

PoW 区块链网络的不稳定性

——基于比特币网络的实证研究

唐敦哲 王靖雯 何平

摘要: 区块链技术因其低成本、高安全性、以及可追溯等优势受到了国内外各行业的广泛关注。工作量证明 (PoW) 是区块链采用时间最久、范围最广的共识机制, 关于 PoW 机制研究的理论研究表明 PoW 区块链网络具有短期不稳定性, 但仍缺乏实证依据。本文基于比特币网络数据, 以短期网络算力波动为外生冲击变量, 考察了算力波动与矿工总手续费收入之间的关系。研究发现, 短期算力波动与矿工总手续费收入呈显著正相关性, 短期算力的下降会显著降低矿工总手续费收入。这说明负向算力冲击有可能使得矿工因亏损而退出挖矿, 造成算力的进一步下跌, 进而形成恶性循环。本文从实证上证明了 PoW 区块链网络作为支付工具具有不稳定性, 抵御算力冲击以及恶意攻击的能力较弱。

关键词: 区块链 工作量证明 比特币 算力 手续费;

中图分类号: F82 **文献标识码:** A

Instability of PoW Blockchain Network as a Payment System

--Evidence from Bitcoin Blockchain Network

Tang Dunzhe, Wang Jingwen, He Ping

Abstract: Proof-of-Work (PoW), the consensus algorithm that adopted by blockchain's first application, bitcoin, is widely used nowadays in blockchain network. Using data from Bitcoin blockchain network, this paper empirically examines the impact of short-term network hashrate shock on total miner transaction fee income. We find that hashrate change is positively correlated with the change in total miner transaction fee income. We further prove that a plunge in hashrate leads to a significant drop in total miner transaction fee income. This result implies that a "vicious cycle" might exist in PoW blockchain: The drop in hashrate might cause miners to exit mining market due to mining loss, which means an even lower network hashrate and miner income. Our paper supports the theoretical research that PoW blockchain network is unstable as a payment system, and is vulnerable to outside attacks.

Key Words: Blockchain; Proof-of-Work; Bitcoin; Hashrate; Transaction Fee

*作者信息:

唐敦哲, 清华大学经济管理学院金融系, 电话: 16602779070,

Email:tangdzh.17@sem.tsinghua.edu.cn, 邮寄地址: 清华大学经济管理学院伟伦楼 112A。

王靖雯, 清华大学经济管理学院经济系, 电话: 18811377320,

Email:wangjw.17@sem.tsinghua.edu.cn, 邮寄地址: 清华大学经济管理学院舜德楼 321。

何平, 清华大学经济管理学院金融系, 电话: 010-62795754,

Email:heping@sem.tsinghua.edu.cn, 邮寄地址: 清华大学经济管理学院伟伦楼 308。

*本文感谢清华大学经济管理学院中国金融研究中心与区块链金融研究中心的支持与建议。
何平为本文通讯作者。

PoW 区块链网络的不稳定性

——基于比特币网络的实证研究

唐敦哲 王靖雯 何平

摘要：区块链技术因其低成本、高安全性、以及可追溯等优势受到了国内外各行业的广泛关注。工作量证明（PoW）是区块链采用时间最久、范围最广的共识机制，关于 PoW 机制研究的理论研究表明 PoW 区块链网络具有短期不稳定性，但仍缺乏实证依据。本文基于比特币网络数据，以短期网络算力波动为外生冲击变量，考察了算力波动与矿工总手续费收入之间的关系。研究发现，短期算力波动与矿工总手续费收入呈显著正相关性，短期算力的下降会显著降低矿工总手续费收入。这说明负向算力冲击有可能使得矿工因亏损而退出挖矿，造成算力的进一步下跌，进而形成恶性循环。本文从实证上证明了 PoW 区块链网络作为支付工具具有不稳定性，抵御算力冲击以及恶意攻击的能力较弱。

关键词：区块链 工作量证明 比特币 算力 手续费

一、引言

区块链作为一个独立的概念最早由中本聪在其比特币白皮书 Nakamoto(2008)中提出，随后 Buterin (2013) 提出了以太坊 (Ethereum)，进一步提升了区块链技术以及潜在应用场景。在过去十多年中，区块链技术快速发展，区块链在加密数字货币 (cryptocurrency) 方向的应用越来越广泛，在其他领域的发展和应用，包括金融管理，医疗健康，教育，供应链，物联网，通讯，食品溯源以及慈善公益，也都处于爆发式增长初期阶段。

以区块链技术作为底层技术的支付方式其功能以及性质虽然与现金相似，但其与现金有着明显的区别。对于现金支付来说，个人之间的现金交易记录属于私人账本 (private ledger)，只有交易双方知道，因此政府通过防伪和法律等手段杜绝私人账本作假的可能。相比之下，区块链网络上的加密数字货币交易属于公共账本 (public ledger)，记账参与方甚至所有网络参与方都能知晓并查阅交易的发生，因此区块链保证公共账本的准确性，公平性以及不可篡改性的方法，即区块链网络的共识机制 (Consensus Algorithm)，有别于传统现金。从定义上来讲，共识机制就是区块链网络内所有参与记账的节点对记录在区块链上的交易数据达成一致所采用的方法。根据应用行业和领域的不同需求，区块链可以采用不同的共识机制，其中主流的共识机制包括工作量证明 (Proof of Work, 或 PoW)，拥有量证明 (Proof of stake, 或 PoS)，委任权益证明 (delegated Proof of Stake, 或 dPoS) 以及实用拜占庭容错算法 (Practical Byzantine Fault Tolerance, 或 PBFT)。比特币作为区块链第一个实际落地应用，采用的是 PoW 共识机制。PoW 的概念和定义最先是由 Dwork 和 Naor (1992) 以及 Jakobsson 和 Juel (1999) 提出，而后应用到区块链领域。简单来讲，

PoW 共识机制是一种按劳分配的竞争记账方式（“挖矿”），贡献工作量（“算力”）越多的记账者（“矿工”）获得一个区块实际记账权（挖到新区块）的概率越大。为了激励矿工竞争记账，在区块链上进行交易的用户会为每一笔交易支付一定的手续费，而这些交易费最终会归获得区块记账权的矿工所有。另外，区块链系统会奖励（区块奖励）挖到新区块的矿工一定数量的代币（Token，区块链上的计价单位）。现阶段矿工的大部分收入来源于区块奖励，但是由于区块奖励会随着时间的推移而减少，最终矿工的收入将全部来源于交易手续费。因此对于 PoW 区块链网络来说，交易手续费是吸引矿工与用户的关键因素（过高的手续费可能无法吸引用户使用，过低的手续费可能导致矿工的流失），PoW 共识机制设计下的代币价格，手续费与算力之间联动关系的稳定性决定了区块链网络是否安全以及是否能长期正常运转。

