区块链经济学的形成与展望

聂辉华,李　靖

(中国人民大学 经济学院,北京 100872)

摘　要:数字经济是中国经济的重要发展方向之一,而区块链是数字经济的基础技术之一。自2008年以来,区块链的技术取得了长足发展,并且在加密货币、金融、供应链管理、企业管理和公共管理等众多领域产生了广泛的应用前景。文章介绍了最近几年来关于区块链的经济学和金融学研究。首先,文章介绍了区块链的发展背景。其次,文章介绍了区块链的运行机制以及背后的经济学原理。再次,文章从博弈论、市场均衡、网络经济学、交易成本经济学、信息经济学和产业组织理论等多个角度,系统地梳理了关于区块链的经济学和金融学研究成果。最后,文章基于我国区块链产业的发展需求,提出区块链经济学的下一步发展,应该重点关注联盟链落地机制、参与方信息结构、主权货币实施方案以及区块链在医疗、公益、食品安全等行业的具体应用机制设计等问题。

关键词:区块链;数字经济;金融科技;博弈论

中图分类号:F062.4　　**文献标志码:**A　　**文章编号:**1009-1505(2021)05-0066-11

DOI:10.14134/j.cnki.cn33-1337/c.2021.05.007

一、区块链的发展和研究背景

区块链是一种基于互联网的交易记账方式,它通过公开的、分布式认证机制把一系列交易记录模块连接起来,构成一个完整的交易链条。区块链技术集密码学、网络安全学、数据库账本等技术于一体,将数据保存在所有接入网络的计算机上,通过网络协议使全网络数据同步更新,保证存储在区块链上的数据可证实和不易篡改。与中心化、科层式、实名制的传统结构不同,区块链技术具有分布式、防篡改和匿名性的特点,因此它有望成为颠覆现有的信息传输模式和交易制度的革命性技术,是未来数字经济发展的底层框架之一。正因为区块链技术可能导致颠覆式创新,所以各国都高度重视区块链技术的发展和应用,以便抢占未来数字经济和数字化治理的制高点。例如,美国已经成为区块链产业

收稿日期:2019-07-20

基金项目:教育部哲学社会科学研究重大课题攻关项目"深化'放管服'改革促进营商环境持续优化研究"(18JZD048)

作者简介:聂辉华,男,中国人民大学经济学院教授,博士生导师,经济学博士,中国人民大学企业与组织研究中心执行主任,教育部"长江学者奖励计划"青年学者,主要从事组织经济学研究;李靖,男,中国人民大学经济学院博士研究生,主要从事组织经济学研究。

最大的市场,加拿大拥有全球最大的区块链生态系统,新加坡正借助区块链技术推进“智能国家”计划。中国在数字经济发展方面后来居上,并且高度重视区块链技术的前景和应用[1]46。2019年10月24日,中共中央政治局举行第十八次集体学习,主题是区块链技术发展现状和趋势。2021年3月,国家《十四五规划纲要》明确提出大力发展数字经济,而区块链、云计算、大数据、物联网等产业被列为七大数字经济重点产业。因此,区块链将成为发展数字经济和建设数字中国的重要载体,并将成为促进数字技术与实体经济深度融合,赋能传统产业转型升级,实现高质量发展的新引擎。

区块链技术最早出现于比特币。2008年11月1日,一个自称中本聪(Satoshi Nakamoto)①的计算机网络安全专家在网络社区上开创性地提出了一种端到端的电子货币解决方案,并将其命名为比特币(Bitcoin),其底层技术即为区块链技术[2]。

近年来,随着区块链技术的进步,相关产业突飞猛进,目前应用范围已经拓展到加密货币、供应链物流、银行信贷、企业管理、公共管理等领域。首先,加密货币是区块链技术最重要的应用。根据 CoinMarketCap 网站的数据,截至2021年5月底,全球加密货币的种类超过1万种,总价值达到1.7万亿美元,日交易额超过1700亿美元。②加密货币的发展,引起了各国央行的注意。加拿大、新加坡等国已经开始了主权数字货币的实验,美国、英国、日本等国也开展了对主权数字货币的研究。此外,在供应链领域,区块链能够准确记录货物存储、运输、交接的状态;供应链信息传递给金融机构,可以为企业进行更加准确的信用评价;在企业管理过程中,使用区块链技术可以保证在隐藏参与人身份信息的情况下准确统计参与人对企业决策的投票结果;在公共管理领域,区块链技术可以帮助多部门的信息同步。根据国际数据公司(IDC)的统计,2020年,全球区块链解决方案花费达到42亿美元,占全部 IT 解决方案花费的0.95%,尽管这一比例还相对较低,但是区块链解决方案正在快速增长,预计到2024年将达到190亿美元,保持年均50%左右的增速。业界憧憬着将区块链技术应用进一步延伸到实物资产领域,与大数据、物联网等技术结合,构建囊括世界上所有资产的万物账本。

随着区块链产业的快速发展,国内外关于区块链技术及应用的研究快速增长,不过相关研究主要集中在计算机网络安全领域[3-4],对于区块链背后的经济学逻辑以及区块链技术的经济影响的研究寥寥无几。英文文献中对区块链的经济学研究较多是针对比特币及其他加密货币的运行机制进行分析,如 Biais[5]、Cong 等[6-7]、Saleh[8],仅有少数文献关注了区块链技术带来的影响以及区块链技术的应用,如 Cong 和 He[9]、Chiu 和 Koeppl[10-11]。

