

区块链技术的主要特征及其应用场景*

——兼论如何进一步提升上海国际金融中心功能

孙立行

(上海社会科学院世界经济研究所,上海 200020)

摘要:所谓区块链,可以理解为一种全民分布式记账的技术,每笔数字交易都将被记录在“块”,区块与区块之间相连,形成区块链。任何人均可查阅交易记录,但任何个体都无法轻易控制、篡改数据,其本质特征是去中介化、去中心化。正是基于上述的技术优势,区块链能够以非常低的成本对网络节点交易进行身份识别和个人征信,从而极大提高金融系统的运行效率,对重构金融行业底层架构将产生深远影响。区块链技术在保险业领域的创新应用,可以作为进一步提升上海国际金融中心功能的助推器。

关键词:区块链;主要特征;应用场景;上海国际金融中心

中图分类号:F830 **文献标识码:**A **文章编号:**1671-2404(2018)87-0038-05

近年来,随着金融科技的快速发展,作为支撑比特币等数字货币的核心技术暨区块链技术逐步成为全球关注的焦点。在 2016 年的 G20 杭州峰会上区块链技术被首次列为重要议题。区块链技术之所以会引起各国政府的极大兴趣和密切关注,是因为它未来的巨大应用价值。未来区块链技术将会改变传统金融服务业的底层技术架构,大幅提升金融系统的核心服务功能。

1 区块链技术的五大特征

区块链(blockchain)作为比特币的底层技术,最初是由一位自称中本聪的人在其 2008 年发表的题为《比特币:一种点对点的电子现金系统》论文里提出的。按照中本聪的描述,区块链技术是一种新型的分布式数据库技术,由一个一个被称为区块(block)的存储单元组成,用于记录各个区块的节点(node)即网络参与者的所有价值交换情况。各区块之间依靠哈希算法驱动实现链接(chain),后一个区块包含前一个区块的哈希值(hash)。随着价值交换的不断扩大,越来越多的区块与区块之间相继链接,形成所谓的区块链。两个月后,中本聪的这一理

论构想付诸了实践,2009 年 1 月初首个“创世区块”诞生。

区块链的创新之处在于交易者不需要通过第三方机构提供授信支持,而可依赖特定的算法程序驱动来解决信任问题,达成共识背书,实现价值交换。从区块链的形成过程看,区块链技术具有去中心化(Decentralized)、去信任(Trustless)、集体维护(Collectively maintain)、高度透明(High transparency)和匿名性(Anonymity)等五大特征(见表 1)。这些特征具体体现在以下四个方面:

表 1 区块链技术的五大特征

特征	具体内容
去中心化	不需要依赖中心服务器或第三方机构,任意节点间的权利和义务是均等的。
去信任	在未取得各节点参与者相互信任的情况下,从技术上确保交易的顺利实施。
集体维护	系统中的交易纪录由所有节点共同维护,任何参与者都无法篡改交易数据。
高度透明	分布式记账及公开的账簿,确保了所有交易记录可被参与者查询及监督。
匿名性	由于区块链技术解决了交易双方的互信问题,故交易可在匿名情况下完成。

资料来源:作者整理

收稿日期:2018-07-02

作者简介:孙立行,研究员,博士生导师,上海社科院世界经济研究所国际投资室主任,国际金融货币研究中心常务副主任,致公党中央经济委员会委员。E-mail:sunlixing@sass.org.cn

* 基金项目:本研究系上海社会科学院国家高端智库 2017 年度资助项目。

第一,区块链最突出的特征是去中心化。区块链技术采用的是分布式核算和存储,所有的交易纪

录无需集中存放在中心服务器或数据中心,而可以分散存放于各区块中的每一个节点。因此,区块链通过去中心化的形式实现了整个网络内的自我证明功能,而不是依靠传统形式下的第三方机构完成统一的交易账簿的更新与验证。

第二,区块链技术具有开源(Open Source)属性。除了交易各方的私有信息被加密外,区块链上的数据都是公开的,任何人都可实现历史交易信息的自我查证。因此,整个系统的信息透明度高。换句话说,所有参与者都能看到系统内发生和记录的每一笔历史交易。