基于以上事实，本文从区块链网络算力以及手续费之间的关系入手，基于 He 等（2019）中关于 PoW 区块链网络中短期算力波动冲击对于用户平均交易手续费以及矿工总手续费收入影响的理论，从实证方向研究了区块链网络作为支付工具可能存在的不稳定性。本文基于 2011 年到 2019 年所有比特币的区块链数据，以短期算力波动作为外生冲击变量，使用最小二乘法回归首先识别了算力波动与矿工总手续费收入的关系，接着分别探究了算力波动与网络交易数量以及平均手续费之间的关系。另外，本文还检验了短期算力影响平均手续费的渠道。本文研究发现，短期算力波动与矿工总手续费收入呈显著正相关性。具体来说，短期算力的波动与区块链交易数量呈显著正相关性，与平均手续费呈显著负相关性，但由于算力波动对平均手续费的影响幅度小于对交易数量的影响幅度，因此最终算力波动与矿工总手续费呈显著正相关性。这一结论说明遭遇算力冲击可能会导致 PoW 区块链网络不稳定。为了增加结果的可信度，我们进行了两部分稳定性检验。第一部分，考虑到挖矿难度调整的时点会对回归结果造成干扰，我们剔除了有难度调整的观测时点并重新进行了回归，其结果与基准回归结果相同。第二部分，考虑到 2013 年以前比特币网络属于不成熟阶段，我们进行了分样本检验，并发现 2013 年到 2019 年的子样本结果与基准结果一致。为了进一步探究 PoW 区块链网络抵御负向算力冲击的能力，本文进行了异质性检验，分别验证了正向和负向算力波动对矿工总手续费收入的影响。结果显示，短期算力的上升会大幅缩减平均手续费，因此不会显著地提高矿工总手续费收入；但短期算力的下降对平均手续费的影响不大，因此矿工总手续费收入会大幅下降。这说明短期内算力下跌所造成的矿工亏损以及用户交易等待时间增加有可能致使矿工和用户离场，而更少的矿工和用户意味着算力的进一步下降以及更少的手续费。如果没有外部干扰，这一恶性循环有可能最终导致 PoW 区块链网络的彻底瘫痪。总结来说，PoW 区块链网络具有不稳定性，抵御算力冲击以及恶意攻击能力较弱。

区块链领域吸引了很多国内外经济金融方向的学者。徐忠和邹传伟(2018)从经济学角度阐述了区块链的应用方向,分析了区块链的功能,并指出了区块链投资领域的过度投机和金融风险。姚前(2016)以及姚前和汤莹玮(2017)梳理了数字货币的概念并分析了区块链技术在央行法定数字货币中应该提供的基础技术支持。有学者关心区块链去中心化设计机制和能耗问题。Abadi 和 Brunnermeier (2018)从理论上研究了区块链的“三元悖论”:去中心化能保记账的准确性和不可篡改,却牺牲了效率。Biais 等(2018)认为,PoW 区块链的挖矿机制会引起算力的“军备竞赛”,最终导致算力(或者矿机)的过度投资。Ma 等(2018)认为是“矿工”的自由进入而不是挖矿机制造成了 PoW 区块链的大量资源消耗。Budish (2018)从安全角度讨论了区块链网络的稳定性,并深入讨论了对 PoW 区块链发起 51%攻击的成本以及可能性。也有部分学者研究了 PoW 区块链手续费相关问题。Pagnotta 和 Buraschi (2018)研究了比特币网络算力与比特币价格之间的关系,并通过矿工与区块链使用者之间的供需均衡给比特币定价,最后发现得出了算力与价格之间的联动效应对供给需求冲击有放大作用的结论。Huberman 等(2017)研究了矿工和用户供需均衡下的手续费价格,指出区块链网络的交易必须足够拥挤才会给矿工带来可观的手续费。Easley 等(2018)通过比特币网络的实证分析得出,当内存池越大(网络越拥挤)的时候,区块链所处理的交易平均费率越高。挖矿也是学者们关心的问题。Cong 等 (2019) 研究矿池(中心化挖矿)的相关问题,认为矿池并不会导致算力中心化,也不会出现矿池一家独大的情况。Prat 和 Walter (2018)认为矿机投资不可逆,所以挖矿市场的进入成本意味着每单位算力的挖矿收益有上限。

现有的研究从理论角度主要探讨了区块链的设计机制(Catalini、Gans, 2018;Raskin、Yermack, 2016;Saleh, 2018),能耗,安全问题,以及代币定价(Cong 等, 2018; Pagnotta、Buraschi, 2018;Schilling、Uhlig, 2018;Sockin、Xiong, 2018),着重研究了挖矿,手续费以及比特币价之间的关系;实证方向的研究主要集中在比特币作为资产的价格(Fernandez、Sanches, 2019;Gandal、Halaburda, 2016)、交易、市场操纵行为(Gandal 等, 2018; Griffin、Shams, 2018)以及比特币矿池(Rosenfeld, 2011)等相关问题。对于比特币以及 PoW 区块链作为支付工具的经济生态稳定性还尚未有实证研究。与现有文献相比,本文的贡献主要在于以下几个方面。第一,本文是第一个研究 PoW 区块链短期稳定性的实证论文,为区块链网络稳定性理论提供了实证分析,并证明了 PoW 区块链网络存在不稳定性。第二,本文研究结果为区块链将来在各行业领域的发展提供了重要参考。PoW 区块链作为支付手段具有不稳定性,其抵抗外部恶意攻击的能力较弱,因此在实际运用当中有可能需要借助技术手段或者政府监管来帮助其正常运行。第三,本文借助

2012 到 2019 年所有的比特币数据量化了 PoW 区块链短期算力波动对于区块链网络包括用户平均手续费，交易平均等待时间以及网络交易处理速度等变量的影响。第四，本文通过渠道检验准确地验证了算力波动影响矿工总手续费收入的途径和方式，并对实证结果进行了稳定性检验以及异质性检验，提升了研究结论的可信度。

本文后续安排如下：第二节介绍使用的数据和变量；第三节说明本文采用的理论背景以及实证分析方法；第四节进行实证分析以及渠道检验；第五节进行了稳健性检验；第六节进行了异质性检验。最后第七节总结全文。

二、数据与变量

（一）数据介绍

本文使用的是比特币（Bitcoin）区块链网络数据，主要来源是比特币区块链节点上记录的原始区块数据，www.blockchain.com 以及 www.btc.com 上统计的矿工节点数据。本文数据包含了 2011 年 1 月 2 日到 2019 年 9 月 7 日的日均数据，原始样本包括网络算力，主要交易所比特币交易价格，比特币区块奖励数量，矿工总手续费收入，交易平均等待时间，用户平均手续费，网络挖矿难度等，数据样本量为 3171。我们对数据进行了初步整理，首先清除了 2011 年 1 月 2 日到 2011 年 12 月 2 日缺少交易平均等待时间的 335 个观测时点，然后剔除了 2011 年 12 月 3 日到 2012 年 1 月 15 日交易平均手续费过小的 44 个观测时点^①，最后得到 2792 个样本观测值。