国内学者对于区块链的研究主要关注应用领域,只有少数学者关注了与区块链有关的经济学分析。例如,张亮和李楚翘[12]介绍了区块链的基本特征以及区块链在共享经济、城市建设、民主选举等领域的应用设想。郭广珍等[13]介绍了区块链的共识机制,并分析了区块链的博弈行为。在应用方面,金融领域和主权货币领域受到的关注最多。在“区块链 + 金融”领域,徐忠和邹传伟[14-15]分析了区块链金融的应用边界,邹传伟等[16]综合介绍了区块链相关的最新技术及其在数字货币领域的应用和监管措施,龚强等[17]讨论了区块链在供应链金融的优缺点以及适用条件,邓爱民等[18]对区块链在保理领域的应用进行了机制设计。针对区块链技术在主权数字货币中的应用,特别是数字人民币的发展,姚前和汤莹玮[19]、徐忠等[20]、穆杰[21]分别分析了区块链技术的优缺点,提出了构建中国法定数字货币的理论方案和设计要点。此外,黄海涛和罗纯[22]讨论了区块链促进跨境贸易中的信任建立机制,渠慎宁和杨丹辉[23]讨论了区块链在公共卫生突发事件领域的溯源机制,汪普庆等[24]结合区块链在食品安全管理领域的具体应用讨论了区块链技术的效果和优势,段琳和张凤侠[25]、李进华和任恒[26]对区块链在廉政反腐领域的应用前景进行了展望,戚学祥[27]分析了区块链应用在精准扶贫领域的优势与

①至今无人能够确认中本聪的真实身份,有人怀疑这是一个团队,而不是一个人。

②这并不是历史最高值,而是刚刚经历了一次大幅下跌之后的价值。

挑战,林木西和张紫薇[28]提出区块链技术促进企业绿色生产的应用前景,章安邦[29]认为区块链可以用于升级司法证人保护制度。

考虑到区块链相关的经济学和金融学论文主要在近五年内涌现,而已有文献缺乏对区块链最新论文的介绍,本文将主要从经济学角度刻画区块链的运行机制,介绍区块链对经济活动尤其是资源配置的最新学术成果,继而展望区块链经济学的发展方向。

本文接下来的内容安排如下:第二部分简要介绍区块链的运行机制,并揭示背后的经济学逻辑。第三部分介绍区块链经济学的研究成果,主要包括区块链的经济学逻辑、经济影响、适用条件及应用等方面。最后在总结全文的基础上,提出下一步区块链研究应该重点关注的问题。

二、区块链的运行机制

(一) 区块链的结构

区块链(Blockchain)是由区块(Block)串联起来组成的链(Chain)。每个区块的内容包含若干信息(通常是交易记录),还包含一个代表区块的哈希值(Hash value)以及代表前一个区块的哈希值①(见图1)。当对某一区块中的一条信息进行修改时,不仅会改变这一区块的哈希值,还会导致其后的所有区块的哈希值发生改变。因此,除非构造一条从该区块之前的区块开始的分叉,并且得到全网络的认可,否则无法对某个区块的内容进行篡改。

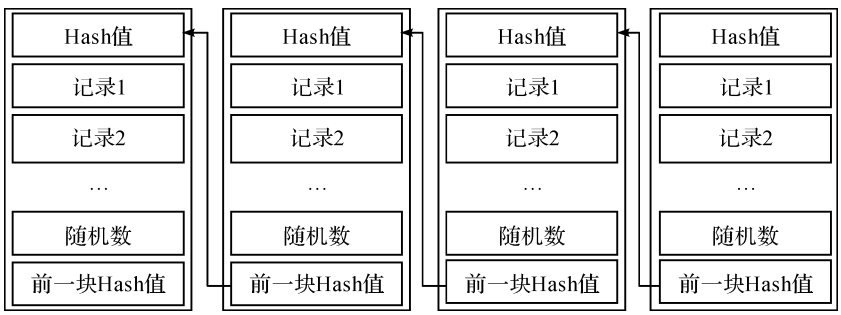

图 1 区块链结构与区块内信息示意图

通俗地说,区块链技术就是把一笔交易的账目公告天下,让每个人都成为历史的见证者,从而防止当事人篡改交易记录。一笔交易要成功记录在区块链上(俗称“上链”),需要经过以下几个步骤:第一,交易方向全网发布交易申请;第二,记账人对交易方身份以及账户金额进行审核,确认没有问题则加入结算池;第三,每隔一段时间,一个被选中的记账人从结算池中选取若干记录打包形成区块,并向全网公布;第四,区块获得全网认可后,成为公共账本中的一部分。

(二) 区块链的激励机制

区块链作为一种分布式记账技术,可能会有多个信息的发布方以及多个记录者。要成为一种可靠、便捷的记账方式,区块链要解决两个关键问题:一是如何确定由谁来制造新的区块(谁来记账),二是如何保证全网络的账本是一致的(防止篡改)。我们不妨将区块链上的交易方和记账人都称为代理人。此时,代理人之间存在严重的信息不对称,比如没人知道对方的真实身份(匿名性)和人品。那么,

①哈希值又称加密散列,是由区块中的其他内容进行哈希计算得到的一个数字。每个区块的哈希值就相当于区块的独一无二的身份证号码。

如何保证记账人是诚实可信的呢?这涉及逆向选择问题。如何保证没人篡改交易记录呢?这涉及道德风险问题。要解决这两类信息不对称导致的代理问题,区块链的创建者必须设计非常精巧的激励机制。因此,区块链的成功,其实暗含了深刻的经济学原理和契约理论。

我们先讨论记账人的问题。根据记账人的组织结构,区块链可以分为三种:一是公有链,所有互联网用户都可以成为公有链的记账人,不需要许可或者认证;二是联盟链,只有经过系统的许可,一个节点才可以参与交易记录的打包整理;三是私有链,记账权完全掌握在一个中心化节点手中。公有链和联盟链系统拥有多个记账人,通常被称为矿工(miner)或者见证官(validator),[①]矿工之间会争夺记账权,这一过程被称为"挖矿"。

