

# 区块链技术在支付结算领域的应用与风险<sup>\*</sup>

马 理 朱 硕

〔摘 要〕近年来区块链技术的应用外延不断拓展,因此厘清区块链的功能与局限性,讨论区块链的应用场景与实施方式,有利于引导理性投资,保护投资者的合法权益,促进金融稳定防范系统性风险。本文将去中心化的节点认证机制引入经典数理模型,研究了区块链技术在商业票据支付结算领域中的应用,发现区块链技术有可能改进传统的支付结算模式的经营效率,降低交易者的成本并提高收益,但是区块链技术存在着很大的风险,应当谨慎使用与推广区块链技术,并对央行使用区块链技术提出了政策建议。

**关键词:** 区块链 支付结算 应用与风险

**JEL 分类号:** E42 E58 G21

## 一、引 言

区块链最早是作为比特币的底层支撑技术被提出。一般认为,区块链技术是指利用加密链式区块结构来验证与存储数据、利用分布式节点共识算法来生成和更新数据、利用智能合约来编程和操作数据的一种全新的去中心化基础架构与分布式计算范式,具有共享、加密、不可篡改等技术特点。通俗来讲,区块链可视为一种特殊的记账系统。以单位的财务报账为例,目前的计算机录入信息与原始凭证,都需要集中保存在单位的财务部门,这种保存方式叫做中心化。区块链技术提供了一种去中心化的记账技术,它将各类信息保存在云端,不再保存在单位的财务部门。由于云端服务器与网络中的每个电子设备不断地进行着后台信息交换,因此记账信息可以迅速地传遍全世界。从理论上实现了由全世界的所有人来监控交易(去中心化),而不是由某个人或某个机构来监控交易(中心化)。由于区块链的信息修改一般原则上要求全链条 51% 的节点同意才能进行,所需节点太多使得恶意篡改信息几乎不可能实现,因而区块链利用大数据的技术特征消除了信息不对称并保证了交易的真实性。

由此可见,区块链技术早期的主要应用可能是在支付结算领域,而区块链的外延能否拓展以及拓展到哪里需要经过严格的讨论分析。目前,各主要国家的央行基本上都涉及了区块链的研究,不少国家已经在开展一些小范围的测试与应用。2015 年 10 月,美国纳斯达克证券交易所率先推出

<sup>\*</sup> 马理,武汉大学经济与管理学院金融系,教授,博士生导师;朱硕,武汉大学经济与管理学院金融系,硕士研究生。本文得到中央高校基本科研业务费专项资金资助,并且为以下基金项目的阶段性成果:教育部哲学社会科学研究重大课题攻关项目“经济新常态下中国金融开放与金融安全研究”(批准号 17JZD015)、国家社科基金重点项目“中国经济新常态下的货币政策设计研究”(批准号 15AJL003)、湖北省教育厅哲学社会科学研究重大项目“十八大以来党中央治国理政新理念新思想新战略研究——促进供给侧改革的货币政策调控”(批准号 18ZD002)、武汉大学自主科研项目(人文社会科学)。

区块链平台 Linq 用于企业发行私人债券以及股票交易；2016 年 4 月，欧洲央行表示将评估区块链技术与支付、证券托管、抵押等银行业务的相关性；2016 年 12 月，德意志联邦银行和德国证券交易所宣布将合作创建一个区块链原型，在中心化数字货币的交割模型中实现证券结算功能；2016 年，韩国央行宣布韩国唯一的证券交易所将开发基于区块链的交易平台；2017 年 9 月，加拿大皇家银行开始部署测试区块链跨境支付系统，测试用于美国和加拿大之间资金转账的区块链系统。区块链技术在我国也受到了高度重视，周小川(2016)指出比特币的底层技术即区块链是一项可选的技术，人民银行已经开始部署重要力量研究区块链应用；2016 年 1 月，中国人民银行召开数字货币研讨会，研究区块链等技术对于支付方式的影响和变革；2016 年 10 月，工信部牵头的中国区块链技术和产业发展论坛发布《中国区块链技术和应用发展白皮书》，首次提出了我国区块链技术应用的标准化路径；2016 年 12 月，区块链技术被列入国务院发布的“十三五国家信息化规划”。我国对区块链技术的研究也取得了一定的成果。2016 年 12 月 15 日，中国人民银行对外宣布，数字票据基于区块链的全生命周期的登记流转和基于数字货币的票款兑付结算功能已经全部实现。2017 年 1 月 25 日，中国人民银行基于区块链的数字票据交易平台已测试成功，发行的数字货币也已在该平台试运行。

支付结算特别是企业的大宗支付结算，一般具有延迟支付的特征，交易双方承担的风险非常大，因此为了降低交易风险，世界各国通常采用央行的支付结算体系与商业银行体系相结合的方式来完成支付结算，在此过程中中央银行需要通过法律的强制性与交易的大批量性来保证支付结算的顺利进行。在此背景下，本文尝试从数理建模的角度分析区块链在支付结算领域的应用机理<sup>①</sup>，希望通过理论分析来科学引导区块链技术和数字货币的健康发展，并有效约束相应的金融风险。相关研究的理论意义在于：弥补区块链技术在金融领域应用的理论空白，通过机理分析探讨区块链技术应用的可行性，为区块链的未来发展提供理论支撑。实践意义在于：明确区块链技术的优势与风险，探索区块链技术可能带来的变革及影响并做好相应的配套措施，防止误用乱用区块链技术而造成金融风险。

## 二、文献综述

近年来，区块链技术的兴起引起了学术界的普遍关注，但相关研究的结论并不一致。有些学者高度认可区块链技术，认为它可以提高交易效率与降低交易成本，将给金融业带来颠覆式的革命，例如 Mainelli and Smith(2015)通过研究分布式总账的配置和区块链技术的运用案例，认为区块链技术将在处理身份、交易和债务信息方面带来巨大变革，并且在票据支付、反洗钱等金融业务中存在巨大的潜力。Kshetri(2017)认为区块链在提高透明度、建立信任和声誉等方面具有重要的作用。Kiviat(2015)从经济学角度说明区块链技术的真正价值在于可以更有效地促进数字资产转移的潜力，可应用在票据交易身份验证与所有权转让等方面。Fico(2016)认为在票据市场中，区块链技术可以提供更好的审计功能，有利于企业进行票据融资。Lamarque(2016)认为区块链技术提供了监视和执行交易的创新方法，不仅不需要中间人参与而且保证了交易记录的防篡改，可以克服现有市场中的低效率和摩擦从而改变金融市场模式。Guo and Liang(2016)认为在互联网金融的背景下，

