DOI:10.13878/j.cnki.jnuist.2019.05.004

洪阳[1]　王立松[1]　葛春鹏[1]

比特币平台挖矿策略及其收益综述

摘要

区块链技术是比特币平台的底层技术,由于其具有透明性、不可伪造性、不可更改性等特点,被广泛应用于虚拟货币、供应链等系统中.然而,大部分区块链平台,如比特币平台,面临包括自私挖矿在内的诸多问题,这将直接导致比特币并不安全,从而严重影响区块链的发展.自私挖矿是一种比特币挖掘策略,它是指自私矿工选择性地发布之前的隐匿的区块从而获得比诚实矿工更多的额外收益.本文在模拟诚实矿工挖矿实验基础上,重点研究自私挖矿情况下矿工的最佳相对收益.采用中心极限定理和节点状态转化图建立了两个节点分布概率模型,再运用马尔可夫随机过程和函数极值法依次求得两个模型下的最佳收益.同时设计并进行自私挖矿模拟实验,得出自私挖矿中节点算力和收益的关系,从而进一步验证模型的合理性.

关键词

区块链;自私挖矿;比特币;马尔可夫随机过程

中图分类号 TP13

文献标志码 A

收稿日期 2019-09-02

资助项目 国家自然科学基金青年基金(61702236)

作者简介

洪阳,男,硕士生,主要研究方向为区块链技术及自私挖矿攻击.hy686996@163.com

王立松(通信作者),男,博士,副教授,主要研究方向为数据库技术.wangls@nuaa.edu.cn

1 南京航空航天大学 计算机科学与技术学院,南京,211106

0 引言

21世纪以来,互联网技术的蓬勃发展极大地改善了人民群众的日常生活,这使得互联网成为信息社会不可或缺的重要保障,但与此同时,互联网也面临各种安全问题,比如黑客攻击、数据泄露等.区块链技术作为一种分布式数据存储、点对点传输、共识机制、加密算法和智能合约等计算机技术应用新模式,具有去中心化、透明性、不可更改性等特点,因此,它在金融、电子政务、能源应用和医疗等诸多领域发挥着重要作用[1].

比特币系统的稳定性依赖于参与交易的节点的共同利益.在诚实节点发现新的区块时,会立即向整个系统公布挖掘到新区块的消息.在接收和确认该消息后,其他矿工会将这笔交易记录在账本上,然后开始挖掘其他分支.率先挖到区块的矿工会得到相应的奖励.这种激励机制让比特币在去中心化的情况下,依然能使交易各方达成共识,从而很好地维护了区块链系统的稳定性.然而,当前的比特币系统中,恶意节点为了获得更大的收益,往往会采用自私挖矿的策略[2].自私挖矿的概念是由康奈尔大学两位研究员Eyal和Sirer于2013年提出的,它是一种比特币的挖掘策略,是一种基于挖矿节点算力的竞争[2].恶意节点依据“自私矿池”中区块的私密性,当一个“自私矿池”挖到新的区块,并没有根据比特币共识协议立即公布该区块,从而让其余的诚实节点浪费算力去挖矿[3].面对区块链出现分叉的情况,最长的那一条链被视作合法链[4-5].当诚实链的长度即将接近自私链的长度时,自私矿工就会释放之前隐藏的区块从而迫使诚实矿工的劳动作废.在自私挖矿的情况下,自私矿工可以获得相对于其采用诚实挖矿策略较多收益,而诚实矿工则会损失自己的合法收益.除此以外,来自康奈尔大学和马里兰大学的区块链研究员Nayak等[6]更进一步提出对于大型参数空间而言,自私挖矿并非最佳选择.因而他们拓展了采矿战略空间,考虑一类顽固的采矿策略,即攻击者继续在他的私人分支上进行挖矿,让公共分支领先,如果他以后碰巧超越公众,他将获得比期望更高的挖矿收益[7].这种情况下,计算表明袭击者的收益最大会提高13%.此外,其他一些研究展示了如何通过非平凡的挖掘组合和网络攻击进一步放大他的收益,从而获得更大的挖矿收益,例如,分布式去中心化的Eclipse攻击的策略[4].

虽然,目前针对比特币挖矿策略的研究有很多,不同的研究工作

研究了自私旷工从不同的角度来进行自私挖矿,从而获得额外的收益.但是,这些研究都没有从一个系统的角度来分析和总结比特币节点可能的挖矿策略.本文将针对现有的比特币平台中挖矿模型进行系统总结,并通过数学模型来定量分析这些自私挖矿策略获取的收益.最后,本文将给出一些可能的策略以防止自私挖矿,希望能为初学研究者提供一个系统、全面地了解比特币的挖矿模型,同时为比特币挖矿策略优化提供一些可行的建议.

1 自私挖矿模型和收益模型

1.1 比特币简介

比特币作为一种加密数字货币,其本质是包含一系列输入输出列表的数据结构,包含了节点与节点之间的转账记录.比特币交易和挖矿过程包含6个步骤,如图1所示[8].