那么,为什么矿工有激励去做一个记账人呢?因为矿工能够从成功记录交易的过程中得到一笔交易费作为回报。以比特币为例,争夺记账权的机制称为工作量证明机制(Proof of Work,PoW)。其原理是:给定每个区块的哈希值处于一定的范围内,矿工在选取好要打包的交易记录后,只能不断地在计算机程序上输入随机数,直到找到一个随机数使得区块的哈希值满足系统的要求。这个过程通常需要花费很多时间和电力。根据比特币协议,大约每两周的时间会调整一次合法哈希值的范围,保持平均每十分钟出现一个新区块的速率。矿工参与记账的经济回报在于,每个区块在获得全网认可后,打包该区块的矿工将获得一定的区块奖励以及每笔交易的交易奖励。由于每个区块的大小是有限的,能包含的交易记录也是有限的,交易方为尽快完成打包结算,可以设定更高的交易奖励。

工作量证明机制在比特币币值上升的情况下,能够不断吸引新矿工的加入,从而提高系统的安全性,但是也带来严重的能源消耗问题。[②]为此,一些区块链系统转而采用权益证明机制(Proof of Stake,PoS),替代工作量证明机制。在权益证明机制中,所有持有代币的人都是矿工。每隔一段时间,系统随机选中一个代币,持有该代币的人将获得记账权,每单位代币获得记账权的概率相同,持有代币越多的矿工获得记账权的概率越大。[③]由于记账权由系统随机指定,矿工不需要为争夺记账权进行算力竞争,只需在被指派打包任务时按协议打包并公布,消耗的电力可以忽略不计。目前,有越来越多的区块链项目开始采用权益证明机制,其中包括全球第二大加密货币系统以太坊。

然后,我们讨论第二个问题,即如果有人试图篡改账本怎么办?这就必须提到区块链的争议解决机制。在区块链中,争议是以分叉的形式存在,即如果区块 A 和区块 B 的前一区块都是区块 C,则区块 A 和区块 B 及其各自的后续区块就构成了分叉。当网络中的所有节点都接受同一个链条时,该链条上的所有交易都成为全网共识,此时不存在争议,也就是说无人能篡改账本。Biais 等[5]总结了 PoW 系统中分叉出现的四种原因。一是网络延迟,两个矿工在接近的时间分别找到合法区块,在不知晓其他合法区块存在的情况下向外广播自己找到的区块;二是双花攻击(double-spending attack),又常被称为 51% 攻击,即某一矿工掌握系统中大部分算力,刻意制造分叉将自己过去的交易记录抹除,使已经支付的货币回到自己的账产;三是协议不同步,即当网络协议升级时,可能出现在一个协议下合法的区块在另一个协议下不合法,导致该区块被部分矿工接受但被另外一部分矿工拒绝;四是系统回滚,即出现大量代币被窃取等意外情况时,矿工们经过协商,从某一区块开始分叉,实现系统回滚。

解决分叉最基本的机制是最长链原则,即在存在分叉的情况下,所有矿工都只在最长的分支上寻

---

①在 PoW 机制下,记账人不断尝试随机数,就像在找一个不知藏在何处的矿藏,成功找到满足合法区块要求的随机数就如同挖到了宝藏,因此他们被称为矿工。不过,基于权益证明机制的记账人一般被称为见证官。为方便起见,在不特定指出基于权益证明系统时,本文用矿工代指系统记账人。

②根据剑桥大学替代金融研究中心的估算,比特币挖矿年均消耗电量已经超过了100TWh,超过了阿根廷、荷兰等国家的年均耗电量。参见剑桥大学替代金融研究中心网站:https://cbeci.org。

③在一些 PoS 系统中,每一代币被选中的概率是不同的,持有时间越久的代币被选中的概率越高。

找新的区块,较短分支上的区块成为孤块,仅记录在孤块上的交易不会被承认,找到孤块的矿工得到的区块奖励和交易见证奖励也不被承认。在比特币最初的设计中,最长链原则就被确定为出现分叉时的解决机制,但是这一原则仅能处理网络延迟和双花攻击两种出现分叉的情况。在网络延迟的情况下,可能存在两条同样长的分支,每个矿工可以选择接受其中任意一条,直到有矿工找到新的区块,使得一个分支的长度超过另外一个,所有矿工都将接受最长的分支。而如果有矿工要进行双花攻击,就要制造一条超过原来链条长度的分支,除非掌握超过一半的算力,否则成功的概率很低。中本聪认为,双花攻击的机会成本(算力的浪费)将超过期望收益,因此理论上拥有超级算力的人与其去篡改原来的账本,不如新建一个区块链。从契约理论的角度讲,这是一种激励相容机制。在实际操作中,为了防范双花攻击,加密货币交易往往要在结算完成后等待若干区块才被确认。①

在处理另外两类分叉问题时,最长链原则并不一定适用,特别是系统回滚操作,直接违背了最长链原则。到目前为止,还没有处理协议不同步和系统回滚问题的统一机制,而是在每一次出现问题时,依赖矿工们的沟通,这被称为治理共识机制。治理共识是一种复杂的利益博弈,未必每次都能协调成功,这导致比特币、以太坊等加密货币经历了多次分裂[5]。

三、区块链经济学的初步形成

关于区块链的经济学研究,大体可以分为以下几个方面:第一,区块链运行的经济学逻辑,包括博弈机制、市场竞争的均衡状态、网络扩散机制等;第二,区块链技术对资源配置效率的影响,主要包括区块链技术在减少交易成本、降低信息不对称方面的优势,对企业管理结构、产业结构等带来的影响。