（二）变量定义

表 1 报告了本文核心变量的描述性统计。哈希率（Hashrate）衡量的是比特币网络中的算力，是本文中的核心解释变量。长期来看，比特币的网络算力随着技术的进步一直在大幅上升，但从短期来看，比特币算力的波动很大程度上是随机的。第一，随着挖矿产业的成熟，矿场已经逐渐代替个人矿工，对于矿场来说，巨大的固定成本意味着挖矿活动在短期内是无法调整的，因此短期内矿场提供的算力是相对稳定的。第二，能引起算力短期波动的因素大多数是不可预测，比如电力中断，自然灾害，矿场迁移，政府监管，网络故障和延迟，以及矿机自身不稳定性等等。因此本文使用日均算力变化作为外生变量，研究其对矿工总手续费收入的影响。本文的核心被解释变量包括(1)总手续费（Total Transaction Fee，单位为美元），衡量的是矿工从挖矿中获得的所有用户为交易支付的手续费，也就是矿工总手续费收入。(2)平均手续费（Per Transaction Fee，单位为美元），测量的是区块链网络上用户为每笔交易平均支付的手续费。(3)交易数量（Confirmed Transactions），代表每天区块链网

络处理的交易数量。为了进一步研究算力影响的渠道，我们考虑中间变量——平均等待时间（MCT，单位为分钟），代表用户交易从提交到最终被区块链网络确认所耗的平均时长。考虑到区块链系统的其他因素影响，我们控制了区块奖励（Block Reward，单位为比特币），市场价格（Market Price，单位为美元），交易平均价值（Tran Size，单位为美元）以及挖矿难度（Difficulty，单位为哈希）。

表1 描述性统计

变量名	变量说明	观测值	均值	标准差	最小值	最大值
<i>Total Transaction Fee</i>	总手续费	2792	354841.17	1407252.47	10.61	22724840.66
<i>Confirmed Transactions</i>	交易数量	2792	161445.90	109571.66	5174.00	490644.00
<i>Hashrate</i>	哈希率	2792	10689409.87	18959643.86	8.45	88354011.67
<i>MCT</i>	平均等待时间	2792	9.62	3.05	4.58	47.73
<i>Block Reward</i>	区块奖励	2792	22.67	11.41	12.50	50.00
<i>Market Price</i>	市场价格	2792	2335.84	3495.39	4.33	19498.68
<i>Difficulty</i>	挖矿难度	2792	1.44E+12	2.56E+12	1.25E+6	1.08E+13
<i>Per Transaction Fee</i>	平均手续费	2792	1.21	4.26	0.00	59.70
<i>Tran Size</i>	交易平均价值	2792	1695.65	2228.69	18.84	15443.97

注：

数据来源包括区块链数据网站——www.blockchain.com, www.btc.com 和比特币区块链原始数据

三、理论分析及实证策略

（一）理论分析

PoW 区块链中矿工的总手续费收入等于交易数量与交易平均手续费的乘积。其中，交易数量由区块容量以及区块平均产生速度决定，而区块平均产生速度又由算力决定。从长期来看，PoW 区块链系统会每隔一段时间根据网络算力自动调整挖矿难度使得区块产生的速度回到系统设定的目标，但从短期来看，在两次难度调整之间，由于区块容量相对稳定，算力的变化会直接导致区块产生速度的变化从而影响整个区块链处理交易的数量以及用户的交易平均等待时间。He 等（2019）从理论上研究了短期算力波动对于区块链网络的影响，并证明了短期算力冲击对于用户平均手续费以及矿工总手续费收入的影响。总的来说，算力和交易数量呈正相关，和用户平均手续费呈负相关，但是算力对于用户平均手续费的影响幅度小于对交易数量的影响，因此总的来看算力冲击和矿工总手续费成正相关关系。

根据 He 等（2019），在均衡状态下，用户的交易平均手续费 \bar{g} 等于：

$$\bar{g} = PS \left[1 - \frac{\theta}{\alpha} \left(1 - e^{-\frac{\alpha}{\theta}} \right) \right] \quad (1)$$

其中 P 代表区块链上的加密数字货币价格， S 是加密数字货币的总供给量， θ 和 α 分别代表用户对区块链的偏好程度以及对交易的耐心程度。当有一个短期算力冲击 λ 时，用户交易平均手续费将变成：

$$\overline{g_\lambda} = \lambda^{\frac{\beta}{1-\theta}} e^{-\left(\frac{1}{\lambda}-1\right)\frac{\alpha}{1-\theta}} PS \left[1 - \frac{\theta\lambda}{\alpha} \left(1 - e^{-\frac{\alpha}{\theta\lambda}} \right) \right] \quad (2)$$

其中 β 代表用户对于区块链的信任程度。

以上算力冲击对用户平均手续费造成的影响可以分为三部分。第一，当算力变化时，区块产生的速度会发生变化，导致用户交易等待时间发生变化，而等待时间的变化会影响区块链作为支付手段的便利性，因此用户对于此区块链的交易需求会发生变化。第二，当算力变化时，区块链的整体安全性会发生变化（理论上来说，算力越大，区块链上的信息就越不容易被篡改，或者说越不容易遭受51%攻击，因此区块链网络越安全），因此用户对于此区块链的交易需求会发生变化。第三，当算力变化时，区块产生的速度会发生变化，导致用户交易等待时间发生变化，因此用户额外支付一单位手续费能缩短的等待时间会发生变化，因此用户会调整手续费策略以实现效用最大化。

从本文的研究角度来说，短期内用户对于区块链网络交易的需求比较固定，因此短期内交易平均等待时间的小幅波动并不影响用户对交易的需求变化；另外，短期的算力波动也并不会明显改变用户对于区块链网络安全的信任。因此我们可以将短期算力波动对于用户交易平均手续费的影响简化为前文中的第三个影响，即交易平均等待时间的变化引起的用户交易平均手续费策略的变化。因此短期算力冲击 λ 对于用户平均手续费的改变可以简化为：

$$\Delta \ln(g) = \frac{1 - \frac{\theta\lambda}{\alpha} \left(1 - e^{-\frac{\alpha}{\theta\lambda}} \right)}{1 - \frac{\theta}{\alpha} \left(1 - e^{-\frac{\alpha}{\theta}} \right)} \quad (3)$$

当算力波动幅度相对小的时候，上述公式近似于以下公式：

$$\Delta \ln(g) = \alpha + \gamma_1 \Delta \ln(H) \quad (4)$$

其中 $\gamma_1 < 0$ ， H 代表算力， $\Delta \ln(H) = \lambda - 1$ 。

从短期来看，在网络算力足够大的情况下，网络算力与预期区块产生的时间的乘积为一个常数，因此假设每个区块中的交易数量不受算力影响，算力波动与区块链处理交易数量变化应当呈正相关。公式上来说：

$$\Delta \ln(N) = \gamma_2 \Delta \ln(H) \quad (5)$$

其中 N 代表区块链网络中交易总数量， $\gamma_2 > 0$ 。

总的来说，用户总手续费，也就是矿工总手续费收入，等于交易平均手续费与交易数量的

乘积。因此根据（4）和（5），矿工总手续费收入 G 与算力波动的关系应为：

$$\Delta \ln(G) = \alpha + (\gamma_1 + \gamma_2) \Delta \ln(H) \quad (6)$$

根据 He 等（2019），算力对矿工总手续费收入的影响应该为正，因此 $\gamma_1 + \gamma_2 > 0$ ，表明数量的正向效应大于交易平均手续费的负向效应。

（二）实证策略

实际情况与理论推断是否一致，有待于实证分析的检验。基于上一部分的理论分析，本文的基准回归使用以下方程：

$$\Delta \ln(G_t) = \beta_1 + \beta_2 \Delta \ln(H_t) + \beta_3 \Delta \ln(P_t) + \beta_4 \ln(R_t) + \beta_5 \Delta \ln(V_t) + Fixed + \varepsilon_t \quad (7)$$

