金融区块链研究报告

CAICT 中国信通院

腾讯研究院
Tencent
Research Institute

二〇一八年七月

CAICT 中国信通院

项目组成员

研究团队

谢智刚　中国信通院产业与规划研究所大数据与数字经济研究部主任

王　强　中国信通院产业与规划研究所大数据与数字经济研究部工程师

李　曼　中国信通院产业与规划研究所大数据与数字经济研究部工程师

姜　莹　中国信通院产业与规划研究所大数据与数字经济研究部工程师

巴洁如　腾讯研究院高级研究员

顾问团队

徐志发　中国信通院产业与规划研究所副所长

杜晓宇　腾讯研究院金融研究中心副主任

目 录

第一章 区块链的技术趋势及意义 03

1.1 区块链与比特币 03
1.2 区块链适用场景 03
1.3 区块链技术发展趋势 04

第二章 区块链在金融领域应用的整体分析 05

2.1 区块链在金融领域应用的整体形势 05
2.2 区块链应用与金融领域的结合点 06
2.3 区块链对金融体系产生的潜在影响 07

第三章 数字货币 08

3.1 数字货币研究历程 08
3.2 加密数字代币研究现状 09
3.2.1 加密数字代币 09
3.2.1.1 加密数字代币特点及应用情况 09
3.2.1.2 加密数字代币风险 09
3.2.2 首次代币发行（ICO） 10
3.2.2.1 ICO 特点 10
3.2.2.2 ICO 风险 10
3.2.3 加密数字代币及 ICO 监管 12
3.3 法定数字货币研究现状 13
3.3.1 法定数字货币研究进展 13
3.3.2 法定数字货币面临的挑战 14
3.3.3 区块链技术与法定数字货币 15

第四章 支付清算 16

4.1 跨境支付业务与区块链 16
4.1.1 跨境支付业务发展现状 16
4.1.2 区块链在跨境支付领域的优势 17
4.1.3 应用探索 18

CAICT 中国信通院

4.2 大额支付系统与区块链 19
4.2.1 大额支付系统发展现状 19
4.2.2 区块链在大额支付系统中的应用优势 20
4.2.3 应用探索 20
4.3 挑战与思考 22

第五章 供应链金融 24

5.1 供应链金融的发展历程 24
5.2 传统供应链金融的行业痛点 25
5.3 区块链在供应链金融领域的应用场景 25
5.4 区块链在供应链金融领域的应用现状 26
5.5 挑战与思考 28

第六章 证券交易 29

6.1 证券行业的发展历程 29
6.2 传统证券的行业痛点 30
6.3 区块链在证券领域的应用场景 31
6.3.1 私募证券的电子化 31
6.3.2 公募证券发行交易平台 32
6.4 挑战与思考 33

第七章 保险 35

7.1 保险的发展历程 35
7.2 区块链在保险业的应用场景 36
7.2.1 优化传统保险流程 36
7.2.2 助力相互保险发展 36
7.3 区块链在保险业的应用现状 37
7.4 挑战与思考 38

第八章 征信 39

8.1 用户征信的发展历程 39
8.2 传统征信的行业痛点 40
8.3 区块链在征信领域的应用场景 40

CAICT 中国信通院

8.4 区块链在征信领域的应用现状 42
8.5 挑战与思考 43

第九章 区块链金融应用的挑战与监管 44

9.1 金融领域区块链应用所面临的挑战 44
9.1.1 商业挑战 44
9.1.2 技术挑战 44
9.1.3 金融设计挑战 45
9.1.4 风险管理挑战 45
9.2 金融领域区块链应用整体监管状况 46

第十章 结论与建议 48

CAICT 中国信通院

核心观点

区块链将对金融体系发挥积极作用

基于区块链在金融资产权益证明发放与流通中的应用，区块链将通过“一升一降三创新”，对货币发行流通、金融工具、金融市场、金融中介以及制度与调控机制等金融体系要素带来潜在的积极影响。

区块链将对法定数字货币的发行和流通机制的建立产生深远影响

加密数字代币不属于信用货币体系，无法有效履行货币基本职能，而法定数字货币是信用货币体系的一部分，将履行货币交易媒介、计价单位和价值贮藏的基本职能。区块链可以作为法定数字货币的底层技术之一，是一项可选技术。从技术的成熟度看，未来法定数字货币也有采用集中化技术的可能性。区块链对将对法定数字货币的发行和流通机制的建立产生深远影响。

区块链在跨境支付及大额支付领域有一定优势

基于区块链的跨境支付模式拥有效率更高、成本更低、流动性更强、权利更平等等优势。在大额支付领域，区块链应用主要从理论层面探讨其对大额支付系统带来的效率、透明度、弹性及稳健性等潜在效益。

供应链金融是较为适合区块链的场景之一

在供应链金融流程中，供应商、核心企业、银行、金融机构等多方并存，这类多主体、非高频交易是较为适合区块链技术应用的场景。基于区块链技术，可实现应收账款、票据、仓单等资产数字化，并且留下数据存证，降低票据作假、重复质押等风险，缓解信息不对称的问题，并基于智能合约属性使供应链金融业务顺利开展。

区块链在证券交易应用领域更多尚在概念阶段

证券领域的区块链应用主要集中于私募证券的电子化与公募证券的发行交易，大多处在概念验证阶段。区块链可以在不改变私募证券流通规则的基础上，替代纸质文件作为证券资产的自治电子化载体，实现私募证券的登记和流通。公募证券方面，相关方在清结算环节存在多方对账等效率问题，区块链可以提供一种证券清结算的解决方案。

区块链在保险领域的应用更加强调公开透明特点

保险领域中的区块链应用特点鲜明。针对保险业理赔效率低、行业信息无法共享等问题，基于区块链的智能合约特性可以用来优化保险业务流程。针对中心化的相互保险存在运作不透明、资金流向不透明的问题，区块链为构建非中心化的信任模式提供了一种新的可能，促进保险平台提升内部监管和外部监管的透明度。

区块链技术有助于搭建征信数据共享交易平台

区块链可在征信的数据共享交易领域着重发力，面向征信相关各行各业的数据共享交易，构建基于区块链技术的联盟链，搭建征信数据共享交易平台，实现数据共享，促进参与交易方风险和成本最小化。

区块链金融应用面临挑战与监管

金融领域区块链应用目前仍处于早期探索阶段，在区块链成为金融领域实际应用的解决方案之前，仍有商业、技术、风险管理等多维度的挑战，各国政府也积极调整监管策略，摸索出适应本国发展的监管方式。

结论

区块链技术在金融领域的应用，只是提供了一种新角度下的、适用于资产权益证明的发放与流通环节的新型解决方案，目前来看并未对金融领域生产关系产生颠覆性的影响。在区块链应用发展过程中，必须要探索包容的审慎监管，“币”应用与“链”应用需要区分对待，对于“币”应用要严防金融风险，对于“链”应用要在合规合法的框架内挖掘区块链的潜力。

鉴于区块链技术与金融市场的结合现阶段还存在较多不确定性，市场参与者未来应首先扎实推进区块链技术应用型研究，根据实际情况，加快相关场景的应用落地，通过持续、深入的实践验证其应用中的利与弊。其次，着力促进产业主体之间的协调与合作，探索搭建政府与市场之间的政策传导和信息反馈桥梁，通过行业协会、联盟等平台，推动产业链上下游主体联动与合作，加强与国外产业主体的交流，提升国际标准制定的话语权。最后，密切关注新兴技术对金融监管体系带来的挑战，区块链在金融领域的应用应遵循金融业的核心原则与规则，应结合相关市场实践，深入研究新兴技术对现有金融市场结构、风险管理模式、监管及法律框架产生的影响，并适时为技术应用提供必要的法律基础，明确现有法律和监管规则的适用性问题。

第一章 区块链的技术趋势及意义

当前，区块链的热潮涌入各行各业，成为当下最受瞩目的信息技术之一，“去中心化”、“不可篡改”、“公开透明”等区块链特性成为人们的谈资，大数据、云计算、人工智能等似乎也望尘莫及。在热潮之下，从技术起源、技术适用场景到技术发展趋势开展区块链研究，冷静分析区块链技术实质，明晰区块链可行的应用点，对当前的区块链发展有重要的意义。

1.1 区块链与比特币

区块链技术是随着比特币的诞生而出现的，毫无疑问，区块链源自比特币。不过换一个视角，区块链是比特币的核心底层技术，比特币的诸多特性无不源于区块链，因此比特币是构建在区块链上的一种应用，也是当前基于区块链的创新应用中最为成熟、最为成功的应用。

抛开比特币来看，区块链本质是一种特殊的分布式账本技术。分布式账本是由网络节点维护、验证、加密以及审核后的共识记录。区块链是一种实现分布式账本的方法，它在分布式账本的基础上还包含了储存信息的“区块”，并通过在原有链条上产生新的区块来验证交易的有效性。基于这种技术架构，区块链以去中心化的方式集体维护一个可信数据库，提供了一种在不可信环境中进行信息与价值传递交换的机制，具有公开透明、安全可靠、开放共识的特点。

尽管当下区块链概念非常火爆，但区块链并非是一种颠覆式技术，而是多种技术的集成式创新。区块链是分布式网络、数据加密、共识机制、智能合约等技术的一种融合，这些技术早已出现。诞生在 2009 年的区块链技术，是将各项相关技术要素在分布式网络技术上进行集成得以实现的，带来了全新的分布式生产关系协作的可能性，用户节点在这种分布式生产关系协作网络中重新被定义，这应当是区块链最大创新所在。

1.2 区块链适用场景

区块链应用的显著优势在于优化业务流程、降低运营成本、提升协同效率，这个优势已经在金融服务、物联网、公共服务、社会公益和供应链管理等领域逐步体现出来。整体而言，区块链与行业的融合应用仍处于探索尝试阶段，落地效果突出、不可替代性强的区块链应用案例仍然较少。

值得注意的是，区块链技术并非一项“普适性”技术，并不是所有领域都适合融入区块链进行“改造”。区块链的适用场景与其核心特点密切相关，需要找准应用领域与区块链的切入点。作为一种分布式账本技术，区块链最具创新性的特点就是用户节点共同记账机制，在多用户节点网络中，安全地共享网络中产生数据的同时，还可保证用户节点平权，每个用户节点可拥有全网的共享数据。根据网络中是否有中心节点，以及用户节点间平权关系，区块链的适用场景可归纳为三类。

应用场景一：无中心，节点平权。区块链适用于无中心、节点地位平等的应用场景。当前完全无中心的场景较少，比特币为代表的加密数字货币体系是依托区块链创造出来的典型的无中心应用场景。

