doi:10.3772/j.issn.1002-0470.2020.06.006

基于离散时间 G-限量排队的区块链系统的社会最优①

袁红莉② 张大鹏③ 金顺福

(燕山大学信息科学与工程学院 秦皇岛 066004)

摘 要 数字货币受到政府部门与金融机构等行业的广泛关注,并引发了学术界对其底层区块链技术的研究热潮。为了最大化区块链系统的社会收益,研究交易个体的纳什均衡到达率与系统整体的社会最优到达率。结合区块链系统的挖矿过程、区块验证过程及矿工之间的同步行为,在离散时域下建立带有批量服务及空载服务期的 G-限量休假模型。采用再生循环法,给出系统内的交易数母函数,得到交易平均确认时间。进行系统实验,在不同的区块容量下,刻画挖矿系数与交易到达率对交易平均确认时间的影响。针对完全不可见情形,构建收益函数,改进布谷鸟寻优算法,得到交易的纳什均衡到达率和社会最优到达率。面向交易制定收费方案,调整交易到达率,最大化区块链系统的社会收益。

关键词 区块链; G-限量休假; 批量服务; 空载服务期; 再生循环法; 平均确认时间; 纳什均衡; 社会最优

0 引 言

区块链是一个由系统中所有节点集体维护的分布式数据库,具有去中心化、不可篡改、数据透明及交易安全等特性。区块链概念在 2008 年被提出,并于 2009 年 1 月正式发布[1]。如今历经 10 余年的发展,区块链技术不断推广,其应用已延伸到金融、医疗、通信等领域。

区块链技术凭借自身的优势推动着众多领域的创新。Khaqqi 等人[2]提出了一种基于信息化与自动化的新型排放交易政策(emission trading scheme, ETS),利用区块链技术和防篡改智能仪表保证了数据的透明性和可信性。基于多准则分析法的结果表明,所提方案可以实现减少排放量并鼓励长期采用减排技术的双重目标。Zyskind 等人[3]建立了一个去中心化的个人数据管理平台,将区块链与区块外存储相结合,使用户在接受第三方服务时,可以拥有和控制自己的数据,提高了数据的安全性。Fu 和 Fang[4]在文献[3]的基础上引入权益证明(proof-of-stake, POS)与可信任证明(proof-of-credibility score, POCS)的混合机制进行“挖矿”,基于节点之间的连接程度衡量节点的工作量。上述文献主要集中于区块链技术的应用研究。

自 2016 年起,部分学者基于排队论方法对区块链基础理论进行了研究。Kasahara 等人[5,6]建立了一个批量服务的 $M/G^b/1$ 模型,使用补充变量法得到了稳态下系统中的平均交易数及交易平均确认时间。然而,该模型没有体现区块的生成过程与区块链的建立过程。Li 等人[7]提出了一种批量服务的 GI/M/1 型随机排队模型,用矩阵几何解方法得到了稳态下系统中的平均交易数、每个区块内的平均交易数及交易平均确认时间。与文献[5,6]相比,该模型的服务过程包含了区块的生成过程和区块链的建立过程 2 个阶段。要指出的是,上述文献均未考虑空块 coinbase 交易,并缺少对矿工收益的研究。

本文将区块的生成过程抽象为休假,区块链的

① 国家自然科学基金(61872311, 61973261)和河北省自然科学基金(F2017203141)资助项目。

② 女,1994 年生,硕士生;研究方向:区块链,排队论应用;E-mail: 981017736@qq.com

③ 通信作者,E-mail: daniao@ysu.edu.cn

(收稿日期:2019-08-12)

建立过程抽象为服务,考虑区块容量,在离散时域下建立带有批量服务及空载服务期的G-限量休假模型。利用再生循环法,求得稳态下交易平均确认时间,研究区块容量、挖矿系数与交易到达率对区块链系统性能的影响。结合博弈理论,构建收益函数,在完全不可见情形下得到交易的纳什均衡到达率与社会最优到达率。改进布谷鸟寻优算法,以区块链系统社会收益最大化为目标,面向交易制定合理的收费方案。

1 区块链交易确认过程及系统模型

1.1 交易确认过程

区块链是一种把区块以链的方式组织在一起的数据结构,主要解决在没有第三方信任机构参与的情况下如何在所有节点之间达成共识的问题。专注于一个矿工,给出区块链中的交易确认过程如图1所示。