1)某客户向P2P网络发出交易请求;

2)接收到用户请求的节点验证交易信息,将其向P2P网络进行广播;

3)各矿工接收到交易信息,验证其正确后将其放入交易池,并继续广播该交易信息,直到全网都接收到该笔交易信息;

4)将多条交易信息打包成一个新的区块;

5)将新的区块加入到已经存在的区块链中;

6)客户的交易完成.

比特币的有效性建立在交易发起者的签名上,交易签名的作用是为了防止他人冒充签名,产生数据造假.交易输入的签名是指放在交易输入中的签名(Signature)字段,其中包括了用户的公共秘钥(Pubkey).签名字段主要用于之后的交易有效性验证.

交易完成后,系统会把交易广播给邻居.挖矿节点,俗称矿工,在挖矿时,会把交易池中的交易记录打包形成一个新的区块.在成功加入区块链交易系统以后,这笔交易就会被系统确认,但是在挖矿节点进行交易之前,需要验证交易真伪,防止数据造假[9].

1.2 自私挖矿模型

自私矿工通过隐匿和公布私有区块从而获得额外收益,但关键问题在于自私矿工何时选择公布自己隐匿的区块或者何时继续隐藏挖掘到的新区块才能使得自己的相对收益达到最大.

本文采用〈S,A,P,R〉模型[10],将自私挖矿问题转化为决策问题,目标函数是相对收益函数.需要阐明的是此处的目标函数是非线性的,因为自私挖矿者所追求的并不是所获区块的具体数量,而是使自己所获得的区块的份额最大化.换而言之,自私挖矿者想得到的是相对其他挖矿节点更高的投资回报率.其中,S代表区块状态集中的某种状态.可以用三元式(l_a,l_h,$fork$)表示S的空间状态.其中前两个参数分别表示自私矿链的长度和诚实矿链的长度,第三个参数表示区块链的分叉.A为行动集,该行动集中有4种元素:接受、发布、隐匿和竞争.P表示在某种行动下,当前区块的状态转化到下一状态的概率.R表示当前状态下的期望收益.

1.2.1 节点分布概率分析

本文从节点分布概率的角度出发,建立2个自私挖矿过程模型.第1个模型直接利用泊松分布和大数定律来拟合诚实节点和自私挖矿节点的概率分布.第2个模型基于状态转换图中的转换频率来分析矿池中的节点概率分布.需要指明的是,在2个模型建立与分析过程中,都忽略区块大小、网络通信延

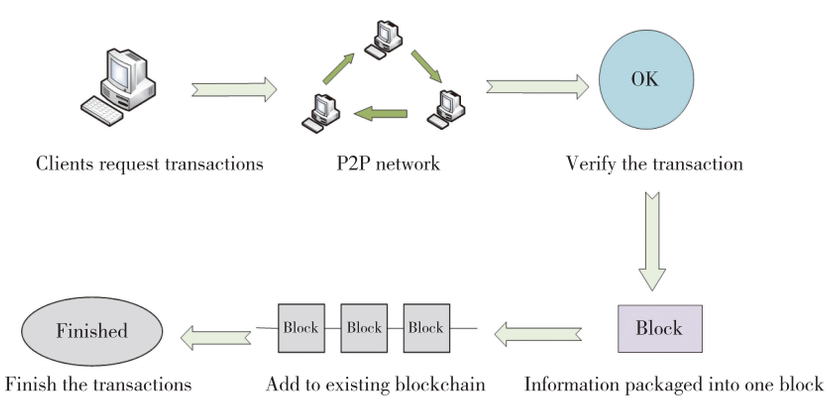

图1 比特币交易过程

Fig. 1 Bitcoin transaction process

迟等因素.

1)模型 1:概率分析

① 诚实节点概率分布

诚实节点的概率分布近似于泊松分布[11].一般而言,比特币每 600 s 挖掘出一个新块,由文献[12]可知,一个诚实节点挖到块的概率为 P_h.

$$p_h = \frac{1}{d} = 1 - e^{-\frac{1-\alpha}{600}\cdot t},$$

其中,$1-\alpha$ 指诚实矿工的算力,d 是挖矿难度,t 是挖矿的时间(以 s 为单位).

② 自私节点概率分布

由于自私挖矿池中节点的算力基本稳定,所以本文假定自私节点发掘一个新区块的概率基本不变.

$$p_a = 1 - e^{-\frac{\alpha}{600}\cdot t},$$

这里,记自私挖矿节点为 x_i,当 x_i 挖掘到新的区块时,记为 1,否则记为 0.

利用中心极限定理可得自私挖矿节点 $X = \sum_{i=1}^{n} x_i$ 的标准化公式:

$$y = \frac{\sum_{i=1}^{n} x_i - n\mu}{\sqrt{n}\sigma} = \frac{\bar{x} - \mu}{\sigma/\sqrt{n}} \sim N(0,1),$$

σ 为标准差,μ 为期望值.

考虑到随着自私挖矿的深入,不断会有诚实节点加入到自私挖矿的行列中来,这就导致了自私矿池的算力发生变化.所以,用 p' 表示自私矿池变化后的概率分布.

$$p' = \begin{cases} (1-\beta)(1-p_a), & 0' \to 0 \cap N_h \in C_h, \\ \beta(1-p_a), & 0' \to 0 \cap N_h \in C_a, \end{cases}$$

其中,$(1-\beta)(1-p_a)$ 是指有一部分诚实节点加入自私矿池后,新区块被诚实节点发现的概率.而 $\beta(1-p_a)$ 则表示诚实节点挖到的区块最后链接在自私挖矿链上的概率.

