区块链51%双花攻击的进化博弈及防控策略研究

王 雷[1],任 南[1],李保珍[2]
1.江苏科技大学 经济管理学院,江苏 镇江 212003
2.南京审计大学 国家审计大数据研究中心,南京 211815

摘 要:双花攻击作为支付领域的一种安全隐患,给区块链系统的正常运行带来了严重影响。针对双花攻击中破坏力较强的51%双花攻击,构建了区块链中51%双花攻击的进化博弈模型,揭示了节点策略的动态演化趋势,并通过推导进化稳定策略,预测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,探究该变量的不同取值对博弈结果的影响规律。仿真实验验证了上述模型的有效性,最后从交易费用和交易价格两个方面提出了51%双花攻击风险防控的策略和建议。

关键词:区块链;51%双花攻击;进化博弈;交易费用;交易价格
文献标志码:A **中图分类号:**TP391.9 doi:10.3778/j.issn.1002-8331.1907-0344

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.计算机工程与应用,2020,56(3):28-34.
WANG Lei, REN Nan, LI Baozhen. Research on evolutionary game and prevention and control strategy of blockchain 51% double spend attack. Computer Engineering and Applications, 2020, 56(3):28-34.

Research on Evolutionary Game and Prevention and Control Strategy of Blockchain 51% Double Spend Attack

WANG Lei[1], REN Nan[1], LI Baozhen[2]
1.College of Economics and Management, Jiangsu University of Science and Technology, Zhenjiang, Jiangsu 212003, China
2.National Audit Big Data Research Center, Nanjing Audit University, Nanjing 211815, China

Abstract: As a security risk in the field of payment, the double spend attack has brought a serious impact on the normal operation of the blockchain system. Aiming at 51% double spend attacks with strong destructive force in double spend attacks, an evolutionary game model of 51% double spend attacks in blockchain is built to reveal the dynamic evolution trend of node strategies, and the probability of 51% double spend attacks is predicted by deducing evolutionary stability strategies. At the same time, transaction price and transaction fee are taken as two important variables in evolutionary game model to explore the influence of different values of this variable on game results. Simulation experiments verify the effectiveness of the above model, and finally the risk prevention and control strategy and suggestions are put forward from the two aspects of transaction fee and transaction price.

Key words: blockchain; 51% double spend attack; evolutionary game; transaction fee; transaction price

1 引言

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。双花攻击曾经是传统在线支付中困扰多年的难题,Nakamoto提出的区块链技术通过对每一个区块加时间戳保证了交易记录的真实性,一定程度上减小了双花攻击的概率[1]。但在基于POW(Proof Of Work)共识的区块链中,挖矿节点通过工作量证明的方式竞争记账,如果节点占有超过全网50%的算力,就可以创造一条长于公链的侧链,使公链中的交易被回滚,借此完成双重花

基金项目:教育部-中国移动科研基金(No.MCM20170306);国家自然科学基金(No.71673122)。
作者简介:王雷(1995—),男,硕士,研究领域为信息管理与信息系统、区块链的原理与应用,E-mail:wl582737582@qq.com;任南(1973—),女,博士,教授,研究领域为信息管理与信息系统;李保珍(1975—),男,博士,教授,研究领域为信息管理与信息系统。
收稿日期:2019-07-23 **修回日期:**2019-09-29 **文章编号:**1002-8331(2020)03-0028-07
CNKI**网络出版:**2019-10-30, http://kns.cnki.net/kcms/detail/11.2127.TP.20191030.1429.012.html

(C)1994-2020 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

费，这种双花攻击也叫51%双花攻击[2]。另外，Pinzón(2016)还提出了种族攻击和芬妮攻击两种新的双花攻击，前者是通过给向自己支付的交易中加入更多的交易费用实现双花，后者则是通过控制区块的广播时间实现双花[3]。随着算力的市场流动性越来越强，节点现在可以通过租借、加入矿池等多种方式积攒算力，2018年比特币黄金BTG(Bitcoin Gold)就遭到了51%双花攻击，恶意节点预先准备了大量算力完成套现，最终系统损失超过1 800万美元。因此双花攻击正成为区块链中不可忽视的安全隐患。