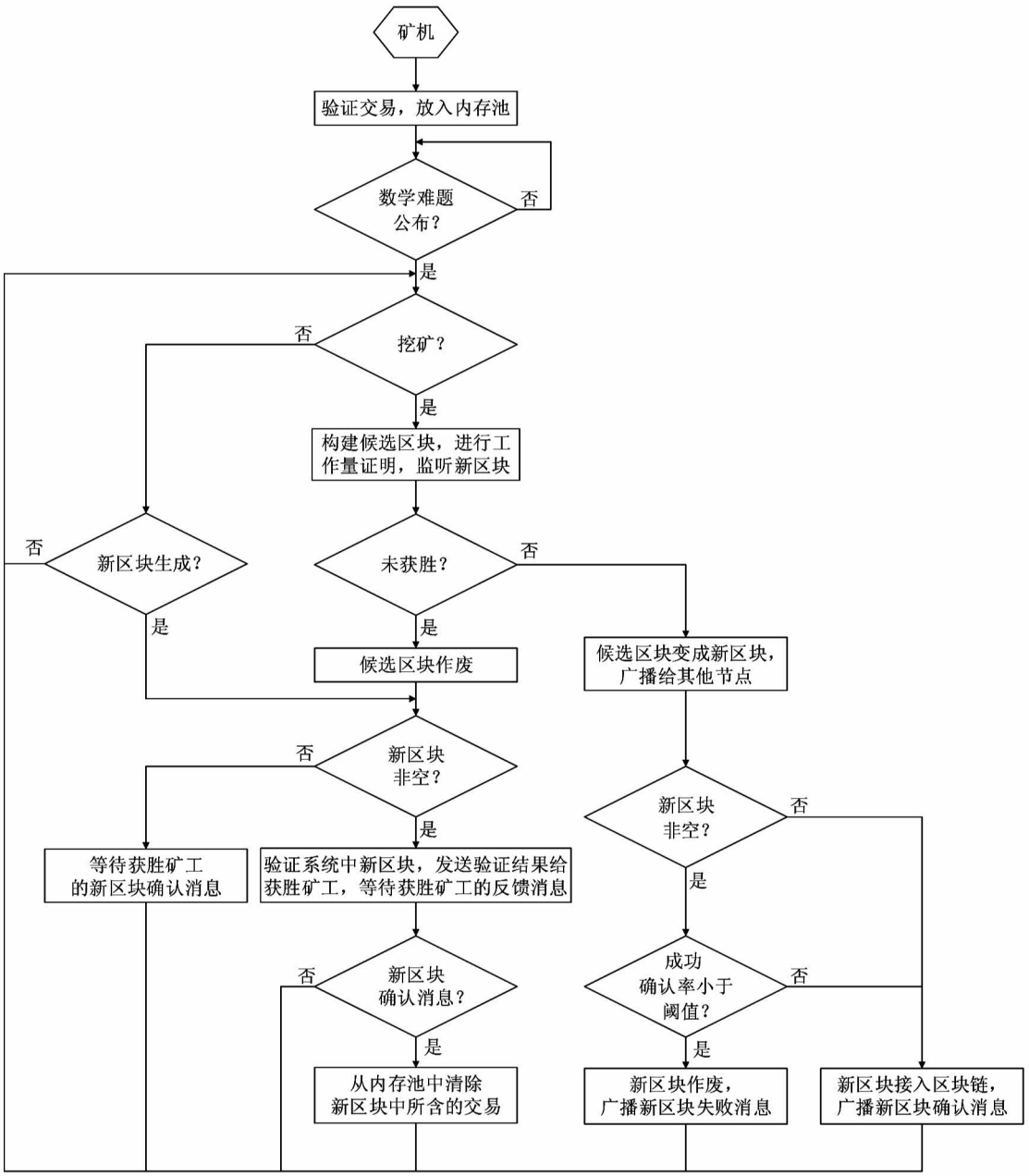


图1 区块链中的交易确认过程

区块链系统中的交易不断产生。用户产生某笔交易后,需要广播该交易至区块链系统中的所有矿工。每个矿工先进行交易验证,再把验证通过的交易放入各自的内存池中。争夺区块记账权的矿工从内存池中选出交易构建候选区块,并通过求解数学难题,即挖矿过程,进行工作量证明。获胜矿工的候选区块升级为新区块,同时将新区块广播给其余未获胜矿工。未获胜矿工首先将各自的候选区块作废并验证收到的新区块,然后将验证结果发送给获胜矿工。只有当成功验证新区块的矿工数目超过系统规定的阈值时,获胜矿工才可以将新区块接入区块链,并反馈新区块确认消息给其余矿工。获胜矿工之外的所有矿工收到新区块确认消息后,从各自的内存池中清除新区块中所含的交易。若新区块是空块,获胜矿工直接将新区块接入区块链。

由图 1 可知,区块链交易的一个生命周期由交易产生、交易传播、交易放入区块及区块接入区块链构成。

在区块链系统中,区块容量、挖矿系数及单位时间内到达的交易数目等都会影响交易用户的体验质量(quality of experience,QoE)。为了提高区块链系统的性能,需要建立合理的数学模型,定量刻画交易平均确认时间的变化趋势。

1.2　新型 G-限量休假模型

由区块链系统中的交易确认过程可知,每个区块的容量均有上限,且一个区块内的所有交易同时得到验证。将挖矿过程视为休假,空块接入区块链的过程视为空载服务期,非空新区块的验证(假设每个区块均可以通过验证)及接入区块链的过程视为普通服务期,建立一种带有批量服务及空载服务期的新型 G-限量休假模型。该模型的状态转移过程如图 2 所示。