(一)区块链运行的经济学逻辑

1. 区块链的博弈论分析。前文介绍的区块链运行机制主要是基于既定协议的机制。在区块链系统的实际运行中,矿工可以选择不遵守协议,修改代码或者出现策略性行为。矿工之间的博弈机制关系到区块链系统的安全,是区块链相关研究最丰富的一个领域。受区块链技术的发展历程影响,对区块链的博弈机制研究多数是针对工作量证明机制,少数是针对权益证明机制,而对于无代币区块链的博弈机制则几乎没有文献讨论。

比特币的发明人中本聪当初提出了最长链原则,来解决可能的争议。但从计算机网络安全的角度讲,中本聪的设想并不是十全十美的。一些学者提出,矿工并不需要拥有超过50% 的算力就可以选择偏离策略。其中,最具有代表性的偏离策略是 Eyal 和 Sirer[3] 提出的自挖矿(self-mining)策略和 Nayak 等[4] 提出的固执挖矿(stunborn-mining)策略。这两种偏离策略的核心思想为,恶意偏离的矿工在找到一个区块后,先不对外公布该区块的存在,而是将其作为私有链的区块,并继续寻找下一个区块,然后等待合适的时机再向外公布。其目的是使其他矿工找到的区块成为孤点,浪费竞争对手的时间和算力,使自己获得的区块奖励比例提高。由于区块链的难度是动态调整的,主链保持平均每十分钟出一个新区块,这意味着采取偏离策略的矿工会获得更多奖励。采取偏离策略能否获益,主要依赖于矿工掌握的算力占比、对其他矿工的影响力等参数。Eyal 和 Sirer[3] 计算得到,当所有竞争对手都诚信挖矿、严格遵循比特币协议时,若一个恶意偏离矿工掌握的算力超过总算力的1/3,即使其对其他矿工的影响力为0,其采取自挖矿策略也是其最优策略。Nayak 等[4] 比较了诚信挖矿策略、自挖矿策略、多种固执挖矿策略在不同参数下的表现,发现在很大的参数空间下,固执挖矿是最优策略,期望收益相比采用诚信挖矿策略高100% 以上,相比采用自挖矿策略高25% 以上。在上述两种偏离策略下,一旦诚信挖矿

①比特币交易所一般规定交易完成后要等待6个区块的确认时间。

的矿工发现收益率不如采取偏离策略的矿工,就会加入偏离策略的联盟,最终导致采取偏离策略的矿工联盟控制整个网络。此外,在一些偏离策略下,矿工不会如实打包区块。比如,Houy[30]关注到了区块的传播速度会受到区块大小的影响,越大的区块传播速度越慢。那么,在两矿工博弈机制下,矿工为争取区块奖励会制造打包空块,即不打包任何交易记录(这是一种道德风险行为)。尤其是在矿工算力不平等的情况下,算力较小的矿工会严格采取打包空块的策略。在多矿工模型下,当所有矿工的算力都不超过50% 时,打包空块是所有矿工的最优策略。

另外一些博弈论研究关注内部攻击和外部攻击对区块链价值的影响,把币值波动影响纳入攻击者的成本与收益分析后,求解均衡状态和均衡条件。大部分研究认为,区块链系统受攻击的条件是比较严苛的。在比特币的发展过程中,很多大型矿池的算力占比早就超过了1/3的自挖矿策略占优阈值,甚至个别矿池算力曾经超过50% ,却极少出现自挖矿以及双花攻击的情况。① Kroll 等[31]认为,内部攻击(51% 攻击)会导致加密货币的价值消散,而攻击者需要布置大量的算力,最终得不偿失。更需要注意防范的是外部攻击,为此,加密货币拥有者应该合理设置挖矿奖励,以吸引足够的合法算力,抵御竞争对手的攻击。此外,也可以通过区块链用户社区达成共识、拒绝外部攻击者恶意制造的分支等方法,保护加密货币合法拥有者的利益。Budish[32]进一步认为,在技术手段、算力资源分布不同的情形下,攻击者的成本和收益分析应该是不同的。当最有效的挖矿芯片具有专用性时,攻击者若采用最有效的专用性芯片,需要付出一定的专用性投资;若采用被淘汰的专用性芯片或者通用型芯片,则需要付出高于均衡状态的电力成本。若攻击造成币值下降,很可能无法通过双花以及攻击过程中获得的区块奖励来弥补投资成本和用电成本,此时攻击者只存在进行扰乱攻击的动力,即通过扰乱币值市场获得外部收益来弥补其攻击付出的成本。Saleh[8]讨论了 PoS 机制下的博弈。研究者和业界对 PoS 机制的主要担心是无法达成共识的问题(Nothing at Stake)。②Saleh 提出,在 PoS 机制下,矿工一定是代币的拥有者,相比 PoW 机制下的矿工,有更加强烈的维护币值稳定的动力。在某矿工被系统指定成为见证官时,如果不对分支的合法性进行甄别,会造成币值下降。当矿工掌握的代币与区块奖励之比超过一定阈值时,只在合法分支上增加区块是其最优策略。双花攻击则要求矿工在支付一定代币后,其剩余的代币数量仍然超过总量的50% ,币值下降带来的成本将是非常高昂的。

2. 区块链的市场均衡。虽然区块链是一套技术系统,但它也是一个内部市场。学者们发现,在这个内部市场中,存在充分的市场竞争,均衡状态仍然满足边际成本等于边际收益等一般规律。比如,基于 PoW 机制的矿工收益等于其付出的电力、矿机投入、制冷设备投入等成本,基于 PoS 机制的见证人收益等于质押代币价值投入其他资本市场的利息收益[33-34]。但是由于协议限制,区块链账本提供的记账服务产出是有限的,这使得区块链系统与传统的自由竞争市场有很大的不同。

