Journal of Computer Applications
计算机应用, 2020, 40(9): 2646 - 2649
ISSN 1001-9081
CODEN JYIIDU
2020-09-10
http://www.joca.cn

文章编号:1001-9081(2020)09-2646-04
DOI:10.11772/j.issn.1001-9081.2020010132

基于排队博弈的最优比特币交易费支付策略

黄冬艳*,李　浪
(广西无线宽带通信与信号处理重点实验室(桂林电子科技大学),广西 桂林 541004)
(*通信作者电子邮箱huangdongyan-gua@163.com)

摘　要:在比特币交易高峰期,为使交易尽快被打包进入区块,用户需要提高交易费以竞争有限的区块空间。针对用户如何自主选择合适交易费的问题,提出了最优的交易费支付策略。首先,结合排队博弈论将交易排队竞争上链的过程建模为一个带优先权的非抢占型排队模型;然后,分析交易费对交易耗时的影响,由此给出交易耗时与交易费之间的函数关系式,并推导出用户的纳什均衡支付策略。仿真结果表明,采用最优的支付策略可以有效降低用户的总花费(等待开销与交易费的加权和)。当系统高负荷时,与不支付交易费和按拥塞度线性增加交易费这两种策略相比,所提策略的用户总花费分别降低了97%和72%。由此可见,在保证交易被尽快处理的同时,所提支付策略可以有效减少交易费支出。

关键词:比特币;区块链;交易手续费;排队博弈;支付策略
中图分类号:TP399　　**文献标志码**:A

Optimal bitcoin transaction fee payment strategy based on queuing game

HUANG Dongyan*, LI Lang
(*Guangxi Key Laboratory of Wireless Wideband Communication and Signal Processing* (*Guilin University of Electronic Technology*), *Guilin Guangxi* 541004, *China*)

Abstract: At the peak of bitcoin transactions, users need to increase the transaction fee to compete for the limited block space in order to pack the transactions into the block as soon as possible. An optimal transaction fee payment strategy was proposed to solve the problem of how to choose the appropriate transaction fees. First, the process of transactions queueing to complete for going up on the blockchain was modeled to a non-preemptive queueing model with priority by adopting the queuing game theory. Then, the impact of transaction fee on transaction time was analyzed, so as to obtain the functional relation between transaction time and transaction fee, and the Nash equilibrium payment strategy for the user was derived. Simulation results showed that the user total cost (weighted sum of the waiting time and the transaction fee) was able to be effectively reduced when the optimal payment strategy was adopted. Compared with the strategy of not paying transaction fees and the strategy of linearly increasing transaction fees according to the congestion, the proposed strategy had the user total cost decreased by 97% and 72% respectively in the system with high load. The proposed payment strategy can effectively reduce the cost of transaction fees while ensuring that the transactions are processed as quickly as possible.

Key words: bitcoin; blockchain; transaction fee; queuing game; payment strategy

0　引言

比特币[1]是以区块链技术为支撑的一种数字货币。在比特币系统中,数据以区块(block)为单位产生和存储,并按照时间顺序连成链式(chain)数据结构。区块之间通过哈希值进行关联。后一个区块的哈希值由前一个区块的哈希值、随机数以及若干等待处理的交易关参数共同决定。新区块的创建需得到全网多数节点的确认并向各节点广播实现全网同步。任何一个区块的改动将会导致该区块的哈希值发生变化,从而与链上其他区块的哈希值无法匹配。因此,比特币具有去中心化、难以篡改等特性,受到广泛关注。其底层技术区块链的应用已经延伸到智能制造[2]、物联网[3-5]、供应链[6]、电力竞价[7]交易等领域。

比特币网络的共识机制为工作量证明(Proof of Work, PoW)。在PoW共识机制下,为获得记账权或称出块权,每个参与节点必须找到符合条件的哈希值所需要的随机数。寻找随机数的过程称为"挖矿",参与"挖矿"的节点称为矿工。

目前矿工的收益由挖矿奖励和交易费两部分组成[8]。挖矿奖励是指,伴随着新区块的产生会生成一定数量的比特币,作为挖出该区块的矿工的工作奖励;交易费也称手续费,由用户自行设置,交易费作为额外奖励发给处理该交易的矿工。