当 $l_a - l_h = m \geqslant 0$ 时,设诚实矿链的长度追上自私矿链的可能性为 p_m:

$$p_m = \begin{cases} 1, & p_a \leqslant p_h, \\ \left(\frac{p_h}{p_a}\right)^m, & p_a \geqslant p_h. \end{cases}$$

最后,进一步思考一种情况:诚实矿链先前已经挖出 j 个区块却最后仍然能赶上自私矿链.设该情况概率为 q:

$$q = \begin{cases} (1 - e^{-\frac{1-\alpha}{600}\cdot t})^j, & j \geqslant m, \\ (1 - e^{-\frac{1-\alpha}{600}\cdot t})^j \left(\frac{1 - e^{-\frac{1-\alpha}{600}\cdot t}}{1 - e^{-\frac{\alpha}{600}\cdot t}}\right)^{m-j}, & j < m. \end{cases}$$

2) 模型 2:概率分析

模型 2 将矿池中的节点的状态进行分类.为了直观表示,本文将节点状态标注为 0′,0,1 等.节点状态转化如图 2 所示[2].其中状态 0 代表只有一条公共链,0′ 表示有两条长度为 1 的链,其中一条是主分支,另外一条是自私挖矿者的私有分支,用以发布隐匿区块从而和主分支竞争[2].另外,本文中用 β 来表示矿池中诚实节点的比例.

在频率为 α(本文将算力 α 等价为转换频率),对于状态 $S = 0,1,2,\cdots$,节点在挖掘出新的区块后状态会从 S 变为 $S+1$.对于状态 $S = 2,3,4,\cdots$,在频率为 $1-\alpha$ 的情况下,状态会从 S 退回 $S-1$. 如果自私矿池中有一个长度为 1 的自私挖矿链,而在其他分支上挖掘到一个新区块的同时自私矿链采取公布隐藏区块的措施,这样系统就会产生故意分叉现象,即出现两个长度为 1 的区块链.自私矿池中的矿工会继续挖掘该矿池上的分支,而诚实矿工则依然在他们之前认定的矿链上继续挖矿.

通过图 2 可以得知,从状态 0′出发有 3 种可能的转换,最终全部通向状态 0.它们的总频率之和为 1.第 1 种情况,矿池以频率 α 在之前的自私链上挖掘到一个新区块;第 2 种情况,其他矿工在之前的自私

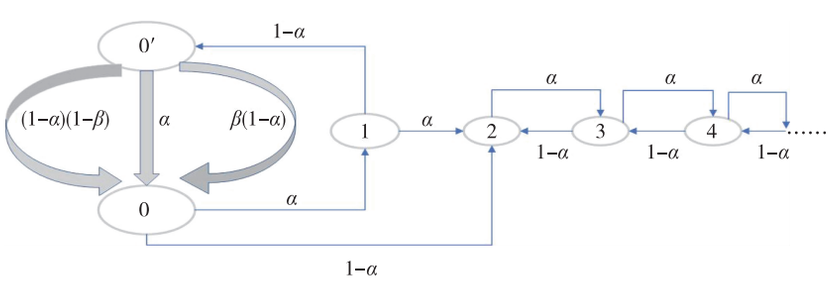

图 2 节点状态转化

Fig. 2 Node state transition diagram

链上以频率$\beta(1-\alpha)$挖掘新的区块;第3种情况,其他矿工在公共链上以频率$(1-\beta)(1-\alpha)$挖掘到新的区块.

由状态转化图可以推导出节点状态概率分布,结论如式(1):

$$\begin{cases}\alpha p_0=(1-\alpha)p_1+(1-\alpha)p_2,\\ p_0'=(1-\alpha)p_1,\\ \alpha p_1=(1-\alpha)p_2,\\ \forall k\geqslant 2:\alpha p_k=(1-\alpha)p_{k+1},\\ \sum_{k=0}^{\infty}p_k+p_0'=1,\end{cases}\tag{1}$$

其中,p_0表示节点状态0的概率,p_0'表示节点状态0′的概率,其余以此类推.

显然,由式(1)变形可以得出式(2):

$$\alpha p_0=(1-\alpha)p_1+(1-\alpha)\frac{\alpha}{1-\alpha}p_1=p_1.\tag{2}$$

由于$1=p_0+p_0'+\sum_{k=1}^{\infty}p_k$,所以将式(2)代入得到式(3):

$$1=\frac{1}{\alpha}p_1+(1-\alpha)p_1+\sum_{k=1}^{\infty}\left(\frac{\alpha}{1-\alpha}\right)^{k-1}p_1.\tag{3}$$

下面,用α将p_1表示出来,其余变量以此类推,推导得到式(4):

$$\begin{cases}p_0=\dfrac{\alpha-2\alpha^2}{\alpha(2\alpha^3-4\alpha^2+1)},\\ p_0'=\dfrac{(1-\alpha)(\alpha-2\alpha^2)}{1-4\alpha^2+2\alpha^3},\\ p_1=\dfrac{\alpha-2\alpha^2}{2\alpha^3-4\alpha^2+1},\\ \forall k\geqslant 2:p_k=\left(\dfrac{\alpha}{1-\alpha}\right)^{k-1}\dfrac{\alpha-2\alpha^2}{2\alpha^3-4\alpha^2+1}.\end{cases}\tag{4}$$

1.2.2 相对收益分析

目标函数是节点相对收益函数,因为自私挖矿者所想的是最大化所获得的区块份额,而不是获得区块的具体数量.换而言之,自私挖矿者想得到的是相对其他挖矿节点更高的投资回报率.