应用场景二：多中心，中心节点平权。区块链适用于多中心、中心节点地位平等的应用场景。涉及多节点协作、交易的场景基本均为多中心，是最适宜使用区块链的场景，如供应链管理等。

应用场景三：中心化成本显著过高。区块链适用于可去中心、节点分摊权利的应用场景。当前大部分应用场景存在中心节点，中介信任成本较高，若可去中心或分散为多个中心，也适合使用区块链，如投票、资产公证等。

1.3 区块链技术发展趋势

区块链技术尚未成熟，基础设施不完善的状况致使应用受到局限，整体应用还处于一个非常早期的阶段。如共识算法等区块链的核心技术尚存在优化和完善的空间，区块链处理效率尚难以达到现实中一些高频度应用环境的要求，目前不能满足高频次和复杂的商用计算。此外，其他配套的基础设施如存储、隐私保护等，也并没有表现出比传统中心化解决方案更优越的性能。总体而言，区块链技术成熟度暂时还无法支撑大规模商用。

从区块链的技术组成来看，其可扩展性、去中心化、安全性这三个特点难以在同一时间取得优化、最佳，必须以牺牲其中若干个因素去换取在另外一个领域上的提升。基于金融等商用场景对实时、高并发、高吞吐、安全等维度的实际需求，去中心化在一定程度上会做出牺牲，可扩展性与安全性将是区块链应用备受关注的关键性能指标。

在区块链技术发展趋势方面，我们认为：

（1）弱中心化的联盟链会是企业级区块链应用的主流方向。与公有链不同，联盟链只允许预设的节点进行记账，加入的节点都需要经过授权，这种区块链技术实质上是在确保安全和效率的基础上进行的“部分去中心化”或“多中心化”的妥协。企业级应用更关注区块链的管控、监管合规、性能、安全等因素，因此联盟链相对强管理的部署模式，更适合企业级应用落地。

（2）可扩展性将是驱动区块链技术持续演进的关键因素。要实现规模化的企业级应用，区块链技术需要克服信息查询验证慢、单节点存储空间小、并发处理效率低等问题，未来，共识算法、服务分片、处理方式、组织形式等技术环节都将成为区块链技术攻克的重点。专注于扩展区块链主链应用范围与创新空间的侧链技术将迎来较大发展。

（3）安全性将是金融等商业场景的区块链应用基础。从数学原理上讲，区块链技术是较为完美的，具有公开透明、难以篡改、可靠加密、防 DDoS 攻击等优点。但从工程角度来看，它的安全性仍然受到基础设施、系统设计、操作管理、隐私保护和技术更新迭代等多方面制约。未来需要从技术和管理上全局考虑，加强基础研究和整体防护，才能确保应用安全。

第二章 区块链在金融领域应用的整体分析

技术驱动金融服务产业转型升级的作用日趋明显，以技术创新引领的金融服务模式变革趋势仍将持续。如何将前沿技术与各类金融服务场景深度整合，使技术创新发挥最大价值，已成为全球金融科技产业的重要研究课题。业界普遍认为，区块链技术有望进一步提升金融交易透明度、强化系统操作弹性、实现流程自动化，进而对金融业务的记录保存、会计核算和支付结算方式产生影响。研究分析区块链技术在金融领域应用的整体情况与典型特征，有助于客观判断其发展现状、趋势及潜在影响。

2.1 区块链在金融领域应用的整体形势

据七麦数据报告显示[1]，在我国全部区块链创业项目中，金融类占比最高，达到 42.72%，企业服务类占比达 39.18%，这两类项目共计占比高达 81.44%。在金融领域内，区块链技术在加密代币、支付清算、供应链金融、证券、保险等细分领域得到落地应用。

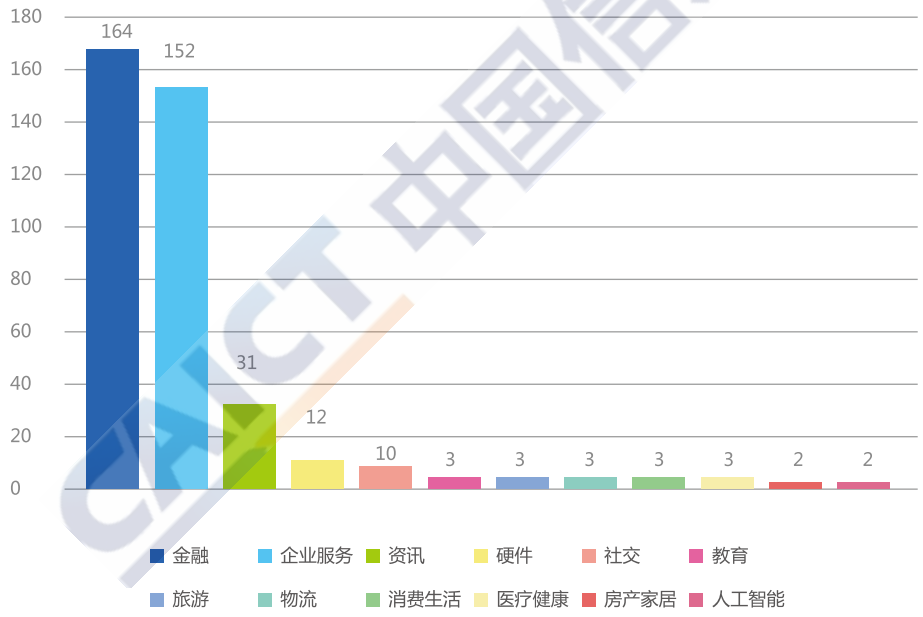

图 1 中国区块链企业类型详情（截至 2018 年 3 月 30 日）

数据来源：七麦研究院

[1] 七麦研究院：《2018 中国区块链 App 项目热点分析报告》.

2.2 区块链应用与金融领域的结合点

在金融市场中流通的资金以及金融工具，都与线下实体资产有一定的对应关系，是实体资产的权益。围绕金融资产权益，金融业务主要有三个关键环节。

图 2 金融资产权益的三个关键环节

第一个环节，资产权益的评估。这个环节需要金融中介来对线下实体资产确定其价值，从而明确资产权益的真实价值。第二个环节，资产权益证明的发放。确定了资产相应的价值之后，会给相应的金融参与者一个金融资产权益的证明，比如股权证明书均由中介发放管理。第三个环节，资产权益证明的流通。金融参与者持有资产权益证明，能够在金融过程中寻找其他参与者，对接他们的融资需求，一般的金融工具都是基于中介的流通化方式。

从金融资产权益的这三个环节切入，进一步分析区块链能发挥的作用。在第一个环节中，区块链目前难以做到线上数据与线下实体资产的完全真实匹配，暂时不能够代替金融中介去评估一个实体金融资产价值。第二个环节主要针对资产权益证明本身文件实现防伪，区块链可以做到电子权益证明去中心化发放，并且保证不可篡改。第三个环节反映金融工具的流动性，区块链可实现资产权益证明的点对点流通，并可以再切分，有助于提升资产流动性。

综合这三个环节来看，现阶段区块链可以用于资产权益证明的发放管理和流通环节，但是难以参与到线下的权益评估。金融领域中的中介其实有着非常重要作用，可以提供评估、风控、增值等服务。在历史上，金融中介的出现和存在是为了解决金融交易中的信息不对称、匹配效率和成本、风险控制等问题，金融中介是否会随着技术发展而消失，需要考虑新技术及相关制度是否能解决上述基本问题[2]。

回到区块链本身技术架构来说，区块链其实就是能够对链内所产生的数据进行有效管理和追踪，对于链外或者是线下资产，或者是对于链外能够导入到链内的数据，本身并不能够进行有效管理，现阶段无法验证真实性及价值。在资产权益证明的发放管理与流通环节，区块链可充分发挥自身低成本建立连接、点对点流通的特性，有助于降低金融业务复杂度，增强金融工具的流动性，提升金融业务效率。

[2] 长铗，韩锋，等．区块链：从数字货币到信用社会 [M]. 中信出版社．2016:191.

2.3 区块链对金融体系产生的潜在影响

分析区块链在金融领域的应用，应先从金融体系宏观层面考虑。从现行金融体系架构着手，分析区块链对金融体系每个构成要素的具体影响，研判区块链在金融领域应用的整体趋势。

金融体系包含货币发行流通、金融工具、金融市场、金融中介、制度与调控机制等构成要素。从这几个核心构成要素来看，基于区块链在金融资产权益证明发放与流通中的应用，区块链将通过“一升一降三创新”，为金融体系带来潜在积极的影响。

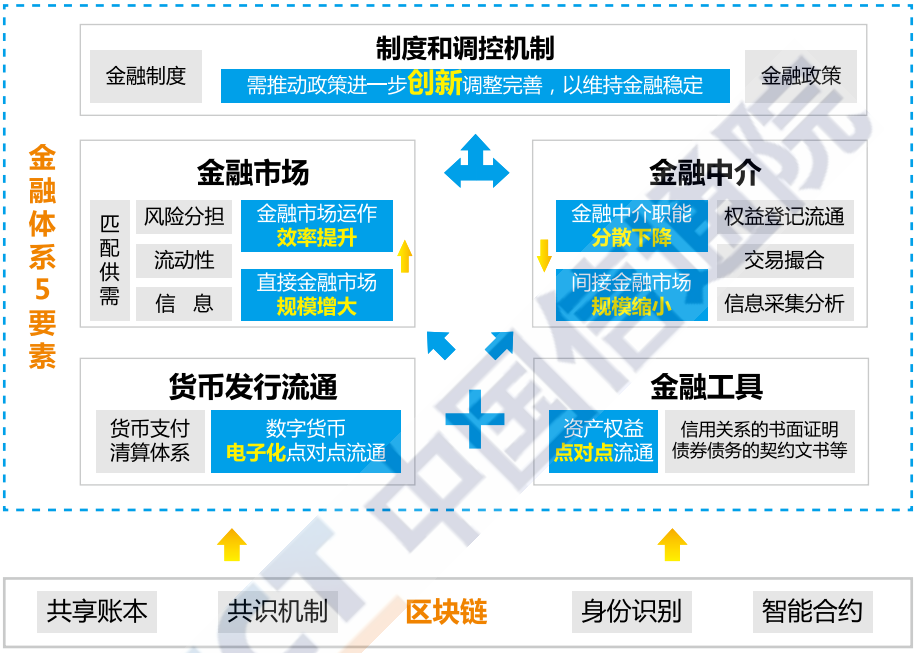

图 3 区块链为金融体系带来潜在的积极影响

从实际应用情况来看，区块链应用最早、且应用最热的金融范畴就是加密数字代币。以比特币为代表的加密数字代币基于区块链创新地实现了资产权益的远程点对点流通，逐步激发人们对于区块链在货币发行流通中应用的探讨，这是第一个“创新”。金融工具，也可以称为金融资产，是作为储蓄者与借款者进行资金转移的重要手段，区块链可创新地实现金融资产权益的高效点对点登记流通，这是第二个“创新”。