<sup>①</sup> 本文侧重于理论分析，而没有提供实证检验，这主要有两个原因。首先，高频的有效数据不可得。目前研究区块链技术的机构包括各国央行、互联网企业，以及商业化的区块链联盟等，由于涉及到商业秘密，很多关于区块链技术的运行数据并不对外公开。其次，区块链技术是一种新兴技术，相关研究还在不断的发展和探索中。比如目前运用在票据支付结算领域的共识算法、加密机制等，与当年中本聪在比特币交易中采用的区块链技术存在较大差别。由于数据的产生背景发生了变化，因此无法获取连续稳定的高频数据序列来进行统计分析。

传统金融业迫切需要转型,区块链技术可以彻底改变支付结算系统从而升级和改造银行的核心技术。Gerstl(2016)以美国抵押贷款市场为例,说明在计算机化程度不高尤其是纸质交易结算系统中,依靠人工审核,错误和损失难以避免,而利用区块链技术的分布式数据库可以很大程度提升工作效率,实现交易过程的自动化。Sayer(2016)建议英格兰银行使用区块链技术改造银行同业结算服务,实现全天候工作并且在几分钟内就可以批准交易。De Meijer(2015)指出在支付结算系统中采用区块链技术可以使效率提高,不需要中介银行,从而减少了昂贵的客户服务费、缓解支付处理的延迟和不透明问题。Caruthers(2015)发现基于区块链技术的全球网络支付平台,在公开测试中,支付交易的时间和成本减半,而且客户可以近乎实时地跟踪整个付款过程。Di Gregorio(2017)指出区块链技术可以大幅降低金融服务成本,每年可以减少 150 亿美元至 200 亿美元的金融服务基础设施费用支出,使更多的员工专注于增值活动。

有些学者认为当前区块链技术优势和运用前景的美好描述言过其实,区块链技术存在诸多问题。例如,Karame(2016)认为区块链技术在抵制黑客攻击、实现大规模交易、去中心化等方面还存在很多局限性。Walch(2015)认为以支付结算系统为代表的金融市场基础设施对全球金融稳定至关重要,但区块链的分散性和开源性、可能出现的区块分岔以及网络黑客攻击等操作风险问题严重破坏了金融市场基础设施的稳定性。Salmony(2016)认为区块链技术并不适合票据支付结算系统,目前它还存在爆炸式存储、耗用大量资源、严重的安全和隐私等问题,而且支付结算系统是否有效应该从兼容性、成本效益等方面来评价。Zamfir(2015)指出基于代币的区块链技术验证成本很大,加密账本的副本储存在每一个网络节点中,新的支付交易在永久保存之前必须集中在验证的区块中,整个过程复杂且消耗成本高,因此目前还不适合交易规模较大的金融体系。Walker and Luu(2016)认为区块链技术理论上可以提高票据交易结算的效率,但如果在不了解系统风险的情况下盲目建立新的金融基础设施,可能会浪费大量的精力财力。Lin and Liao(2017)认为区块链技术的安全问题不容忽视,使用区块链会弱化中心机构的权利。Pinna and Ruttenberg(2016)分析了区块链技术可能对欧洲票据交易市场和金融机构带来的影响,指出尽管我们需要重视技术的发展潜能,但票据交易中的某些过程仍然需要现有机构来执行。Hayes(2016)分析了基于区块链技术的数字货币体系和支付结算体系的建立对中央银行的影响,认为央行作为货币当局的地位不可动摇,区块链只能辅助中央银行的业务处理。Ammous(2016)认为区块链技术实施成本高、数据的重复备份造成极大的浪费,并且还可能存在法律安全问题,尽管区块链技术具有去中心化等优势,但它所带来的经济利益并不能超过现有系统中的中心机构。

有些学者认为在票据支付结算中引入区块链技术的机遇与风险并存。Buitenhek and Kumhof(2016)认为不能过度夸大区块链的技术优势,可以通过行业间的广泛合作来明确区块链中真正有价值的部分并加以运用。Bott and Milkau(2017)认为区块链技术运用在支付系统中可能会彻底改变现有的金融生态系统,在提高效率的同时也需要注意法律风险、操作安全和数据保护等问题。Hemangi(2016)分析了区块链技术在支付结算、票据交易等方面的潜在应用,认为区块链将给金融业带来机遇,但同时也面临着监管限制、数据安全、数据隐私等现实问题的挑战。Cermeño(2016)认为由于技术条件还不成熟,所以目前还不能大规模的应用区块链,但是区块链技术对重构全球数字经济的信任具有重要意义。Price(2016)认为区块链技术可以改变现有的金融基础设施,降低金融风险和提高支付网络的安全性,但监管差异可能妨碍区块链技术的进展。Brummer(2015)认为区块链技术将给支付结算等金融服务带来巨大的影响,而且对金融监管提出了更高的要求,场外私有交易市场将更难实施监管。Raskin and Yermack(2016)认为区块链技术可以改善金融系统支付清算的能力,但数字货币的出现会影响现有的商业银行体系,对信贷创造和货币政策产生溢出效应,给金融机构带来风险。