第三,区块链技术重塑信任基础。区块链中任何交易的信任基础都是通过纯数学背书而非交易双方的身份背书。每一笔交易都需要通过交易双方的加密验证,形成共识后才能记入账簿,而任何交易者虽可检查整个交易记录,但无法随意篡改数据或操纵交易。

第四,区块链技术的安全性强。由于整个区块链系统采用分布式数据存储技术,让每个参与节点都可以获得一份完整的数据库的拷贝,因此,任意区块上某一节点的损坏或者失去都不会影响整个系统的运作,这就使得区块链本身变得相对安全。

此外,在区块链技术中,记录数据的区块是按时间顺序生成的,又称时间戳。每一个时间戳会将前一个时间戳也纳入其随机哈希值中,这样的过程不断重复,依次相连,因而也使得任何交易都会拥有完整的证据链和可信任的追溯环节。

由此可见,区块链技术本质上可以被认为是一个“分布式公共账簿”,但它又完全不同于传统形式的簿记系统,即所有交易的数据记录、数据存储的工作均不是由中心化的第三方机构来完成,而完全是由区块节点参与者共同负责核查、记录和维护。区块链技术也并不是一种单一的全新技术,而是包括哈希算法、非对称加密法等在内的多种现有技术的综合体。这些技术与数据库巧妙地组合在一起,使交易者之间形成了一种通过点对点的记账、数据传输、认证或是合约,而无需依赖第三方机构背书来达成信用共识。对于每一个参与者而言,既是分布式账簿的记录者和维护者,也是使用者和监督者。任何参与者都可采用相同的技术标准添加自己的信息,但只有在系统达成共识的情况下,账簿才允许被更新。信息一旦经过验证被写入区块链中,就会永

久存储。任何参与者要想篡改数据,必须控制超过半数以上的系统节点。因此,区块链技术保证了交易数据库的完整性、连续性和一致性。正是基于上述的技术优势,区块链能够对网络节点交易实行身份识别和个人征信,实现互联网价值交换,故被《经济学家》杂志称之为“信任的机器”。

2 区块链技术在金融领域的应用

尽管目前互联网技术早已应用到金融业,出现了“互联网+金融”的新模式,但这一模式依然没有颠覆传统的金融服务模式,而区块链的应用将对未来金融业的业务拓展与商业模式产生深刻影响,使金融服务越来越具有大众化和生活化。目前,区块链技术已开始被应用至银行业、证券业、保险业等传统金融领域的主要金融服务业务上(见表2),正在从理论探讨走向实践应用。

表2 区块链在三大金融行业的应用场景

金融行业	主要应用场景	代表应用
银行业	金融交易(点对点交易); 跨境支付;确权与登记;智能合约管理等	R3CEV
证券业	证券发行;股权交易;交易所清算系统	Overstock、Nasdaq Linq
保险业	互助保险;保险定价	Edgelogic

资料来源:梅兰妮·斯万(2015)

2.1 金融交易

日常的金融交易一般都需要通过商业银行或第三方支付机构完成支付结算,这不仅需要金融机构投入大量的人力资源成本,而且交易者还将面临难以预测的操作风险。随着区块链技术在金融领域的应用,使原先的金融交易可以不再需要依赖中心化的金融机构,而能直接实现交易者之间的点对点交易。所有相关的交易操作则都由计算机的算法程序驱动完成。此时交易者账户在区块链中转变成了“代码”,“代码”在区块内以及区块与区块之间使用;密码变成相互配对的公钥和私钥,并通过区块链设计好的算法验证后成为交易的“通行证”。利用区块链技术的点对点交易能够自动建立信任,完成交易结算,既降低了交易的成本,同时又增强了交易的安全性。