针对这个问题，有学者从攻击者的动机和平台的安全防控两个角度对区块链中不同的双花攻击进行了研究。对于51%双花攻击的产生动机，Chaudhary运用时间自动机模型验证工具证明了比特币中的51%双花攻击成功概率是比较高的[4]；Liao提出少数攻击者可以通过联结理性节点的方法增加51%双花攻击成功的概率[5]；Biais证明在交易价格满足某些条件时尝试51%双花攻击是有利可图的，但要求投入大量的算力[6]。对于51%双花攻击的防控策略，Budish提出交易成本必须和节点攻击可能获取的最大利益呈正相关关系[7]。Westerlund提出通过主节点和矿工的双层共识机制消除51%双花攻击[8]。Liu研究种族攻击和芬妮攻击，他认为这两种攻击的对象都是接受零确认的商家，只要在多次确认的基础上完成交易，便可有效规避风险[9]。

上述研究并未过多关注双花攻击中节点间的相互作用以及策略的动态变化，不过一些学者已经尝试从博弈角度对区块链中的另外一些安全问题进行过分析。Kiayias曾经指出，通过博弈方法研究区块链中的安全问题，可以更深入的理解不同个体间如何竞争与合作[10]。Sapirstein分析矿工联合形成矿池进行的自私采矿攻击，并对区块链底层协议做适当改进[11]。唐长兵主要研究区块链中的区块截留攻击，并提出基于零行列式的优化方法[12]。Liu[13]和Easley[14]则分别把交易费用作为矿工选择矿池和算力竞争问题中的重要因素进行博弈分析。Abadi构建博弈模型证明了POW共识不是激励兼容的[15]。Liu提到可以基于波动理论和混合策略博弈理论，找到防止区块链网络攻击的最佳策略[16]。

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。因此，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。

2　51%双花攻击的进化博弈分析

2.1　51%双花攻击中的进化博弈问题

传统博弈论采用“完全理性”的假设，要求参与者有完美的判断和预测能力，然而事实上个人决定容易犯错，集体决策也经常失准[17]。针对这个问题，Smith[18]和Price结合达尔文的自然选择理论创立了进化博弈论，认为参与博弈的个体是“有限理性”的。在进化博弈论中，每个参与人都是重复从群体中随机抽取对手并进行博弈，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。他们之间的策略均衡不是通过迅速的最优化计算得到，而是需要经历一个学习调整的过程。进化稳定策略是进化博弈论中的核心概念，是指如果群体中的大多数个体选择进化稳定策略，那么小的突变者群体就不可能侵入到这个群体中，也代表系统此时处于进化稳定均衡。Taylor[19]之后提出了著名的复制动态模型，用来描述单群体策略的动态过程。随着进化博弈理论研究的深入，该理论在经济学、社会学、生态学领域都有非常广泛的应用。

51%双花攻击是区块链中最为典型且破坏力较强的一种双花攻击，在这种攻击中实际上也包含了一个关于进化博弈的策略选择和均衡问题。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。因此，本文构建区块链中51%双花攻击的进化博弈模型，对节点策略的动态进化情况进行分析。

2.2　研究假设与基本参数

首先与实际情况相结合，对于51%双花攻击模型做出如下假设条件：

(1)节点选择攻击时消耗的算力成本足够大，足以使节点顺利完成攻击，并且两个节点选择攻击时的算力成本相同。

(2)当进行博弈的两个节点都选择攻击时，为了减少各自的算力成本消耗，他们会选择在同一条侧链上合作挖矿。

(3)两个节点购买商品的价格，以及挖矿所获得的交易费用奖励和新币奖励都是相同的。

(4)每个区块都只包括一条交易记录。

(5)不考虑由币的市价变化引起的节点收益变化。

另外，本研究模型中的基本参数包括：参与者节点 i 和节点 j；参与双方的策略 Si 和 Sj，可选的策略集均为{攻击，不攻击}；初始状态下选择攻击策略的概率为 x