国内学者对区块链技术的应用也进行了一定的研究。例如,廖理(2016)认为区块链技术在金融领域的运用会对货币政策实施、支付结算体系、反洗钱等领域产生重要影响,但该技术运行所占用的计算和存储资源巨大,难以应对大量的现实交易数据。徐忠和姚前(2016)分析了数字票据交易平台初步方案,认为票据市场是区块链运用的较好场景,区块链的使用可以有效缓解票据业务目前存在的票据伪造假冒、划款即时性不足和违规交易等问题。王晟(2016)研究了基于区块链技术的法定数字货币体系,认为如果政府作为中心节点承担清算职能,并发行中心化的区块链货币,那么支付结算效率会大幅提高,基于区块链货币的代用货币、银行券、存款货币支付体系可能可以加强货币体系的稳健性。李伟(2017)表示区块链技术在系统稳定性、应用安全性、业务模式等方面尚未成熟,目前更适用于像票据交易结算市场这样轻量级信息的、交易吞吐量较小和信息敏感度较低的业务场景。姚前和汤莹玮(2017)研究了法定数字货币与区块链技术的应用,认为区块链技术在算法性能、隐私保护、法律规范、链接标准方面还需要进一步完善,应当充分利用云计算等多种成熟安全的数字技术。李文红和蒋则沈(2018)认为针对 Fintech 的发展,应当遵循“技术中立”原则,对其实施“穿透定性”,加强监管,并提升跟踪研究和监测分析的能力。

以往学者的研究成就不容忽视,但整体来看存在着如下不足:第一,目前关于区块链的理论文献一般由计算机专业或者软件专业的学者提供,主要涉及区块链的计算机原理、加密算法、共识算法等,缺乏经济学应用的理论分析;第二,关于区块链应用的定性分析较多,缺乏区块链应用的深度机理分析;第三,展望区块链应用的美好未来的文献多,研究区块链风险管理的文献相对较少。本文在以往学者研究的基础上做出了改进,创新之处体现在:第一,从经济学角度,对区块链技术在支付结算领域的应用进行理论分析,为区块链技术的应用提供理论解释;第二,通过数理建模,分析区块链技术在支付结算领域中的作用机理,实现从计算机技术到经济学应用的过渡;第三,研究区块链技术在支付结算过程中存在的风险,提出相应的风险防范方案。

### 三、区块链支付结算模式下成本效率的改进

#### (一)传统的支付结算模式

商业票据是一种短期的融资行为,体现出延期支付的特征,由于信息不对称的存在,对交易双方而言风险非常大,因此世界各国一般都是通过央行的支付结算与商业银行体系相结合的方式来完成,在此过程中,央行的支付结算中心主要担负着监督与结算两个职能。

假设央行支付结算中心为 Center,票据市场上的交易者为 a, b, c, …, 其账户开户行分别为各个商业银行 A, B, C, …。我们假设企业 a 与 b 之间进行某项具体业务, a 向 b 开出一张票面金额为  $h$  的商业票据,票面利率为  $r$ , 期限为  $t$ , 由其开户银行 A 进行审核并承兑。票据期满后, b 通过开户行 B 和票据支付结算体系向 A 提示付款, A 再经由 Center 向 B 进行付款,从而完成票据的开票、承兑、提示付款和付款的过程。

假设 b 向 a 借出款项  $\frac{h}{1+rt}$  后获得商业票据, a 将该资金投资于某一项目, 该项目给企业 a 带来的真实收益为随机变量  $\tilde{y}$  ( $0 < \tilde{y} < +\infty$ ),  $\tilde{y}$  的分布对 a 与 b 都是已知的, 且满足(1)式, 其中  $i$  是企业 A 的投资收益率。

$$E(\tilde{y}) \geq \frac{h(1+it)}{(1+rt)} \quad (1)$$

这意味着, 只有当项目投资给企业 a 带来的投资收益率至少为  $i$  时, 企业 b 才会选择向 a 借款并进行投资。此时, 出现了信息不对称。因为 b 只知道 a 的投资收益的分布特征, 而不知道投资收益的

真实值,该具体信息只有企业 a 自己才知道。这种信息不对称对于 b 有可能是致命的,因为企业 a 可能对 b 宣称一个较低的  $y$ , 以期向企业 b 支付尽可能少的资金,从而获得自身更多的收益。最极端情况下,企业 a 可能会宣称投资失败,即  $y = 0$ , 而拒绝向企业 b 支付票据。由于企业 b 无法完全识别 a 的信息真实度,因此企业 b 可能蒙受损失。

承担监督职能的 Center 的介入可以缓解信息不对称,由于掌握了核心的支付结算环节,Center 可以对 a 的资金流向和票据流转进行监督,如果出现了 a 利用信息不对称低报项目收入或未按期缴款的情况,Center 会通过其开户行 A 对其实施惩罚,再将惩罚的金额转移给持票人。假设 Center 面对的企业有  $n$  家,  $Y_n = \sum_{l=1}^n y_l$  表示企业项目总回报,每个项目的回报  $y_l (l = 1, 2, 3, \dots, n)$  均服从随机变量  $\tilde{y}$ , 总票面金额为  $H_n$ 。  $Z_n$  表示出票企业经由 Center 支付给持票人的总额,出票人需要按照结算金额的  $\eta$  比例向 Center 支付手续费  $\eta Z_n$ 。设惩罚函数为  $\phi(Z_n)$ , 是实际支付值  $Z_n$  的减函数,实际支付值越小,惩罚金额就越大。根据 Diamond(1984) 的研究,最优惩罚函数  $\phi^*(Z_n)$  在企业价值最大化的前提下满足式(2),约束条件为式(3)。

$$\phi^*(Z_n) = \max[(H_n - Z_n), 0] \quad (2)$$

$$\operatorname{argmax}_{Z_n \in [0, Y_n]} Y_n - Z_n - \phi^*(Z_n) = \begin{cases} Y_n, & \text{if } Y_n < H_n \\ H_n, & \text{if } Y_n \geq H_n \end{cases} \quad (3)$$

式(3)意味着,当项目收入小于应该支付的本息和时,支付为  $Y_n$ ; 当项目收入大于约定票面金额时,支付本息和  $H_n$ 。但由于惩罚函数  $\phi^*(Z_n)$  存在,若当出票人支付小于票面价值,即  $Z_n < H_n$  时,由支付结算中心对出票人进行惩罚,并最终将惩罚数额  $(H_n - Z_n)$  转移给持票企业,保证持票企业最终获得本息和  $H_n$ 。在这一过程中,Center 承担着监督出票企业缴款的责任,记录并监督着出票企业的资金流向和票据流向,对违约企业调查,并且通过惩罚函数保证了持票企业获得票面金额  $H_n$ 。