其中 G_t 代表 t 时期（天）矿工总手续费收入， H_t 代表网络算力， P_t 代表比特币的市场交易价格， R_t 代表区块奖励， V_t 代表区块链上交易的平均价值， $Fixed$ 代表年份以及季度固定效应。我们将比特币的市场交易价格，区块奖励以及交易平均价值作为控制变量加入到方程中来控制可能影响矿工总手续费的因素。另外，我们还加入了年份及季度固定效应来控制年度和季节性因素。系数 β_2 表示算力增长率对矿工总手续费收入增长率的影响，若该系数为正，则表明负向算力波动会使得矿工总手续费收入下降，矿工面临亏损风险；若该系数为负，算力增长率与矿工收入增长率呈现反比，当面临算力下降冲击时，矿工总手续费收入反而上升。依据理论部分的分析，我们预期 β_2 为正数，即算力下降冲击使得矿工总手续费收入下降。

方程（7）从总效应的角度检验了算力冲击对矿工手续费收入的影响，根据理论分析以及式（4）（5）（6），总效应可以分解为两个部分，一方面，根据式（5）算力的下降冲击使得交易数量下降，给矿工总手续费收入带来下行压力，由此我们估计方程（8）。另一方面，根据式（4）算力下降使得平均手续费上升，使得矿工总手续费收入有上行推动力，由此我们估计方程（9）。我们由式（7）验证了两种效应的总和，结合方程（8）（9）探讨两种效应的强弱主导效应。

$$\Delta \ln(N_t) = \alpha_1 + \alpha_2 \Delta \ln(H_t) + \alpha_3 \Delta \ln(P_t) + \alpha_4 \ln(R_t) + \alpha_5 \Delta \ln(V_t) + Fixed + \varepsilon_t \quad (8)$$

$$\Delta \ln(\bar{g}_t) = \beta_1 + \beta_2 \Delta \ln(H_t) + \beta_3 \Delta \ln(P_t) + \beta_4 \ln(R_t) + \beta_5 \Delta \ln(V_t) + Fixed + \varepsilon_t \quad (9)$$

其中 N_t 代表 t 时间区块链网络交易的总数量， \bar{g}_t 代表 t 时期用户交易平均手续费，其余变量的定义如方程（7）。式（8）和（9）中的系数 α_2 和 β_2 分别代表算力变化对交易总数量变化和平均交易费用变化的影响，依据理论部分分析，我们预期系数 α_2 为正， β_2 为负且绝对值小于 α_2 ， α_2 和 β_2 之和应为方程（7）中所估计的系数 β_2 。

为了验证 He 等（2019）中算力冲击是通过影响用户平均等待时间而影响用户平均手续费的理论结论，本文进行了以下渠道检验。首先方程（10）以及方程（11）分别验证了算力与平均等待时间，平均等待时间与用户平均手续费之间的关系。然后，方程（12）将中介变量--平均等待

时间作为自变量加入方程(9)。若算力冲击主要通过影响用户平均等待时间而影响用户平均手续费，则方程(10)与(11)中系数 α_2 与 β_2 应均显著，并且在方程(12)中，当用户交易平均等待时间加入自变量后，系数 γ_3 应该正显著，同时算力的系数 γ_2 应该不显著并且系数值大幅缩小。

$$\Delta \ln(M_t) = \alpha_1 + \alpha_2 \Delta \ln(H_t) + \alpha_3 \Delta \ln(P_t) + \alpha_4 \ln(R_t) + \alpha_5 \Delta \ln(V_t) + Fixed + \varepsilon_t \quad (10)$$

$$\Delta \ln(\bar{g}_t) = \beta_1 + \beta_2 \Delta \ln(M_t) + \beta_3 \Delta \ln(P_t) + \beta_4 \ln(R_t) + \beta_5 \Delta \ln(V_t) + Fixed + \varepsilon_t \quad (11)$$

$$\Delta \ln(\bar{g}_t) = \gamma_1 + \gamma_2 \Delta \ln(H_t) + \gamma_3 \Delta \ln(M_t) + \gamma_4 \Delta \ln(P_t) + \gamma_5 \ln(R_t) + \gamma_6 \Delta \ln(V_t) + Fixed + \varepsilon_t \quad (12)$$

其中 M_t 表示 t 时期的平均等待时间， \bar{g}_t 代表 t 时期用户的交易平均手续费，其余变量的定义如方程(7)。

四、算力波动对矿工总手续费收入的影响

(一) 短期算力波动对矿工总手续费收入的影响

我们首先使用比特币区块链 2012 年到 2019 年的数据估计方程(7)，研究短期算力波动对矿工总手续费收入的影响，回归结果报告在表 2。从列(1)中我们可以看出，当网络算力单独作为自变量时，矿工总手续费收入的系数为正显著，说明当网络算力提升时，用户支付的总手续费将增加。具体来说，网络算力波动率每增加 1 个百分点，矿工总手续费波动率增加 0.114 个百分点。随后我们加入了包括市场价格，区块奖励以及交易大小作为控制变量，回归结果在第二列。列(2)的回归结果与列(1)的结果相似，表明在控制可能的其他因素之后，算力变动对总手续费收入影响仍然为正。具体来说，网络算力波动率每增加 1 个百分点，矿工总手续费波动率增加 0.141 个百分点。表 2 与我们模型中所估计的短期算力下降会降低矿工总手续费收入的结果一致②。

表 2 算力对总手续费收入的影响

	因变量	
	$\Delta \ln(\text{Total Transaction Fee})$	
	(1)	(2)
$\Delta \ln(\text{Hashrate})$	0.114** (0.048)	0.141*** (0.047)
$\Delta \ln(\text{Market Price})$		1.108*** (0.131)
$\ln(\text{Block Reward})$		0.011 (0.043)
$\Delta \ln(\text{Tran Size})$		0.184*** (0.019)
常数项	0.001	-0.017

	(0.009)	(0.073)
年份固定效应	Yes	Yes
季度固定效应	Yes	Yes
观测值	2792	2792
R 方	-0.001	0.060

注:

*代表 10%显著, **代表 5%显著, ***代表 1%显著

(二) 算力波动对交易数量以及交易平均手续费的影响

在 PoW 区块链中, 矿工的总手续费收入等于用户交易平均手续费乘上对应时间的交易数量。在 (一) 的回归中, 我们发现短期算力的减少会降低矿工总手续费收入, 在这一部分中我们将估计式 (8) 和 (9), 分别检验短期算力波动对交易平均手续费和区块链日均交易数量的影响。

表 3 算力对交易数量和平均手续费的影响

	因变量	
	$\Delta \ln(\text{Confirmed Transactions})$	$\Delta \ln(\text{Per Transaction Fee})$
	(1)	(2)
$\Delta \ln(\text{Hashrate})$	0.264*** (0.020)	-0.123*** (0.042)
$\Delta \ln(\text{Market Price})$	0.180*** (0.056)	0.928*** (0.118)
$\ln(\text{Block Reward})$	-0.006 (0.018)	0.017 (0.039)
$\Delta \ln(\text{Tran Size})$	0.044*** (0.008)	0.140*** (0.017)
常数项	0.012 (0.031)	-0.029 (0.066)
年份固定效应	Yes	Yes
季度固定效应	Yes	Yes
观测值	2792	2792
R 方	0.067	0.049