交易费的存在增加了欺诈交易与无效交易的成本,从一定程度上避免了系统滥用;同时,交易费的高低很大程度上影响着交易的优先级。由于比特币中每一个区块的空间大小有一定限制,矿工需要依据多种因素(如块龄、交易费、交易大小等),选择将待处理的交易打包进入区块。为最大化自身的收益,矿工往往更愿意处理交易费高的交易。因此,交易费越高

收稿日期:2020-02-15;**修回日期**:2020-03-17;**录用日期**:2020-03-24。
基金项目:广西科技基地和人才专项(桂科AD19110042);广西无线宽带通信与信号处理重点实验主任基金资助项目(GXKL06160111)。
作者简介:黄冬艳(1984—),女,广西南宁人,副教授,博士,主要研究方向:区块链;　李浪(1996—),男,湖北黄冈人,硕士研究生,主要研究方向:区块链。

的交易被优先打包进入区块的概率越高，相应的交易耗时就越少。实际上，自2016年初以来，比特币网络容量的限制已经造成交易之间的竞争，从而导致更高的费用，免费交易彻底成为过去式。零费用或非常低费用的交易鲜少被处理，有时甚至不会在网络上传播[8]。文献[9]的调查结果也表明，交易的处理速度与交易的金额无关，而与交易费强相关，非零交易费的交易的处理速度比零交易费的交易要快。

对用户而言，交易能否被快速处理和所需交易费都是其关心的主要问题。交易费过高增加了用户交易成本，过低则会增加用户的交易耗时。因此，研究交易费与交易耗时之间的关系有助于揭示系统的交易运作规律，从而帮助用户选择合适的支付策略。

文献[10]研究了在股权证明的联盟链中，共识延迟与用户交易费之间的权衡。文献[11]结合排队理论，分析了区块链中的三个关键性能指标（系统中的平均交易数、单个区块中的平均交易数、交易的平均确认时间），设计了一个具有两个不同服务阶段的马尔可夫批量服务排队系统。文献[12]通过在用户交易之间引进第三方保险机构的做法来解决比特币的双花风险问题，给用户提供了交易安全保障。文献[13]将比特币交易按照交易金额大小分类，发现小额交易（交易金额小于1比特币）的用户占比更高，处理速度更慢。文献[14-16]基于排队论研究了系统容量、交易速率等问题。以上文献分析了系统容量、交易安全和交易速率等，但未能考虑用户之间的博弈以及用户个体的策略性决策行为对交易速率的影响。

结合排队博弈论，本文研究了比特币网络中用户交易手续费对交易耗时的影响，旨在为用户提供最优的交易手续费支付策略。本文的主要贡献如下：1）将比特币网络中交易排队竞争上链的过程建模为一个带优先权的非抢占型排队博弈模型；2）分析了交易费对交易耗时的影响并推导出用户的纳什均衡支付策略。

1　系统模型

一笔交易从提交到比特币系统中到被记录到区块中的过程如图1所示。由PoW共识机制决定，比特币的交易不是实时完成的，只有交易被写入区块并广播交易才算完成。通常认为，连续篡改6个以上区块[8]难度极大，因此真正确认一笔交易需经历6个区块。

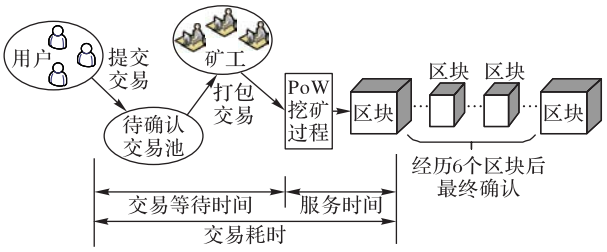

图1　交易上链示意图

Fig. 1　A transaction going up on blockchain

每个区块的大小上限为1 MB[17]（比特币在2017年8月24日实施了隔离见证（Segregated Witness，SegWit）方案，将交易数据与交易签名进行了分离，区块的实际大小仍为1 MB，但是加上签名信息后，总大小突破了1 MB上限）。其中，前50 KB保留给UTXO（Unspent Transaction Output）优先级高的交易，剩下的区块空间由其他交易竞争，矿工优先选择交易手续费高的交易来填充剩下的空间。

交易的UTXO优先级由交易的UTXO模型[8]决定。UTXO从被记录到区块链中到当前交易处理时的区块链末端所经历的区块数，称为“块龄”。交易输入值高、“块龄”大的交易比那些新的、输入值小的交易拥有更高的优先级。具体地，UTXO优先级的定义为：

$$Hp = \frac{1}{l}\sum_{i}^{N} V_i \cdot A_i \tag{1}$$

其中：N是交易的总输入个数，l表示交易的总大小，V_i表示交易第i个部分输入的金额，单位是聪，A_i是其“块龄”。当一笔交易的$Hp > 5.76 \times 10^7$时（相当于1比特币、块龄为144（大约为1 d）、交易大小为250 B），可以被打包进前50 KB中。