除了监督之外,结算也是 Center 的一项重要职能,通过支付结算体系各个企业才能实现票据的流转和资金的融通。票据的结算职能贯穿于票据的签发、承兑、提示付款和最终付款等业务流程的全过程。在前文分析的情况中,a 和 b 之间确实有真实的业务交易。而另一种可能存在的情况是 a 和 b 之间并没有真实的业务交易,通过共同骗取 A 的承兑,伺机在二级市场转手套现。在传统票据支付结算体系中,出票人开户银行更多的依赖于对其提供的证明材料的审核,以此来判断票据是否依托于真实的业务交易。一旦开户行对交易的真实性存疑,该票据业务将在承兑环节终止。若银行审核通过,票据承兑完成,才可以正式进入流通环节。票据到期后,企业 b 向其开户行 B 发出提示付款申请,银行 B 向 Center 提交提示付款的指令,Center 登记并向承兑行 A 转发付款指令,A 根据 a 的账户余额情况向 Center 发送回执。接着 Center 根据同意付款的回执,连接支付清算系统完成清算工作,并将信息结果回馈给银行 A 和 B,进而送达企业 a 和 b。

## (二) 区块链技术可能可以降低传统的支付结算成本

支付结算体系的运营成本主要分为监督成本和结算成本。监督成本包括监督企业资金、票据流向和调查违约企业的成本,结算成本包括审核票据交易真实性和清算票据的成本。总监督成本  $S_n$  为

$$S_n = s_1 n + s_2 n P \quad (4)$$

其中,监督特定的出票企业 a 资金流向和票据流向的成本为  $s_1$ , 企业违约率为  $P$ , 每次的调查成本是  $s_2$ 。总结算成本为(5)式。

$$C_n = c_1 n + c_2 \quad (5)$$

其中,每张票据交易真实性的审核成本为  $c_1$ 、总清算成本为  $c_2$ 。传统的支付结算模式虽然能够为票

据交易提供顺畅的交易通道,而且在企业价值最大化的条件下,可以通过惩罚函数尽量保障持票人的利益不受侵害,但是传统的支付结算模式存在一定的局限性。一是在监督方面的局限性:首先,完整的票据流向信息只存储于 Center 的系统中(即存储的中心化),各银行只有接入 Center 系统才能进行查询和验证,而接入不同系统一般会存在代理成本。其次,当出票企业 a 不按时缴款时,支付结算体系需要对 a 进行深入调查,辨别其是否为恶意逃避债务。对当事企业进行深入的调查需要付出比较高的成本,而支付结算体系还承担着其他企业的支付结算等繁重的工作,不见得有能力强从事该项调查,因此不能很好的实施惩罚,保障持票人的利益。二是在结算方面的局限性:出票企业的开户行需要对票据交易的真实性进行审核,这一审核更多的是依赖于出票企业提供的材料,很容易受到信息不对称的负面影响,而且票据的清算成本还取决于票据开户行接入的支付清算体系。

联盟区块链综合了管理中心化与业务经营去中心化的双重特点,Center 掌握中心化特权,具备强制的惩罚能力,而商业银行作为联盟区块链的节点,有点对点支付的权利但需要接受 Center 的监督。因此 Center 可以确保惩罚函数  $\phi(Z_n)$  的执行具有强制力,以保障持票企业的权益。联盟区块链上,票据的每一步交易都会对联盟链的节点公示,商业银行可在本地数据库对企业票据流向进行实时监控,智能合约也可自动监控并中止违规交易。而且,联盟链上对企业的监督工作不再仅由 Center 完成,区块链社区中的每个节点都可以对出票人进行监督(即去中心化)。每次资金和票据交易之后,企业通过开户银行对交易进行评价。出于保护隐私的目的,资金和票据流向的具体信息只有作为授权节点的商业银行可以获取,而作为普通节点的交易者只能查看历史交易评价。

如果企业 a 不诚信,不按约定偿还企业 b 的本息,那么 b 可以把 a 不诚信的信息公布在联盟区块链中,按照区块链的约定,相关信息需要联盟区块链 51% 以上的节点同意才能修改,修改成本极高几乎不太可能,考虑到差评会影响到企业 a 以后的交易与融资,对将来造成巨大负面影响,因此 a 不敢违约。另一方面,如果企业 b 对企业 a 做出了一个恶意差评,那么企业 a 可以提供申诉证据,一旦被大多数节点认可,恶意评价的企业 b 将形成信用污点,今后的交易与融资将受到影响,因此 b 不敢随意给出差评。联盟区块链中的央行具有中心化特权,可以根据情节的严重性对违约企业进行分级惩罚。企业违约成本被大幅提高,这在一定程度上也可以降低企业的违约率。在节点认证机制的保障下,式(4)的监督成本  $S_n$  会大大降低。

在传统票据支付结算的承兑环节,开户银行只能通过出票企业单方面信息确认,而在联盟区块链中可以获得多方的信息甚至实现全网共同审核,所以式(5)中的审核成本  $c_1$  也会下降。当票据为电子形式,交易双方开户银行均接入大额支付结算系统,清算成本  $c_2$  可以达到最低。因此,采用联盟区块链技术可以降低传统票据支付结算体系的成本。

$$(C_n + S_n)_{\text{联盟链}} < (C_n + S_n)_{\text{传统}} \quad (6)$$

激励相容的政策必须要让所有局中人都觉得有利可图。因此我们再来讨论引入联盟区块链之后,企业的成本收益状况是否会发生变化。基于 Diamond(1984)的研究,票据持有者的预期回报应当满足

$$PE(Z_n | Z_n < H_n + \frac{s_0}{2}n) + (1-P)(H_n + \frac{s_0}{2}n) \geq H_n \quad (7)$$