2.2 跨境支付

传统的跨境交易支付一般都必须借助可以信赖的第三方机构或系统完成。例如,目前的跨境支付业务是通过 SWIFT 系统完成,不仅需要支付较高的手续费,而且跨境交易的处理时间过长,在途资金占用量过大。可见,成本和效率成为当前跨境支付结算的瓶颈所在。区块链技术使用后,不仅将会省去所有的中间环节费用,实现“点对点”的跨境支付结算,而且还可以全天候支付、实时到账,既降低了交易成本,同时又提升了支付结算服务的效率与便捷性。此外,从安全性上讲,由于区块链技术采用的是分布式支付,而非传统的集中式支付,故用户只需将付款金额直接发送至商家,而不用提供自己的私人银行账户信息,从而增强了网络交易环境的安全性。

2.3 确权与登记

区块链的分布式账簿对股票、债券与其他金融资产的登记、质押等业务的开展将产生深远影响。与经由中心化的中央登记机构进行资产确认、登记和保管的传统方式不同,区块链的去中心化、分布式记账及存储技术不仅能够以全新的方式记录、管理和保存这些数据,使其无法被篡改,而且还能提高交易信息的透明度和可靠性,降低交易成本。此外,作为可信赖的数据库,区块链技术还可用于存储反洗钱客户身份资料及其交易记录,以及对股权等合约或财产的真实性验证及转移业务。

2.4 智能合约

应用区块链技术可将受条件约束的契约型交易转化成“智能合约”,通过将操作规则或协议代码化,使其能够在满足规定条件下自动执行并完成价值转移,从而既有助于实现更便捷、精准高效的金融服务,同时又极大地降低了系统性风险。例如,在网络借贷业务中,金融机构可借助“智能合约”方式开展资产抵押贷款业务,通过预先设计的大数据分析程序自动处理及执行借款合同条款,从而有效减少借贷双方可能发生的争执与矛盾。再譬如,中央银行也可依靠智能合约方式精准实施产业政策,确保发行的数字货币只有在进入特定行业时才允许被支付。

2.5 证券发行与交易

在证券领域,无论是 IPO 发行还是证券交易,都需要有第三方机构的参与,并且证券的发行申请、审批以及市场交易的流程过长,成本较高。应用区

块链技术后,上市机构及投资者均可在去中心化的平台上自主完成 IPO、自由交易,并且可以全天候 24 小时不中断交易。不仅如此,交易双方还能借助智能合约直接实现自动配对,并通过分布式账簿系统,自动实现清算和结算。这不仅大幅降低了资金成本,而且又极大提高了交易效率,同时还能减少人工操作风险。目前,区块链技术已被应用在股权交易领域,其中最典型的案例便是 2015 年 10 月美国纳斯达克推出的专门服务私人股权市场的 Linq 平台。该平台是由世界知名区块链企业(Chain.com)参与搭建的。纳斯达克通过区块链平台于同年 12 月 30 日完成了首个证券交易。纳斯达克表示,通过应用去中心化的区块链分布式账簿证明了股权交易的可行性,而不再需要任何第三方中介或者清算所。而且借助区块链技术股权交易的结算时间从标准的 3 天大幅缩短至 10 分钟,从而大幅减少了结算风险。

2.6 互助保险

传统的保险业务通常是由保险机构全面负责资金归集、投资、理赔,这也导致了保险机构日常的运营和管理成本较高。但是,应用区块链技术,能够实现点对点的互助保险。这样的保险模式能够在发生保险理赔时,让参与者直接将资金支付给参与互助保险的病患者,而不需要借助任何保险中介机构。保险资金的归集和分配也变得公开透明,管理成本也大幅下降。同时,还可便于参与者将互助保险信息发布至公开网络。

3 以“区块链+保险”为突破口,进一步提升上海国际金融中心功能

与其他兄弟省市相比,上海的区块链技术发展起步较晚,推进力度也显不足。如果上海在区块链研究及其创新应用上毫无建树、无所作为,则将严重削弱上海国际金融中心的金融服务功能及其全球影响力。为此,上海应依托金融人才、资源集聚的比较优势,将区块链发展纳入顶层设计,积极谋划加快推动上海的区块链发展。鉴于上海的保险业发展起步早,体制机制相对健全,且风险容易控制,故应以推动区块链技术在保险业的创新应用为突破口,发挥保险科技在提升上海国际金融中心服务功能中的重要作用。