由于相较于1 MB的区块空间，前50 KB的字节占比很小，后面的大部分的区块空间通过交易费的高低竞争。因此本文仅讨论交易手续费对交易耗时的影响。交易耗时为交易的等待时间与交易的处理时间之和，如图1所示。其中，等待时间为交易提交到系统到被打包进区块的时间，交易处理的时间为服务时间，也即挖矿过程。

后续分析中的优先级区别于UTXO优先级，专指用户通过支付交易费获得的被优先打包进入除前50 KB字节以外的区块空间的优先权。

2　排队博弈模型与均衡支付策略

2.1　排队模型

假设每个到达的用户不知道当前系统中的交易数量，也不知道其他用户支付的交易费。用户在进队时要选择最优的支付策略使得自己的总花费最小，并且交易一旦提交交易费不可更改。

矿工处理交易的流程如图2所示。矿工根据交易费将当前交易池中的交易按照交易费高低进行排序，选取当中的前若干笔交易组成一个批次进行处理，生成一个区块，该批次中的交易费虽有不同，却一同被处理，因此将其视为同优先级的一笔业务，用其交易费均值表示此笔业务的优先级。接着，矿工开始进行PoW工作处理这笔业务。基于PoW的特性，交易一旦选定不可更改，因此，此时到达系统的交易无论交易费的高低，都必须等待当前交易处理完毕，即非抢占型优先权。基于比特币的出块特性（一次只能出一个单块），因此将矿工视为单一性服务台处理。一笔业务交易处理完成后，加入新到达的交易，对交易池进行重排列。

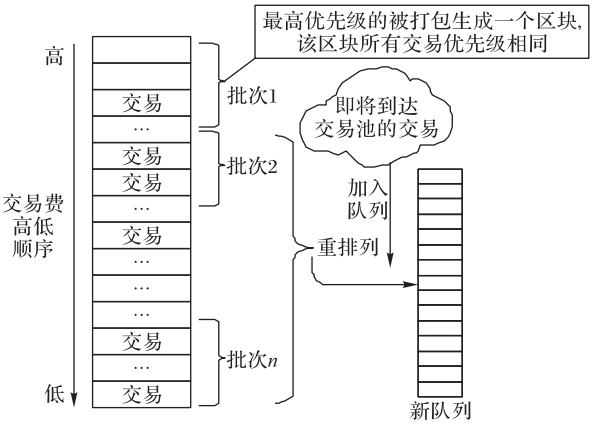

图2　矿工交易处理流程

Fig. 2　Miners processing transactions

参照文献[17-18]，本模型设定交易到达（指批次，下同）是参数为λ的泊松流，交易的处理时间（服务时间）服从参数为μ的指数分布。记$\rho = \lambda/\mu$，为系统的拥塞指标。ρ越大意味着系统越拥挤，在区块生成时间稳定的情况下意味着交易量增大。因此，整个过程可建模为一个有非抢占型优先权和

随机服务的M/M/1排队系统。

2.2 平均交易耗时

假设当前系统中有n批交易，且$n \geqslant 0$。第i批用户u_i支付的交易费均值为x_i，则用户u_i的优先级等价于交易费的总占比

$$p_i = x_i \Big/ \sum_{i=0}^{n} x_i \tag{2}$$

令$h(n,x)$为目标批次交易费为x而其他批次交易费为1时，目标批次的平均耗时。根据排队博弈论[19]可得：

$$h(n,0) = (n+1)\frac{1}{1-\rho}\frac{1}{\mu} \tag{3}$$

$$h(n,\infty) = 1/\mu \tag{4}$$

对于所有的$0 < x < \infty$，有：

$$h(n,\infty) < h(n,x) < h(n,0) \tag{5}$$

其中，$h(n,x)$满足以下差分方程：

$$h(n,x) = 1 + \lambda h(n+1,x) + \mu\frac{n}{n+x}h(n-1,x);\ n \geqslant 0 \tag{6}$$