注:

*代表 10%水平上显著, **代表 5%水平上显著, ***代表 1%水平上显著

表 3 展示了回归结果。通过表 3 我们可以看出, 网络算力对交易数量以及交易平均手续费均有显著影响。具体来说, 第 (1) 列中, 算力对交易数量的回归系数为 0.264, 说明短期算力的增长能够加快区块链交易处理速度: 算力波动率每增加 1 个百分点, 区块链交易数量波动率增加 0.264 个百分点, 表明了算力与交易数量之间的正向效应。第 (2) 列中, 网络

算力与交易平均手续费呈负相关关系，系数为 0.123，意味着网络算力增长率每上升 1 个百分点，用户手续费增长率就下降 0.123 个百分点，证明了理论分析中算力与平均交易费用之间的负向效应。上述回归结果中算力变量的系数均在 1% 的水平上显著。总的来说，表 3 中的结果说明短期算力下降会导致区块链交易数量减少，因此可能降低矿工总手续费收入；同时结果也说明算力下降会使得用户交易手续费升高，从而可能提升矿工总手续费收入。但是由于交易数量下降的程度远超于平均手续费上升程度，矿工的手续费收入从总体上来说会因为算力的下降而下降。上述结果与前文中的理论推导结论一致。

（三）渠道检验：交易平均等待时间

在上一部分中，我们发现算力波动与用户交易平均手续费之间存在负相关关系，依据前文的理论研究，算力波动应该通过影响交易平均等待时间从而导致交易平均手续费的改变。为了检验上述理论是否成立，我们估计方程（10）（11），使用最小二乘法回归分别验证算力波动与交易平均等待时间，交易平均等待时间与平均手续费之间的关系。在此基础上我们估计方程（12），将算力和平均等待时间同时作为自变量对平均手续费进行回归以探究算力影响总手续费收入的渠道。回归结果见表 4。

表 4 渠道检验—平均等待时间

	因变量		
	$\Delta \ln(MCT)$	$\Delta \ln(Per\ Transaction\ Fee)$	
	(1)	(2)	(3)
$\Delta \ln(Hashrate)$	-1.004*** (0.030)		-0.005 (0.049)
$\Delta \ln(MCT)$		0.119*** (0.022)	0.117*** (0.026)
$\Delta \ln(Market\ Price)$	-0.061 (0.085)	0.935*** (0.117)	0.935*** (0.118)
$\ln(Block\ Reward)$	-0.003 (0.028)	0.017 (0.038)	0.017 (0.038)
$\Delta \ln(Tran\ Size)$	0.036*** (0.012)	0.136*** (0.017)	0.136*** (0.017)
常数项	0.007 (0.047)	-0.030 (0.065)	-0.030 (0.065)
年份固定效应	Yes	Yes	Yes
季度固定效应	Yes	Yes	Yes
观测值	2792	2792	2792
R 方	0.287	0.056	0.056

注：

*代表 10%水平上显著, **代表 5%水平上显著, ***代表 1%水平上显著

表 4 第 (1) 列表明等待时间随着短期算力的下降而显著增加, 算力增长率每降低 1 个百分点, 交易平均等待时间增长率增加 1.004 个百分点, 与前文的理论分析完全一致。第 (2) 列验证了前文理论部分中关于交易平均等待时间以及平均手续费的推论, 平均等待时间增长率每增加 1 个百分点, 用户手续费增长率就增加 0.119 个百分点。从第 (3) 列的结果中我们可以看出, 当算力和交易平均等待时间同时作为自变量时, 交易平均等待时间与平均手续费呈正相关关系, 其系数为 0.117, 并且在 1%的水平上显著。对比来说, 算力与交易平均手续费的关系在控制了平均等待时间之后在 10%的水平上不显著。综合来看, 表 4 中的回归结果说明算力波动主要是通过影响交易平均等待时间而改变交易平均手续费的。

第四部分实证回归结果表 2-4 证明了 PoW 区块链网络具有短期不稳定性, 负向算力冲击会导致矿工总手续费收入下降, 导致矿工可能因亏损而退出网络, 进入恶性循环。进一步的, 算力波动影响了交易数量和平均交易手续费两个部分, 对交易数量的正向影响大于对平均交易手续费的负向影响, 导致最终对总手续费收入的正向影响。最后, 算力波动主影响平均手续费的渠道是交易平均等待时间。

五、稳定性检验

(一) 挖矿难度调整

采取 PoW 共识机制的区块链通常都会定期调整挖矿难度来保证区块产生速度的稳定性。对于比特币来说, 系统设定的出块时间为 10 分钟, 并且每 2016 个区块 (约两周) 根据网络算力进行一次挖矿难度调整, 使得预期出块时间重新回到 10 分钟。对于本文来说, 有难度调整当天的交易数量以及用户交易等待时间等变量都会因为难度调整而受到干扰, 从而影响回归结果的准确性。在稳定性检验中我们剔除了受难度调整影响的观测值, 然后重新进行了回归。本文的基本观测时点有 2792 个, 去掉了难度调整所影响的 428 个观测时点, 还剩 2364 个观测时点。回归结果如下表 5。

表 5 稳健型检验—排除难度调整干扰

	因变量					
	$\Delta \ln \left(\frac{Total\ Transaction\ Fee}{Fee} \right)$	$\Delta \ln \left(\frac{Confirmed\ Transactions}{Transactions} \right)$	$\Delta \ln(MCT)$	$\Delta \ln(Per\ Transaction\ Fee)$		
	(1)	(2)	(3)	(4)	(5)	(6)
$\Delta \ln(Hashrate)$	0.171***	0.286***	-1.023***	-0.114**		0.011
	(0.053)	(0.022)	(0.033)	(0.048)		(0.056)

$\Delta \ln(MCT)$				0.119*** (0.025)	0.122*** (0.029)	
$\Delta \ln(Market Price)$	1.010*** (0.143)	0.145** (0.060)	-0.087 (0.090)	0.875*** (0.128)	0.865*** (0.128)	0.876*** (0.128)
$\Delta \ln(Block Reward)$	0.010 (0.047)	0.006 (0.020)	0.001 (0.029)	0.004 (0.042)	0.004 (0.042)	0.004 (0.042)
$\Delta \ln(Tran Size)$	0.179*** (0.021)	0.047*** (0.009)	0.035*** (0.013)	0.128*** (0.018)	0.132*** (0.019)	0.128*** (0.018)
常数项	-0.014 (0.080)	-0.008 (0.034)	0.001 (0.050)	-0.006 (0.071)	-0.006 (0.072)	-0.006 (0.071)
年份固定效应	Yes	Yes	Yes	Yes	Yes	Yes
季度固定效应	Yes	Yes	Yes	Yes	Yes	Yes
观测值	2,364	2,364	2,364	2,364	2,364	2,364
R 方	0.054	0.072	0.287	0.050	0.043	0.049

注:

*代表 10%显著, **代表 5%显著, ***代表 1%显著

表 5 的回归结果与基准回归的结果十分接近, 并且去掉难度调整后短期算力波动对于矿工总手续费收入的影响系数更大。具体而言, 算力波动对矿工总手续费收入的回归系数由 0.141 上升至 0.171, 表明当网络算力增长率每增加 1 个百分点时, 矿工总手续费增长率就增加 0.171 个百分点; 短期算力波动以及交易平均等待时间对于其他因变量的影响与第四部分的回归系数相比没有太大变化。总体来说, 剔除了挖矿难度调整之后的回归结果与基准回归结果基本相同, 表明了算力对矿工总手续费收入的正向作用, 及其分别对交易数量和平均手续费的对立效应, 并且验证了平均交易时间作为中间渠道的存在及合理性, 使得我们基准回归的结果更加稳健和可信。

(二) 分样本检验

本文在这一部分里将全样本分为了两个子样本, 第一个子样本是从 2012 年 1 月 16 日到 2013 年 1 月 31 日, 第二个子样本是从 2013 年 2 月 1 日到 2019 年 9 月 7 日。比特币第一台专业 ASIC 矿机诞生于 2013 年 1 月, 在此之前, 矿工是通过 CPU 以及 GPU 挖矿。专业矿机的诞生标志着比特币挖矿进入了全新的阶段, 从属于极客等极小众人物的活动转变成了一个以盈利为目的的产业。因此本文以第一台矿机的诞生为分水岭将全样本分开, 分别进行了第四部分中的回归, 考虑到挖矿难度的调整, 以下所有回归剔除了难度调整日期。

2013 年 2 月到 2019 年 9 月的回归结果 (表 6) 与全样本结果相似。首先短期算力波动与矿工总手续费收入呈现正相关关系, 并在 1%的水平上显著。其次, 算力波动与交易数量呈正相关, 与用户交易手续费呈负相关, 并且算力波动影响用户手续费的主要途径为交易等

待时间。这部分样本与全样本的结论完全相同，而且系数没有明显差异，表明我们提出的稳定性挑战适用于比特币挖矿进入正式发展的阶段。2012 年 1 月到 2013 年 2 月的回归结果（表 7）与全样本有几处不同之处。短期算力波动对于用户等待时间仍然显著，但是对于矿工总手续费收入以及每笔交易手续费在 5%的水平上不显著。其中可能的原因如下：第一，2012 年到 2013 年间，比特币网络处于发展初期，交易数量以及交易金额很小，用户多属于特殊人群（例如极客，毒贩，洗钱者等），因此比特币作为一种隐蔽的支付方式，用户对于交易等待时间并不敏感。在此条件下，尽管算力波动能够影响等待时间，但是并不会进一步影响交易手续费。第二，2012 到 2013 年间平均每笔交易手续费非常小（<0.01 美元），因此用户本身对于手续费并不敏感。第三，本文通过回归发现，2012 到 2013 年间交易平均手续费和比特币价格高度相关。比特币交易一般会通过比特币钱包，而钱包一般会设置有默认的手续费金额（比如 0.00001 比特币/kb），因此当用户对于手续费价格不敏感的时候，一般会使用以比特币计价的默认金额，因此比特币价格会在很大程度上决定交易手续费。基于以上原因，12-13 年间比特币挖矿机制发展尚不成熟，手续费收入仅占矿工收入的较小部分，因此本文的分析不适用于该阶段。

表 6 分样本检验：2013 年到 2019 年

	因变量					
	$\Delta \ln \left(\frac{Total\ Transaction\ Fee}{Fee} \right)$	$\Delta \ln \left(\frac{Confirmed\ Transactions}{Transactions} \right)$	$\Delta \ln(MCT)$	$\Delta \ln(Per\ Transaction\ Fee)$		
	(1)	(2)	(3)	(4)	(5)	(6)
$\Delta \ln(Hashrate)$	0.138*** (0.047)	0.303*** (0.021)	-1.007*** (0.036)		-0.166*** (0.042)	-0.031 (0.049)
$\Delta \ln(MCT)$				0.142*** (0.022)		0.134*** (0.026)
$\Delta \ln(Market\ Price)$	0.903*** (0.122)	0.087 (0.055)	-0.111 (0.094)	0.833*** (0.109)	0.816*** (0.110)	0.831*** (0.109)
$\Delta \ln(Block\ Reward)$	0.000 (0.044)	0.010 (0.020)	0.008 (0.034)	-0.011 (0.039)	-0.010 (0.040)	-0.011 (0.039)
$\Delta \ln(Tran\ Size)$	0.218*** (0.019)	0.094*** (0.008)	0.052*** (0.014)	0.116*** (0.017)	0.123*** (0.017)	0.116*** (0.017)
常数项	-0.002 (0.063)	-0.015 (0.029)	-0.010 (0.049)	0.015 (0.056)	0.013 (0.057)	0.014 (0.056)
年份固定效应	Yes	Yes	Yes	Yes	Yes	Yes
季度固定效应	Yes	Yes	Yes	Yes	Yes	Yes
观测值	2,037	2,037	2,037	2,037	2,037	2,037
R 方	0.092	0.132	0.282	0.073	0.061	0.073

注:

*代表 10%显著, **代表 5%显著, ***代表 1%显著

表 7 分样本检验: 2012 年到 2013 年

	因变量					
	$\Delta \ln \left(\frac{\text{Total Transaction Fee}}{\text{Fee}} \right)$	$\Delta \ln \left(\frac{\text{Confirmed Transactions}}{\text{Transactions}} \right)$	$\Delta \ln(\text{MCT})$	$\Delta \ln(\text{Per Transaction Fee})$		
	(1)	(2)	(3)	(4)	(5)	(6)
$\Delta \ln(\text{Hashrate})$	0.377 (0.250)	0.164* (0.084)	-1.131*** (0.089)		0.214 (0.227)	0.304 (0.279)
$\Delta \ln(\text{MCT})$				-0.011 (0.117)		0.080 (0.143)
$\Delta \ln(\text{Market Price})$	2.406*** (0.921)	0.861*** (0.307)	0.186 (0.326)	1.506* (0.835)	1.545* (0.834)	1.530* (0.835)
$\Delta \ln(\text{Block Reward})$	0.572 (0.446)	0.018 (0.149)	-0.086 (0.158)	0.570 (0.404)	0.555 (0.403)	0.561 (0.404)
$\Delta \ln(\text{Tran Size})$	-0.018 (0.086)	-0.187*** (0.029)	-0.050 (0.030)	0.163** (0.078)	0.169** (0.078)	0.173** (0.078)
常数项	-0.963 (0.757)	-0.026 (0.253)	0.145 (0.268)	-0.962 (0.687)	-0.936 (0.686)	-0.948 (0.687)
年份固定效应	Yes	Yes	Yes	Yes	Yes	Yes
季度固定效应	Yes	Yes	Yes	Yes	Yes	Yes
观测值	327	327	327	327	327	327
R 方	0.010	0.118	0.328	0.011	0.013	0.011

注:

*代表 10%显著, **代表 5%显著, ***代表 1%显著

六、异质性检验

在第四部分, 我们从整体上验证了算力波动与矿工总手续费收入的关系, 并且验证了等待时间作为其传导机制。我们力图探讨负向冲击造成的不稳定性, 为了进一步研究负向冲击的影响, 我们在本节进行异质性检验, 探究正向算力波动和负向算力波动对矿工总手续费收入的影响是否存在不对称性。异质性检验的意义在于, 正向算力波动能提高 PoW 区块链网络的交易处理速度, 缩短用户等待时间, 以及提高矿工总手续费收入增长率, 因此对于 PoW 区块链网络是有益的。而相比于正向算力波动, 负向算力波动对于 PoW 区块链网络稳定运行的危害更大。如果较大的算力下降不仅会导致网络交易处理速度的变慢, 用户交易等待时间的延长, 而且会大幅降低矿工总手续费收入, 那么这一结果有可能导致矿工退出挖矿市场, 进而致使网络算力进一步下跌, 形成恶性循环, 最终导致 PoW 区块链网络的瘫痪。

因此本文基于正负向算力波动对于区块链网络的不同影响，分别考察正负向算力波动对于矿工总手续费收入的影响，这有助于帮助我们进一步探究区块链网络可能存在的不稳定性和抵御恶意攻击的能力。文章在以上分析的基础上添加了两个二元变量， D_{1t} 和 D_{2t} 。其中 D_{1t} 在算力冲击为正的时候取值为1，在算力冲击为负的时候取值为0； D_{2t} 与 D_{1t} 的取值相反，在算力冲击为正的时候取值为0，在算力冲击为负的时候取值为1。将以上两个二元变量分别乘以算力，添加至第四部分中的基准方程（7）后，基准方程变更为：

$$\Delta \ln(G_t) = \beta_1 + \beta_2 D_{1t} \Delta \ln(H_t) + \beta_3 D_{2t} \Delta \ln(H_t) + \beta_4 \Delta \ln(P_t) + \beta_5 \ln(R_t) + \beta_6 \Delta \ln(V_t) + Fixed + \varepsilon_t \quad (13)$$

其中 β_2 和 β_3 分别代表正向和负向算力对于矿工总手续费收入的影响，其他变量定义如方程（7）。同理，我们对方程（8）至（10）进行了相同的处理，考察正向冲击和负向冲击的异质性影响。为了进一步考察平均等待时间作为中间渠道存在的异质性，我们将平均等待时间同样与二元变量相乘，添加到方程（11）：

$$\Delta \ln(\bar{g}_t) = \beta_1 + \beta_2 D_{1t} \Delta \ln(M_t) + \beta_3 D_{2t} \Delta \ln(M_t) + \beta_4 \Delta \ln(P_t) + \beta_5 \ln(R_t) + \beta_6 \Delta \ln(V_t) + Fixed + \varepsilon_t \quad (14)$$

其中 β_2 和 β_3 分别代表算力冲击为正向和负向时平均等待时间对于平均手续费的影响。同理，方程（12）也进行了相应更改。在调整完上述回归方程后，我们使用了2012到2019年的数据，在剔除有难度调整的时点之后，分别进行了回归，结果如下表（8）。

表8 异质性检验：正向和负向算力冲击

	因变量					
	$\Delta \ln \left(\frac{Total}{Transaction} \right)$ Fee	$\Delta \ln \left(\frac{Confirmed}{Transactions} \right)$	$\Delta \ln(MCT)$	$\Delta \ln(Per Transaction Fee)$		
	(1)	(2)	(3)	(4)	(5)	(6)
$D_{1t} \Delta \ln(Hashrate)$	0.132 (0.097)	0.310*** (0.041)	-1.048*** (0.061)		-0.178** (0.087)	-0.014 (0.096)
$D_{2t} \Delta \ln(Hashrate)$	0.215** (0.106)	0.257*** (0.045)	-0.995*** (0.067)		-0.042 (0.095)	0.030 (0.104)
$D_{1t} \Delta \ln(MCT)$				0.160*** (0.036)		0.159*** (0.041)
$D_{2t} \Delta \ln(MCT)$				0.067* (0.039)		0.072* (0.043)
$\Delta \ln(Market Price)$	1.011*** (0.143)	0.144** (0.060)	-0.086 (0.090)	0.881*** (0.128)	0.867*** (0.128)	0.881*** (0.128)
$\Delta \ln(Block Reward)$	0.009 (0.047)	0.006 (0.020)	0.003 (0.029)	0.003 (0.042)	0.003 (0.042)	0.003 (0.042)
$\Delta \ln(Tran Size)$	0.179*** (0.021)	0.047*** (0.009)	0.035*** (0.013)	0.129*** (0.018)	0.133*** (0.019)	0.129*** (0.018)
常数项	-0.011	-0.010	0.002	-0.002	-0.001	-0.001

	(0.080)	(0.034)	(0.050)	(0.071)	(0.072)	(0.072)
年份固定效应	Yes	Yes	Yes	Yes	Yes	Yes
季度固定效应	Yes	Yes	Yes	Yes	Yes	Yes
观测值	2,364	2,364	2,364	2,364	2,364	2,364
R 方	0.054	0.072	0.286	0.050	0.043	0.049

注:

*代表 10%显著, **代表 5%显著, ***代表 1%显著

表(8)第一行为正向算力冲击,从第(1)列中我们发现,正向算力波动与矿工总手续费收入的相关系数并不显著。具体来讲,从第(2)、(5)列来看,我们发现算力增长率与交易数量呈正相关关系,与用户平均手续费呈负相关关系,系数分别为 0.310 和 0.178,且在 5%的水平上显著。这说明算力增长虽然能显著提高网络处理交易的速度,但是由于用户平均手续费的明显下降,最终两种效应相互抵消,矿工能收到的总手续费并没有显著提高。

表(8)第二行代表负向算力冲击的影响,从第(1)列中我们发现,负向算力波动与矿工总手续费收入的相关系数为正的 0.215,且在 5%的水平上显著。具体来讲,从第(2)列来看,我们发现算力增长率与交易数量呈正相关关系,系数为 0.257,且在 1%的水平上显著;第(5)列来看,算力波动与用户平均手续费的相关系数仅为 0.042,且不显著。这说明当有负向算力波动时,交易数量也会随之降低,但交易平均手续费没有明显受到算力波动影响而上升,因此矿工总手续费会显著降低,且增加幅度与交易数量下降幅度相近。通过列(3)、(4)以及(6)的渠道检验结果我们发现,虽然算力增长率与交易等待时间呈显著负相关关系,但是交易等待时间与用户平均手续费之间的回归系数不显著,并且当负向算力波动与交易等待时间同时加入方程对交易平均手续费回归时,两者系数均不显著。这说明当有负向算力波动时,PoW 区块链网络处理交易的速度会同比下降,造成用户交易等待时间的增加,但是用户并不会因为等待时间的增加而提高交易平均手续费。因此总的来说,矿工总手续费收入会明显下降。

异质性检验证明了正向的算力波动并不能显著影响矿工总手续费收入,但是负向的算力波动会大幅降低矿工总手续费收入。这说明负的算力冲击有可能会导导致矿工亏损,而亏损会导致矿工退出挖矿市场,从而进一步降低网络算力,形成恶性循环。因此 PoW 区块链网络系统不仅不具有稳定性,而且抵御负向冲击和恶意攻击的能力较弱。