基于区块链对加密数字代币以及金融资产权益实现电子化、点对点流通的创新应用，能增强金融过程中的投资者与借款者之间的点对点关联，继而金融市场的运作效率会整体提升，使得直接金融市场的规模增大，即“一升”。在这个过程中可能带来金融中介职能的下降、聚焦和转变，今后金融中介职能主要会针对于实现投资者与借款者的交易撮合、信息采集分析等最重要的功能，即“一降”。

区块链对金融市场与金融中介带来一升一降的影响，继而可能推动金融制度与调控机制的创新调整与完善，从而在这一大机遇的背景下维持货币稳定与金融稳定，即第三“创新”。

第三章 数字货币

近年来，随着比特币为代表的一系列加密数字代币价格不断高涨，区块链“造币”的浪潮愈演愈烈。与此同时，世界各国货币当局纷纷关注法定数字货币的实现技术并进行积极探索，数字货币成为区块链在金融领域应用的重要阵地。

广义的数字货币，从发行机制上可分为两类：不以国家信用为背书发行的加密数字代币与以国家信用为背书发行的法定数字货币。厘清加密数字代币、法定数字货币等数字货币概念的本质，才能找准区块链技术可能在现有货币发行流通机制发挥的作用。

3.1 数字货币研究历程

国际社会对数字货币的探索研究已有三十余年时间。1982 年，“数字货币之父”David Chaum 在美密会议上发表论文提出利用盲签名构建一个具备匿名性、不可追踪性的电子货币系统，该论文的观点被视为最早的数字货币理论。1990 年，David Chaum 成立了 DigiCash 公司，并研发了 E-Cash，其后的群盲签名、公平交易、离线交易、货币的可分割性等研究都是在这个基础上展开的。1997 年出现的 HashCash 使用了工作量证明系统，这后来成为比特币核心要素之一。同年，Haber 和 Stornetta 提出用时间戳保证数字文件安全。1998 年出现的 B-money 则强调点对点交易和交易记录的不可更改。这些早期探索为数字货币的后续研究打下了坚实的基础。

真正让数字货币概念盛行起来的是 2008 年出现的比特币。2008 年 10 月，中本聪发表论文《比特币：一种点对点的电子现金系统》，阐述了比特币点对点、去中心化的核心思想。2009 年 1 月，比特币正式诞生。比特币以区块链技术较好地解决了去中心化、去信任问题，基于算法达成共识稳定运行了 10 年，在世界范围内受到追捧，并掀起了区块链“造币”浪潮。

部分国家央行与大型金融机构在“造币”浪潮中研究基于区块链的法定数字货币，探索法定数字货币在货币发行、流通体系中的角色，如英国央行曾提出的 RSCoin。也有金融机构正在研究加密数字代币在金融平台交易和结算中的作用，如瑞士信贷银行的“多用途结算货币”、花旗银行的“花旗币”（Citicoin）。

3.2 加密数字代币研究现状

3.2.1 加密数字代币

3.2.1.1 加密数字代币特点及应用情况

以比特币为代表的加密数字代币具有三个典型特点：一是无中央发行机构，算法自动产生数字代币；二是采用区块链实现远程点对点流通；三是供求决定价格，代币本身无内在价值。持续高强度的价格波动，使得比特币等加密数字代币更多被人们视为投机资产持有和交易，而非交易媒介[3]。

据CoinMarketCap数据显示，截至2018年7月20日，全球已有797种数字货币（Coin），市值前三位是比特币、以太币与瑞波币，其中比特币市值约1275亿美元，单价7433美元；全球已有859种代币（Token），市值前三位是Tether、Binance Coin与OmiseGO，其中Tether市值约27亿美元，单价约1美元[4]。

除投资投机需求外，加密数字代币已在部分国家或地区用于经济生活支付领域。比如，日本电子零售商Bic Camera与日本比特币交易所bitFlyer联合推出比特币支付服务，于2017年4月宣布旗下试点商店接受比特币支付，并于7月把接受比特币支付的选择扩展到了其全国各地的店铺[5]。日本Recruit Lifestyle与日本比特币交易所Coincheck达成合作，帮助其“Air Regi移动支付”购物APP接受比特币支付，并于2017年7月宣布Air Regi APP开始提供比特币支付选项，持有比特币的消费者可通过扫描Air Regi APP上的二维码来支付比特币[6]。英国化妆品巨头Lush于2017年7月宣布其线上商城接受加密数字代币支付[7]，旨在为英国线上商城带来更多的国际订单，通过这个全球性的去中心化货币的应用打开与国际市场、供应商，甚至是各国乡村地区慈善组织合作的大门。

3.2.1.2 加密数字代币风险

去中心化的加密数字代币体系，以区块链技术为基础，缺少内在价值及政府信用背书，其价格极易受市场预期影响，波动率极高，市场流动性难以得到保证，存在交易匿名、资金可跨国自由流动以及交易不可逆、防篡改等特征，可能给市场参与者及整个金融体系带来多种风险[8]。

一是洗钱及恐怖主义融资风险。加密数字代币体系中服务提供商和用户均为匿名，模糊的交易链使得不法分子易于掩盖其资金来源和投向，这为洗钱、恐怖融资及逃避制裁提供了便利。国际货币基金组织（IMF）、国际清算银行（BIS）、经合组织（OECD）等国际组织，以及英格兰银行、澳大利亚央行、新加坡金融管理局等监管机构都对加密数字代币相关的洗钱及恐怖主义融资风险表示了高度关注。加密数字代币体系很可能作为逃避资本管控的渠道，非法资金可通过加密数字代币体系实现跨国流动，这给打击洗钱、恐怖主义融资活动带来了挑战。

---

[3] 谢平，石午光．数字加密货币研究：一个文献综述 [J]. 金融研究，2015(01):1-15.
[4] https://coinmarketcap.com/coins/views/all/.
[5] http://www.biccamera.co.jp.e.lj.hp.transer.com/shopguide/campaign/bitcoin/index.html
[6] Rollout of 260,000+ Bitcoin-Accepting Stores in Japan Begins, https://news.bitcoin.com/rollout-of-260000-bitcoin-accepting-stores-in-japan-begins/
[7] https://uk.lush.com/article/doing-our-bitcoin-lush-digital-accepts-cryptocurrency
[8] 王信，任哲．虚拟货币及其监管应对 [J]. 中国金融，2016(17):22-23.

二是金融稳定相关风险。各大国际组织和各国监管机构普遍认为，目前加密数字代币市场价值及交易额较小，且金融机构极少参与，并未对金融稳定造成系统性威胁。IMF 于 2017 年 6 月发布报告，指出随着加密数字代币使用范围和规模的扩大，单个加密数字代币体系风险演变为系统性风险的概率也将提升[9]。此外，加密数字代币体系不具备稳定货币机制的特征，加密数字代币近乎刚性的供给规则可能造成结构性通货紧缩，且加密数字代币体系中没有可以承担最后贷款人角色的公共机构，缺乏最后贷款人为货币稳定提供保障，一旦出现风险事件，加密数字代币兑换商很容易遭到挤兑，对金融稳定造成冲击。

三是消费者权益保护面临的风险。加密数字代币流动性管理难度高，兑换商流动性管理出现问题时，消费者可能无法将加密数字代币兑换为法币。加密数字代币价格出现大幅波动时，持有者很可能遭受资金损失，投资风险极高。加密数字代币体系中的市场参与者几乎不受监管，用户资金安全缺乏保障。由于交易不透明，诈骗者建立虚假的电子商务交易网站，将收集的加密数字代币兑换为任意国家货币而不留任何交易痕迹。不仅如此，去中心化的加密数字代币体系中交易不可逆，且无法律框架明确交易各方之间的权利和义务关系，发生诈骗、盗窃、造假等事件时难以确定哪一方应当为事件负责，消费者权益缺乏保障。

3.2.2 首次代币发行（ICO）

3.2.2.1 ICO 特点

区块链作为比特币等加密数字代币的底层技术，其防篡改、去中心化等特点引发了各行业的研究和探索，从而逐渐出现了一批区块链创新项目，同时从比特币衍生出来的虚拟代币又成为这些项目的重要融资手段。各场景下的区块链项目开始运用区块链生态系统中内生的 ICO 融资方式获得启动和发展资金。

首次代币发行（ICO，Initial Crypto-Token Offering）指的是 ICO 项目方通过出售发行加密代币筹集资金，资金用于项目方启动资金或实现项目由概念设计向现实转化。区块链创业公司不以公司股票或债券为融资工具，而是发行自己的加密代币，通过众筹的方式，交换比特币、以太币等主流数字货币，以达到融资创业目的。

按照加密代币的类型可分为应用代币、权益代币和资产代币三类。其中应用代币赋予投资者参与区块链项目活动的权利；权益代币用于持有区块链应用的股份，享有收益分红、投票权等；资产代币由现实中的真实资产作为支撑[10]。

3.2.2.2 ICO 风险

作为区块链创业企业前期融资的一种方式，ICO 融资方式日渐活跃。据 CB Insights 数据显示，2017 年全球 ICO 融资金额超过 50 亿美元，而同期区块链领域的风险投资（VC）融资规模约为 7.16 亿美元[11]。

[9] https://www.imf.org/en/Publications/Staff-Discussion-Notes/Issues/2017/06/16/Fintech-and-Financial-Services-Initial-Considerations-44985.
[10] 哲 .ICO 国际监管与趋势 [J]. 中国金融 ,2018(05):81-83.
[11] https://www.cbinsights.com/research/report/fintech-trends-q1-2018/