1)模型1:相对收益分析

结合自私挖矿过程分析和挖矿节点概率分布,对于何时公布隐匿区块的关键问题,给出以下算法描述(算法1).

根据算法1,建立自私挖矿节点的相对收益函数[13],如式(5)所示:

$$R=E\left[\lim_{n\to\infty}\frac{\sum_{i=1}^{n}r_{a_i}}{\sum_{i=1}^{n}(r_{a_i}+r_{h_i})}\right].\tag{5}$$

算法1

1) When $\Delta l=0$&& fork // 当自私链和诚实链的长度差$\Delta l=0$且产生分叉
  If(Nextnode == N_a) // 如果下一个节点是自私节点
    Append N_a to C_a and Hide // 将自私挖矿块加到自私链上并隐藏
    Then continue to mine // 继续挖掘
2) When $\Delta l=1$ // 当$\Delta l=1$时
  If(Nextnode == N_h) // 当下一个节点是诚实节点
    Publish C_a // 发布自私链
  If(Nextnode == N_a) // 如果下一个节点是自私节点
    Append N_a to C_a and Hide // 将自私节点加到自私链上并隐藏
    Then continue to mine // 然后继续挖掘
3) When $\Delta l=2$ && fork // 当$\Delta l=2$且分叉
  If(Nextnode == N_h&& have mined one node && the probability of mining nextnode is q)
    If($q>p_a$) // 如果可能性q大于下一个节点是自私节点可能性
      Publish C_a // 发布自私链
    Else Use Match Action(Publish the C_a with the same length of C_h) // 采取竞争措施
  If(Nextnode == N_a) // 如果下一个节点是自私节点
    Append N_a to C_a and Hide // 将自私节点加到自私链上同时隐藏
    Then continue to mine // 继续挖掘
4) When $\Delta l\geqslant 3$ // 当$\Delta l\geqslant 3$
  If(Nextnode == N_a) // 当下一个节点是自私节点
    Append N_a to C_a and Hide // 将自私节点加到自私链上并隐藏
    Then continue to mine // 然后继续挖掘
   If(Nextnode == N_h) // 如果下一个节点是诚实节点
  Use Match Action(Publish the C_a with the same length of C_h) // 采取竞争措施

为求出相对收益函数的最优解,本文借鉴 Sapirshtein 等[14]的研究成果,定义以 r_a 和 r_h 为参数的转化函数 $\tilde{\omega}_\rho$,

$$\tilde{\omega}_\rho(r_a,r_h)=(1-\rho)\,r_a-\rho r_h.$$

其中参数 $\rho\in(0,1)$.这样就将最佳收益问题转化为了无限状态下的马尔可夫随机过程决策问题.接下来再定义策略 π 下的马尔可夫链期望值为 v_ρ^π:

$$v_\rho^\pi=E\left[\lim_{n\to\infty}\frac{1}{n}\sum_{i=1}^{n}\tilde{\omega}_\rho(r_i(\pi))\right],$$

其中 $r_i(\pi)$ 表示策略 π 下第 i 步的收益,定义期望值的最优解为 $v_\rho^*=\max_{\pi\in A}\{v_\rho^\pi\}$.

为了优化相对收益函数的最优解,本文有以下 2 个命题[14]:

命题 1:如果对于一些 $\rho\in(0,1)$,有 $v_\rho^*=0$,则最优策略 π^* 下的相对收益 $R=\rho$.

命题 2:因为标准的马尔可夫链过程解法不能解决无限状态下的马尔可夫链过程决策问题,只能限制各个链的长度为 l(l 为常数),将无限状态转化为有限状态.记有限状态情况下的马尔可夫链为 M_ρ^l.在循环反复的马尔可夫链过程中,初始状态会在有限的步骤 C 中被反复访问.所以,自私挖矿者在此过程获得的收益为 $r_a=E\left[\sum_{c=1}^{C}r_{a_i}\right]$,$\bar{r}_a=E\left[\frac{1}{C}\sum_{c=1}^{C}r_{a_i}\right]$,同理 $r_h=E\left[\sum_{c=1}^{C}r_{h_i}\right]$,$\bar{r}_h=E\left[\frac{1}{C}\sum_{c=1}^{C}r_{h_i}\right]$.