Easley 等[35]从消费者竞争的角度揭示了区块链的竞争均衡,主要结论是记账服务的稀缺性是消费者愿意支付交易费的原因。由于区块的大小有限,写入的交易数量有限,为了最大化自己的收益,矿工会优先选择交易费更高的交易记录写入区块。在交易量较少时,所有交易都能及时上链,用户没有动力支付交易费;当交易量较多时,若交易方不承诺支付足够的交易费,就需要付出更高的等待成本。在交易数量超过一定数值时,所有希望交易记录上链的用户都将支付一定交易费,不愿支付交易费或只愿意支付少量交易费的用户将退出网络。

Ma 等[36]从生产者竞争的角度揭示了区块链的竞争均衡,主要结论是挖矿产业的高耗能是市场自由

---

①本文作者所知道的成功双花攻击只有一次,发生在比特币黄金(Bitcoin Gold)系统上,这次攻击造成了比特币黄金币值的大幅下跌。参考:https://www.ccn.com/bitcoin-gold-hit-by-double-spend-attack-exchanges-lose-millions。

②无法达成共识的问题(Nothing at Stake)是指,当系统出现分叉后,后续的见证官为了最大化获得代币的期望,会向所有分支后面继续增加区块,导致所有分支始终存在并不断延长,无法确定以哪个分支为准。

竞争的均衡结果。如果是有许可网络,即只存在有限数量的在位矿工,市场达到均衡状态时,单个矿工的投入较高,但是总的算力水平相比矿工自由进入时会较低。与寡头竞争市场相似,有许可网络会产生租金,由在位的矿工瓜分,但不同于寡头竞争市场的是,区块链系统限制市场竞争并不会减少产品供给,只会影响系统的去中心化水平。如果是无许可网络,允许矿工自由进入,租金的存在会吸引更多矿工进入,直至完全消失。可见,仅从能源消耗角度,区块链系统允许矿工自由竞争并不符合社会最优。

进一步,Huberman 等[33]分析了同时考虑生产者和消费者的竞争均衡。他们发现,保持一定的交易拥堵是必要的,因为只有这样才能迫使消费者支付服务费,为矿工投入设备提供必要的补偿,从而保持矿工之间的充分竞争,避免产生垄断力量、收取垄断价格,保证系统的稳定性。但是系统拥堵带来的损失可能会比垄断价格带来的损失更大,可以考虑动态调整区块产生频率以及采用"小区块、快结算"等方法,来减少系统拥堵造成的无效率损失。

在区块链系统中,不仅有矿工和记账服务的消费者,还有矿池①等其他参与者。对区块链系统安全性的担忧并不是针对个体矿工,而是针对大型矿池,因为单个矿工难以掌握50% 以上的算力,因此对矿池竞争的分析也非常重要。Cong 等[6]将矿工的风险规避性和矿池之间的竞争纳入分析范畴。矿工是区块链服务的生产者,同时也是矿池服务的消费者,加入矿池是为了降低风险,因此矿工的最佳投资方式是将算力分配到所有矿池。由于大矿池的风险分担水平更高,收取的服务费也会更高,吸引的外部算力与其原有算力的比例会更低。比特币的矿池发展历史证明了他们的结论,大矿池收费更高,小矿池收费更低,不会出现单个大矿池占比越来越大的情况。这一理论发现可以大大打消人们对于区块链安全性的质疑。

3. 区块链的网络经济学分析。在区块链网络的扩散过程中,加密货币起到了至关重要的作用,这是网络经济学研究中不曾出现的新要素。Catalini 和 Gans[37]总结了一些区块链网络的发展过程,认为网络通过发放初始币,在建立初期可以便利地募集资金。区块奖励不仅可以吸引矿工加入网络,促进网络的扩散,还可以鼓励矿工投入资源,满足网络不断发展的资源需求。在网络的正常发展阶段,随着使用者增多,代币的价值会逐渐提高,又会吸引更多矿工和使用者,推动网络步入良性发展轨道。Athey 等[38]就加密货币的价格波动和用户扩散机制进行了建模讨论。相比于传统货币,加密货币价格波动较大,而且随时面临崩溃风险,为了吸引用户,一般收费较低。随着时间推移,相信加密货币发展前景的用户逐渐增多,加密货币的使用者也会越来越多,直到所有用户都采用加密货币,这反过来会逐步推高加密货币价格。加密货币升值的预期也会吸引投资者购买,单纯的投资行为会减少加密货币的实际供应量,推高加密货币的价格,对加密货币的发展带来不利影响。Cong 等[7]构建了一个与 Athey 等[38]相近的机制,讨论使用加密货币的交易平台的发展与代币价格变化的互动机制,认为代币升值的预期一方面能够促进平台吸引新用户,另一方面也能够帮助平缓平台发展过程中受到的冲击。

同时,区块链网络的扩散过程也会遇到阻力。事实上,比特币、以太坊等都曾产生分裂。Biais 等[5]分析了区块链网络保持统一或出现分裂的机制。一方面,区块链存在网络的规模效用,加密货币的价值与该区块链的使用人数呈正相关关系。另一方面,区块链的利益分配不平等,在分叉恢复到唯一链的过程中,被抛弃的分支上的矿工利益会严重受损,在缺乏补偿机制的情况下,这将阻碍共识机制的形成。因此,两种作用会导致多种均衡,一些均衡会导致全网共识无法达成。

(二) 区块链技术的经济社会影响

1. 区块链对交易成本的影响。区块链技术降低了交易成本,最直接的影响是降低了信息验证成本,并且提高了信息质量。在传统的交易市场上,有很多信息难以验证,比如农产品的原产地、买方是