引理1 对于所有的$n \geqslant 0$，$h(n,x)$是关于n的仿射函数，即：

$$h(n,x) = A(x)n + B(x) \tag{7}$$

其中$B(x) = (1+x)A(x)$。

将式(7)代入式(6)可得：

$$A(x) = \frac{1}{1+x-\rho}\frac{1}{\mu} \tag{8}$$

证明 假设目标批次支付x，其他批次支付为单位1。若目标批次到达时队列为空，则它的平均耗时记为$B(x)$；若目标批次到达时队列中已经存在的交易每增加1批，目标批次的平均耗时增加$A(x)$。显然目标批次会以$x/(1+x)$的概率优先于其他批次获得交易处理服务，在这种情况下，目标批次的平均耗时为$B(x)$，另外，目标批次以$1/(1+x)$概率晚于其他批次获得服务，则它的条件平均耗时为$2B(x)$，由全期望公式得$A(x) = B(x)/(1+x)$。类似地，当系统中有n批交易时，每批交易对目标批次增加的平均耗时与n无关，都是$A(x)$。 证毕。

命题1 在其他交易的交易费为单位1的情况下，交易费为x的交易的平均交易耗时$W(x)$为：

$$W(x) = \frac{1+x-\rho x}{1+x-\rho}\frac{\rho}{1-\rho}\frac{1}{\mu} \tag{9}$$

证明 设系统稳定状态下，即$0 < \rho < 1$。系统中有i批交易的概率为$P_i(i = 0,1,2,\cdots)$。其中，P_0表示系统空闲的概率且$P_0 = 1-\rho$，因此：

$$\sum_{i=0}^{\infty} P_i = 1;\ P_i \geqslant 0, i = 0,1,2,\cdots,K \tag{10}$$

平衡方程：

$$\begin{cases} \lambda P_0 = \mu P_1 \\ \lambda P_{K-1} + \mu P_{K+1} = (\lambda+\mu)P_K \end{cases} \tag{11}$$

根据数列推导，可得当目标批次到达时系统有n批交易的概率为$\rho^n(1-\rho)$，由式(6)和引理1可得：

$$W(x) = \rho\left[A(x)\sum_{n=0}^{\infty}(1-\rho)\rho^n n + B(x)\right] \tag{12}$$

计算式(12)可以得到式(9)。 证毕。

2.3 均衡交易费支付策略

命题2 设单位等待费用为c，用户总花费为$x + cW(x)$，用户的纳什均衡支付策略为支付交易费$\bar{x}$，有：

$$\bar{x} = \sqrt{\frac{c\rho^2(2-\rho)}{(1-\rho)\mu}} + \rho - 1 \tag{13}$$

证明 假设所有批次交易支付的交易费为1，若最优策略为支付$\bar{x}$，需满足：

$$\frac{\mathrm{d}}{\mathrm{d}x}(cW(x)+x)\big|_{x=\bar{x}} = 0 \tag{14}$$

由式(9)可知，$W(x)$是下凸函数，因此当$c > 0$时必存在唯一最优解$\bar{x}$。求解式(14)可以得到式(13)。 证毕。

3 仿真与评估

3.1 交易费对交易耗时的影响

根据式(9)得到平均交易耗时随交易费的变化如图3所示。

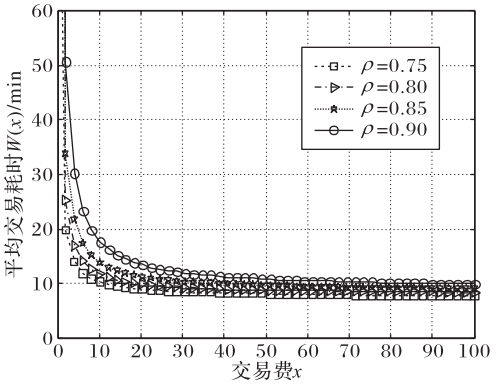

图3 不同ρ下平均交易耗时随交易费的变化

Fig. 3 Average transaction time changing with transaction fee with different ρ

从图3中可以看出，给定系统拥塞ρ，用户的平均交易耗时随着交易费的增加而减小。在支付交易费一定时，如果交易增多，系统的拥塞指标增大即系统交易量增大，则用户的平均交易耗时也会随之增加。