3.1 区块链技术对提升保险业的金融服务功能将发挥越来越重要的作用

尽管目前互联网技术已经应用到保险业,出现

了“互联网+保险”的新模式,但这一模式依然没有颠覆传统的保险服务模式,而区块链的应用将对未来保险业的业务拓展与商业模式产生深刻影响,使保险服务越来越具有大众化和生活化。

首先,区块链技术将推动保险业务的创新发展,进一步提升金融保险的服务功能。区块链技术的出现将会开创相互保险的新时代。区块链与相互保险的结合并不是传统意义上的相互保险互联网化,而是针对传统保险商业模式的“痛点”,不仅利用区块链技术重构信任基础,破解互联网相互保险的信任难题;更重要的是还能够利用区块链与大数据等技术的结合,尤其是利用“分布式”、“去中心化”等区块链技术构建一个更加公平、透明、安全和高效的互助机制,为投保者提供更精准的保险服务。同时,在区块链技术给传统保险业带来创新与变革的环境下,保险机构也面临角色转换问题,从保险营销逐渐转变为专业咨询和相互资金管理,这将有助于降低公司所承担的业务风险。

其次,在创新保险商业模式方面,区块链的分布式数据库,实现了基于全网共识机制的跨区域的信息和价值交流,不仅能够打破信息不对称对保险业务区域拓展的阻碍,而且还能够满足个性化、定制化、差异化和碎片化的保险服务需求,推动互联网保险产品的创新发展。

再者,区块链技术还可实现金融领域的信息流与资金流的实时对接,这将彻底改变现有众多商业模式,甚至完全颠覆整个金融业态。未来可能会出现智能型平台互助保险公司,即由平台提供结算系统,按照互助保险的基本规则,搭建一个交互系统,投保者可以根据自身的基本情况和风险偏好,发起或参与一个“互助团体”,一旦有人出险,系统会根据实际情况进行分摊和结算。这一平台机制的最大特点是不再依赖一个第三方的存在,完全由智能型系统自动完成,它会赋予每一个参保者以“金融个体”属性,形成各自独立的金融节点形态。

3.2 把握发展机遇加快推动区块链技术的应用

由于区块链技术在金融领域的应用能够兼顾效率、安全及公平,这是传统金融难以同时实现的目标,因此,区块链技术可以成为助推上海国际金融中心建设实现从“量变”走向“质变”的重要手段。借助区块链技术,上海不仅可以提升金融中心的规模、

能级与功能,缩小与纽约、伦敦、东京、新加坡及香港等全球五大金融中心城市的差距,而且还能在某些金融领域掌握“话语权”、提升全球影响力。当前,上海的区块链发展仍处在起步阶段,但未来发展潜力巨大。2016年10月,中国金融信息中心、上海市互联网金融行业协会及上海金融业联合会携手业内金融机构共同发起成立了“陆家嘴区块链金融发展联盟”,翌年2月中国区块链应用研究中心又落户上海。上海的区块链发展迎来了新的历史机遇。为此,“十三五”时期上海应把握时机,充分利用金融要素市场齐全、金融人才资源集聚的比较优势,加快推动区块链技术的研究与应用。

3.2.1 设立金融科技办公室,统筹推进区块链技术的研究及其在金融领域的应用

区块链技术的应用是一项复杂的系统工程,需要跨行业的通力协作和统筹实施,因而离不开政府的顶层设计。政府不仅应高度重视区块链对重构金融服务业底层技术的作用,将其纳入金融信息技术发展的总体规划,加快推动区块链技术的发展和创新发展;而且还要为“区块链型金融服务”的发展营造环境,留出空间,提供支持。为此,建议上海市政府专门设立金融科技办公室,负责制定与实施上海加快区块链技术的创新研究及其应用的规划与策略。同时,通过与央行今年刚成立的金融科技委员会对接,推动国家金融科技战略的落地实施。