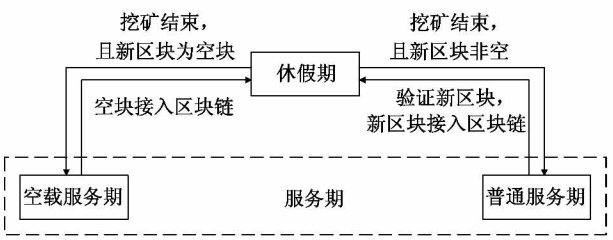


图 2　新型 G-限量休假模型的状态转移

休假期内,矿工求解数学难题。数学题越难,即挖矿系数越小,休假期越长。难题求解成功后,休假结束。此时,若获胜矿工产生的新区块为空块,系统转入空载服务期,否则转入普通服务期。

若系统转入空载服务期,获胜矿工将空块接入区块链后,空载服务期结束。若系统转入普通服务期,获胜矿工之外的所有矿工验证非空新区块内的交易,获胜矿工将非空新区块接入区块链后,普通服务期结束。任何一个服务期结束,系统均返回休假期,进行下一次的挖矿过程。相邻 2 次挖矿过程起始点之间的时间长度称为一个挖矿循环。

区块链系统中的状态转移持续进行。与已有模型不同,新型 G-限量休假模型中交易验证呈现出批量服务特点且具有空载服务期。

2　模型解析

在离散时间排队系统中,交易的到达和离去均只能发生在单位时隙处,假设交易的到达与离去分别发生在时隙末端与时隙首端,且在该时隙末端到达的交易不会在此时隙首端离去,将会在下一个时隙首端离去。

文献[5-7]对新型 G-限量休假模型作出如下假设。

交易到达构成参数为 $p(0 < p < 1, \bar{p} = 1 - p)$ 的 Bernoulli 过程。一个时隙内到达交易数的母函数为 $\Lambda(z) = pz + \bar{p}$。

空载服务期与普通服务期形态相同,简称为服务期。服务期的时间长度 S 服从一般分布,其概率分布、均值和母函数分别为

$$b_k = P\{S = k\},\ k \geqslant 1$$

$$E[S] = \frac{1}{\mu},\ 0 < \mu < 1$$

$$S(z) = \sum_{k=1}^{\infty} z^k b_k$$

令 A_S 表示一个服务期内到达的交易数量,其概率分布和母函数分别为

$$a_j = P\{A_S = j\}$$

$$A_s(z) = \sum_{j=0}^{\infty} z^j a_j = S(pz + \bar{p}) = S(\Lambda(z))$$

休假期的时间长度 V 服从一般分布,其概率分布、均值和母函数分别为

$$v_k = P\{V = k\},\ k \geqslant 1$$

$$E[V] = \frac{1}{\theta},\ 0 < \theta < 1$$

$$V(z) = \sum_{k=1}^{\infty} z^k v_k$$

按照先到先服务的规则将交易放入区块,且每个区块最多可容纳 M 个交易。将一个服务期与其后的休假期之和称为忙循环。当一个忙循环内平均到达的交易数小于区块容量,即 $p(E[V] + E[S]) < M$ 时,系统趋于稳态。

2.1 服务期开始时刻的交易数母函数

令 Q_b 表示一个服务期开始时刻系统内的交易数,其概率分布和母函数分别为

$$q_k = p\{Q_b = k\},\ k \geqslant 0$$

$$Q_b(z) = \sum_{k=0}^{\infty} z^k q_k$$

考虑相继 2 个服务期开始时刻系统内的交易数,有:

$$\begin{aligned} q_k &= \sum_{j=0}^{M-1} q_j P\{S + V \text{内到} k \text{个交易}\} \\ &\quad + \sum_{j=M}^{M+k} q_j P\{S + V \text{内到} k + M - j \text{个交易}\} \\ &= \sum_{j=0}^{M-1} q_j \sum_{a=k}^{\infty} P\{S + V = a\} \binom{a}{k} p^k \bar{p}^{a-k} \\ &\quad + \sum_{j=M}^{M+k} q_j \sum_{a=k+M-j}^{\infty} P\{S + V = a\} \\ &\quad \binom{a}{k + M - j} p^{k+M-j} \bar{p}^{a-(k+M-j)} \end{aligned}$$

对上式取母函数,可得:

$$\begin{aligned} Q_b(z) &= S(\Lambda(z))V(\Lambda(z)) \sum_{j=0}^{M-1} q_j \\ &\quad + \frac{1}{z^M} \sum_{j=M}^{\infty} q_j z^j S(\Lambda(z))V(\Lambda(z)) \end{aligned} \tag{1}$$

引入部分母函数,可得:

$$Q_M(z) = \sum_{k=0}^{M-1} z^k q_k$$

式(1)可改写为

$$Q_b(z) = \frac{(z^M Q_M(1) - Q_M(z))S(\Lambda(z))V(\Lambda(z))}{z^M - S(\Lambda(z))V(\Lambda(z))} \tag{2}$$