①矿池(mining pool)是建立在区块链上的一种风险分担机制,加入矿池的矿工投入算力,一旦某个矿工成功挖到矿,所有矿工按投入的算力平分奖励。

否有足够的资金等,因此往往需要可信赖的第三方来监控参与者、实施信息确认和披露、维护值得信赖的声誉系统以及执行合同条款。当市场越大、交易金额越高的时候,可信赖的第三方就越重要,收费也越高昂。区块链提供的公共账本对于所有参与方是同步更新的,可以随时查验过去的交易信息,无需依赖第三方,建立声誉系统也更加容易[37]。区块链的交互见证机制,会要求每个合同参与人对交易中的某个环节提供信息验证,提供错误信息会给该参与人的声誉带来损失,参与人越多,提供错误信息导致的声誉损失将越高,从而瞒报的参与人越少,信息质量更高[9]。

与此同时,区块链可以降低科斯提出的三项主要的交易成本[39]。一是降低搜索成本[1]92。相比于互联网上的海量信息,区块链上的信息通常只与交易内容有关,无用信息较少,信息准确性更高,并且区块链技术增加了信息的时间维度,能够反映用户需求随时间的变化。二是降低协调成本[1]101。区块链技术保证了合作参与方之间的信息透明,这为多个参与方采取相互配合的措施奠定了基础。同时,区块链上所有行为都留有痕迹,信息只要被记录到区块链上,即使最后区块被网络共识抛弃,只要有一个参与方保存了这个区块,就能证明这个区块曾经存在。因此,参与方更有动力信守承诺[40]。三是降低履约成本。区块链的智能合约可以自动执行,一些数字资产的交易一旦上链就已完成,不需要针对交易中出现的情况进行再谈判,能够缓解不完全契约面临的敲竹杠问题[41]。

2. 区块链对信息不对称的影响。区块链技术使交易参与方信息同步,因而降低了信息不对称程度,这会影响参与方的行为和策略。信息不对称程度降低后,企业可以有更多信号发射的选择。例如,在金融领域,传统的信号发射理论认为,高质量企业为了与低质量企业区分开,需要向银行提出高于实际需求的贷款额,来发射信号证明自己的类型。在企业取得贷款后,银行无法准确核实贷款的用途,部分贷款没有被投入使用,造成了资源配置的扭曲和无效率。如果企业采用了区块链技术,银行可以核实贷款的最终使用情况,高质量企业可以通过实际的投资额来发射信号。通过比较两种信号发射方法,Chod 等[42]认为,采用区块链技术、通过投资额发射信号,低质量企业模仿的成本更高,高质量企业更容易将自己与低质量企业进行区分,因此能够减少扭曲,提高经济效率。

Cong 和 He[9]讨论了信息不对称对市场参与企业的两方面影响。一方面,引入区块链和智能合约后,水平较高的进入者可以证实自己的能力、定价与产品质量相匹配,不需要建立企业声誉,因此降低了进入者的进入门槛,这会提高资源配置效率。另一方面,信息不对称的消除也方便了在位企业之间互相监督,更容易建立合谋,这可能导致消费者福利降低。

龚强等[17]比较了利用区块链技术和传统调查方法降低信息不对称的优劣。一方面,上链企业越多,经过多方关联验证的信息准确性越高,越不容易出现企业合谋瞒报现象。另一方面,信息上链的容易程度会影响总体信息质量。因此,当上链企业数量较多、链上信息能够较完整地反映企业情况时,应该采用区块链技术对企业进行评估,反之则更适合采用传统的调查方法。

区块链技术能够解决企业和政府以及消费者之间的信息不对称问题,为政府实现发展目标提供了新的政策工具。例如,通过搭建区块链平台,强制企业将生产信息上链,可以揭示企业是否采用了绿色生产技术,不需要担心企业骗补或者获得补贴后的道德风险行为,同时破解了企业拿补贴越多污染越严重的“政府补贴悖论”和企业全部谎称进行绿色生产的“社会信任悖论”[28]。类似地,区块链技术有助于降低审计和监管要付出的信息验证成本,提高审计和监管力度,迫使企业如实报告信息[43]。

3. 区块链对企业管理的影响。对于区块链系统或者运行区块链系统的公司来说,由于区块链本身的去中心化,企业管理也相应变得扁平化。一方面,在开放的公有链系统中,任何人都可以随时加入网络,甚至占据一定的市场份额,市场权力很有可能从初创者和初始参与者手中流失,网络运行不依赖于一个或几个关键参与者运行[37]。另一方面,区块链运行主要依赖协议共识,对链下管理的依赖很低,并不需要“命令与控制”的科层结构。

对于通过区块链技术进行交易的公司来说,区块链会提高交易的透明性,进而提高所有权的透明

性,对经理、大股东等参与者的行为产生影响。在传统的委托 - 代理模型中,股权激励是保证经理和股东利益一致的重要激励工具。但是区块链技术带来的透明性会导致股权对经理的激励作用减弱,公司将不得不调整激励结构,或者向经理支付更多费用以抵消这种损失[44]。

4. 区块链对产业组织的影响。区块链技术不仅会推动企业管理的扁平化,还可能会导致市场结构的扁平化。在传统市场上,垄断权力的产生有时是由于企业的规模效应。对于平台型网络来说,这种规模效应也明显存在,导致了互联网行业的垄断巨头出现。与 Biais 等[5]不同, Catalini 和 Gans[37]认为,区块链系统用户都是依赖于同样的分布式基础设施,即使网络分裂也不会对用户使用造成很大影响,还可以消除垄断权力的损失。随着跨链交易技术的不断发展与完善,网络分裂对网络服务的规模效应的影响将不断降低,在位企业的分裂将更加频繁。这意味着企业的边界将快速变化。

同时,区块链技术降低了潜在进入企业的初始融资难度,使得初创企业无需提前完成资本积累,数据的开放性也降低了初创企业进入市场的知识门槛[37]。但是在分布式记账方式下,信息容易被复制,潜在进入企业通过制造分叉,进入市场的成本降低,可以收取更低费用进行市场竞争,打破在位企业垄断[29]。