3.2 用户的交易费支付策略

不同交易费支付策略下用户的平均交易耗时与用户的总花费的对比分别如图4和图5所示。

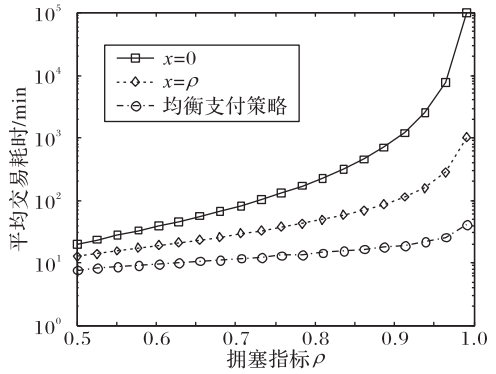

图4 平均交易耗时对比

Fig. 4 Comparison of average transaction time

仿真中，用户的总花费最小时的均衡支付策略由命题2给出，即$\bar{x} = \sqrt{\frac{c\rho^2(2-\rho)}{(1-\rho)\mu}} + \rho - 1$。对比策略设定为按$x = 0$(不交交易费)和按$x = \rho$支付交易费，将$x = \bar{x}$、$x = 0$、$x = \rho$分别代入式(9)得到不同策略下平均交易耗时随系统拥塞指标关系。进一步，由$x + cW(x)$可以得到不同策略下用户的总花费。

从图4中可以看出，在不同的系统状态下，用户采用均衡支付策略都可以将平均交易耗时维持在服务时间附近，即用户可以获得最高优先级，享受优先服务。当$\rho = 0.5$时，均衡支付策略的耗时约为7.7 min，比$x = \rho$策略减少了38%，比不支付交易费策略减少了61.3%。当$\rho = 0.9$(系统高负荷)时，

均衡支付策略的平均交易耗时比不支付交易费策略减少了98%,比$x=\rho$支付策略减少了81.2%。

同时从图5可以看出,虽然采用均衡策略需要支付交易费,但是因为交易耗时下降,时间成本大幅度降低,所以用户的总花费相对更小。当$\rho=0.7$时,均衡支付策略的用户总花费比支付$x=\rho$的策略下降了45%,比不支付交易费的策略下降了79.5%。当$\rho=0.9$时,均衡支付策略的用户总花费比支付$x=\rho$的策略下降了72%,比不支付交易费的策略下降了97%。从图4和图5可以看出,随着ρ的增大,均衡支付策略的优势更加明显。

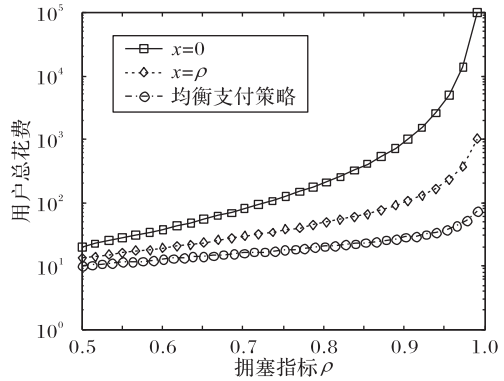

图5　用户总花费对比

Fig. 5　Comparison of user total cost

综上所述,用户可根据系统拥塞程度采用最优的支付策略,保证交易被尽快处理的同时避免过高的交易费支出;另一方面,用户还可以根据系统拥塞程度和自身对交易耗时的要求,根据命题1的结论,计算出保证自己的交易在预期时间内上链所需的交易费。

4　结语

本文通过排队博弈论研究了比特币系统中交易费对平均交易耗时的影响,推导出了平均交易耗时与交易费、系统拥塞指标之间的关系式,并给出了用户的纳什均衡支付策略。在后续研究中,可以从矿工收益出发,考虑区块大小一定的情况下,如何选择交易填满有限的区块空间来最大化矿工收益的问题。

参考文献(References)

[1] NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system[EB/OL]. [2019-12-12]. https://bitcoin.org/bitcoin.pdf.

[2] 孙柏林. 国内外区块链技术概况及其在制造业中的应用[J]. 自动化博览, 2018(7): 48-53. (SUN B L. Overview of blockchain technology at home and abroad and its application in manufacturing [J]. Automation Panorama, 2018(7): 48-53.)

[3] 赵明慧,张琭,亓晋. 基于区块链的社会物联网可信服务管理框架[J]. 电信科学, 2017, 33(10): 19-25. (ZHAO M H, ZHANG L, QI J. A framework of trusted services management based on blockchain in social internet of things [J]. Telecommunications Science, 2017, 33(10): 19-25.)