(C)1994-2020 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

$(0\leqslant x\leqslant 1)$,则选择不攻击策略的概率为 $1-x$,进化稳定策略用 x^* 表示;参与双方的收益函数分别为 $Ui(Si,Sj)$,$Uj(Si,Sj)$;参与双方与第三方商家的交易分别为 $i1$、$j1$,发送给自己的用于双重支付的交易分别为 $i2$、$j2$,无 i 和 j 参与的其他交易用 k 表示;第三方商家商品的价格为 p;对一个区块进行挖矿消耗的算力成本为 h;挖矿获得的奖励包括:每笔交易中由交易发起人承担的交易费用 f,每个区块产生后由系统发放的新币 b。基于博弈双方不同的策略组合,节点的收益会是由 p、h、f、b 组合而成的函数。

2.3　51%双花攻击进化博弈模型

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。

(1)当 i 和 j 都选择攻击时,i 从第三方商家购买某商品价格为 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。具体流程如图1(a)。

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。

综上,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)当 i 选择攻击,j 选择不攻击时,i 和 j 分别从商家购买价格为 p 的商品,并支付交易费用 f 后被矿工记录到公链上;接着 i 重复利用上笔交易 $(i1)$ 中的币 p 发送给自己,并通过挖矿将这笔交易 $(i2)$ 记录在侧链中,作为矿工获得相应的奖励;之后 i 继续挖矿并将 j 的交易 $(j1)$ 和其他交易 k 记录在侧链中,并获得相应的奖励。最终侧链长度超过公链,i 第一笔交易 $(i1)$ 的金额 p 回到自己账户,i 完成双花攻击。具体流程如图1(b)。

节点 i 的收益由以下几部分组成:交易 $i1$ 中获取的商品价值 p,支付的交易费用 f;交易 $i2$ 支付的交易费用 f,通过挖矿获取的奖励 $f+b$,消耗算力成本 h;交易 $i1$ 中获取的奖励 $f+b$,消耗算力成本 h;其他交易 k 中获取的奖励 $f+b$,消耗算力成本 h。节点 j 的收益包括交易 $j1$ 中支付的交易费用 f。

综上,节点 i 的收益:Ui(攻击,不攻击)$=p+f+3b-3h$,节点 j 的收益:Uj(攻击,不攻击)$=-f$。

(3)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,具体流程如图1(c)。

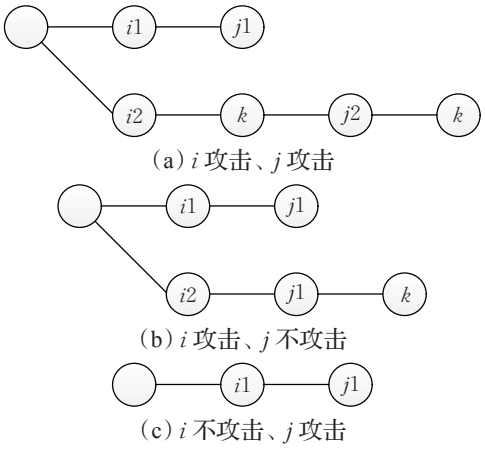


图1　双花攻击博弈流程图

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)$=-f$。

综上,节点 i 和 j 的收益矩阵见表1。

表1　51%双花攻击节点收益矩阵

		节点 j	
		攻击(x)	不攻击$(1-x)$
节点 i	攻击(x)	$p+2b-2h$, $p+2b-2h$	$p+f+3b-3h,-f$
	不攻击$(1-x)$	$-f,p+f+3b-3h$	$-f,-f$

根据收益矩阵,当节点选择攻击策略时,可以求出其期望收益为:

$$E1=p+(3-x)b+(x-3)h+(1-x)f \tag{1}$$

当节点选择不攻击策略时,其期望收益为:

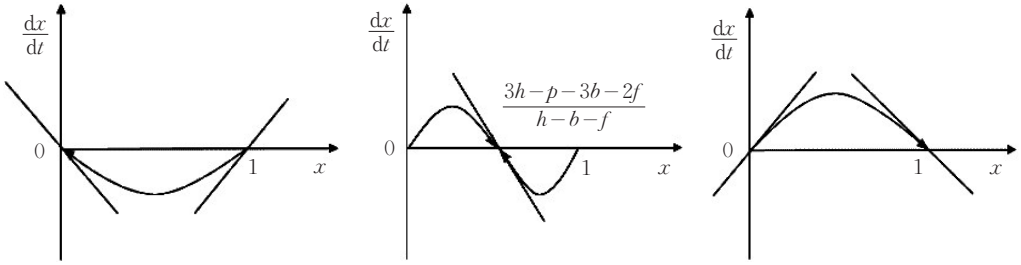
$$E2=-f \tag{2}$$

节点选择攻击策略的概率为 x,选择不攻击策略的概率为 $1-x$,因此节点的平均期望收益为:

$$E3=xE1+(1-x)E2 \tag{3}$$

博弈类型动态变化的速度取决于两个因素,即可模仿对象数量的大小(该类型博弈方的比例)和模仿对象的成功程度(该类型博弈方收益超过整体平均收益的幅度)[20]。由式(1)~(3)得到节点选择攻击策略的复制动态方程为:

(C)1994-2020 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net



(a) f 位于第一区间　(b) f 位于第二区间　(c) f 位于第三区间

图2　$p<h-b$ 时的动态相位图

$$F(x)=\frac{\mathrm{d}x}{\mathrm{d}t}=x(E1-E3)=$$
$$x(1-x)[p+(3-x)b+(x-3)h+(2-x)f] \quad (4)$$

令式(4)等于0可求出3个稳定状态:

$x1=0$, $x2=1$, $x3=\dfrac{3h-p-3b-2f}{h-b-f}$

由于在常见的区块链平台(比特币BTC、比特现金BCH)中,新币奖励一般几年才变动一次,因此本模型中假设新币奖励 b 为定值,另外假设算力成本 h 也是足够大的定值。将商品价格 p 和交易费用 f 作为模型中的两个变量,根据 p 和 f 的不同取值,节点的进化稳定策略可分以下几种情况进行讨论:

(1)当 $p<h-b$ 时,如果 $f\leqslant\dfrac{3h-p-3b}{2}$ 或 $f>2h-2b-p$,此时 $x3\leqslant 0$ 或 $x3\geqslant 1$,复制动态只有两个稳定状态 $x1=0$ 与 $x2=1$。如果 $\dfrac{3h-p-3b}{2}<f<2h-2b-p$,复制动态有三个稳定状态 $x1=0$, $x2=1$ 和 $x3=\dfrac{3h-p-3b-2f}{h-b-f}$。

由于在复制动态相位图上,复制动态曲线与横坐标轴相交并且交点处切线斜率为负的点就是进化稳定策略[21]。所以当 $p<h-b$ 且 $f\leqslant\dfrac{3h-p-3b}{2}$ 时,复制动态相位图如图2(a),该博弈有唯一的进化稳定策略,即 $x^*=0$,表明节点在长期都会选择不攻击策略。当 $p<h-b$ 且 $\dfrac{3h-p-3b}{2}<f<2h-2b-p$ 时,如图2(b), $x^*=\dfrac{3h-p-3b-2f}{h-b-f}$ 是唯一的进化稳定策略。表明节点选择攻击策略的比例为 $\dfrac{3h-p-3b-2f}{h-b-f}$,比例越小节点选择攻击策略的可能性就越小。当 $p<h-b$ 且 $f>2h-2b-p$ 时,如图2(c), $x^*=1$ 是进化稳定策略,表示即使有少量节点选择不攻击策略,随着不断的学习和调整,最终所有节点都会采取攻击策略。

(2)在 $h-b<p<2h-2b$ 条件下,分三种情况进行分析,当 $f<2h-2b-p$ 时,复制动态相位图与图2(a)相同, $x^*=0$ 是进化稳定策略,节点在长期都会选择不攻击策略。当 $2h-2b-p<f<\dfrac{3h-p-3b}{2}$ 时,复制动态相位图如图3。博弈有两个进化稳定策略,即 $x^*1=0$ 和 $x^*2=1$,博弈结果取决于 x 的大小,如果 x 位于区间 $(0,\dfrac{3h-p-3b-2f}{h-b-f})$,最终会收敛到 $x^*1=0$,节点选择不攻击策略;相反,如果 x 位于区间 $(\dfrac{3h-p-3b-2f}{h-b-f},1)$,则收敛到 $x^*2=1$,节点选择攻击策略。分界点 $\dfrac{3h-p-3b-2f}{h-b-f}$ 越大,节点选择攻击策略的可能性越小。当 $f\geqslant\dfrac{3h-p-3b}{2}$ 时,复制动态相位图与图2(c)相同, $x^*=1$ 是节点的进化稳定策略,节点在长期都会选择攻击策略。

