自己的经验获得决策信息，也 可以通过观察其他参与人的决策并模仿而获得决策信息。在区块链系统中， 所有节点组成一个节点群体，每个节点关于是否选择 51%双花攻击都拥有一个初始策略，之后节点重复从群体中随机选取其他节点进行博弈，在这个过程中采用策略收益较低的节点会改变自己的策略，转向模仿有高收益的策略，而低收益的策略逐渐被淘汰，经过这样不断的学习与调整后节点群体最终会达到一个均衡状态，即群体中的所有节点都选择进化稳定策略。

最简单的情况：双人情况下的双花问题–两个节点基于是否进行 51%双花攻击的问题进行 博弈，策略组合包括以下四种情况：Si =攻击，Sj =攻击；Si=攻击，Sj =不攻击；Si =不攻击，Sj =攻击；Si不攻击， Sj =不攻击。

简单的情景阐述：当 i 和 j 都选择攻击时， 从第三方商家购买某 i 商品价格为 p ，另外支付交易费用 f 广播到网络中，交 易会被挖矿节点记录到公链上；接着 i 重复利用上笔交 易 (i1) 中的币 p 发送给自己，并投入较高的算力成本 h 在另一条侧链中挖矿，将这笔交易 (i2) 记录在侧链中， i 作为矿工获得相应的交易费用与新币奖励；之后 i 继续 在这条侧链上挖矿，并获得相应的奖励；j 也选择攻击， 并且与 i 选择同一条侧链，攻击流程与 i 完全相同。 由 于 i 和 j 在算力方面的优势，最终通过合作挖矿使侧链 的长度超过公链，两者第一笔交易消费的金额 p 都回到 自己账户，商品也在自己手中，因此 i 、j 分别完成双花攻击。节点 i 的收益由以下几部分组成：交易 i1 中获取的 商品价格 p ，支付的交易费用 f ；交易 i2 中支付的交易 费用 f ，通过挖矿获取的交易费用奖励 f 和新币奖励 b ，消耗的算力成本 h ；对网络中的其他交易 k 挖矿获取 的奖励 f + b ，消耗算力成本 h 。

(1): 都攻击：节点 i 的收益：Ui（攻击，攻击）= p + 2b − 2h ， 节点 j 的收益与 i 完全相同：Uj（攻击，攻击）= p + 2b − 2h 。
(2): i攻击，j不攻击：Ui（攻击，不攻击）= p + f + 3b − 3h ，节点 j 的收益：Uj（攻击，不攻击）= − f 。
(3): i不攻击，j攻击：当 i 选择不攻击，j 选择攻击时，情况与（2）正 好相反。节点 i 的收益：Ui（不攻击，攻击）= −f ，节点 j 的 收益：Uj（不攻击，攻击）= p + f + 3b − 3h 。

(4): 当 i 和 j 都选择不攻击时，i 和 j 各支付 p 购买商品，并支付交易费用 f 后被记录到公链上，节点 i 的收益：Ui（不攻击，不攻击）= –f ，节点 j 的收益：Uj（不攻击，不攻击）= –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