接下来重新推导相对收益函数 R,过程如下:

$$R=E\left[\lim_{n\to\infty}\frac{n\bar{r}_a}{n(\bar{r}_a+\bar{r}_h)}\right]=E\left[\lim_{n\to\infty}\frac{\bar{r}_a}{(\bar{r}_a+\bar{r}_h)}\right]=E\left[\frac{\bar{r}_a}{(\bar{r}_a+\bar{r}_h)}\right]=\frac{\bar{r}_a}{(\bar{r}_a+\bar{r}_h)}.$$

同时,进一步推导最优解 v_ρ^*,得到式(6):

$$v_\rho^*=E\left[\lim_{n\to\infty}\frac{1}{n}\sum_{i=1}^{n}\tilde{\omega}_\rho(r_i(\pi^*))\right]=E\left[\lim_{n\to\infty}\frac{1}{n}\sum_{i=1}^{n}((1-\rho)r_{a_i}-\rho r_{h_i})\right]=(1-\rho)r_a-\rho r_h. \tag{6}$$

最后一步是要确定取得最优解时 ρ 的值.由于 $\rho\in(0,1)$,所以可以采用二分查找的方法来确定 ρ 的最优值,二分查找法伪代码表述如算法 2.

2)模型 2:收益分析

结合节点状态转化图 2,利用节点状态转化频率来分析自私挖矿的预期收入.目标函数是相对收益函数,如式(7)所示:

算法 2

```
1) Start
2) Int low=0,high=1
3) While(high-low>=0)                    // 当 high 比 low 大时保持循环
     ρ = (high + low)/2                  // 取中间节点
     (π,v_ρ*) = MDP_Solver(M_ρ^c)        // MDP_Solver是标准马尔可夫链求解函数
   If(v_ρ* > 0)                          // 如果期望值的最优解大于0
     low = ρ
   Else
     high = ρ
   Return π, ρ
4) End
```

$$R=\frac{r_a}{r_a+r_h}. \tag{7}$$

下面根据自私链和诚实链的不同状态来讨论相对收益.

情况 1.系统产生长度均为 1 的自私链和诚实链的分叉,自私链发现一个新的区块并将它链接到自私链上隐藏.这样,自私链就领先诚实链 1 个区块的长度,收益也由此决定,如图 3 所示.

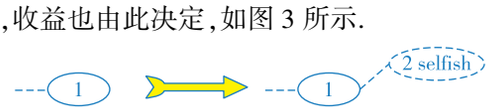

图 3 情况 1

Fig. 3 Condition 1

情况 2.区块链产生两个分支长度均为 1 的分叉,此时,自私链发现一个新的区块.自私矿池选择发布自私链上的所有区块.因此,诚实链上的所有区块收益无效,自私链获得两个区块的收益,如图 4 所示.

情况 3.区块链产生两个分支长度均为 1 的分叉.当诚实链先挖到区块,并将新挖到的区块链接到自己的诚实链上.自私挖矿链会采取接收行动,即放弃自私链上所有的区块.这种情况下,诚实链获得两个区块的收益,如图 5 所示.

情况 4.区块链产生两个分支长度均为 1 的分叉.如果诚实链挖矿到一个区块,诚实链可以采取一种策略,即将新挖到的区块链接到自私链的后面,这样自私链和诚实链先各自获得一个区块的收益.然后,自私挖矿链后续的收益就会被诚实挖矿链所有,如图 6 所示.

情况 5.没有自私分支,若诚实链发掘一个新区

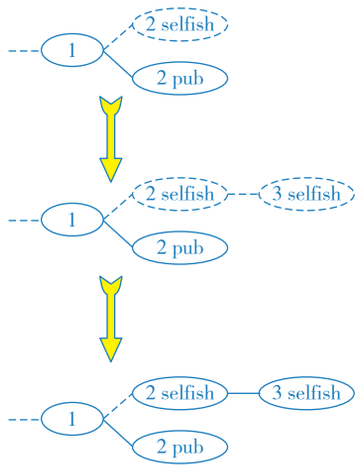

图 4　情况 2

Fig. 4　Condition 2

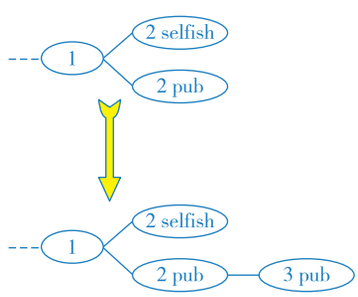

图 5　情况 3

Fig. 5　Condition 3

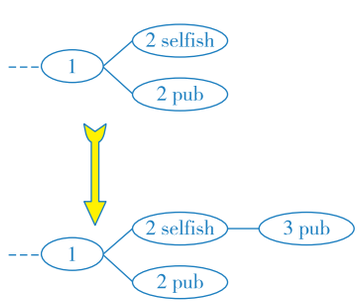

图 6　情况 4

Fig. 6　Condition 4

块,则诚实链获得一个区块的收益.此时,诚实链的相对收益为 $p_0(1-\alpha)$.

情况 6.在自私链领先诚实链一个区块的情况下,诚实链率先挖掘到一个区块.此时,两者的长度一样,此时利益归属取决于两者之间的算力博弈的结果.

情况 7.当自私链领先诚实链两个区块的情况下,如果诚实链挖到 1 个新区块,则 $l_a - l_h \geqslant 1$,自私链会采取发布措施,从而迫使诚实链上的收益全部作废,两个区块的收益归属自私链.