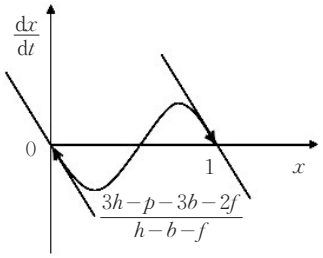


图3　$h-b<p<2h-2b$ 时的动态相位图

(3)在 $2h-2b<p<3h-3b$ 条件下, $f<\dfrac{3h-p-3b}{2}$ 时的复制动态相位图与图3相同,博弈有两个进化稳定策略: $x^*1=0$ 和 $x^*2=1$。博弈结果取决于 x 与 $\dfrac{3h-p-3b-2f}{h-b-f}$ 的大小比较。 $f\geqslant\dfrac{3h-p-3b}{2}$ 时的复制动态相位图与图2(c)相同, $x^*=1$ 是节点的进化稳定策略,节点在长期选择攻击策略。

(4)在 $p>3h-3b$ 条件下,无论 f 的取值是多少,复制动态相位图都和图2(c)相同, $x^*=1$ 是节点的进化稳定策略,节点在长期都会选择攻击策略。

综上所述,当交易价格和交易费用处于不同区间时,节点的进化稳定策略如表2所示。

3　仿真分析

3.1　仿真环节设计

为了更直观地体现节点进行51%双花攻击意愿的进化过程,本文使用Matlab软件进行仿真分析。首先对

(C)1994-2020 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

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

p、b、h、f 进行赋值,根据进化博弈模型中得到的结论,并结合实际情况,本文将算力成本 h 和新币奖励 b 分别设置为定值200元和80元,然后将交易价格 p 分为四种情况,在每种情况下交易费用 f 有多种取值,具体赋值情况如表3所示。

表3　关键参数赋值情况　元

算力成本h	新币奖励b	交易价格p	交易费用f
200	80	60	200
			170
			100
		200	100
			70
			20
		280	60
			20
		400	100
			50

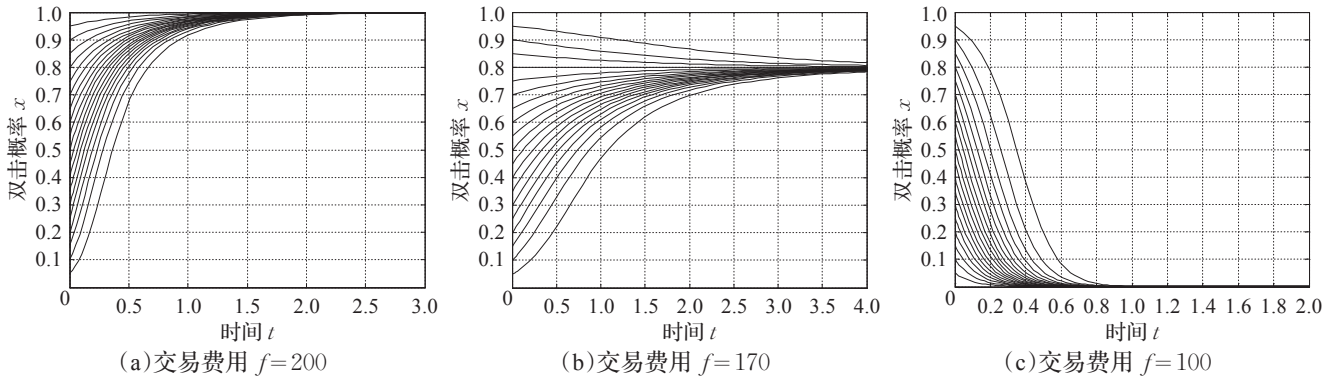
2.3节中已经得到了节点选择策略的复制动态方程:$F(x)=\frac{dx}{dt}=x(1-x)[p+(3-x)b+(x-3)h+(2-x)f]$,把经过赋值的 p、b、h、f 依次填入该方程形成节点策略迭代和进化的函数。