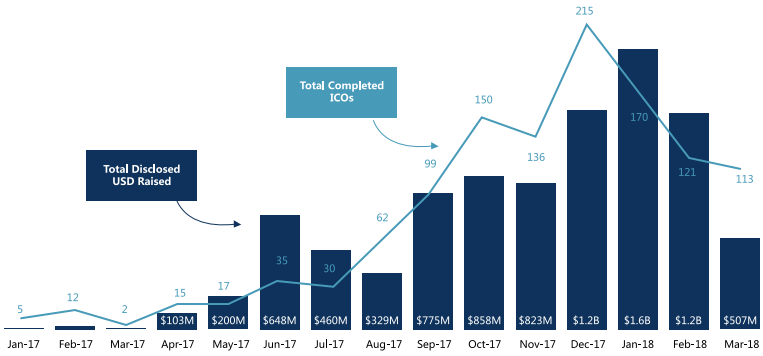

图 4 全球已完成的 ICO 融资规模（2017 年 1 月 -2018 年 3 月）

数据来源：CB Insights

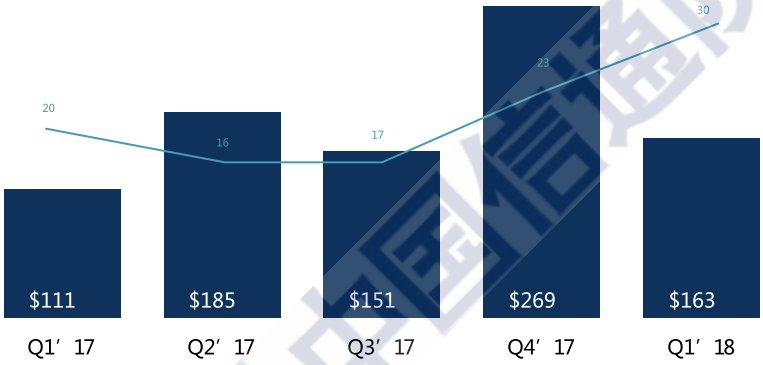

图 5 区块链领域 VC 融资趋势（2017Q1-2018Q1）

数据来源：CB Insights

注：数据不含非金融领域投融资情况

相对于 VC 融资方式，ICO 具有门槛低、退出周期短等特点，但同时这些特点也使得 ICO 项目极具风险。

ICO 投融资门槛低 ,创业者成本极低 ,不受监管 ,而且广泛吸引了风险承担能力较低的普通投资者加入 ICO 大潮。对于创业者来说，寻找 VC 是一个复杂而漫长的过程，企业融资要经过寻找机会、路演、实地调研、评估分析等过程，而 ICO 模式下，创业者只需一份 PPT 或白皮书，营造一些新的概念，即可面向公众筹资，没有任何报备要求和专门的监管，创业者可以有意无意地遗漏那些让投资者能够判断项目合法性的重要信息，成本极低，跑路风险极大。对于投资者来说，VC 方式一般由私募投资基金公司投资，个人很难参与直接投资，而 ICO 模式则拉近了创业者和直接投资者之间的距离，不具备风险承受能力的个人投资者也可以参与投资，受到欺诈的风险极大。

在 VC 模式中，投资者看中的是企业长期发展后的股权分红或 IPO 退出，一般参与企业的重要决策，收益周期一般较长。而 ICO 一般发行的是不具备股权权益的代币，代币具有较强的流动性，在发行后马上就可以在 ICO 交易平台进行交易，投资者通过交易代币获得收益，且公司运营决策也无需投资者参与，投资者只有使用权、退出周期短，代币价值直接影响投资者收益，因此大部分 ICO 投资者看中的不是项目内在价值及远期的收益，一般都持严

重的投机心态。在这种情况下，与事实严重不符的一些项目，为了提高融资成功率，甚至从事内幕交易，形成利益集团，互相支持吹捧，以持续出售代币不断获取资金。

此外，ICO 项目存在较大的法律风险。2017 年 9 月 4 日，国家七部委联合发文[12]，指出 ICO 本质是一种未经批准的非法公开融资的行为，涉嫌非法发售代币票券、非法发行证券以及非法集资等违法犯罪活动。与此同时，区块链领域的相关创业项目也屡屡遭受质疑。但在“9.4 禁令”发布之后，又陆续出现了 IFO（分叉发行）、ITO（通证发行）、IMO（专属设备挖矿）等模式，需引起业界和投资者的高度警惕。

3.2.3 加密数字代币及 ICO 监管

以比特币为代表的加密数字代币的市场火爆程度远远超出了预期，与此同时，加密数字代币及 ICO 市场中出现的风险也给现有监管体系带来了诸多挑战。2017 年以来，针对虚拟货币和 ICO 行为，部分国家或地区的金融监管机构采取了一系列具体措施。

美国证监会（SEC）于 2017 年 7 月发布 DAO 调查报告[13]，认定 DAO 提供和出售的代币属于有价证券，应受联邦证券法调整，对代币的是否是证券的认定，应从交易的经济属性加以判断。自 2018 年 2 月以来，美国参议院、众议院中的多个委员会先后围绕虚拟货币监管[14]、区块链技术应用[15]、加密货币及 ICO 市场[16]、利用区块链技术改善供应链管理[17]等主题，召开四次听证会，整体的态度比较冷静客观，既讨论了区块链浪潮中所裹挟的风险，也对技术应用的潜在效益给予了充分关注。

2017 年 8 月，新加坡金管局（MAS）发布《关于在新加坡数发售数字代币的监管立场》[18]，明确提出，如果数字代币构成《证券及期货法案》（SFA）第 289 章第所规定的产品，则在新加坡发行与销售的数字代币应受到新加坡金管局监管。如果数字代币符合 SFA 中对于证券的定义，除非获得豁免，否则代币发行机构必须在发行之前，向 MAS 提交招股说明书。除非获得豁免，此类代币的发行和中介机构，还应根据 SFA 和《金融顾问法案》的相关要求，取得牌照，并同等适用反洗钱和反恐怖融资领域的相关规定。此外，为此类代币提供二级交易服务的平台，应根据 SFA 相关规定，经 MAS 批准，作为授权交易所或市场经营机构开展业务活动。

2017 年 9 月，香港证券及期货事务监察委员会（证监会）发表有关首次代币发行（ICO）的声明[19]，阐明根据个别 ICO 的事实和情况，所发售或销售的数码代币可能属于《证券及期货条例》所界定的“证券”，并因此受到香港证券法例的规管。虽然在一般 ICO 中发售的数码代币通常被认为具有“虚拟商品”的特点，但某些 ICO 的条款及特点，可能意味着有关数码代币属于“证券”。如 ICO 所涉数码代币符合“证券”定义，需接受香港证监会监管，并取得证券业相关牌照后，方可开展业务。

---

[12] 人民银行等七部门关于防范代币发行融资风险的公告，http://www.gov.cn/xinwen/2017-09/04/content_5222657.htm

[13] Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO, https://www.sec.gov/litigation/investreport/34-81207.pdf

[14] https://www.banking.senate.gov/hearings/virtual-currencies-the-oversight-role-of-the-us-securities-and-exchange-commission-and-the-us-commodity-futures-trading-commission

[15] https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=106862

[16] https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=108012

[17] https://science.house.gov/legislation/hearings/subcommittee-oversight-and-subcommittee-research-and-technology-hearing-0

[18] MAS clarifies regulatory position on the offer of digital tokens in Singapore, http://www.mas.gov.sg/News-and-Publications/Media-Releases/2017/MAS-clarifies-regulatory-position-on-the-offer-of-digital-tokens-in-Singapore.aspx

[19] 證監會發表有關首次代幣發行的聲明，http://www.sfc.hk/edistributionWeb/gateway/TC/news-and-announcements/news/doc?refNo=17PR118

2017 年 4 月，日本《支付服务修正法案》正式生效，增加了“虚拟货币”章节，引入虚拟货币交易机构的强制登记注册制度，明确包括虚拟货币买卖以及与其他虚拟货币交换、提供媒介、经销及代理、管理交易者资金和虚拟货币的行为应纳入监管的核心业务范围，对交易机构提出明确的行为规范，强化交易机构信息与风险提示义务等。同时，虚拟货币交易机构还应履行新修订的《防止犯罪收益转移法案》中规定的反洗钱相关义务。同年 7 月，日本取消了加密数字代币消费税，批准免除代币交易税，使得日本成为了全球最为活跃的加密数字代币交易市场之一。

2018 年 2 月，欧盟三大金融监管机构——欧洲银行业监管局（EBA）、欧洲保险与职业养老金监管局（EIOPA）、欧洲证券与市场监管局（ESMA）联合发布虚拟货币风险提示[20]，指出虚拟货币不具有货币的法定地位，不具备有形资产支持，不受欧盟法律法规监管和保护。虚拟货币风险极高，一般具有较高投机性，因价格急剧波动、信息披露缺失或不完整、缺乏退出保障机制等因素，消费者在购买虚拟货币及与其相关的金融产品时，可能面临极高的投资风险。

2018 年 4 月，印度储备银行宣布禁止其监管的金融机构为国民个人和企业处理加密货币业务和结算，已经提供加密货币服务的金融机构要在一定期限内终止服务[21]。

鉴于加密数字代币从诞生之日起，就具备国际性、超主权性，从监管层面，国际社会应进一步促进共识，在明确非法定货币性质和地位的基础上，确立对于加密数字代币的一致性监管原则，加强对加密数字代币流通以及相关的交易事项和主体的追踪，防止加密数字代币成为洗钱等非法行为的工具。

3.3 法定数字货币研究现状

3.3.1 法定数字货币研究进展

法定数字货币在履行货币职能的同时，相关的支付清算系统有可能成为新一代金融基础设施，并对银行间清算结算、电子支付体系产生深远影响。法定数字货币发行流通体系下，银行金融机构间可能基于区块链部署分布式账本，银行间的大额结算、票据业务将依托分布式账本与数字货币实现结算和清算的合二为一，从而极大提升银行金融机构间清结算效率。在交易支付过程中法定数字货币就是一种新型的电子支付工具，可实现“任意时间、任意地点、使用任意设备”进行交易的功能，同时势必会与其他电子支付工具形成竞争之势。这些因素都将对货币发行与流通、支付清算体系产生深远影响。当前不少央行已投入相当精力进行法定数字货币的研究。

英格兰银行研究法定数字货币较早，但目前其对法定数字货币的态度有所转变。英格兰银行早在 2015 年 2 月就发布研究报告[22]，开始考虑发行官方数字货币，并与伦敦大学合作开发出央行控制的数字货币 RSCoin 代码并进行测试，同时启动其面向更多公司的创业公司加速器。不过，2018 年 3 月，英格兰银行行长 Mark Carney 曾公开表示，英格兰银行对创建中央银行数字货币（CBDC）持“开放态度”，但一个流通使用的、可靠的 CBDC 并不是近期就能实现的，主要原因在于分布式账本技术目前尚不成熟，以及为所有人提供中央银行账户可能存在风险[23]。

[20] ESMA, EBA and EIOPA warn consumers on the risks of Virtual Currencies, http://www.eba.europa.eu/documents/10180/2139750/Joint+ESAs+Warning+on+Virtual+Currencies.pdf

[21] Prohibition on dealing in Virtual Currencies (VCs), https://rbi.org.in/scripts/NotificationUser.aspx?Mode=0&Id=11243

[22] One Bank Research Agenda: Launch Conference - opening remarks by Mark Carney, https://www.bankofengland.co.uk/speech/2015/one-bank-research-agenda-launch-conference