3.2.2 推进区块链技术公司与金融机构的合作,探索形成统一的行业技术标准

目前,区块链行业发展处于各自为战状态,尚未形成统一的行业技术标准,导致可能存在多种区块链应用架构和标准并存的局面,这不仅将直接影响区块链技术在金融领域的应用,而且很可能造成区块链市场发展混乱和无序竞争,甚至引发危机。为此,上海市政府应在积极支持区块链技术创新发展的同时,充分发挥陆家嘴区块链金融发展联盟在整合和协调行业内外的力量和资源中的作用,大力推进区块链技术公司与金融机构的合作,共同参与制定区块链技术在金融服务业中使用的行业技术标准和协议,夯实区块链技术的应用基础。

3.2.3 依托上海保险交易所组建的小型联盟链,加快金融保险交易模式的创新发展

由于区块链技术的“去中心化”与传统金融系统呈现的“中心化”特征存在明显的冲突,因而在目

前的金融体系下,“去中心化”是不现实的,多中心的分布式体系更适合中国金融发展现状。去年3月由上海保险交易所联合业内9家保险机构发起成立的小型联盟链,采用的是多中心的分布式体系。其中,9家保险机构成为区块链中的各个节点,平等且都能发挥交易及验证的重要作用,而上海保险交易所作为管理节点。借助这一联盟链平台,上海保险机构可尝试引入智能合约技术,将保费、佣金、理赔分成等信息上链,通过设立附加限制条件实现自动履行合约功能,以达到保险交易的低成本、高效率与安全性。

3.2.4 改变现有的监管理念和方式,探索金融科技监管的创新模式

区块链技术的创新发展及其应用不仅受到现行的法律制度的制约,而且更面临传统监管模式的挑战。一方面,区块链技术在金融领域的应用需要对现行的法律条例、规章制度与业务规则进行修正。鉴于目前金融资产是否可以在区块链上登记、发行和交易等在现行法律制度内并未有明确规定,故增加了区块链技术在金融领域应用的难度。另一方面,中国传统的分业监管模式赋予各类监管主体各

自依法行使监管职能以及特定的操作特权,也不利于对区块链技术跨界创新应用的风险监管。为此,建议上海的区块链企业、金融机构与监管部门应加强相互间的沟通与合作,确保信息技术与金融业务、监管法规之间的协调发展。此外,上海还应尝试将区块链技术应用用于自贸试验区的自由贸易账户系统,依靠智能合约管理技术,提升对资金流向监控与金融风险防范的功效。

参考文献

- [1] James Schneider, et al., Blockchain: Putting Theory into Practice[C]//The Goldman Sachs Group, Inc., EQUITY RESEARCH, 2016.
- [2] 蒋润祥,魏长江.区块链的应用进展与价值探讨[J].甘肃金融,2016(2).
- [3] 麦肯锡大中华区金融机构咨询团队.区块链——银行业游戏规则的颠覆者[M].中国银行业白皮书,2016.
- [4] 梅兰妮·斯万.区块链:新经济蓝图及导读[M].新星出版社,2015.
- [5] 张苑.区块链技术对我国金融业发展的影响研究[J].国际金融,2016(5).

Main Features and Application Scenario of Blockchain Technology ——On how to further Enhance the Function of Shanghai International Financial Center

SUN Lixing

(Institute of World Economy, Shanghai Academy of Social Sciences, Shanghai200020, China)

Abstract: The so-called blockchain can be understood as a universal distributed ledgers technology. Each digital trade will be recorded in the "block", which be linked each other to form a blockchain. Anyone can access to transaction records, but nobody can easily control or tamper with the data. Its key feature is "Decentralized". Based on the above technical advantages, the blockchain can realize identity identification of network node transaction and personal credit at a very low cost, thereby which greatly improves the operational efficiency of the financial system, and has a profound impact on restructuring the underlying architecture of the financial industry as well. The innovative application of blockchain technology in the insurance industry can be used as a booster to further enhance the function of Shanghai international financial center.

Key words: blockchain; main features; application scenario; Shanghai international financial center