七、结论

区块链始于比特币,但区块链的未来不仅仅是比特币。作为一个具有颠覆性的创新概

念，区块链未来将在各个领域改变人们的生活。工作量证明（PoW）作为区块链最初的共识机制之一，帮助区块链实现了公共记账的准确性以及安全性，但 PoW 区块链运行机制是否具有稳定性，还有待更多的理论以及实证证明。本文基于 He 等（2019）中关于 PoW 区块链网络短期稳定性的理论，以短期算力波动对矿工总手续费收入作为切入点，用比特币 2012 到 2019 年的区块链数据，评估了 PoW 区块链系统的稳定性以及抵抗外部冲击的能力。

本文研究发现，短期算力波动与矿工总手续费收入有显著相关性。具体来说，矿工总手续费收入会随着短期算力的上升而上升，随着短期算力的下降而下降。这一结论说明 PoW 区块链网络具有不稳定。为了增加结果的可信度，我们进行了两部分稳定性检验，其结果与基准结果一致。为了进一步探究 PoW 区块链网络抵御负向算力冲击的能力，本文进行了异质性检验，分别验证了正向算力波动和负向算力波动分别对矿工总手续费收入的影响。本文发现，短期算力的上升不会显著地提高矿工手续费收入，但短期算力的下降会导致矿工总手续费收入的大幅下降。这说明短期内算力的持续大幅下跌所造成的矿工亏损以及用户交易等待时间增加有可能意味着矿工和用户的离场，而更少的矿工和更少的用户意味着算力的进一步下降以及更少的手续费。如果没有外部干扰，这一恶性循环有可能最终导致 PoW 区块链网络的彻底瘫痪。

本文一系列的实证研究为 PoW 区块链网络稳定性的理论分析提供了支撑，也验证了区块链网络不稳定性的理论推导结果。从整体上来说，区块链技术以及区块链应用还处于初级发展阶段，各国政府，业界以及学界也正在积极探索区块链在各领域中应当扮演的角色。PoW 是区块链最早落地应用所采用的共识机制，因此研究 PoW 区块链对于帮助区块链研究者，从业者，以及相关政策制定者更深入的了解区块链技术以及其经济学含义是至关重要的。本文仅仅从其中一个侧面研究了 PoW 区块链网络作为潜在的支付工具可能存在的稳定性隐患，更多有关 PoW 区块链的运行机制，技术改进，政策制定等问题还有待未来研究解决。

注释

① 2012 年 1 月 15 日之前用户交易平均手续费 89% 的时点低于 0.01 美元，第一次连续 3 天超过 0.01 美元是 2012 年 1 月 16 日到 1 月 18 日。

②为了提高本文结论的可靠性，本文在数据分别进行了上下 1% 和 5% 的缩尾处理以后，又再次进行了正文中所有回归，结果与正文中结论基本一致。故以上回归结果正文中不再赘述。

参考文献

(1) 徐忠、邹传伟：《区块链能做什么、不能做什么？》，《金融研究》，2018 第 11 期。

- (2) 姚前,《中国法定数字货币原型构架》,《金融研究》,2016年第17期。
- (3) 姚前、汤莹玮,《关于央行法定数字货币的若干思考》,《金融研究》,2017第7期。
- (4) Abadi, J. and Brunnermeier, M., 2018, “Blockchain Economics,” *NBER Working Paper*, No. 25407.
- (5) Budish, E., 2018, “The Economic Limits of Bitcoin and the Blockchain,” *NBER Working Paper*, No. 24717.
- (6) Buterin, V., 2016, “A Next Generation Smart Contract & Decentralized Application Platform,” *Ethereum White Paper*.
- (7) Catalini, C., and Gans, J. S., 2016, “Some Simple Economics of the Blockchain,” *NBER Working Paper*, No.22952.
- (8) He, P., Tang, D. Z., and Wang, J.W., 2019, “Proof-of-Work (PoW) Blockchain Network and Its Viability as a Payment System,” *SSRN Electronic Journal*, No.3441605.
- (9) Cong, L. W., Li, Y. and Wang, N., 2018, “Tokenomics: Dynamic Adoption and Valuation,” *Columbia Business School Research Paper*, No.18-46.
- (10) Cong, L. W., He, Z. G., and Li, J. S., 2019, “Decentralized Mining in Centralized Pools,” *NBER Working Paper*, No.25592.
- (11) Dwork, C., and Naor, M., 1992, “Pricing via Processing or Combatting Junk Mail,” *international cryptology conference*, pp.139-147.
- (12) Easley, D., Ohara, M., and Basu, S., 2019, “From mining to markets: The evolution of bitcoin transaction fees,” *Journal of Financial Economics*, Forthcoming.
- (13) Fernandez-Villaverde, J., and Sanches, D., 2019, “Can Currency Competition Work?” *Journal of Monetary Economics*, vol.106, pp.1-15.
- (14) Gandal, N., and Halaburda, H., 2016, “Can We Predict the Winner in a Market with Network Effects? Competition in Cryptocurrency Market” *Games*, 7(3), pp.1-21
- (15) Gandal, N., Hamrick, J. T., Moore, T., and Oberman, T., 2018, “Price manipulation in the Bitcoin ecosystem,” *Journal of Monetary Economics*, 95, pp.86-96
- (16) Griffin, J. M., and Shams, A., 2018, “Is Bitcoin Really Un-Tethered?” *SSRN Electronic Journal*, No.3195066
- (17) Huberman, G., Leshno, J. D., and Moallemi, C. C., 2018, “Monopoly Without a Monopolist: An Economic Analysis of the Bitcoin Payment System,” *SSRN Electronic Journal*, No.3025604
- (18) Jakobsson, M., and Juel, A., 1999, “Proofs of work and bread pudding protocols,” *In CMS’ 99 Proceedings of the IFIP TC6/TC11 Joint Working Conference on Secure Information Networks: Communications and Multimedia Security*, pp.258 - 272
- (19) Ma, J., Gans, J. S., and Tourky, R., 2018, “Market Structure in Bitcoin Mining,” *NBER Working Paper*, No.24242
- (20) Nakamoto, S., 2008, “Bitcoin: A Peer-to-Peer Electronic Cash System,” *White paper*
- (21) Pagnotta, E., and Buraschi, A., 2018, “An Equilibrium Valuation of

- Bitcoin and Decentralized Network Assets,” *SSRN Electronic Journal*, No.3142022
- (22) Prat, J., and Walter, B., 2018, “An Equilibrium Model of the Market for Bitcoin Mining,” *CESifo Working Paper*, No. 6865
- (23) Raskin, M., and Yermack, D., 2016, “Digital Currencies, Decentralized Ledgers, and the Future of Central Banking,” *NBER Working Paper*, No. 22238
- (24) Rosenfeld, M., 2011, “Analysis of Bitcoin Pooled Mining Reward Systems,” *ArXiv, abs/1112.4980*
- (25) Saleh, F., 2018, “Blockchain Without Waste: Proof-of-Stake,” *SSRN Electronic Journal*, No.3183935
- (26) Schilling, L., and Uhlig, H., 2018, “Some simple Bitcoin Economics,” *Journal of Monetary Economics*, 106, pp.16-26
- (27) Sockin, M. and Xiong, W., 2018, “A Model of Cryptocurrencies,” *Working Paper Preliminary Draft*