[23] https://www.bankofengland.co.uk/speech/2018/mark-carney-speech-to-the-inaugural-scottish-economics-conference

巴巴多斯央行与区块链初创公司 Bitt 于 2016 年 2 月合作发行了基于区块链的数字货币巴巴多斯元，在区块链上正式发行法币[24]。Bitt 的巴巴多斯元可作为数字资产使用，并且其价值等同于政府发行货币。公司数字货币交易记录将以点对点形式存储在 Bitt 钱包中，方便政府和当地监管机构进行监控。

丹麦央行于 2016 年 12 月确定工作重点由纸钞转向数字货币 E-krone 项目的研发[25]，计划发行自己的基于区块链的数字货币作为其储备货币，并进一步计划将本国货币数字化。但是考虑到区块链和数字货币概念在技术和密码评估方面还需要进一步完善，需要对相关技术进行持续跟踪和研究。同时，民众期待财务自由和隐私，所以中央银行还未决定是否应该监测和跟踪本国人民的交易。

相比于全球其他央行，我国央行对待数字货币的态度一直较为前瞻主动。2016 年 1 月 20 日，人民银行在召开的数字货币研讨会上首次对外公开发行数字货币目标[26]，同年 11 月，人民银行印制科学研究所公开招聘相关专业人员，从事数字货币研究与开发工作。随后，央行数字票据交易平台原型系统测试成功。2017 年 7 月，央行数字货币研究所正式成立。2018 年 1 月，央行副行长范一飞向公众介绍数字货币推进进展，指出我国央行数字货币应采取双层投放体系，必须保证央行在投放过程中的中心地位[27]。2018 年两会期间，央行行长周小川指出央行最新动作是与业界共同组织分布式研发，依靠和市场共同合作的方式研发数字货币[28]。

3.3.2 法定数字货币面临的挑战

法定数字货币的发行与流通，除技术体系与发行环境外，仍有很多方面的限制因素需要逐一克服。

法定数字货币必须解决安全方面的隐患。迄今为止，安全性一直是制约数字货币发展的最重要的瓶颈因素之一。数字货币的使用者一般将其储存在移动设备、计算机或在线钱包中。如果其设备丢失或损坏，用户就会丢失其拥有的数字货币。此外，存放在在线钱包中也有可能被黑客攻击而窃取。目前，公有链系统存在 51% 攻击隐患，对于国家法定货币来说，这样的安全威胁是不能容忍的。

法定数字货币在个人隐私保护和信息公开方面需要进一步权衡利弊。数字货币以纯数字化形式存储，以身份信息代码和私钥作为确定所有权归属的重要依据，并主要以信息传输方式实现所有权转移的特征，使得数字货币比传统货币面临更为严峻的个人信息保护问题——一旦个人信息泄露，不仅可能侵犯个人隐私，而且还可能导致个人丧失对数字货币本身的控制，进而侵犯其财产权益。实践中，黑客攻击、相关参与主体泄密、系统缺陷等原因都可能导致信息泄露，如电子认证服务中心保存的用户身份信息及数字货币绑定的身份代码泄露、数字货币客户端中数量和面额信息被窃取，以及受理数字货币的商户非法获取和泄露交易信息等。针对上述风险，除应采取技术保护措施以外，还应建立相应的法律保护制度。

[24] Bitt Launches Barbados Dollar on Blockchain, Calls for Bitcoin Unity, https://www.coindesk.com/bitt-launches-barbados-dollar-on-the-blockchain-calls-for-bitcoin-unity/

[25] Central bank of Denmark is considering an e-krone based on blockchain - but tech is the least of the problems involved, http://nordic.businessinsider.com/the-danish-central-bank-is-considering-an-ekrona-based-on-blockchain---but-privacy-could-be-a-problem-2016-12/

[26] 中国人民银行数字货币研讨会在京召开，http://www.gov.cn/xinwen/2016-01/20/content_5034826.htm

[27] 范一飞 . 范一飞：关于央行数字货币的几点考虑 [N]. 第一财经日报 ,2018-01-26(A05).

[28] 周小川：传统的纸币、硬币未来可能将不复存在，http://lianghui.people.com.cn/2018npc/n1/2018/0309/c418389-29858471.html

3.3.3 区块链技术与法定数字货币

区块链技术对数字货币的发展有着重要影响，尤其是以比特币为代表的加密数字代币，更是视区块链为其核心。不过，法定数字货币是否必须依托区块链发行流通呢？答案是否定的。

区块链不是法定数字货币的唯一实现技术。我国央行数字货币研究所所长姚前曾指出，建议将数字货币与比特币、区块链松绑，区块链只是法定数字货币的可选技术之一。不可否认，区块链在以比特币为代表的加密数字代币领域表现得非常优异，但优异不代表唯一。区块链只是可以作为法定数字货币的底层技术之一，这是一项可选技术。应当具体分析研究区块链的技术特性、模式与架构哪些适合应用于法定数字货币领域，哪些不适合。仔细甄别后灵活使用，如果以区块链的特性为主反推法定数字货币的研究，那就本末倒置了。比特币分叉等事件反映了“点对点”的区块链技术尚处于初级阶段，需要看清楚区块链的不足，需要认识到区块链技术不仅不是加密数字代币可选择的唯一实现技术，更不是法定数字货币的唯一实现技术。事实上传统集中化技术和区块链的“点对点”技术各有优劣势。从技术的成熟性看，未来法定数字货币也有采用集中化技术的可能性。

不过，区块链对法定数字货币的研究与实践也有较高的借鉴价值，如共识机制、加密算法、对等系统与智能合约等方面，都将对法定数字货币的发行和流通机制的建立产生深远影响[29]。银行等金融机构的现行系统多采取分布式架构，分布式架构在保证各节点数据一致性的策略中，所需处理的意外事务通常只考虑普通故障，如节点发生宕机、网络出现部分阻塞等非人为情况，未纳入恶意节点等人为因素。而依托区块链进行部署的系统，其保障各节点数据一致性的策略中，可基于区块链去中心化的特性忽略节点宕机与网络部分阻塞等普通故障的影响，直接考虑存在恶意节点的情况，并通过区块链的拜占庭共识协议随时防范恶意节点的攻击，这为法定数字货币的系统设计提供了很好的借鉴。此外，区块链的智能合约特性为智能化操作奠定了必要基础，能够对以法定数字货币为基础的支付工具提供有益的设计参考。

展望未来，法定数字货币的实践应用，一定是结合经济生活的实际需求再采取合适的技术方式来实现的，因此说区块链是有益的参考，但不是唯一方案。

[29] 姚前 . 数字货币的发展与监管 [J]. 中国金融 ,2017(14):38-40.

第四章 支付清算

支付清算系统是经济金融活动的基础性支撑，是用以实现债权债务清偿及资金转移的一种金融安排。支付清算是区块链应用热度及成熟度仅次于数字货币的金融领域，其中尤其以跨境支付领域为典型代表。支付清算流程是一种典型的多中心场景，与区块链特性匹配度较高。当前，国内外市场主体开始尝试将区块链技术应用于跨境支付场景，以及部分中央银行对区块链（DLT）技术作为大额支付系统的备选技术方案开展了测试。

4.1 跨境支付业务与区块链

4.1.1 跨境支付业务发展现状

随着全球一体化进程的不断加快，跨境贸易规模持续增大，跨境支付的交易量也在不断攀升。埃森哲研究显示，每年通过银行进行的跨境支付交易有 100 亿到 150 亿笔，规模在 25 万亿美元到 30 万亿美元之间[30]。

以目前跨境支付采用的 SWIFT（Society for Worldwide Interbank Financial Telecommunication，环球同业银行金融电讯协会）模式为例。SWIFT 成立于 1973 年，主要业务是以可靠的方式交换标准化的金融报文帮助用户安全地通信，目前报文传送平台、产品和服务已对接全球超过 11000 家银行、证券机构和企业用户，覆盖 200 多个国家和地区[31]。SWIFT 建立了统一的账户的表达方式，加入 SWIFT 的机构都会有自己的身份代码，它又被称为银行识别码（Bank Identifier Code，BIC）。每个 SWIFT 成员机构也会有统一的客户账户的表达标准，即国际银行账户号码（International Bank Account Number，IBAN）。通过 SWIFT 网络进行跨境支付交易时，收付款银行需同为 SWIFT 会员机构，若有一方不是 SWIFT 会员，则需要借助第三方 SWIFT 会员代理银行完成支付交易。

在目前的跨境支付流程中，每笔交易都需要在多家机构间进行传送，存在中间费用高、支付效率低、会员门槛高、中心化安全隐患等问题。一是支付中间费用高。传统跨境支付模式有四块成本：支付处理成本、接收费用、财务运营成本和对账成本。麦肯锡报告显示，银行使用代理银行完成一笔跨境支付的平均成本在 25 美元到 35 美元之间，该成本是使用自动票据交换所（Automatic Clearing House，ACH）完成一笔国内清结算支付成本的 10 倍以上[32]。二是支付效率低。传统跨境支付模式流程复杂，例如跨境汇款流程会涉及到国内汇款行、境外清算系统、境外收款银行。三是会员制进入门槛高。传统跨境支付模式中，并不是所有银行都能加入 SWIFT，非会员银行开展跨境支付业务只能通过中间代理银行开展，造成不便。四是中心化存在安全风险。SWIFT 系统持续被攻击，造成的损失也越来越大。孟加拉国、厄瓜多尔、越南、菲律宾等多个国家的银行陆续曝出曾经遭遇黑客攻击并试图窃取金钱事件，这些事件中黑客都瞄准 SWIFT 银行间转账系统，对相关银行实施攻击和窃取。

[30] https://www.accenture.com/t20160624T022901__w__/us-en/_acnmedia/PDF-23/Accenture-Banking-Real-time-Cross-Border-Payments.pdf
[31] https://www.swift.com/swift_in_chinese
[32] https://www.mckinsey.com/~/media/McKinsey/Industries/Financial%20Services/Our%20Insights/A%20mixed%202015%20for%20the%20global%20payments%20industry/Global-Payments-2016.ashx

4.1.2 区块链在跨境支付领域的优势

区块链在跨境支付的应用主要体现在，通过一种金融交易的标准协议，实现全世界的银行、企业或个人互相进行点对点金融交易，无需类似 SWIFT 的中心管理者，直接实现跨国跨币种的支付交易。基于区块链的跨境支付实际上是用比特币或 Ripple 币等虚拟货币做中介来实现的跨境支付。具体而言，系统会将代币 / 数字资产作为中介，先把汇款人所在地的法币转换为代币 / 数字资产 ,再在收款端把代币转换为收款人所在地的法币 ,以此完成跨境支付，如 Ripple 在跨境资产中使用的数字资产是 XRP，OKLink 使用的是 OKD，SnapCard 使用的是比特币。相较于传统的跨境支付模式，基于区块链的跨境支付模式拥有效率更高、成本更低、流动性更强、权利更平等的优势。