其中,  $\frac{s_0}{2}n$  表示出票人支付的监管费用,Center 与持票人平分这部分收益。如前假设,企业 a 是出票企业,企业 b 是持票企业,b 不会轻易借款给 a,除非 a 能找到一个被 b 认可的第三方背书。因此企业 a 会交付一笔费用给 Center,Center 中心化的监管相当于对 b 出具了一份信用报告,有了这层

监管关系之后,企业 b 才会放心地将钱借给企业 a,因此相当于企业 a 支付了一笔费用,而支付结算中心与企业 b 同时享有这部分收益。为了避免不必要的繁琐推导,假设两者平分。

由于  $Z_n \geq 0$ , 意味着  $E(Z_n | Z_n < H_n + \frac{s_0}{2}n) \geq 0$ , 所以票据持有者总的预期回报将满足式(8)。

$$(1-P)(H_n + \frac{s_0}{2}n) = (1-P)n(h + \frac{s_0}{2}) > \frac{2h}{2h + s_0}n(h + \frac{s_0}{2}) = H_n \quad (8)$$

此时,企业违约率满足

$$0 < P < \frac{s_0/2}{h + s_0/2} = \frac{s_0}{2h + s_0} \quad (9)$$

根据弱大数定理,存在某个  $n = N < +\infty$  时,  $P < \varepsilon$  对所有的  $\varepsilon < 0$  成立,当票据交易企业数量  $n$  足够大时,企业违约率  $P$  将很小。由式(9)可知,更小的违约率  $P$  意味着更小的调查费用  $s_0$ 。所以当监督对象足够多的时候,每个企业付出的监督费用会减少。

在初期,Center 可以兼做监控和调查职能,引导区块链社区的制度形成,一旦形成了完善的联盟区块链支付结算系统,将足够多的企业引入区块链社区,Center 就不需要进行调查工作了。因为所有的真实交易结果评价都被暴露在阳光下,信息不对称问题得到极大的解决。此时 Center 只需要保障系统内的资金流和票据流顺利运转,并根据局中人是否违约的具体情况来进行相应的惩罚。对票据交易者来说,需要支付的监督调查费用随着联盟区块链体系的完善而减少,甚至不再需要支付监督调查费用,这将大大降低企业的票据交易成本。

### (三) 区块链技术可能可以提高传统的支付结算效率

在开票和承兑环节:传统支付结算模式下,出票企业 a 通过开户银行的网上银行提出票据签发申请,然后企业 a 携带真实、有效的可以证实真实交易关系或者债券债务关系的交易合同等纸质证明材料到银行 A 处申请承兑;银行 A 审核无误确定承兑后,向 Center 提交票据信息;Center 系统登记信息后转发至收款人开户银行 B,银行 B 提示企业 b 签收;企业 b 在网上银行签收后,银行 B 向 Center 转发签收信息,Center 登记信息并转发至银行 A;银行 A 在行内系统中登记票据出票成功信息,并告知 a。以上传统模式中的票据的开票和承兑环节,过程相当繁琐,票据的开票成功信息需要分别在银行 B、Center 系统和银行 A 之间重复登记多次,信息传递需要通过多次转发,而且不同银行对不同企业的承兑审核的业务效率可能存在较大的个体差异。而在联盟链支付结算模式中,出票企业 a 提出票据签发申请后,可上传电子证明材料,银行 A 将信息在链上公布,全网可共同审核,提高审核效率和质量。审核无误后,银行 A 在链上承兑,该信息立刻在链上广播,企业 b 可通过银行 B 的链上系统签收,即表示出票成功,票据出票信息在链上同步广播。因此从理论上说,区块链技术可以简化流程节约成本。

在提示付款和付款环节中:传统支付结算模式下,持票企业 b 首先通过银行 B 的网上银行系统进行票据提示付款操作,银行 B 向 Center 提交提示付款的指令;Center 系统登记并转发指令,银行 A 接收指令并向 Center 发送同意付款的回执;Center 登记回执结果并接入大额支付清算系统进行清算,大额支付清算系统完成清算后,Center 将系统清算结果分别回馈给银行 A、B,进而送至企业 a、b。以上过程在实际中,并不能真正做到即时清算。但是在联盟区块链上,如果引入央行的数字货币有可能实现真正的即时清算。央行是联盟链上的一个特殊节点,而每个商业银行节点拥有一定数量的数字货币。在票据清算时,企业 b 首先通过银行 B 的链上系统发出提示付款的指令,该指令在链上广播;银行 A 接收后同意付款即向银行 B 发送足额的数字货币,同时,票据付款成功的信息在全网广播。由于全部操作都在联盟链上完成,不需要经过 Center,也不需要接入其他支付清算系统,所以从理论上说,交易效率将被大大提高。

联盟区块链技术之所以可以促使票据支付结算效率的提高,原因有如下几点:一是分布式账本。联盟区块链中的数据分布式存储在每一个商业银行支付节点中,不但可以省去中间处理环节,而且数据可以通过区块共识实现同步,效率大幅提高。二是智能合约的灵活运用。智能合约让许多业务实现自动化,比如持票企业到期自动提示付款,以及 Center 对违规交易的监督。三是票据信息的实时广播。交易各方不但可以及时获得票据最新动向,而且票据的二级市场交易者、市场监督者等都可以减少信息搜寻工作。四是数字货币的运用。数字货币中的信息流和资金流高度统一,交易和结算同步完成,交易体系可以实现即时的券款兑付,提高资金周转效率<sup>①</sup>。

#### 四、区块链支付结算模式下的风险转变

##### (一) 区块链支付结算模式下的风险分担机制

传统支付结算模式下的主要风险在于信息不对称。一方面票据承兑时,银行对票据背后交易真实性的审核主要依赖出票企业提供的证明材料,存在逆向选择;另一方面出票企业一旦违约,支付结算体系对于票据违约企业的调查难度比较大,存在道德风险。