接着在[0,1]区间内以0.05为间隔,取20个不同的节点攻击的初始概率值(0、0.05、0.1、0.15……),再设置所观察节点攻击概率变化的时间区间。根据节点策略迭代和进化的函数,以时间 t 为横坐标,以节点选择攻击策略的概率 x 为纵坐标,绘制20种初始条件下节点攻击意愿进化情况的曲线。

然后根据交易价格和交易费用的不同取值对每种情况下节点攻击意愿的进化情况进行具体分析。

3.2　交易价格在最小区间

当交易价格为60时,p 小于临界值 $h-b$。首先当交易费用 $f=200$ 时,节点的攻击意愿进化情况如图4(a),可以看出进化稳定策略是 $x^*=1$,所有节点在长期都会选择攻击策略。接着减少交易费用使 $f<2h-2b-p$,当 $f=170$ 时的节点攻击意愿进化情况如图4(b),进化稳定策略是 $x^*=4/5$,表明会有4/5的节点选择攻击策略,1/5的节点选择不攻击策略,此时攻击概率仍然较高。进一步减少交易费用使 $f=100$,节点攻击意愿进化情况如图4(c),此时节点的进化稳定策略变为 $x^*=0$,无论节点选择不同策略的初始比例是多少,最终所有节点都会选择不攻击策略。



(a)交易费用 $f=200$　(b)交易费用 $f=170$　(c)交易费用 $f=100$

图4　交易价格在最小区间的攻击意愿进化情况

(C)1994-2020 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

3.3　交易价格在第二区间

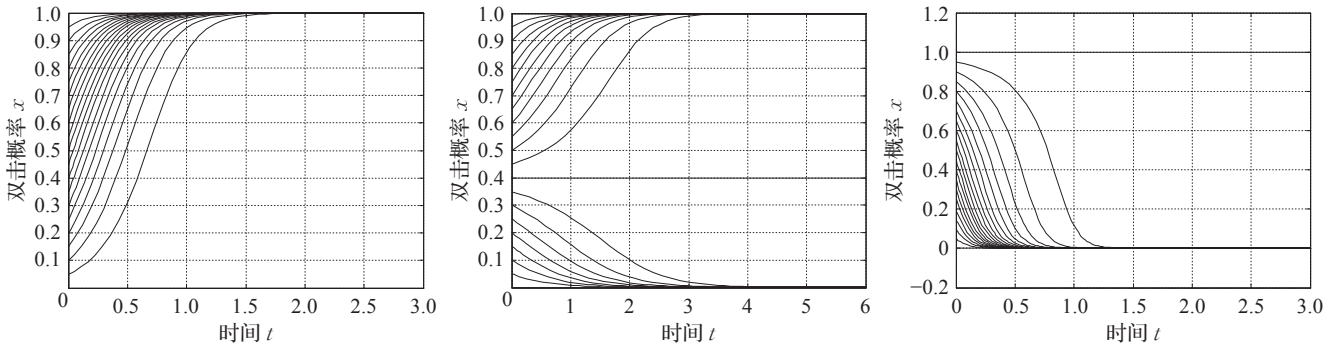
当交易价格为200时，p 大于临界值 $h-b$，小于临界值 $2h-2b$。首先当交易费用 $f=100$ 时，节点攻击意愿进化情况如图5(a)，进化稳定策略是 $x^*=1$，所有节点都会选择攻击策略。减少交易费用使 $f<\frac{3h-p-3b}{2}$，当 $f=70$ 时节点的攻击意愿进化情况如图5(b)，此时的进化稳定策略取决于 x 的初始值，$x<2/5$ 时所有节点都会选择不攻击策略，相反会选择攻击策略。进一步减少交易费用，$f=20$ 时的节点攻击意愿进化情况如图5(c)，可以看出节点的进化稳定策略变为 $x^*=0$，节点都会选择不攻击策略。

3.4　交易价格在第三区间

当交易价格为280时，p 大于临界值 $2h-2b$，小于临界值 $3h-3b$。首先当交易费用 $f=60$ 时，节点攻击意愿进化情况如图6(a)，此时的进化稳定策略是 $x^*=1$，节点都会选择攻击策略。减少交易费用使 $f<\frac{3h-p-3b}{2}$，$f=20$ 时节点的攻击意愿进化情况如图6(b)，此时进化稳定策略取决于 x 的初始值，$x<2/5$ 时所有节点都会选择不攻击策略，相反会选择攻击策略。