引理 1 对任意小实数 $\varepsilon > 0$,当 $|z| = 1 + \varepsilon$ 时,一个非负整数随机变量 C 的母函数满足如下不等式:

$$|C(z)| \leqslant 1 + \varepsilon E[C] + o(\varepsilon)$$

其中,$|C(z)|$ 为母函数 $C(z)$ 的模,$E[C]$ 为随机变量 C 的均值。

证明 令一个非负整数随机变量 C 的概率分布和母函数分别为 c_k 和 $C(z)$。

$$c_k = P\{C = k\},\ k \geqslant 0$$

$$C(z) = \sum_{k=0}^{\infty} z^k c_k$$

对任意小实数 $\varepsilon > 0$,当 $|z| = 1 + \varepsilon$ 时,有:

$$|C(z)| = \left|\sum_{k=0}^{\infty} z^k c_k\right| \leqslant \sum_{k=0}^{\infty} c_k (1 + \varepsilon)^k \tag{3}$$

根据泰勒公式[8],可得:

$$\begin{aligned} \sum_{k=0}^{\infty} c_k (1 + \varepsilon)^k &= \sum_{k=0}^{\infty} c_k (1 + k\varepsilon) + o(\varepsilon) \\ &= 1 + \varepsilon E[C] + o(\varepsilon) \end{aligned} \tag{4}$$

综合式(3)和式(4),可得:

$$|C(z)| \leqslant 1 + \varepsilon E[C] + o(\varepsilon)$$

证毕。

由式(2)可知,为了确定服务期开始时刻的交易数母函数 $Q_b(z)$,必须给出部分母函数 $Q_M(z)$ 的系数 $q_0, q_1, \cdots, q_{M-1}$。

在式(2)的分母中,令 $g(z) = -S(\Lambda(z))V(\Lambda(z))$,由引理 1 可得:

$$|g(z)| \leqslant 1 + \varepsilon p(E[V] + E[S]) + o(\varepsilon) \tag{5}$$

令 $f(z) = z^M$,根据泰勒公式[8],$f(z)$ 表示为

$$|f(z)| = (1 + \varepsilon)^M = 1 + \varepsilon M + o(\varepsilon) \tag{6}$$

综合式(5)和式(6),在系统稳态条件 $p(E[V] + E[S]) < M$ 下,$|g(z)| < |f(z)|$。

$f(z)$ 在 $|z| = 1 + \varepsilon$ 内有 M 个零点。由 Rouche 定理[9]可知,$g(z) + f(z)$ 在 $|z| = 1 + \varepsilon$ 内也有 M 个零点,即式(2)的分母有 M 个零点。略去零点 $z = 1$,其他 $M - 1$ 个零点记为 z_m,$m = 1, \cdots, M - 1$。

式(2)的分子与分母有相同的零点,给出 $M - 1$ 个方程如下:

$$z_m^M \sum_{j=0}^{M-1} q_j - Q_M(z_m) = 0, m = 1, \cdots, M - 1 \tag{7}$$

在式(2)中,令 $z=1$,使用洛必达法则,给出方程如下:

$$Q'_M(1)=p(E[V]+E[S])-M(1-Q_M(1)) \tag{8}$$

结合式(7)和式(8)可唯一确定部分母函数 $Q_M(z)$ 的系数 q_0, q_1,…, q_{M-1},进而可以给出服务期开始时刻交易数母函数 $Q_b(z)$。

2.2 交易平均确认

交易确认时间定义为从一个交易进入区块链系统到包含这笔交易的区块接入到区块链为止的时间间隔,记为 T。

处理非空竭休假模型的常用工具之一是再生循环法[10]。使用该方法需要给出一个服务期内平均服务的交易数和每个交易服务完成时刻系统内尚存交易数的母函数。

一个服务期内服务的交易数均值 $E[\Phi]$ 为 $E[\Phi]=\sum_{k=0}^{M-1}kq_k+M\sum_{k=M}^{\infty}q_k=Q'_M(1)+M(1-Q_M(1))$。将式(8)代入上式可得:

$$E[\Phi]=p(E[V]+E[S]) \tag{9}$$

一个区块内的交易是批量服务的,为了方便解析,人为设定区块内的交易顺序,但是不同交易服务完成时刻的间隔为 0。

令 L_n 表示一个区块内的第 n 个交易服务完成时刻系统内尚存交易的数量,则 $L_n=Q_b+A_s-n$, $n=1,\cdots,\Phi$。L_n 的母函数 $L_n(z)$ 为

$$\begin{aligned}L_n(z)&=E[z^{Q_b+A_s-n}]\\&=\sum_{k=0}^{M-1}q_kz^{k-n}S(\Lambda(z))+\sum_{k=M}^{\infty}q_kz^{k-n}S(\Lambda(z))\end{aligned}$$

利用再生循环法和 PASTA 性质[11],得到稳态下任意时刻系统内的交易数母函数 $L(z)$ 为

$$\begin{aligned}L(z)&=\frac{\sum_{n=1}^{\Phi}L_n(z)}{E[\Phi]}\\&=\frac{S(\Lambda(z))((z^M-1)Q_b(z)+Q_M(z)-z^MQ_M(1))}{p(E[V]+E[S])(z-1)z^M}\end{aligned}$$

将式(2)代入上式,整理后可得:

$$L(z)=\frac{S(\Lambda(z))(Q_M(z)-z^MQ_M(1))(S(\Lambda(z))V(\Lambda(z))-1)}{p(E[V]+E[S])(z-1)(S(\Lambda(z))V(\Lambda(z))-z^M)} \tag{10}$$