而在联盟链支付结算模式下,区块链的去中心化使 Center 系统中各个节点之间充分实现信息共享,由多个节点共同监督出票企业,有效改善信息不对称难题。根据 Ramakrishnan and Thakor (1984) 风险分担的金融中介理论,区块链支付结算模式恰好满足风险分担的前提条件。在传统支付结算模式下,金融中介对出票企业的调查主要依靠其开户银行,相当于 1 家中介机构单独对 1 家企业进行监督;而在区块链支付结算中,Center 系统中的多家中介机构形成一个中介联盟,联盟中的信息是完全透明的,不存在联盟内部的道德风险和激励问题,通过区块链节点认证的方式,各个中介机构共同监督 1 家出票企业,那么每一家中介机构承担的风险均会降低。Diamond (1984) 也指出“多样化”可以降低风险,N 个风险规避的中介机构组成一个信息共享的团体,共同开展 N 个相同且独立的项目工作的  $1/N$ ,其中每一个中介获得的期望效用将高于其独自承担一个完整项目的期望效用。

我们假设每一家开户银行都是风险厌恶的,其效用函数  $U(\cdot)$  连续可微可逆且有界,满足  $U(\cdot) > 0$ ,  $U'(\cdot) < 0$ , 其反函数为  $\Psi(\cdot) = U^{-1}(\cdot)$ 。在传统模式下,每一家开户银行对一家出票企业进行监督。 $\alpha$  表示开户银行为监督工作付出的努力程度,  $\alpha \in [0, 1]$ ,  $\alpha = 1$  表示开户银行的监督工作是尽职的,  $\alpha < 1$  表示开户银行工作不尽职。由于  $\alpha$  是不可观测的,由事后观测指标  $\beta$  来表示公众对银行监督工作的评判,  $\beta = 1$  表示认可,反之  $\beta = 0$  表示不认可。类似于“声誉”机制,公众对开户银行的评价影响其愿意向开户银行支付的酬劳,进而影响开户银行的效用。每一家出票企业按照评价高低,愿意支付的金额分别为  $W$ 、 $X$ , 则  $U(W) = w$ ,  $U(X) = x$ ,  $w > x$ 。

事后观测指标  $\beta$  与开户银行的努力程度  $\alpha$  之间可能会出现偏差,偏差出现的概率如式(10)所示。为简化过程,我们仅考虑开户银行尽职 ( $\alpha = 1$ ) 的情况。其中,  $0 < \gamma < 1$ 。

$$\begin{aligned} P(\beta = 1 | \alpha = 1) &= \gamma \\ P(\beta = 0 | \alpha = 1) &= 1 - \gamma \end{aligned} \quad (10)$$

开户银行对监督工作的期望效应可表示为式(11),式中  $V$  为正实数,表示银行尽职监督的消

<sup>①</sup> 本部分从理论上分析了联盟区块链技术对支付结算体系效率的改善。但在实际中,由于受到计算机算力的限制,区块链上的交易记录并不能实时生成。以比特币为代表的公有链,每秒仅能处理约 7 笔交易,一般交易确认的时间平均为 10 分钟。联盟链的共识节点小于公有链,其处理效率提高到了每秒 1000-10000 笔交易,但即便如此,仍然难以应对大量高频交易的需求。只有当计算机算力达到足够的水平后,区块链技术提高交易效率的作用才能真正发挥出来。



耗值。

$$U(\alpha = 1) = \gamma w + (1 - \gamma)x - V \quad (11)$$

在联盟区块链票据支付结算体系中,两家银行组成联盟共同监督 2 家出票企业,事后观测指标  $\beta$  有三种情况 0、0.5 和 1。其中,  $\beta = 0.5$  表示公众认为中介联盟仅对某 1 家出票企业的监督是尽职的,此时愿意支付的金额为  $K$ , 则  $U(K) = k, w > k > x$ 。

根据 Ramakrishnan and Thakor(1984),在激励相容和理性人的约束下,有:

$$k > \frac{w + x}{2} \quad (12)$$

联盟的效用满足:

$$U^*(\alpha = 1) = \gamma^2 w + 2\gamma(1 - \gamma)k + (1 - \gamma)^2 x - V > \gamma^2 w + \gamma(1 - \gamma)(w + x) + (1 - \gamma)^2 x - V = \gamma w + (1 - \gamma)x - V = U(\alpha = 1) \quad (13)$$

所以,联盟区块链中各个开户银行联合起来监督出票人的效用将高于传统模式下各个银行单独监督产生的效用。

## (二) 区块链技术应用于支付结算的可能风险

虽然从理论上说,联盟区块链的分布式存储、多节点共同监督、智能合约等特点可以有效地降低传统支付结算体系下的信息不对称,但是也可能产生新的风险点,包括爆炸式存储风险、数字货币风险,以及系统应用风险。

### 1. 爆炸式存储风险

在金融行业的高频交易数据的冲击下,区块链技术的分布式存储成本会急速上升。因为每增加一个共识节点,就意味着增加一份整个市场数据的存储成本。假设联盟区块链支付结算体系中共有  $M$  家开户银行,各个银行间实现信息共享需要付出高昂的直接成本。另假设存在监督体系,信息共享的直接成本为  $\pi_1, \pi_1 \in (0, \infty)$ , 出票企业愿意支付给中介的金额为  $\delta_f = \Psi(s_0)$ , 其中,如前文所设  $s_0$  表示中介机构调查出票企业的边际成本,则监督体系的总成本为  $\pi_1 + \delta_f$ 。

在传统模式下,银行单独监督出票企业,出票企业愿意支付给银行  $\delta = \gamma\Psi(w) + (1 - \gamma)\Psi(x)$ 。在联盟区块链模式下,各个银行信息共享的直接成本为  $\pi_2$ , 出票企业愿意支付给中介联盟的金额为

$$\delta^* = \gamma^2 \Psi(w) + 2\gamma(1 - \gamma)\Psi(k) + (1 - \gamma)^2 \Psi(x) \quad (14)$$