[4] 梅颖. 基于区块链的物联网访问控制简化模型构建[J]. 中国传媒大学学报(自然科学版), 2017, 24(5): 7-12. (MEI Y. Simplification model construction of Internet access control based on block chain [J]. Journal of Communication University of China (Science and Technology), 2017, 24(5): 7-12.)

[5] 叶小榕,邵晴,肖蓉. 基于区块链、智能合约和物联网的供应链原型系统[J]. 科技导报, 2017, 35(23): 62-69. (YE X R, SHAO Q, XIAO R. A supply chain prototype system based on blockchain, smart contract and Internet of Things [J]. Science and Technology Review, 2017, 35(23): 62-69.)

[6] 陆尧,文婕. 基于比特币技术的供应链管控与溯源方案[J]. 计算机工程, 2018, 44(12): 85-93, 101. (LU Y, WEN J. Scheme of supply chain control and traceability based on bitcoin technology [J]. Computer Engineering, 2018, 44(12): 85-93, 101.)

[7] 衡星辰,董灿,林克全,等. 基于区块链技术的电力竞价交易研究[J/OL]. 计算机工程 [2019-10-31]. https://kns.cnki.net/KCMS/detail/31.1289.tp.20190717.1027.002.html. (HENG X C, DONG C, LIN K Q, et al. Research on competitive price power transaction based on blockchain technique [J/OL]. Computer Engineering [2019-10-31]. https://kns.cnki.net/KCMS/detail/31.1289.tp.20190717.1027.002.html.)

[8] ANTONOPOULOS A M. Mastering Bitcoin: Unlocking Digital Cryptocurrencies [M]. Sebastopol, CA: O'Reilly Media, 2014: 128-157.

[9] MÖSER M, BÖHME R. Trends, tips, tolls: a longitudinal study of Bitcoin transaction fees [C]// Proceedings of the 2015 International Conference on Financial Cryptography and Data Security, LNCS 8976. Berlin: Springer, 2015: 19-33.

[10] KANG J, XIONG Z, NIYATO D, et al. Incentivizing consensus propagation in proof-of-stake based consortium blockchain networks [J]. IEEE Wireless Communications Letters, 2019, 8(1): 157-160.

[11] LI Q, MA J, CHANG Y. Blockchain queue theory [C]// Proceedings of the 2018 International Conference on Computational Social Networks, LNCS 11280. Cham: Springer, 2018: 25-40.

[12] FENG S, WANG W, XIONG Z, et al. On cyber risk management of blockchain networks: a game theoretic approach [EB/OL]. [2020-03-16]. https://arxiv.org/pdf/1804.10412.pdf.

[13] KASAHARA S, KAWAHARA J. Effect of Bitcoin fee on transaction-confirmation process [EB/OL]. [2020-03-16]. https://arxiv.org/pdf/1604.00103.pdf.

[14] SCHRIJVERS O, BONNEAU J, BONEH D, et al. Incentive compatibility of Bitcoin mining pool reward functions [C]// Proceedings of the 2016 International Conference on Financial Cryptography and Data Security, LNCS 9603. Berlin: Springer, 2016: 477-498.

[15] LI J, YUAN Y, WANG S, et al. Transaction queuing game in Bitcoin BlockChain [C]// Proceedings of the 2018 IEEE Intelligent Vehicles Symposium. Piscataway: IEEE, 2018: 114-119.

[16] KIM S. Group bargaining based Bitcoin mining scheme using incentive payment process [J]. Transactions on Emerging Telecommunications Technologies, 2016, 27(11): 1486-1495.

[17] RIZUN P R. A transaction fee market exists without a block size limit [EB/OL]. [2020-03-14]. https://www.bitcoinunlimited.info/resources/feemarket.pdf.

[18] LIU X, WANG W, NIYATO D, et al. Evolutionary game for mining pool selection in blockchain networks [J]. IEEE Wireless Communications Letters, 2018, 7(5): 760-763.

[19] 王金亭. 排队博弈论基础[M]. 北京:科学出版社, 2016: 31-40. (WANG J T. Basics of Queueing Game Theory [M]. Beijing: Science Press, 2016: 31-40.)

This work is partially supported by the Scientific Base and Talent Special Project of Guangxi (GuikeAD19110042), the Director Fund of Guangxi Key Laboratory of Wireless Broadband Communication and Signal Processing (GXKL06160111).

HUANG Dongyan, born in 1984, Ph. D., associate professor. Her research interests include blockchain.

LI Lang, born in 1996, M. S. candidate. His research interests include blockchain.