对式(10)求导,令 $z=1$,可得任意时刻系统内的交易数均值 $E[L]$ 为

$$\begin{aligned}E[L]&=pE[S]+\frac{Q''_M(1)+M(M-1)(1-Q_M(1))}{2(Q'_M(1)-MQ_M(1))}\\&-\frac{M_p(E[V(V-1)]+E[S(S-1)]+2E[V]E[S])}{2(E[V]+E[S])(Q'_M(1)-MQ_M(1))}\end{aligned} \tag{11}$$

由 Little 公式[12]可得,交易平均确认时间 $E[T]$ 为

$$\begin{aligned}E[T]&=\frac{E[L]}{p}\\&=E[S]+\frac{Q''_M(1)+M(M-1)(1-Q_M(1))}{2p(Q'_M(1)-MQ_M(1))}\\&-\frac{M(E[V(V-1)]+E[S(S-1)]+2E[V]E[S])}{2(E[V]+E[S])(Q'_M(1)-MQ_M(1))}\end{aligned} \tag{12}$$

直观地,交易平均确认时间随交易到达率单调不减。为了在不同的区块容量与挖矿系数下定量刻画交易平均确认时间的变化趋势,需进行系统实验。

3 交易平均确认时间的系统实验

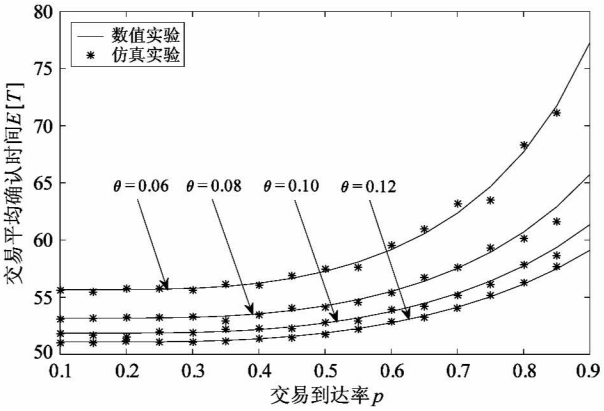
实验所用 CPU 型号为 Intel(R) Core(TM) i7-4790,CPU 运行频率为 3.60 GHz,系统内存为 8.00 GB。数值实验在 Matlab 2016a 环境中运行,仿真实验在 Myeclipse 2014 环境中采用 Java 语言实现。

文献[13,14]假设挖矿过程服从参数为 θ 的几何分布,服务期的时间长度服从参数为 μ 的几何分布,进行数值实验与仿真实验。在稳态条件的约束下,实验参数设定为服务强度 $\mu=0.04$,区块容量 $M=50$、100,挖矿系数 $\theta=0.06$、0.08、0.10、0.12。

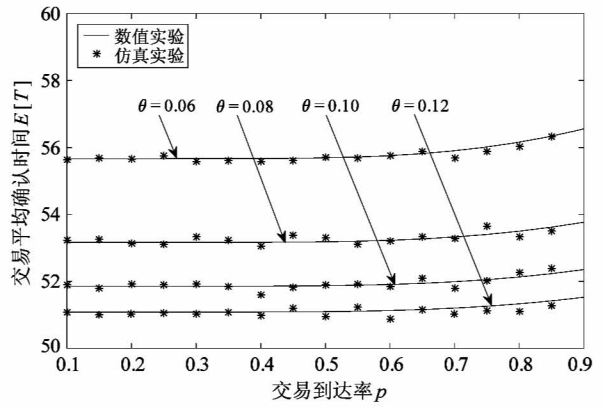
针对不同的区块容量 M,图 3 刻画了挖矿系数 θ 与交易到达率 p 对交易平均确认时间 $E[T]$ 的影响。

图 3 表明,当区块容量 M 与挖矿系数 θ 固定时,交易平均确认时间 $E[T]$ 随交易到达率 p 的增大呈上升趋势。交易到达率越大,区块链系统中的交易数越多。由于一个区块所能容纳的交易数是有限

的,系统中的交易数越多,服务完成全部交易所需要的区块数越多,每个交易平均经历的挖矿循环次数也就越多。因而交易平均确认时间呈上升趋势。



(a) $M = 50$



(b) $M = 100$

图 3　交易平均确认时间的变化趋势

纵向分析图 3,在相同的区块容量 M 与交易到达率 p 下,挖矿系数 θ 越大,交易平均确认时间 $E[T]$ 越小。挖矿系数大,意味着矿工求解数学难题的时间短,即挖矿过程短,交易可以更早地放入区块并得到确认。因而交易平均确认时间呈下降趋势。

对比图 3(a)与图 3(b),在相同的挖矿系数 θ 与交易到达率 p 下,区块容量 M 越大,交易平均确认时间 $E[T]$ 越小。一个区块所能容纳的交易数越多,服务完成全部交易所需的区块数越少,每个交易平均经历的挖矿循环越少,因而交易平均确认时间下降。随着交易到达率 p 的增大,区块容量 M 对交易平均确认时间 $E[T]$ 的影响变大。当交易到达率较小时,系统中的交易几乎可以放入一个区块内,此时区块容量对交易平均确认时间的影响小。当交易到达率较大时,往往需要多个区块才能服务完成全部交易。区块容量越小,所需区块数越多,每个交易平均经历的挖矿循环越多,此时区块容量对交易平均确认时间的影响变大。