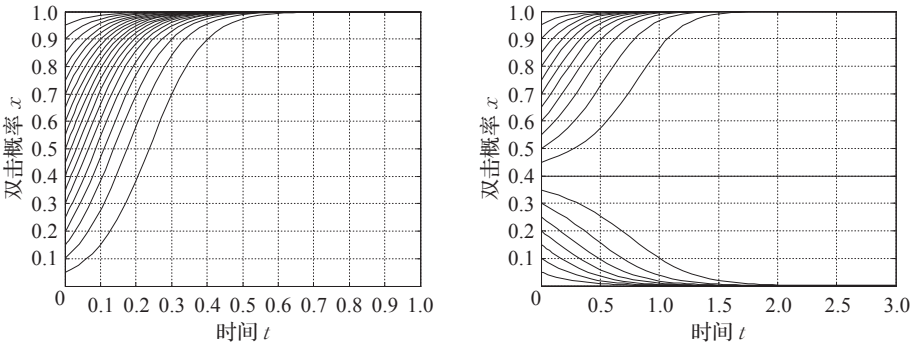
3.5　交易价格在最大区间

当交易价格为400时，p 大于临界值 $3h-3b$，首先当交易费用 $f=100$ 时节点攻击意愿进化情况如图7(a)，此时的进化稳定策略是 $x^*=1$。减少交易费用至 $f=50$，节点攻击意愿进化情况如图7(b)，进化稳定策略还是 $x^*=1$。因此无论交易费用 f 为多少，节点最终都会选择攻击策略。



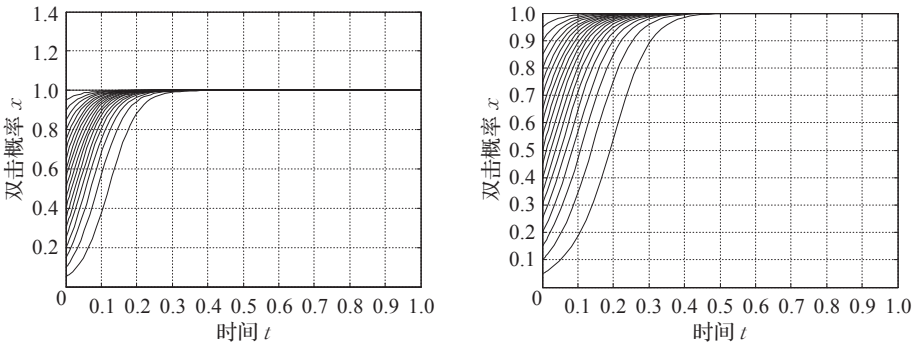
(a)交易费用 $f=100$　(b)交易费用 $f=70$　(c)交易费用 $f=20$

图5　交易价格在第二区间的攻击意愿进化情况



(a)交易费用 $f=60$　(b)交易费用 $f=20$

图6　交易价格在第三区间的攻击意愿进化情况



(a)交易费用 $f=100$　(b)交易费用 $f=50$

图7　交易价格在最大区间的攻击意愿进化情况

(C)1994-2020 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

经过上述仿真实验可以看出,当交易价格和交易费用取不同值时,实验结果与进化博弈模型中的结论完全吻合。

4 对策与建议

通过对区块链中的51%双花攻击进行进化博弈分析,本文揭示了51%双花攻击的内在机理,基于相关内在机理,尝试提出如下风险防控策略:

(1)平台调控与市场调节相结合

对于比特币、以太坊这些知名的区块链平台,交易费用都是由矿工和交易发起者自愿决定的,属于市场调节机制,然而这种方法会造成交易费用的极不稳定,为节点进行51%双花攻击提供了机会。为了有效抑制51%双花攻击的出现,平台需要制定严格的交易费用标准。对于不同交易价格的交易,都要设定相应的交易费用最大值,交易发起者需在规定的范围内支付交易费用,这样会使节点基于收益最大化的考虑趋向于选择不攻击策略。此外,考虑到对矿工的激励,可由矿工来决定每笔交易的最低费用。这种将平台调控与市场调节相结合的方法,有利于在提高区块链安全性的基础上保证资源配置的效率。