根据 Ramakrishnan and Thakor(1984),出票企业支付给信息共享的金融中介联盟的金额低于其支付给单独行动的金融中介的金额,即

$$\delta^* < \delta \quad (15)$$

而且,当联盟中金融中介的数量无穷大时,每个企业支付给金融中介联盟的金额收敛到金融中介监督的边际成本,即

$$\lim_{M \rightarrow \infty} \delta^* = \delta_f$$

$$\delta^* = \delta^*(M), \partial \delta^*(M) / \partial M < 0 \quad (16)$$

所以,在联盟区块链支付结算模式下的总成本为  $\pi_2 + \delta^*(M)$ , 只要式(17)成立,构成信息共享的金融中介将优于单独行动的金融中介。

$$\pi_2 + \delta^*(M) \leq \min(\pi_1 + \delta_f, \delta) \quad (17)$$

如果  $\pi_2$  为固定不变的高昂成本,  $\bar{M}$  是使得上式成立的最小的  $M$ , 那么只要加入联盟中的金融中介的数量大于  $\bar{M}$ , 支付结算体系的福利将被提高。但是,由于联盟区块链支付结算体系中各个金融中介之间是通过分布式存储来实现信息共享的,每增加一个节点,实现信息共享的成本就将成倍提高。因此  $\pi_2$  不是固定不变的成本,应满足

$$\pi_2 = \pi_2(M), \partial\pi_2(M)/\partial M > 0 \quad (18)$$

此时,支付结算体系福利改善的条件由式(17)变为式(19):

$$\pi_2(M) + \delta^*(M) \leq \min(\pi_1 + \delta_f, \delta) \quad (19)$$

爆炸式存储问题使得联盟中的节点数量并不确定。金融中介的数量不再是越多越好,而主要取决于  $\pi_2(M)$  和  $\delta^*(M)$  函数的具体形式,区块链的技术发展影响着节点的最优数量。式(19)更加直观地说明,构建联盟区块链票据支付结算体系时,由于爆炸式存储风险的存在,我们需要更加谨慎地设置联盟链共识节点数量。

## 2. 数字货币风险

数字货币是提高票据支付结算效率的重要因素,而数字货币的不确定性导致了联盟区块链支付结算体系的新风险,因为数字货币的去中心化特征可能会将央行推向两难的困境。首先,如果实施去中心化的数字货币制度,就意味着央行可能会放弃法币的主动发行权,无法决定货币政策的传导效果,中央银行将失去存在的意义。其次,按照货币理论,货币发行量应当与国家的经济增长相适应。正常情况下,一个国家的产出是每年递增的,这就意味着货币供应量也应当同比增长才能正常行使支付手段的职能。具有发行上限的数字货币在长期中将导致货币供应量不足,出现严重的通货紧缩。而且,发行上限决定了数字货币的稀缺性,当价格涨到一定程度,数字货币的支付手段与职能就会丧失,投资品性质凸显将不再适合作为“固定的一般等价物”。如果央行坚持发行中心化的数字货币,且希望灵活调整发行量的话,则与目前市场中的数字货币体系属于完全不同的两类技术体系和发行流通框架。那么,全新的数字货币生态体系如何建立,法定数字货币的技术路径如何选择,与现行的货币体系如何更好地契合,市场对于数字货币如何反应等系列问题都值得认真研究。

## 3. 系统应用风险

首先,央行的支付结算成本在实践中不一定会降低。区块链技术的做法是将监督职能交给市场,让联盟区块链上的节点来监督结算双方。但从理论上说,合谋可能会摧毁这种运行机制,出票人可能可以与关联人进行多次的小额结算往来,形成良好的信用记录,最后在大额的支付结算时卷走所有资金。而央行的惩罚措施也不一定能够落到实处,如果一家公司违约以后能够诚恳地接受处罚并愿意拿出惩罚金补偿对手公司,那这家公司就是好公司也根本不会违约,因此完全靠节点来监督节点的做法具有很大的局限性。

其次,企业的支付结算成本在实践中也不一定会减少。企业之所以愿意加入区块链,看中的是区块链能够降低结算成本,所以企业愿意交一笔费用保障支付结算的流畅进行。如果区块链技术的节点监督节点的模式行不通,那么企业会退出联盟区块链,没有了节点,联盟链也就自然瓦解了。因此在短期内,区块链技术可能还存在着应用难度。

## 五、政策建议

本文研究了区块链技术在商业票据支付结算领域中的应用,研究发现区块链技术有可能改进传统的支付结算模式的经营效率,降低交易者的成本提高收益,但是当前的区块链技术应用还存在着很大的风险。基于此,我们给出相关政策建议如下。

第一,可能暂时不宜在全经济领域推广区块链的应用。区块链技术是数字货币的底层支撑技术,独特的节点认证机制可以较好地消除信息不对称。因此有很多学者做了拓展,尝试将区块链技术应用到更广的领域来消除信息不对称。现在有很多关于区块链应用的美好前景的展望,例如在税收征管、政府管理、健康、科技、文化、物联网等,这些展望的出发点都是好的,但是笔者对此持谨

慎乐观的态度,区块链技术有其适用背景,也存在一定的局限性,当不具备实施前提时,强行推广可能会存在很大的风险。

第二,央行可尝试在支付结算体系中做小范围试点。区块链技术最初是保障数字货币的正常支付结算而使用的一种计算机算法技术,因此如果央行要进行尝试,我们建议选择支付结算体系进行小范围试点。票据支付结算体系相对封闭,交易量较小,信息敏感度较低,但同时又承担着信用、交易、支付、清算等众多金融职能,是区块链技术运用试点的较好业务场景。

第三,推行区块链技术要充分权衡好风险、效率和成本因素。尽管从理论上讲,使用区块链技术可以降低票据支付结算体系的成本,并且提高系统运行效率,但是爆炸式存储风险、数字货币风险、系统应用风险等因素的存在,可能会抵消掉区块链技术应用带来的收益。如果要在票据支付结算体系中运用区块链技术,需要权衡好风险、效率和成本的关系,同时合理设置联盟链共识节点数量和区块链社区运行规则。