情况 8.自私链领先诚实链的长度超过 2 块,此时,诚实链缩短两者差距至 2 个区块.自私链会选择发布它的分支上的某一个区块.这种情况下,诚实链挖到的新区块没有链接到诚实链上,而是链接到其他主链上了.这样诚实链上的区块收益都作废,自私挖矿链可以盈利一个区块的收益,如图 8 所示.

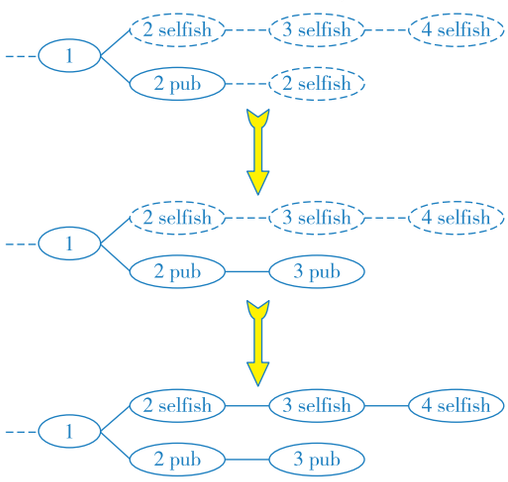

图 7　情况 7

Fig. 7　Condition 7

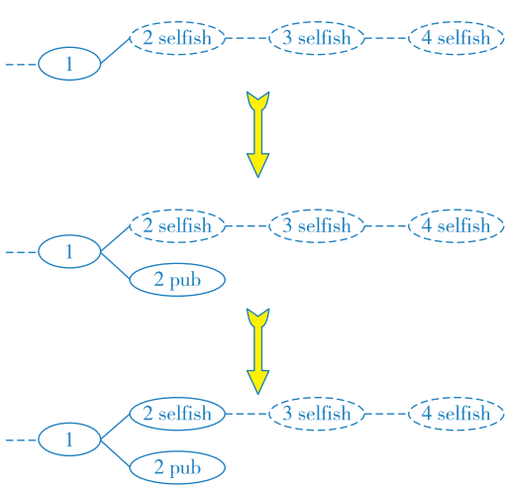

图 8　情况 8

Fig. 8　Condition 8

接下来将根据上述 8 种情况分别计算诚实链的收益和自私链的收益.其中,情况 3,4,5 的收益为诚实链所有,情况 1,2,6,7,8 的收益为自私链所有.然后,再依据状态转化图可得到自私节点和诚实节点各自的相对收益,双方各自的相对收益如式(8)所示.

$$\begin{cases} r_a = p_0' \cdot \beta(1-\alpha) + p_0' \cdot \alpha \cdot 2 + p_2 \cdot \\ \qquad (1-\alpha) \cdot 2 + \sum_{i=3}^{\infty} p_i(1-\alpha), \\ r_h = p_0' \cdot \beta(1-\alpha) + p_0' \cdot (1-\alpha)(1-\beta) \cdot \\ \qquad 2 + p_0 \cdot (1-\alpha), \end{cases} \tag{8}$$

其中,$\alpha \in \left(0, \frac{1}{2}\right)$.将式(8)代入目标函数式(7)中,化简得到表达式(9):

$$R = \frac{r_a}{r_h + r_a} = \frac{\alpha(1-\alpha)^2(4\alpha + \beta(1-2\alpha)) - \alpha^3}{1 - \alpha(1 + (2-\alpha)\alpha)}. \tag{9}$$

规定好 α,β 的范围,将求 R 的最优解转化为定义域内求二元函数的极值问题.同时,利用 MATLAB 做出相对收益函数 R 的图像,如图 9 所示.

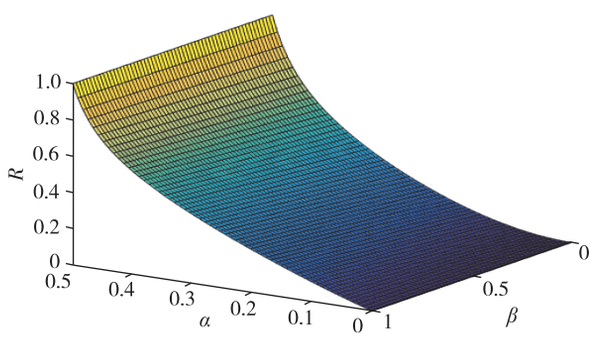

图 9 收益函数 R

Fig. 9 Reward function R

由表达式(9)可以看出,相对收益函数是由 α,β 共同决定的,所以将最佳收益问题转化为在 α,β 的可行域内求函数极值.根据文献[15],利用相关挖矿系数,可以发现当 β 为 0 时,α 的阈值为 1/3,即自私矿工只要掌握全网 1/3 的算力就可以保证获得额外收益,这符合我们之前的认知.当 β 的值为 0.5 时,α 的阈值为 1/4,即当自私节点占据总节点数的一半时,自私矿工只要拥有全网 1/4 的算力就可以获得比诚实矿工更多的额外收益.

2 挖矿实验模拟

2.1 诚实挖矿模拟实验结果与分析

2.1.1 实验环境

模拟系统采用 Go 语言实现,基于以下软、硬件环境开发模拟系统并进行实验数据的收集与处理.