四、总 结

区块链横空出世已经超过十年,随着这项技术的不断发展,被人们接受的程度也在不断提高。众多国家央行、金融机构、科技巨头以及初创企业都已经开始布局投入或者正在研究如何结合区块链技术,希望重塑行业运营机制。未来,区块链技术会进一步渗透进入社会经济的方方面面,给社会的声誉体系、信任机制带来颠覆性的变革。

区块链经济学还有很多领域有待完善,尤其考虑到我国区块链产业的发展特点,区块链的成熟落地应用仍相对较少,应加强研究区块链与其他产业融合发展的路径和方式。未来,区块链相关研究应重点关注以下问题。

其一,联盟链的激励机制。目前的区块链经济学逻辑研究几乎全部讨论公有链的相关设计,但是联盟链才是区块链企业级应用的主要形式。联盟链中,参与者之间相互熟悉,传统的声誉体系本身就是一种信任机制,同时,参与人之间更容易形成合谋。例如,区块链无法避免参与方之间共谋上传假信息,在比特币系统上甚至存在大量的诈骗行为[45]。区块链技术能够带来哪些新的变化?在声誉体系能够为维护系统安全提供一定正向激励下,是否需要代币,代币能发挥什么样的作用?如何保证网络的有序发展,在吸纳合法参与者的同时,避免个别恶意参与者不断引入同伴?

其二,参与人的隐私保护问题。在早期的公有链系统中,虽然用户信息是匿名的,但是把用户信息与线下交易信息结合后,很容易判断用户的真实身份。此时,用户的所有交易信息都公开就涉及很大的隐私问题。因此,在未来区块链的具体应用中,必须合理设计用户的信息结构。要探讨哪些信息可以公开,哪些需要信息的发布者授权后定向公开,如何防止个别参与人在获取他人信息后向外传播,等等。

其三,数字人民币的落地方案。数字人民币已经经过了多轮测试,关于测试中的经验和教训分析仍然比较少,大规模推广还需要进一步明确相关机制。例如,一个重要的问题是数字人民币与传统货币的衔接方式。如果数字人民币和传统货币完全合为一体,可能会存在货币实时转换形式的困难,而且记录所有货币实时状态的成本也将非常高昂。而如果两者完全分离开,可能会影响数字人民币的流通效率,因为大量普通用户可能没有意愿使用数字人民币,传统银行和支付宝等网络支付软件已经能够实现数字人民币的大部分功能。

其四,针对具体应用的机制设计。具体机制应考虑参与人间的利害关系、隐私保护需求等因素。比如,在供应链管理领域,上下游企业除了合作关系,也存在直接的利益冲突,不太可能合谋伪造交易;

而在社会公益领域,受助人和公益组织之间更接近利益共同体,有可能合谋伪造受助人信息,包括医院等其他参与人往往也缺少动力核实受助人信息,需要政府等关心社会总体福利的外部监督者参与信息核实。国内现有研究对区块链在金融、供应链、电子商务、社会公益、公共管理等重点领域的应用模式还处在初级阶段,缺少严谨的经济学分析。

参考文献:

[1]唐·塔普斯科特,亚力克斯·塔普斯科特. 区块链革命[M]. 凯尔,孙铭,周心园,译. 北京:中信出版集团,2016:46-101.

[2]NAKAMOTO S. Bitcoin: A Peer-to-Peer Electronic Cash System[OL]. Working Paper, 2008. Https://www.bitcoinpaper.info/bitcoinpaper-html/.

[3]EYAL I, SIRER E G. Majority is not Enough: Bitcoin Mining is Vulnerable[C]. International Conference on Financial Cryptography and Data Security. Springer, Berlin, Heidelberg,2014:436-454.

[4]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 (Euro S & P). IEEE, 2016:305-320.

[5]BIAIS B, BISIERE C, BOUVARD M, et al. The Blockchain Folk Theorem[J]. The Review of Financial Studies,2019, 32(5):1662-1715.

[6]CONG L W, HE Z, LI J. Decentralized Mining in Centralized Pools[J]. The Review of Financial Studies,2021,34(3): 1191-1235.

[7]CONG L W, LI Y, WANG N. Tokenomics:Dynamic Adoption and Valuation[J]. The Review of Financial Studies,2021, 34(3):1105-1155.

[8]SALEH F. Blockchain without Waste:Proof-of-Stake[J]. The Review of Financial Studies,2021,34(3):1156-1190.

[9]CONG L W, HE Z. Blockchain Disruption and Smart Contracts[J]. The Review of Financial Studies,2019,32(5):1754-1797.

[10]CHIU J, KOEPPL T V. The Economics of Cryptocurrencies—Bitcoin and Beyond[J/OL]. SSRN Working Paper, 2017. Https://papers.ssrn.com/sol3/papers.cfm? abstract_id = 3048124.

[11]CHIU J, KOEPPL T V. Blockchain-Based Settlement for Asset Trading[J]. The Review of Financial Studies,2019,32 (5):1716-1753.

[12]张亮,李楚翘. 区块链经济研究进展[J]. 经济学动态,2019(4):112-124.

[13]郭广珍,李立卓,赵绪帅. 区块链经济学:基本内容、学科关联及研究框架[J]. 财经问题研究,2020(12):11-21.

[14]徐忠,邹传伟. 区块链能做什么、不能做什么? [J]. 金融研究,2018(11):1-16.

[15]徐忠,邹传伟. 金融科技[M]. 北京:中信出版集团,2021:118-174.

[16]邹传伟,郝凯,钱柏均. 数字经济基石[M]. 北京:经济管理出版社,2021:4-59.

[17]龚强,班铭媛,张一林. 区块链、企业数字化与供应链金融创新[J]. 管理世界,2021(2):22-34.