在区块链系统中,交易到达率越小,交易平均确认时间越短,用户体验的服务质量越好。而交易到达率越大,区块链系统的收益越高。综合考虑区块链用户的体验质量与区块链系统的收益,需要研究交易的纳什均衡行为与社会最优行为。

4　交易费方案

4.1　纳什均衡行为

每个交易都愿意进入区块链系统得到服务,但又不愿意承受过长的等待时间。假设交易到达区块链系统时,在完全不可见情形下,每个交易均从个体利益的角度出发,决定是否进入区块链系统接受服务[15]。

交易的个人收益定义为完成服务所获得的回报减去等待确认所花费的成本。交易的个人收益 $G_{ind}(p)$ 表示如下。

$$G_{ind}(p) = R - CE[T]$$

其中,R 为交易完成服务所获得的回报,C 为交易在区块链系统滞留时单位时间所花费的成本。为了保证新到达的交易一定选择进入空的区块链系统,须满足 $R > CE[T]$。

考虑系统的稳态条件,设置交易到达率的上界为 $p_{\max}$,分析交易的纳什均衡到达率。

当 $G_{ind}(p_{\max}) \geqslant 0$ 时,区块链系统的全部交易都将获得非负的收益,即每个交易的收益为非负值。交易以概率 $q_e = 1$ 进入系统为一个均衡策略,区块链系统的纳什均衡到达率 $p_e = p_{\max}$。

当 $G_{ind}(0) \leqslant 0$ 时,即使进入区块链系统的交易可以直接接受服务,其所获收益也为非正值。交易以概率 $q_e = 0$ 进入系统为一个均衡策略,区块链系统的纳什均衡到达率 $p_e = 0$。

当 $G_{ind}(0) \leqslant G_{ind}(p) \leqslant G_{ind}(p_{\max})$ 时,只有部分

进入区块链系统的交易可以获得非负的收益。交易以概率 $0 < q_e < 1$ 进入系统为一个均衡策略，区块链系统的纳什均衡到达率 $0 < p_e < 1$。

为了揭示交易个人收益的变化规律，进行数值实验。沿用第 3 节的实验参数，并设置 $R = 350$，$C = 6$。在 $M = 50$ 下，交易个人收益 $G_{ind}(p)$ 随交易到达率 p 的变化情况如图 4 所示。

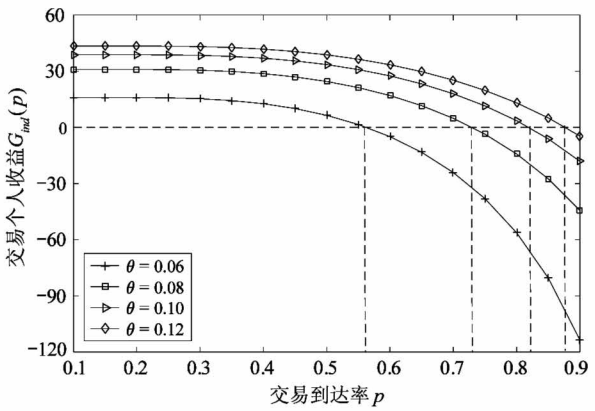


图 4　交易个人收益的变化趋势

由图 4 观察到，对于所有的挖矿系数 θ，交易个人收益 $G_{ind}(p)$ 均随交易到达率 p 的增大呈下降趋势。随着交易到达率的增加，交易平均确认时间延长，交易所花费的时间成本提高，因而交易个人收益下降。个人收益为 0 时所对应的交易到达率即为纳什均衡到达率。在相同的区块容量 M 下，挖矿系数 θ 越大，纳什均衡到达率 p_e 越大。交易完成服务所获得的回报是固定的，挖矿系数越大，交易所花费的成本越小。增大交易到达率，直至成本与服务所获得的回报持平，即达到均衡状态。因此纳什均衡到达率变大。

4.2　社会最优行为

区块链系统的社会收益定义为单位时间内所有交易的个人收益与获胜矿工获得的区块奖励之和。社会收益 $G_{soc}(p)$ 表示如下：

$$G_{soc}(p) = p(R - CE[T]) + Q \tag{13}$$

其中，Q 为单位时间内获胜矿工获得的区块奖励。

通过最大化社会收益 $G_{soc}(p)$，可以得到交易的社会最优到达率 p^* 表示如下。

$$p^* = \underset{0<p<p_{\max}}{\operatorname{argmax}}\{p(R - CE[T]) + Q\} \tag{14}$$

从式(12)无法得到交易到达率 p 的显示解，同时式(13)中社会收益 $G_{soc}(p)$ 关于 p 的单调性也无法确定。为了得到较准确的社会最优到达率，使用智能寻优算法。