硬件环境:Intel(R) Core(TM) i5-8300 CPU @ 2.30GHz,8G 内存.

软件环境:Ubuntu 18.04,LiteIDE X35.5,go 1.11.1.

实验过程中以 Linux 系统的终端来模拟各个节点,节点间通过广播信息进行信息交互,产生的实验结果采用 Excel 和 MATLAB 进行分析.

2.1.2 诚实挖矿实验内容设计

为简化实验,假设一条记录为一个区块,矿工挖矿成功的收益为 1,且交易费用为 0.本文针对诚实矿工挖矿设计了一个实验,对具有不同算力的 10 个矿工进行了 2 000 次模拟交易,统计各个节点的收益,并对数据进行了分析,得出节点的算力和收益之间的关系.

2.1.3 实验结果分析

为方便计算,事先设置好总的算力值为 80 000,其中矿工 M1 至 M10 各自所占总算力的比例为:6%,7%,7.5%,8.5%,9.5%,10.5%,11%,12%,13% 和 15%.

经过 2 000 笔交易以后,各矿工的最终收益如表 1 所示.

表 1 不同算力下 10 个矿工挖矿收益

Table 1 Profit of ten miners with different computing power

矿工	收益	收益率/%
M1	106	5.31
M2	162	8.11
M3	144	7.21
M4	153	7.66
M5	183	9.16
M6	213	10.66
M7	227	11.36
M8	243	12.16
M9	281	14.06
M10	286	14.31
累计	1 998	99.99

实验中不同算力下的 10 个诚实挖矿节点的理论收益率与实际收益率对比如表 2 所示.实验数据表明理论收益与实际收益的误差率在合理范围内.

从表 1 可知,2 000 笔交易中丢失了两笔交易记录.同时,表 2 显示各个矿工的算力所占百分比和节点收益百分比基本持平,即节点拥有多少挖矿算力就几乎可以获得多少收益.对于一个诚实节点而言,其拥有的挖矿算力越大所获得的收益就越多.

2.2 自私挖矿模拟实验结果与分析

2.2.1 实验环境

自私挖矿模拟实验的实验环境和诚实挖矿实验

表 2 各矿工理论收益与实际收益对比

Table 2 The comparison table of theoretical profit and actual profit

矿工	理论收益/%	实际收益/%	具体算力值
M1	6.00	5.30	4 800
M2	7.00	8.15	5 600
M3	7.50	7.20	6 000
M4	8.50	7.65	6 800
M5	9.50	9.15	7 600
M6	10.50	10.65	8 400
M7	11.00	11.35	8 800
M8	12.00	12.15	9 600
M9	13.00	14.05	11 200
M10	15.00	14.30	12 000

环境相似,此处不再赘述.

2.2.2 *自私挖矿实验内容设计*

本次自私挖矿实验共建立 4 个挖矿节点,1 个发送节点和 1 个统计节点(即在 Linux 系统中建立 4 个挖矿终端节点,1 个发送终端,1 个统计终端).在本实验中,我们设置用每分钟计算哈希值的个数来表示算力,4 个挖矿节点分为 2 个算力分别为 15 000(占总体算力的 18.2%)和 27 500 的自私节点(占总体算力的 33.3%),以及 2 个算力均为 20 000(占总体算力的 24.2%)的诚实节点.实验共进行 1 000 次模拟挖矿实验,统计各个挖矿节点的收益.

2.2.3 *自私挖矿模拟实验结果与分析*

自私挖矿模拟实验的结果如表 3 和表 4 所示.其中,SM1 和 SM2 分别表示算力为 15 000 和 27 500 的自私挖矿节点,M11 和 M12 别表示另外 2 个相同算力的诚实挖矿节点.

表 3 自私挖矿收益统计

Table 3 Experimental data of selfish mining

交易数	SM1	SM2	M11	M12
100 笔后	5	33	14	15
200 笔后	12	57	25	35
300 笔后	25	87	40	58
400 笔后	34	118	65	72
500 笔后	44	140	90	85
600 笔后	51	166	110	98
700 笔后	62	189	129	111
800 笔后	70	213	148	129
900 笔后	84	240	168	145
1 000 笔后	98	271	186	161

表 4 1 000 笔交易节点算力和收益对比

Table 4 Comparison table of node computing power and revenue

节点	算力	算力比率/%	实际收益	实际收益比率/%
SM1	15 000	18.18	98	13.68
SM2	27 500	33.33	271	37.85
M11	20 000	24.24	186	25.98
M12	20 000	24.24	161	22.49

由表 3,表 4 可以得知,两个自私挖矿节点同时进行自私挖矿的情况下,整个系统交易丢失率整体上趋于平稳,丢失率基本稳定在 30%左右.两个自私挖矿节点由于算力的不同,存在收益上的差异.自私挖矿节点 SM1 的算力占系统总算力的 18.18%,收益却只有总收益的 13.68%;而自私挖矿节点 SM2 的算力占系统总算力的 1/3,收益却达总收益的 37.85%.由此可见,SM1 和 SM2 之间存在以算力为主要因素,其他多因素共同作用的博弈过程,同时 SM1 的算力也低于其余两个诚实节点.