### 参考文献

- 李伟(2017):《央行科技司解答区块链适用场景等问题》,《中国新闻网》,http://www.chinanews.com/cj/2017/01-27/8136933.shtml。
- 李文红、蒋则沈(2018):《分布式账户、区块链和数字货币的发展与监管研究》,《金融监管研究》,第6期。
- 廖理(2016):《数字货币时代渐行渐近》,《清华金融评论》,第5期。
- 王晟(2016):《区块链式法定货币体系研究》,《经济学家》,第9期。
- 徐忠、姚前(2016):《数字票据交易平台初步方案》,《中国金融》,第17期。
- 姚前、汤莹玮(2017):《关于央行法定数字货币的若干思考》,《金融研究》,第7期。
- Ammous, S. (2016): "Blockchain Technology: What is it Good for?", *Social Science Electronic Publishing*, https://ssrn.com/abstract=2832751.
- Barrdear, J. and M. Kumhof (2016): "The Macroeconomics of Central Bank Issued Digital Currencies", Working Paper, Bank of England, No. 605.
- Bott, J. and U. Milkau (2017): "Central Bank Money and Blockchain: A Payments Perspective", *Journal of Payments Strategy and Systems*, 11, 145-157.
- Brummer, C. (2015): "Disruptive Technology and Securities Regulation", *Fordham Law Review*, 84, 977-1037.
- Buitenhek, M. (2016): "Understanding and Applying Blockchain Technology in Banking: Evolution or Revolution?", *Journal of Digital Banking*, 1, 111-119.
- Caruthers, R. (2015): "Global Payments Startup Leverages Blockchain Engine to Reduce Cross-border Friction", *Fierce Finance IT*, https://www.reddit.com/r/Bitcoin/comments/36sgqa/global\_payments\_startup\_leverages\_blockchain/.
- Cermeño, J. (2016): "Blockchain in Financial Services: Regulatory Landscape and Future Challenges for its Commercial Application", Working Paper, BBVA Research, No. 16/20.
- De Meijer, C. (2015): "The UK and Blockchain Technology: A Balanced Approach", *Journal of Payments Strategy and Systems*, 9, 220-229.
- Di Gregorio, M. (2017): "Blockchain: A New Tool to Cut Costs", *Middle East Insurance Review*, 2, 50-51.
- Diamond, D. (1984): "Financial Intermediation and Delegated Monitoring", *Review of Economic Studies*, 56, 393-414.
- Fico, P. (2016): "Virtual Currencies and Blockchains Potential Impacts on Financial Market Infrastructures and on Corporate Ownership", *SSRN Electronic Journal*, https://ssrn.com/abstract=2736035.
- Gerstl, D. (2016): "Leveraging Bitcoin Blockchain Technology to Modernize Security Perfection under the Uniform Commercial Code", In: Maglyas, A. and A. Lamprecht (eds.), *International Conference of Software Business, ICSOB 2016*, Switzerland: Springer International Press.
- Guo, Y. and C. Liang (2016): "Blockchain Application and Outlook in the Banking Industry", *Financial Innovation*, 2, 24-36.
- Hayes, A. (2016): "Decentralized Banking: Monetary Technocracy in the Digital Age", In: Tasca P., Aste T., Pelizzon, L. and N. Perony (eds.), *Banking Beyond Banks and Money*, Switzerland: Springer International Press.
- Hemangi, G. (2016): "Blockchain Technology: Opportunities and Challenges for Financial Industry", Master Dissertation, Graduate School of International Studies, Seoul National University.
- Karame, G. (2016): "On the Security and Scalability of Bitcoin's Blockchain", *Proceedings of the 2016 ACM SIGSAC Conference on*

*Computer and Communications Security*, New York: ACM.

Kiviat, T. (2015): “Beyond Bitcoin: Issues in Regulating Blockchain Transactions”, *Duke Law Journal*, 65, 569–589.

Kshetri, N. (2017): “Will Blockchain Emerge as a Tool to Break the Poverty Chain in the Global South?”, *Third World Quarterly*, 38, 1710–1732.

Lamarque, M. (2016): “The Blockchain Revolution; New Opportunities in Equity Markets”, Master Dissertation, Massachusetts Institute of Technology.

Lin, I. and T. Liao (2017): “A Survey of Blockchain Security Issues and Challenges”, *Network Security*, 19, 653–659.

Mainelli, M. and M. Smith (2015): “Sharing Ledgers for Sharing Economies: An Exploration of Mutual Distributed Ledgers (Aka Blockchain Technology)”, *Journal of Financial Perspectives*, 3, 38–69.

Paech, P. (2016): “Securities, Intermediation and the Blockchain: An Inevitable Choice between Liquidity and Legal Certainty?”, *Uniform Law Review*, 21, 612–639.

Pinna, A. and W. Rutenber (2016): “Distributed Ledger Technologies in Securities Post – Trading Revolution or Evolution?”, Working Paper, ECB Occasional Paper, No. 172.

Price, E. (2016): “Regulatory Divergence Could Hamper Blockchain”, *International Financial Law Review*, 35, 37–45.

Ramakrishnan, R. and A. Thakor (1984): “Information Reliability and a Theory of Financial Intermediation”, *Review of Economic Studies*, 51, 415–432.

Raskin, M. and D. Yermack (2016): “Digital Currencies, Decentralized Ledgers, and the Future of Central Banking”, NBER Working Paper, No. 22238.

Salmony, M. (2016): “Blockchain-Not for Payments?”, *BIT – Banking and Information Technology*, 56, 6–8.

Sayer, P. (2016): “Bank of England Wants Next Payment System to Be Blockchain Ready”, *CIO Newsletter*, <https://www.cio.com/article/3121225/bank-of-england-wants-next-payment-system-to-be-blockchain-ready.html>.

Walch, A. (2015): “The Bitcoin Blockchain as Financial Market Infrastructure: A Consideration of Operational Risk”, *New York University Journal of Legislation and Public Policy*, 18, 837–895.

Walker, M. and J. Luu (2016): “Blockchain and the Nature of Money”, *Social Science Electronic Publishing*, <https://ssrn.com/abstract=2939042>.

Zamfir, V. (2015): “Introducing Casper ‘the Friendly Ghost’”, *Ethereum Blog*, <https://blog.ethereum.org/2015/08/01/introducing-casper-friendly-ghost>.

(责任编辑:程 炼)