一是效率更高。传统跨境支付模式中银行会在日终对支付交易进行批量处理，银行间需要进行人工对账，通常一笔跨境支付需要至少 24 小时才能完成。而基于区块链的跨境支付接近于实时，并且是自动的，它可以 7*24 小时不间断服务。汇款方可以很快知道收款方是否已经收到款，从而了解这笔支付是否出现了延迟或者其他问题。全球第一笔基于区块链的银行间跨境汇款在传统支付模式中需要 2 到 6 个工作日，但使用了 Ripple 的技术，8 秒之内即完成了交易 [33]。

二是成本更低。麦肯锡报告称区块链技术在 B2B 跨境支付与结算业务中的应用将使每笔交易成本从约 26 美元下降到 15 美元，其中约 75% 为中转银行的支付网络维护费用，25% 为合规、差错调查，以及外汇汇兑成本 [34]。Ripple 称基于区块链的跨境支付应用能将支付处理成本降低 81%，通过更少的流动性成本和更低的交易对方风险将财务运营成本降低 23%，通过即时确认和实时进行流动性监控将对账成本降低 60%[35]。

三是降低了跨境支付参与方的门槛。传统跨境支付模式中，并不是所有银行都能加入 SWIFT，而且加入 SWIFT 的经济性有待商榷。而基于区块链的支付模式则更为平等，无论大小银行、大小金融机构，都能成为平等交易的主体，而这种平等对接的实现所仰仗的是所有使用区块链技术的机构对区块链技术的信任。

[33] ReiseBank integrates Ripple to make payments faster and cost-effective, https://ripple.com/files/case_study_reisebank.pdf
[34] http://www.mckinsey.com.cn/wp-content/uploads/2016/05/%E5%8C%BA%E5%9D%97%E9%93%BE.pdf
[35] The Cost-Cutting Case for Banks: The ROI of Using Ripple and XRP for Global Interbank Settlements, https://ripple.com/files/xrp_cost_model_paper.pdf

4.1.3 应用探索

Ripple 是跨境支付区块链应用最早也是最成熟的解决方案。Ripple 由 Ripple 实验室（RippleLabs, Inc.）于 2012 年开发出来，是一个开源的用于金融交易结算的互联网协议。Ripple 通过 RippleNet 连接银行、支付服务供应商、数字化货币交易平台和企业，使用数字货币 XRP 为全球支付提供流畅体验。RippleNet 作为 Ripple 的核心，是一个共享的公开数据库，数据库中记录着账号和结余的总账，任何用户都可以阅读这些总账，也可读取 RippleNet 中的所有交易活动记录。RippleNet 中所有节点通过共识机制修改总账，且可以在几秒之内达到共识。Ripple 的用户进行交易转账时有两种模式可供选择，网关模式与 XRP 模式。网关是法定货币进出 RippleNet 的关口，任何可以访问 RippleNet 的商家都可以成为网关。用户进行外汇交易时，无需通过中间人或货币兑换所，RippleNet 会找到最有效的途径来撮合交易，也没有最低数额的限制。XRP 是 Ripple 在 RippleNet 中发行流通的数字货币。如果两个交易对手间没有公用的货币及其相应的网关组合，那么就可使用 XRP 作为媒介货币。在 XRP 的使用客户中，银行可按需获得实时流动性而无需在银行往来帐户中预存款项，支付服务提供商可使用 XRP 降低汇兑成本，提供更快的支付结算服务。截至 2017 年底，Ripple 已经实现横跨 27 个国家的实时全球支付，全球知名银行中不少都在参与 Ripple 的技术测试与相关合作 [36]。

Visa 和 Chain 共同开发基于区块链的 Visa B2B Connect[37]。Visa B2B 可以实现企业之间的数额巨大且过程复杂的跨境支付，资金实时转移，加快交易速度，减少了在付款失败的情况下所需的复杂法律协议的环节。该系统可能最终会和区块链初创公司（如 R3 和 Ripple）开发的产品展开竞争，同时也可能会与部分银行内部的跨境支付项目展开竞争。Visa 已经在数千家银行安装了网络，并在全球 10 个国家的 30 家银行运营了 B2B Connect 原型。

OKCoin 币行于 2016 年推出了从跨境支付服务切入的新一代全球金融网络 OKLink[38]，基于区块链连通网络中各个汇款和收款账户，让汇款公司和收款公司直接进行支付、结算，省掉了所有中间环节费用，包括 OKLink 和收款公司的所有费用，整个网络只在中间汇率基础上收取不超过 0.5% 的费用，极大地节省了中小企业在小额跨境汇款中的成本。并且，OKLink 网络中的每个账户能够实现交易信息的一致同步，借记和贷记同时完成，达成最理想交易状态“交易及结算”，10 分钟之内完成包括支付、汇率换算、结算在内的所有汇款过程，相较于传统跨境汇款流程中平均等待三四个工作日可以说是飞跃式的发展。目前，OKLink 网络已有遍及全球的数百家合作方加入，覆盖超过数十个国家和地区。

[36] https://ripple.com/cn/use-cases/banks/

[37] Visa Introduces International B2B Payment Solution Built on Chain’ s Blockchain Technology, https://investor.visa.com/news/news-details/2016/Visa-Introduces-International-B2B-Payment-Solution-Built-on-Chains-Blockchain-Technology/default.aspx

[38] https://www.oklink.com/howWorks

分布式账本项目 Stellar.org，可用于建立数字货币和法定货币之间传输的去中心化网关，其最重要的应用方向是建立开放的全球支付体系[39]。在 Stellar 进行跨境支付的原理与其他分布式账本的原理类似，不过 Stellar 不局限于银行间结算，更主张多样化的用户和场景，如跨国企业财务管理、手机钱包转账、个人 / 企业汇款等等。目前 Stellar.org 覆盖的地区包括菲律宾、印尼、新加坡、中国、尼日利亚、加纳、印度、荷兰、法国、德国等。同样是分布式账本，Ripple 主要服务于银行间清结算，而 Stellar 服务于机构间清结算，Stellar 的服务可以在小公司上得到更好的实践。

SWIFT gpi 是 SWIFT 为应对互联网企业、区块链等新兴支付机构和新技术的挑战，牵头全球主流银行启动的重要跨境支付改革。自 2017 年 1 月上线以来，已有超过 160 家金融机构签约加入该项服务，每天使用 gpi 支付的资金超过 1 亿美元[40]。另外，作为 SWIFT gpi 路线图技术评估的一部分，SWIFT 于 2017 年初启动区块链的概念验证（POC），以确定该项新技术可否用于跨境支付的银行账户实时对账环节，即资金和汇款信息同步到达，从而降低成本和运营风险。2018 年 3 月，SWIFT 发布区块链概念验证的认证结果，认为银行可以使用分布式账本进行实时交易[41]。基于超级账本 Hyperledger Fabric，SWIFT 试运行项目重点验证了银行往来账、以及银行在其他银行中持有账户的交易处理，设想了一些“多对多”的银行转账交易场景，还特别检查了在处理往来账调配流程时，区块链系统是如何满足有关管理、安全和数据隐私要求的。

4.2 大额支付系统与区块链

4.2.1 大额支付系统发展现状

大额实时支付一般是指金融机构之间发生的支付业务[42]，与零售支付业务相比，单笔支付金额较大，且对交易处理时间要求较高，需在特定日期或特定时间完成结算。在大多数经济体中，大额实时支付在支付业务总笔数中占比较低，但在总金额中占比极高，因此大额支付业务的安全有序结算对于金融市场的平稳运行至关重要。

20 世纪 80 年代，大额支付系统以延迟净额结算系统（DNS）为主要形式，90 年代开始，实时全额结算系统（RTGS）得到迅速发展，目前成为大多数国家大额支付系统的主要形式[43]。RTGS 在交易处理期限内，以连续、逐笔方式，实现跨行资金的最终结算。考虑到 RTGS 系统的业务处理规模极为庞大，及其与其他金融市场基础设施关联度较高，因此，系统在设计上必须具备足够的稳健性，以维护整体的金融稳定。

当前，世界各国（地区）都在不断升级完善辖区内的大额支付系统，如美国的 FEDWIRE（联邦电子资金转账系统）和 CHIPs（清算所同业支付清算系统）、瑞士的 SIC（跨行清算系统）、伦敦的多币种清算系统 CLS（持续联结清算系统）、日本的 BOJ-NET（银行金融网络系统）、欧洲的 TARGET 系统（跨国大批量自动实时快速清算）等。

---

[39] https://www.stellar.org/cn/how-it-works/stellar-basics/?noredirect=zh

[40] https://www.swift.com/our-solutions/global-financial-messaging/payments-cash-management/swift-gpi

[41] SWIFT explores blockchain as part of its global payments innovation initiative, https://www.swift.com/news-events/press-releases/swift-explores-blockchain-as-part-of-its-global-payments-innovation-initiative

[42] Tom Kokkola (ed.). The Payment System: Payments, securities and derivatives, and the role of the Eurosystem.[R]. 2010.

[43] CPSS. Real-time gross settlement systems[R]. 1997.