上述实验数据表明,在自私挖矿过程中,如果节点的算力过小,将很难获得额外的收益,甚至会少于其采用诚实挖矿策略的收益.当自私节点的挖矿算力达到整个系统算力的 1/3 时,自私节点可以获得比诚实挖矿策略更多的额外收益.

3 总结

本文研究了比特币平台中的比特币挖掘策略,系统地展示了不同挖矿策略下旷工的收益情况.首先简要介绍了自私挖矿的概念和比特币的原理,然后利用大数定律和矿池中节点状态转化图建立了两个自私挖矿模型.分别采用马尔可夫随机过程和函数极值法求得各模型下的最佳相对收益,最后实验验证自私挖矿与算力之间的关系.

参考文献

References

[1] 邹均,于斌,庄鹏,等.区块链核心技术与应用[M].北京:机械工业出版社,2018
ZHOU Jun, YU Bin, ZHUANG Peng, et al. Blockchain core technology and application[M]. Beijing: Machine Press,2018

[2] Eyal I,Sirer E G.Majority is not enough:bitcoin mining is vulnerable[J]. Communications of the ACM, 2013, 61(7):95-102

[3] 袁勇,王飞跃.区块链技术发展现状与展望[J].自动化学报,2016,42(4):481-494
YUAN Yong, WANG Feiyue. Blockchain: the state of the art and future trends[J]. Acta Automatica Sinica, 2016,

42(4):481-494
[4] Heilman E,Kendler A,Zohar A,et al.Eclipse attacks on Bitcoin's peer-to-peer network[C]// Usenix Conference on Security Symposium. USENIX Association, 2015: 129-144
[5] 夏清,张凤军,左春.加密数字货币系统共识机制综述[J].计算机系统应用,2017,26(4):1-8
XIA Qing,ZHANG Fengjun,ZUO Chun.Review for consensus mechanism of cryptocurrency system [J]. Computer Systems & Applications,2017,26(4):1-8
[6] Nayak K,Kumar S,Miller A,et al.Stubborn mining:generalizing selfish mining and combining with an eclipse attack[C]//2016 IEEE European Symposium on Security and Privacy (EuroS&P).IEEE,2016
[7] Eyal I. The miner's dilemma [C] // 2015 IEEE Symposium on Security and Privacy.IEEE,2015:89-103
[8] Anish L J.Bitcoin and other cryptocurrencies-all you need to know[EB/OL].[2017-06-02].https://www.insurancefunda.in/Bitcoin-cryptocurrency/
[9] 李旭东,牛玉坤,魏凌波,等.比特币隐私保护综述[J].密码学报,2019,6(2):133-149
LI Xudong,NIU Yukun,WEI Lingbo,et al.Overview on privacy protection in bitcoin[J].Journal of Cryptologic Research,2019,6(2):133-149
[10] 高永琳,程晓荣.区块链中的自私挖掘研究与分析[J].计算机工程与应用,2018,54(15):62-66
GAO Yonglin,CHENG Xiaorong.Research and analysis of selfish mining for blockchain [J]. Computer Engineering and Applications,2018,54(15):62-66
[11] Nakamoto S. Bitcoin: a peer-to-peer electronic cash system[EB/OL].(2017-02-03)[2019-08-08].https://bitcoin.org/bitcoin.pdf
[12] Heilman E.One weird trick to stop selfish miners:fresh bitcoins, a solution for the honest miner [C] // International Conference on Financial Cryptography and Data Security.Springer,Berlin:Heidelberg,2014:161-162
[13] Gervais A,Karame G O,Wüst K,et al.On the security and performance of proof of work blockchains[C]//Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security.ACM,2016:3-16
[14] Sapirshtein A,Sompolinsky Y,Zohar A.Optimal selfish mining strategies in bitcoin[M]//Financial Cryptography and Data Security. Berlin, Heidelberg: Springer Berlin Heidelberg, 2017: 515-532. DOI: 10.1007/978-3-662-54970-4_30
[15] Swanson E.Bitcoin mining calculator[EB/OL].(2017-02-03)[2019-08-08].http://www.alloscomp.Com/bitcoin/calculator

A security survey of mining strategies on bitcoin platform

HONG Yang[1] WANG Lisong[1] GE Chunpeng[1]
1 School of Computer Science and Technology,Nanjing University of Aeronautics and Astronautics,Nanjing 211106

Abstract Blockchain,the underlying technology of Bitcoin,has been widely deployed in many systems including the cryptocurrency,supply chain system due to its transparency,unforgeability and immutability.However,the most of the blockchain platforms such as the Bitcoin are facing the security problems including selfish mining attack, which cause serious effects to the development of blockchain technology.Selfish mining is a kind of strategy in the blockchain technology where selfish miners increase their profit by selectively publishing hidden blocks.Utilizing the central limit theorem and node state transition diagram to establish two probability models in theory,then we use Markov stochastic process and function extremum method to figure out the optimal relative profit.Meanwhile,the simulation experiment of selfish mining is designed and conducted,and the relationship between node computing power and profit in selfish mining is obtained,so as to further verify the rationality of the above models.

Key words blockchain;selfish mining;bitcoin;Markov stochastic process