(2)根据价格区间划分相应风险监控等级

虽然规范交易费用可以有效抑制51%双花攻击的出现,但无法完全消除,因此需要制定平台的监督机制,制约和惩罚节点的恶意行为。根据前文得到的结论,不同交易价格区间节点攻击意愿的进化情况不同,受到抑制的效果也不同。因此可以基于不同价格将平台中的交易划分4个风险等级,由低到高分别为:稍有危险、一般危险、高度危险、极其危险。风险等级更高的交易进行攻击的可能性更大,产生的危害也更大,需要对其进行重点监督。在监督过程中收集和分析与风险相关的各种信息,预测可能发生的风险,及时提出预警。对于已发生的攻击行为,立即限制节点的交易和挖矿活动,并进行处罚。这种方法可以更有效及时地减小51%双花攻击产生的危害。

参考文献:

[1] Nakamoto S.Bitcoin:a peer-to-peer electronic cash system[EB/OL].(2008)[2019-09-14].https://bitcoin.org/en/bitcoin-paper.

[2] Karame G O,Androulaki E,Capkun S.Double-spending fast payments in bitcoin[C]//Proceedings of the 2012 ACM Conference on Computer and Communications Security,2012:906-917.

[3] Pinzón C,Rocha C.Double-spend attack models with time advantange for bitcoin[J].Electronic Notes in Theoretical Computer Science,2016,329:79-103.

[4] Chaudhary K,Fehnker A,Pol J V D,et al.Modeling and verification of the Bitcoin protocol[J].Computer Science,2015,196:46-60.

[5] Liao K,Katz J.Incentivizing double-spend collusion in bitcoin[C]//Financial Cryptography Bitcoin Workshop,2017.

[6] Biais B,Bisière C,Bouvard M,et al.The blockchain folk theorem[J].The Review of Financial Studies,2019,32(5):1662-1715.

[7] Budish E.The economic limits of bitcoin and the blockchain[R].National Bureau of Economic Research,2018.

[8] Westerlund M,Kratzke N.Towards distributed clouds:a review about the evolution of centralized cloud computing,distributed ledger technologies,and a foresight on unifying opportunities and security implications[C]//2018 International Conference on High Performance Computing & Simulation,2018:655-663.

[9] Liu Z,Zhao H,Chen W,et al.Double-spending detection for fast Bitcoin payment based on artificial immune[C]//National Conference of Theoretical Computer Science,2017:133-143.

[10] Kiayias A,Koutsoupias E,Kyropoulou M,et al.Blockchain mining games[C]//Proceedings of the 2016 ACM Conference on Economics and Computation,2016:365-382.

[11] Sapirshtein A,Sompolinsky Y,Zohar A.Optimal selfish mining strategies in bitcoin[C]//International Conference on Financial Cryptography and Data Security,2016:515-532.

[12] 唐长兵,杨珍,郑忠龙,等.PoW共识算法中的博弈困境分析与优化[J].自动化学报,2017,43(9):1520-1531.

[13] Liu X,Wang W,Niyato D,et al.Evolutionary game for mining pool selection in blockchain networks[J].IEEE Wireless Communications Letters,2017(99):1.

[14] Easley D,O'Hara M,Basu S.From mining to markets:the evolution of bitcoin transaction fees[J].Journal of Financial Economics,2019.

[15] Abadi J,Brunnermeier M.Blockchain economics[R].Mimeo Princeton University,2018.

[16] Liu Z,Luong N C,Wang W,et al.A survey on blockchain:a game theoretical perspective[J].IEEE Access,2019,7:47615-47643.

[17] 谢识予.有限理性条件下的进化博弈理论[J].上海财经大学学报,2001,3(5):3-9.

[18] Smith J M,Price G R.The logic of animal conflict[J].Nature,1973,246(5427):15.

[19] Taylor P D,Jonker L B.Evolutionary stable strategies and game dynamics[J].Mathematical Biosciences,1978,40(1/2):145-156.

[20] 杜晓君,马大明,张吉.基于进化博弈的专利联盟形成研究[J].管理科学,2010,23(2):38-44.

[21] 高文军,郭根龙,石晓帅.基于演化博弈的流域生态补偿与监管决策研究[J].环境科学与技术,2015,38(1):183-187.

(C)1994-2020 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net