4.2.2 区块链在大额支付系统中的应用优势

当前，许多国家和地区正着手对本国或地区的 RTGS 系统等金融市场基础设施进行升级和优化，区块链技术成为系统改造过程中的备选技术方案。区块链技术对大额支付系统所能产生的效益，以及技术方案是否能够实现传统 RTGS 中心化技术架构下[44]的功能和优势，目前仍停留在理论探讨阶段[45]。

一是提高支付清算效率。从理论层面来看，依托区块链技术特性，网络中的节点对于重要信息的维护达成一致意见，无需额外的人工对账操作，交易处理速度得以加快。此外，通过智能合约的应用，能够减少人为干预因素，进一步提高合同的执行效率，由此带来支付清算整体效率的提升。

二是提升业务流程透明度。区块链系统中的信息可以实时同步给参与者，在提升交易记录透明度的同时，有效避免逻辑冲突产生的几率。与传统中心化维护和控制模式不同，相关系统参与者在数据添加进账本之前，具有一定的话语权。这种分布式系统治理模式，在一定程度上使得系统中的信任机制得到强化。区块链网络中的全部历史交易记录公开、透明、可追溯，具备权限的系统参与者能够审查到交易信息创建的具体时点，动态掌握交易全貌。

三是强化系统弹性及稳健性。由于大额支付系统对稳健性的要求极高，提高系统操作弹性是区块链技术最具吸引力的优势。区块链系统的操作弹性来自于其分布式的技术特征。由于每个节点维护的账本是相同的，因而可以有效降低数据存储环节中“单点失败”导致的风险。随着系统参与者数量的增加，系统弹性还可不断提高。在大部分区块链系统中，任何一笔交易在被记入账本之前，系统中的多数参与者需对交易状态形成一致意见。因此，在对区块链系统进行攻击时，同样需要取得多数参与者的一致同意，加大了成功实施网络攻击的难度。此外，系统参与者通过加密技术和电子签名，验证身份和交易的真实性，行使账本读写的权利，也有助于提升区块链系统的稳健性。

4.2.3 应用探索

从 2016 年开始，加拿大银行（BoC）、英格兰银行（BoE）、日本银行（BoJ）、欧洲中央银行（ECB）、新加坡金融管理局（MAS）等中央银行，纷纷启动概念验证项目，围绕区块链技术（DLT 技术）在大额支付系统中的应用开展研究，对该技术作为 RTGS 系统底层技术的可行性进行论证。

加拿大开展 Jasper 项目。2016 年，加拿大大额支付系统运营机构——加拿大支付协会（Payments Canada），会同加拿大央行、R3 和 R3 成员中的部分商业银行，共同启动了名为 Project Jasper 的概念验证项目，探索 DLT 技术在大额支付系统中的应用，成为全球首个中央银行深度参与的 DLT 验证项目[46]。Project Jasper 的直接目标，是使用中央银行发行和控制的结算资产，设计开发原型系统[47]。

[44] 部分 RTGS 系统（如 TARGET2）已采用分布式数据库，传统 RTGS 系统仅指未应用 DLT 技术的系统。
[45] FSB. Financial Stability Implications from FinTech: Supervisory and Regulatory Issues that Merit Authorities' Attention[R]. 2017.
[46] Bank of Canada. Project Jasper: Are Distributed Wholesale Payment Systems Feasible Yet?[R]. 2017.
[47] 由于该项目并未计划成为生产级系统，仅作为概念验证系统，因此部分适用于生产级金融市场基础设施的原则，如反洗钱等法律和治理方面的要求，并未涵盖在项目评估范围内。

在项目的第一阶段，参与者在以太坊中开发结算功能，实现结算资产的转移，对 DLT 应用于大额跨行支付结算功能进行测试。项目第二阶段以 R3 Corda 平台为基础，进一步评估 DLT 技术的可扩展性和稳健性，并尝试引入流动性节约机制（LSM）[48]，进一步降低对系统参与者日间流动性要求。之后，Project Jasper 项目组还将围绕 DLT 系统如何与金融市场基础设施原则（PFMI）进行衔接开展研究。Project Jasper 两阶段测试结果显示，基于以太坊工作量证明（PoW）的共识机制，目前仍无法满足核心结算系统中的结算最终性要求，且操作性风险相对较高。而 Corda 平台的“公证人”（notary）模式虽然能够改进结算最终性、可扩展性、隐私及信息安全等问题，但是，操作性风险仍未得到有效解决。

2017 年 10 月底，Project Jasper 的第三阶段测试正式开始[49]，新引入加拿大 TMX 集团作为项目参与方，该集团旗下公司包括多伦多证券交易所、蒙特利尔交易所、加拿大衍生品清算公司等主体，负责加拿大衍生品市场的运营，以及包括股票、固定收益、能源等不同金融资产的清算业务。项目第三阶段旨在合作开发一个基于 DLT 技术的证券清结算原型平台，通过证券结算的流程自动化，测试该技术对证券交易速度和效率的改进效果。

英格兰银行针对新一代 RTGS 系统开展调研项目。2014 年 10 月，英国大额支付系统 CHAPS 曾发生中断，随后，英格兰银行着手对本国大额支付体系进行全面调查。2016 年 9 月，英国央行在新一代 RTGS 系统的调研报告中，分析了采用区块链技术改造现有 RTGS 系统的可行性，提出区块链技术三个可能的应用设想，一是作为核心 RTGS 结算业务的平台；二是作为需使用中央银行货币进行证券 DvP 结算或外汇 PvP 结算业务的平台；三是作为未来需与 RTGS 系统实现互联互通的数字货币的平台[50]。2017 年 5 月，英国央行公布了 RTGS 系统规划方案，虽然新一代 RTGS 系统不会以区块链技术为基础，但将在系统设计中预留未来与区块链系统之间进行交互的接口。

新加坡开展 Ubin 项目。为促进产业共识，强化市场主体对 DLT 技术及其潜在优势的理解，2016 年 11 月，新加坡金融管理局与 R3 及部分商业银行等机构推进合作项目——Project Ubin，探索将 DLT 技术应用于支付和证券清结算环节。作为多阶段项目，Project Ubin 的最终目标是探索开发基于中央银行发行的数字代币的，更为便捷、高效的新一代支付系统。

Project Ubin 第一阶段的重点任务是使用 DLT 技术，实现国内跨行支付。该阶段于 2016 年 12 月 23 日结束，已实现的阶段性目标包括：通过对新加坡元（SGD）进行代币化处理，实现国内跨行结算；对银行系统与 DLT 系统的连接模式进行测试；应用 DLT 技术，实现大额支付系统 MEPS+ 的抵押自动化管理[51]。

项目的第二阶段由新加坡金管局、新加坡银行协会（ABS）共同主导，参与机构包括商业银行和新加坡交易所等 11 家金融机构，以及微软、R3、IMB 等 4 家技术企业和咨询机构埃森哲（Accenture）。在为期 13 周的测试中，分别在 R3 Corda、Hyperledger Fabric 和 Quorum 平台上开发了三个原型，成功地在去中心化的环境中，引入了流动性节约、系统排队管理、僵锁处理等 RTGS 系统核心机制，实现了银行间支付与结算功能，同时兼顾了隐私保护。

---

[48] 与 DNS 系统相比，RTGS 能够有效降低银行间的信用风险，但对流动性要求较高。为节约流动性，许多国家在 RTGS 系统设计中引入流动性节约机制（LSM），在相同流动性需求水平基础上，提高系统结算效率。

[49] Bank of Canada. Project Jasper: A Canadian Experiment with Distributed Ledger Technology for Domestic Interbank Payments Settlement[R]. 2017.

[50] Bank of England. A new RTGS service for the United Kingdom: safeguarding stability, enabling innovation -A Consultation Paper[R]. 2016.

[51] Deloitte, Monetary Authority of Singapore. The future is here: Project Ubin: SGD on Distributed Ledger[R]. 2017.

下阶段，Project Ubin 将在新加坡金管局、商业银行、新加坡交易所（SGX）等主体的共同合作下，开发去中心化的债券交易系统，以期通过 DLT 技术进一步改善固定收益类证券的交易和结算流程[52]。

欧央行与日本央行联合开展 Stella 项目。2016 年 12 月，日本央行（BoJ）与欧央行（ECB）启动了 DLT 技术联合研究项目——Project Stella[53]。该项目着重分析 DLT 技术应用于金融市场基础设施的可行性，旨在评估现有支付结算系统各项功能是否能够在 DLT 技术架构中安全、高效地实现。Stella 项目基于 Hyperledger Fabric 开源平台，采用拜占庭容错（PBFT）算法，使用模拟数据，在完全虚拟的环境中进行测试。项目第一阶段结果显示，DLT 系统可以满足欧盟和日本 RTGS 系统（TARGET2 和 BOJ-NET）的交易处理需求。但 DLT 系统的性能受制于网络规模和节点距离，节点数量越多、节点分散度越高，交易处理的延迟现象越明显。此外，Stella 项目也验证了 DLT 技术在提高系统弹性和稳健性方面的潜在优势，在测试条件下，DLT 网络中验证节点失败和数据格式错误不会对系统整体功能产生影响。

在上述各国央行开展的区块链实验项目中，区块链技术的探索仍处于概念验证阶段，欧央行、英国央行和加拿大央行已公开表示，鉴于现阶段技术尚未足够成熟，本国（地区）的新一代 RTGS 系统暂时不会以区块链技术为底层技术基础。因此，区块链技术对大额支付系统所能产生的潜在效益，仍停留在理论层面。传统的 RTGS 系统多以中心化技术架构为基础，区块链技术模式是否具备中心化系统所提供的功能和优势，还需要市场主体通过持续深入的测试和实验加以印证。

4.3 挑战与思考

支付清算系统是一国（地区）的核心金融基础设施，支付体系的平稳有序运行，对于维护经济金融稳定、密切各金融市场有机联系、畅通货币传导机制等方面具有重要作用。区块链技术特性可针对性地解决现行支付清算系统中的部分痛点，但也需认识到基于区块链的支付清算解决方案仍有不少亟待突破的问题。

一是结算最终性问题。区块链可能带来无法确定结算最终性的问题。在交易后清结算中，结算最终性是一个法定或约定时点，交易双方及各自的中介机构依据最终性的定义和时间，更新各自账本以实现结算、确定资产所有权并衡量和监控相关风险。在区块链中，多个主体可以更新共享账本，并通过共识机制确定账本的特定状态，结算最终性取决于概率。通过概率确定最终性，法律责任可能难以分配或较为模糊，且这种不确定性对于参与者的资产负债表及其客户和债权人的权利都会产生影响。如果同时考虑资产交割和资金交付两方面，结算最终性问题就更为复杂，比如 DvP 结算方式，资产与资金同步进行结算并互为结算条件。此时，如果资产交割和资金交付不是在同一个网络、平台或账本中发生，且没有中介机构提供结算最终性担保，那么这种相互依赖性就成为了新的挑战。

[52] Accenture, Monetary Authority of Singapore, The Association of Banks in Singapore. PROJECT UBIN PHASE 2: Re-imagining Interbank Real-Time Gross Settlement System Using Distributed Ledger Technologies.[R]. 2017.

[53] European Central Bank, Bank of Japan. Payment systems: liquidity saving mechanisms in a distributed ledger environment – Stella project report [R]. 2017.