布谷鸟寻优算法[16]的全局搜索能力强，但收敛速度较慢。为了提高收敛速度同时也能获得较高的寻优精度，引入自适应步长与动态步长缩放因子改进布谷鸟寻优算法，沿用第 4.1 节的实验参数，并设置 $Q = 10$，求解不同挖矿系数下的社会最优到达率。改进的布谷鸟寻优算法的主要步骤如下。

步骤 1　初始化鸟窝数量 n，宿主发现外来蛋的概率 p_a，鸟窝位置的上界 U_b 与下界 L_b，当前迭代次数 $Gen = 0$，最大迭代次数 $MaxGen$，步长 s 的最大值 $s_{\max}$ 与最小值 $s_{\min}$，步长缩放因子 r 的最大值 $r_{\max}$ 与最小值 $r_{\min}$。

步骤 2　初始化鸟窝位置 $nest_i$。

for $i = 1:n$

$nest_i = L_b + (U_b - L_b) \times rand$

endfor

步骤 3　更新鸟窝位置对应的目标函数值 $fnew_i$。

for $i = 1:n$

计算第 i 个鸟窝位置所对应的平均队长

% 平均队长由式(11)得到

计算第 i 个鸟窝位置所对应的平均确认时间

% 平均确认时间根据 Little 公式得到

$fnew_i = G_{soc}(nest_i)$

% 社会收益由式(13)得到

endfor

步骤 4　寻找当前最优鸟窝位置 $bnest$，计算当前最大目标函数值 $fmax$。

$best = \underset{i\in\{1,2,\cdots,n\}}{\operatorname{argmax}} fnew_i$

$fmax = G_{soc}(best)$

$Gen = Gen + 1$ % 更新当前迭代次数

if $Gen > MaxGen$

then 跳转到步骤 7

endif

步骤 5　使用自适应步长 s 更新鸟窝位置。

for $i = 1:n$

$d_i = (nest_i - best)/d_{\max}$

% $d_{\max}$ 表示当前最优位置与其余鸟窝位置距离的最大值

$s_i = s_{\min} + (s_{\max} - s_{\min}) \times d_i$

$nest_i = best + s_i$

endfor

步骤 6 以概率 p_a 更新鸟窝位置。

for $i = 1:n$

if $rand > p_a$

$r = r_{\max} - (r_{\max} - r_{\min}) \times Gen/MaxGen$

% 确定动态步长缩放因子

$s_i = r \times (nest_m - nest_w)$

$nest_i = nest_i + s_i$

endif

endfor

返回步骤 3

步骤 7 输出鸟窝位置 $best$ 为社会最优到达率 p^*,目标函数值 $fmax$ 为最大社会收益 $G_{soc}(p^*)$。

基于参数 $n = 10$, $r_{\max} = 0.999999$, $MaxGen = 40$, $p_a = 0.25$, $U_b = 0.9$, $L_b = 0.1$, $s_{\max} = 0.01$, $s_{\min} = 0.01$, $r_{\min} = 0.000001$,利用改进的布谷鸟算法解出社会最优到达率与最大社会收益如表 1 所示。

表 1 社会最优到达率

挖矿系数 θ	社会最优到达率 p^*	最大社会收益 $G_{soc}(p^*)$
0.06	0.3803	15.0993
0.08	0.4856	22.2976
0.10	0.5423	27.0079
0.12	0.5784	30.1551

比较图 4 的纳什均衡到达率与表 1 的社会最优到达率,观察到在相同的挖矿系数下,交易的纳什均衡到达率大于社会最优到达率。为了降低交易的纳什均衡到达率使之与社会最优到达率一致,制定交易费收取方案,实现区块链系统的社会最优。

4.3 交易费

考虑交易费 f,交易的个人收益 $G'_{ind}(p)$ 为

$$G'_{ind}(p) = R - CE[T] - f \tag{15}$$

区块链系统的社会收益 $G'_{soc}(p)$ 为

$$\begin{aligned} G'_{soc}(p) &= p(R - CE[T] - f) + Q + pf \\ &= p(R - CE[T]) + Q \end{aligned} \tag{16}$$

比较式(15)与式(16)可以发现,区块链系统的社会收益并不受交易费的影响。区块链系统包括交易与矿工 2 部分。面向交易收取的费用全部转移给了矿工,因此区块链系统的社会收益不变。

将社会最优到达率 p^* 代入式(15)并令 $G'_{ind}(p^*) = 0$ 可得交易费 f 表达式:

$f = G_{ind}(p^*)$

使用与图 4 相同的实验参数,基于不同的挖矿系数计算出交易费如表 2 所示。

表 2 交易费数值结果

挖矿系数 θ	纳什均衡到达率 p_e	最大社会收益 p^*	交易费 f
0.06	0.5631	0.3803	13.4086
0.08	0.7299	0.4856	25.3247
0.10	0.8196	0.5423	31.3626
0.12	0.8772	0.5784	34.8463

从表 2 可以看出,随着挖矿系数 θ 的增大,交易费 f 呈上升趋势。挖矿系数越大,即矿工求解数学难题越快,交易平均确认时间越短,可能有更多的交易到达系统。为控制交易到达率,使之与社会最优到达率一致,需设置较高的交易费。