[18]邓爱民,李云凤. 基于区块链的供应链"智能保理"业务模式及博弈分析[J]. 管理评论,2019(9):231-240.

[19]姚前,汤莹玮. 关于央行法定数字货币的若干思考[J]. 金融研究,2017(7):78-85.

[20]徐忠,汤莹玮,林雪. 央行数字货币理论探讨[J]. 中国金融,2016(17):33-34.

[21]穆杰. 央行推行法定数字货币 DCEP 的机遇、挑战及展望[J]. 经济学家,2020(3):95-105.

[22]黄海涛,罗纯. 区块链支持下跨境贸易信任机制构建——基于中国与中亚五国贸易的场景分析[J]. 南开学报(哲学社会科学版),2021(2):98-110.

[23]渠慎宁,杨丹辉. 突发公共卫生事件的智能化应对:理论追溯与趋向研判[J]. 改革,2020(3):14-21.

[24]汪普庆,瞿翔,熊航,等. 区块链技术在食品安全管理中的应用研究[J]. 农业技术经济,2019(9):82-90.

[25]段琳,张凤侠. 区块链技术在腐败治理中的作用研究[J]. 会计之友,2018(22):157-160.

[26]李进华,任恒. 基于区块链技术的廉政监督机制构建研究[J]. 学习论坛,2020(7):42-50.

[27]戚学祥. 精准扶贫 + 区块链:应用优势与潜在挑战[J]. 理论与改革,2019(5):126-139.

[28]林木西,张紫薇. "区块链 + 生产"推动企业绿色生产——对政府之手的新思考[J]. 经济学动态,2019(5):42-56.

[29]章安邦. 人工智能时代的司法权嬗变[J]. 浙江工商大学学报, 2020(4): 149-160.

[30]HOUY N. The Bitcoin Mining Game[J]. Ledger,2016,13(1):53-68.

[31]KROLL J A, DAVEY I C, FELTEN E W. The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries [C]. Workshop on the Economics of Information Security,2013.

[32]BUDISH E. The Economic Limits of Bitcoin and the Blockchain[R]. National Bureau of Economic Research Working Paper,2018,No. w24717.

[33]HUBERMAN G, LESHNO J, MOALLEMI C C. Monopoly without a Monopolist:An Economic Analysis of the Bitcoin Payment System[R/OL]. Bank of Finland Research Discussion Paper,2017,No. 27. Https://ssrn. com/abstract=3032375.

[34]FANTI G, KOGAN L, VISWANATH P. Economics of Proof-of-Stake Payment Systems[R/OL]. Working Paper, 2019. Https://econ. hkbu. edu. hk/eng/Doc/20210520_KOGAN_2. pdf.

[35]EASLEY D, O'HARA M, BASU S. From Mining to Markets:The Evolution of Bitcoin Transaction Fees[J]. Journal of Financial Economics,2019,134(1):91-109.

[36]MA J, GANS J S, TOURKY R. Market Structure in Bitcoin Mining[R]. National Bureau of Economic Research Working Paper,2018,No. w24242.

[37]CATALINI C, GANS J S. Some Simple Economics of the Blockchain[J]. Communications of the ACM,2020,63(7):80-90.

[38]ATHEY S, PARASHKEVOV I, SARUKKAI V, et al. Bitcoin Pricing, Adoption, and Usage:Theory and Evidence[R/OL]. Stanford University Graduate School of Business Research Paper, 2016, No. 16-42. Https://ssrn. com/abstract=2826674.

[39]COASE R H. The Nature of the Firm[J]. Economica,1937,4(16):386-405.

[40]LUMINEAU F, WANG W, SCHILKE O. Blockchain Governance—A New Way of Organizing Collaborations? [J]. Organization Science,2021,32(2):500-521.

[41]HOLDEN R T, MALANI A. Can Blockchain Solve the Hold-up Problem in Contracts? [R]. National Bureau of Economic Research working paper,2019,No. w25833.

[42]CHOD J, TRICHAKIS N, TSOUKALAS G, et al. On the Financing Benefits of Supply Chain Transparency and Blockchain Adoption[J]. Management Science,2020,66(10):4378-4396.

[43]CAO S, CONG L W, YANG B. Auditing and Blockchains:Pricing, Misstatements, and Regulation[R]. Working Paper,2018.

[44]YERMACK D. Corporate Governance and Blockchains[J]. Review of Finance,2017,21(1):7-31.

[45]VASEK M, MOORE T. There's no Free Lunch, even Using Bitcoin:Tracking the Popularity and Profits of Virtual Currency Scams[C]. International Conference on Financial Cryptography and Data Security. Springer, Berlin, Heidelberg,2015:44-61.

Development and Outlook of Blockchain Economics

NIE Huihua, LI Jing

(*School of Economics, Renmin University of China, Beijing 100872, China*)

Abstract: Blockchain is one of the basic technologies of digital economy, which is an important direction in the development of China's economy. Since 2008, blockchain technology has made great progress and has emerged in various fields such as crypto currency, finance, supply chain management, enterprise management, and public management. In this article, we review the directions and results of the economics and finance research on blockchain in recent years. We start by introducing the development background of blockchain. Then, we briefly introduce the operating mechanism of the blockchain technology and discuss the economic principles behind it. After that, we systematically sort out the economics and finance research results on blockchain from different perspectives, such as game theory, market equilibrium, network economics, transaction cost economics, information economics, and industrial organization theory. Finally, based on the development needs of blockchain industry of our country, we propose that the next development of blockchain economics should focus on the operating mechanism of the alliance blockchain, the information structure of the participants, and the specific application mechanism design of blockchain in medical, public welfare, food safety and other industries.

Key words: blockchain; digital economy; financial technology; game theory

(责任编辑 孙 豪)