5 结 论

基于区块链系统的交易确认过程,提出了一种带有批量服务及空载服务期的 G-限量休假模型,研究交易纳什均衡到达率与社会最优到达率。采用再生循环法,给出了稳态下交易平均确认时间的表达式。进行数值实验与仿真实验,研究了区块容量、挖矿系数及交易到达率对交易平均确认时间的影响。构建交易的个人收益函数,给出了交易的纳什均衡到达率。构建区块链系统的社会收益函数,改进布谷鸟寻优算法,得到了交易的社会最优到达率。实验结果表明,在相同的挖矿系数下,交易的纳什均衡到达率高于社会最优到达率。基于该偏差,制定交易费方案,实现区块链系统社会收益的最大化。

参考文献

[1] Nakamoto S. Bitcoin: a peer-to-peer electronic cash system[EB/OL]. https://bitcoin.org/bitcoin.pdf: Bitcoin, 2008

[2] Khaqqi K N, Sikorski J J, Hadinoto K, et al. Incorporating seller/buyer reputation-based system in blockchain-enabled emission trading application[J]. *Applied Energy*, 2018, 209: 8-19

[3] Zyskind G, Nathan O, Pentland A. Decentralizing privacy: using blockchain to protect personal data[C]//Proceedings of International Conference on Security and Privacy Workshops, San Jose, USA, 2015: 180-184

[4] Fu D Q, Fang L R. Blockchain-based trusted computing in social network[C]//Proceedings of International Conference on Computer and Communications, Chengdu, China, 2016: 19-22

[5] Kasahara S, Kawahara J. Effect of Bitcoin fee on transaction-confirmation process[J]. *Journal of Industrial and Management Optimization*, 2019, 15(1): 365-386

[6] Kawase Y, Kasahara S. Transaction-confirmation time for Bitcoin: a queueing analytical approach to blockchain mechanism[C]//Proceedings of International Conference on Queueing Theory and Network Applications, Qinhuangdao, China, 2017: 75-88

[7] Li Q L, Ma J Y, Chang Y X. Blockchain queueing theory[C]//Proceedings of International Conference on Computional Social Networks, Shanghai, China, 2018: 25-40

[8] Benjemaa M. Taylor's formula involving generalized fractional derivatives[J]. *Applied Mathematics and Computation*, 2018, 35: 182-195

[9] 张益宁, 孙炯, 李昆, 等. 一类具有转移条件的 Sturm-Liouville 问题的特征值的渐近估计[J]. 数学的实践与认识, 2018, 48(6): 263-27

[10] Takagi H. Queueing Analysis[M]. Amsterdam: North-Holland, 1991

[11] 管世恒, 王安民. 多服务台排队系统下提高顾客等待满意度的两类排队管理策略[J]. 系统科学与数学, 2017, 37(4): 1067-1084

[12] 王秀双, 金顺福. 基于新型休眠机制的云任务调度策略的研究[J]. 高技术通讯, 2018, 28(11-12): 27-34

[13] Zhu Y, Sheng M, Li J D, et al. Performance analysis of intermittent satellite links with time-limited queuing model[J]. *IEEE Communications Letters*, 2018, 22(11): 2282-2285

[14] 王敏, 唐应辉. 基于 Min(N,D,V)-策略和单重休假的 M/G/1 排队系统的最优控制策略[J]. 系统科学与数学, 2018, 38(9): 1067-1084

[15] Hassin R, Haviv M. To Queue or Not to Queue: Equilibrium Behavior in Queueing Systems[M]. London: Kluwer Academic Publishers, 2003

[16] Raha S B, Mandal K K, Chakraborty N. Hybrid SMES based reactive power dispatch by Cuckoo search algorithm[J]. *IEEE Transactions on Industry Applications*, 2019, 55(1): 907-917

Social optimization of blockchain system based on a discrete-time G-limited queuing

Yuan Hongli, Zhang Dapeng, Jin Shunfu

(School of Information Science and Engineering, Yanshan University, Qinhuangdao 066004)

Abstract

Digital currency has attracted wide attention from government departments, financial institutions and other industries, and has triggered a research boom in its underlying blockchain technology. In order to maximize the social benefits of the blockchain system, the Nash equilibrium and the socially optimal arrival rates of transactions are studied from the perspective of the individual and the whole, respectively. Considering the mining process, the block verification process and the synchronization among miners, a discrete-time G-limited vacation model is established with a batch service and a zero-load service. By using regenerative cycle method, this work obtains the generating function for the number of transactions in the system and the average confirmation time of transactions. With system experiments, this work illustrates the impact of mining coefficient and the arrival rate of transactions on the average confirmation time of transactions for different block capacity. From a fully unobservable perspective, this work constructs benefit functions and improves Cuckoo search algorithm to obtain the Nash equilibrium and the socially optimal arrival rates of transactions. This work charges fee on transactions to adjust the arrival rate of transactions aiming to maximize the social benefits of the blockchain system.

Key words: blockchain, G-limited vacation, batch service, zero-load service, regenerative cycle, average confirmation time, Nash equilibrium, socially optimization