二是信用及流动性风险。信用风险是对手方无法完全履行结算义务的风险，流动性风险是对手方没有充足资金履行义务，这两种风险之间往往具有相关性。在传统金融体系中，对手方之间的信用和流动性风险，由支付、清结算领域的金融中介机构集中承担及管理。信用风险管理工具包括在支付账户中预存足额资金，或者提供担保等方式，这些要求都可能影响参与者的流动性。在区块链方案中，对手方信用风险的处理方式，同样可能会对参与者的流动性需求产生重要影响。

三是操作风险。操作风险包括处理错误或延迟、系统终端、容量不足、欺诈和数据丢失或泄漏。系统弹性和安全性是操作风险管理中的核心要素。与任何软硬件都可能存在漏洞的系统一样，区块链存在端点(节点)安全性问题，其分布式结构使端点更易遭到攻击。区块链中的加密强度和密钥安全管理是另一个有待解决的重要问题。另外，随着风险和安全威胁不断变化发展，分布式账本系统安全管理流程和控制措施应持续对风险进行评估，对于开放式 公有链系统而言存在一定挑战性。传统的操作风险管理措施需进一步调整和修订，以适应分布式网络环境。在大规模投入市场应用之前，需持续分析并妥善处理区块链技术应用可能面临的安全问题。

CAICT 中国信通院

第五章 供应链金融

在供应链金融流程中，供应商、核心企业、银行、金融机构等多方并存，多主体、非高频交易场景是较为适合区块链的场景。针对中小企业所面临的融资难、融资贵、融资乱、融资险的情况，运用区块链技术，可实现应收账款、票据、仓单等资产数字化，并且留下数据存证，防止票据作假、重复质押等风险发生，从而打通供应链金融中的信任传导机制，提升资产流动性，降低中小企业的融资成本，深度盘活金融资源，有效助力实体经济发展。

5.1 供应链金融的发展历程

供应链金融是对供应链的不同节点提供封闭的授信及其他结算、理财等综合金融服务，能够帮助供应链中处于弱势的中小企业解决融资难的问题，进而稳定核心企业的供销渠道，促进并提高整个供应链链条中资金的利用与统筹效率。其实质就是通过及时获取真实的贸易背景信息，实现风控，帮助企业盘活其流动资产从而解决融资问题，这也是其与传统金融业务的主要区别所在。

供应链金融有三种主要的融资模式：应收账款融资模式、预付款融资模式和动产质押融资模式。应收账款融资是指在供应链核心企业承诺支付的前提下，供应链上下游的中小型企业可用未到期的应收账款向金融机构进行贷款的一种融资模式。预付款融资是指企业通过未来货权向金融机构贷款的融资模式。动产质押融资是指企业以存货作为质押，经过专业的第三方物流企业的评估和证明后，金融机构向其进行授信的一种融资模式。

供应链金融概念源自国外，当前在国内发展迅速，不过整体还处于初级阶段。20 世纪 80 年代，世界级企业巨头在全球范围内采购和业务外包，寻求供应链管理成本最小化，随着全球化贸易的深化，供应链管理从最初的物流、信息流管理层面逐渐扩大到解决资金流瓶颈和降低融资成本的财务价值再发现层面，供应链金融应运而生。原深圳发展银行是国内供应链金融业务的先行者，于 2001 年下半年在广州和佛山两家分行开始试点存货融资业务，并于 2006 年在银行业率先推出“供应链金融”品牌。此后供应链金融模式开始在国内银行业广泛推行。现阶段，包括股份制商业银行、大型商业银行均已在供应链金融领域开展布局。建行先后与金银岛、敦煌网、京东商城合作共同开发在线融资平台。2012 年，中行与京东商城推出供应链金融服务平台。

当前，除商业银行之外，部分电商平台等市场主体也越来越多地关注并涉足供应链金融领域，并且依靠雄厚的资金实力、灵活的放款方式以及大数据资源等优势，开始独树一帜。2013 年苏宁宣布将供应链金融业务面向中小微企业全面开放，其中授信业务已覆盖交行、中行、光大、花旗、渣打、平安、汇丰国内外 7 家知名银行[54]。

由此可以看出，现阶段国内供应链金融主要有三种融合类型：传统的供应链金融模式，即银企合作触网，如中信银行 + 海尔 ,交行 + 生意宝等；拥有完整供应链企业资源的传统电商自建 P2P ,为供应链上下游企业提供金融服务，如京东、阿里巴巴等；“电商 +P2P”模式，P2P 平台通过合作、收购的方式对借贷的资源进行整合，为有融资需求的中小企业和个人服务，如工商贷、甬商贷和积木盒子等。

[54] 苏宁易购李斌：供应链金融有助小微企业快速发展，http://www.suning.cn/cms/mediaReports2013/3297.htm.

5.2 传统供应链金融的行业痛点

供应链金融主要是由供应链上下游的全量业务数据驱动进行风险评估，数据流的透明度与流畅性是供应链金融发挥作用的重要基础。而在供应链金融业务实际运行过程中，往往存在数据信息不对称以及交易信息伪造问题，此外还存在业务操作风险。

一是信息不对称。供应链运行过程中，各类信息分散保存在各个环节中，供应商的货物信息存储在供应商的仓储信息中，发货信息掌握在物流公司手里，资金信息分布在银行系统内，信息流信息则由核心企业掌握，整个供应链信息不透明、不流畅，各个参与主体难以了解交易事项的进展情况，信息的高度不对称影响了整个链条的效率，最终也导致整个供应链信用体系难以建立。而针对供应链贸易背景而提供的金融服务，也因为信息的不对称而难以高效开展。金融机构往往会出于风控的考虑而较为谨慎。

二是贸易背景真实性问题。在供应链融资中，商业银行是以实体经济中供应链上交易方的真实交易关系为基础，利用交易过程中产生的应收账款、预付账款、存货为质押 / 抵押，为供应链上下游企业提供融资服务。在融资过程中，真实交易背后的存货、应收账款、核心企业补足担保等是授信融资实现自偿的根本保证，一旦交易背景的真实性不存在，出现伪造贸易合同，或融资对应的应收账款的存在性、合法性出现问题，或质押物权属、质量有瑕疵，或买卖双方虚构交易恶意套取银行资金等情况出现，银行在没有真实贸易背景的情况下盲目给予借款人授信，就将面临巨大的风险。

三是业务操作风险。供应链金融通过自偿性的交易结构设计，专业化的操作环节流程安排，以及独立的第三方监管引入等方式，构筑了独立于企业信用风险的第一还款来源。但这无疑对操作环节的严密性和规范性提出了很高的要求，容易出现操作性风险，因此操作制度的完善性、操作环节的严密性和操作要求的执行力度将直接关系到第一还款来源的效力，进而决定信用风险能否被有效屏蔽。

四是融资成本高。供应链中的中小微企业融资成本高是制约供应链金融发展的另一个重要因素，供应链金融涉及多方交易，为了验证交易的真实性，金融机构需要投入巨大的时间和资金成本。由于供应链涉及的节点不一，多的时候甚至能跨越十多个地理区域，金融机构很难跟踪、调查清楚所有环节，难以验证产品和服务的真正价值，因此融资时间变长，手续费变贵，中小微企业难以承受。

5.3 区块链在供应链金融领域的应用场景

在基于区块链的解决方案中，可以以节点可控的方式建立一种联盟链的网络，涵盖供应链上下游企业、财务公司、金融机构、银行等贸易融资参与主体。然后，将各个节点贸易数据上链，通过区块链记录贸易主体资质、多频次交易、商品流转等信息，上链目的就是为了让各个节点保持同步，金融机构可获取二、三级中小型企业贸易的真实情况。有融资需求的企业将合同、债权等证明上链登记，可保证这些资产权益数字化以后不可篡改、也不可复制。最后，在联盟当中流转这些资产权益证明，实现点对点的连通，进一步提升数字资产证明流动性。基于区块链的供应链金融解决方案，可深度融合物流、资金流、信息流，构建行业数据业务真实性验证的统一方法，缓解信息不对称的问题，并基于智能合约属性使供应链金融业务顺利开展。

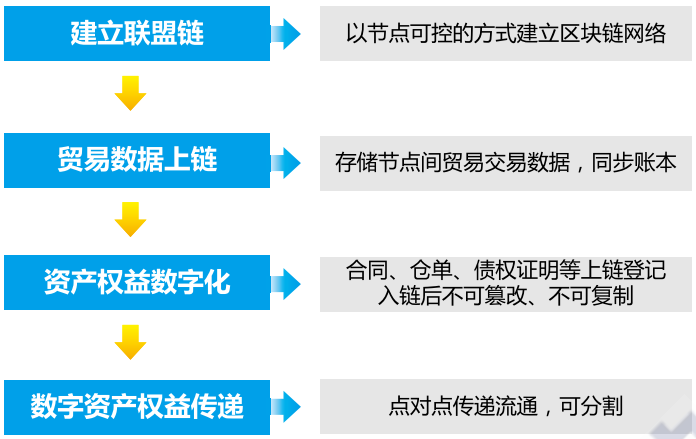

图 6 基于区块链的供应链金融解决方案流程

第一，区块链技术自带的时间戳与数据不可篡改性，可从一定程度上解决贸易背景真实性的问题。从供应商、核心企业、分销商到物流企业、仓储监管公司、金融机构等其他参与者，均可运用区块链技术形成并共享各自在该供应链各环节中的各种交易——每个交易形成网络节点，节点信息通过全网认定，物流信息通过货物的地理位置信息体现，资金信息通过回款信息的更新及时通知收款方与金融机构，应收账款信息与应付账款信息及时准确更新给交易双方以及金融机构，仓储监管信息通过数字化信息及时提供给企业以及提供动产质押融资的金融机构。各方从源头上获取了第一手真实有效的数据，构建了全新可靠的供应链信用体系，从而缓解了供应链金融服务中的信用风险问题。

第二，区块链技术可提升供应链金融业务中各主体的信用资质，重塑信用体系。在传统的供应链金融模式中，始终存在对核心企业的依赖，这是中心化的模式。而区块链技术具有去中心化的显著特征，能够保证链条中各个主体之间的信息完整和通畅，提升各个主体整体的信用资质，建立分布式的信用体系。通过区块链技术，有望将传统的 1+N 模式的供应链金融扩展到 M+N 模式的供应链金融。让核心企业不需要专门为供应链金融而做供应链金融，而是通过区块链技术在供应链业务中，自然获得供应链金融服务。

第三，区块链的智能合约属性可融入供应链金融业务中，提升全链的运营效率和风控等级。智能合约可提供项目立项、尽职调查、业务审批、保理协议 / 合同签约、账款登记及转让、贸易融资（贷款发放）、贷后管理、账款清算等保理业务全过程的应用服务，助力保理企业构建及完善互联网 + 金融的经营模式，从而更为有效地提高其获客、展业、风险识别与控制的能力，为供应链上下游企业提供更优质的金融服务，进而形成完整的供应链金融生态圈。

5.4 区块链在供应链金融领域的应用现状

国内区块链供应链金融应用发展势头迅猛，落地效果较好，并已初具规模。以布比网络科技、33 复杂美等为代表的区块链技术初创企业，与供应链核心企业合作，提供供应链金融的区块链技术解决方案。京东旗下京东金融较早投身供应链金融领域，依托自身技术、资金优势研究区块链解决方案。近期腾讯基于区块链领域的技术优势，也推出了供应链金融的区块链技术方案。

布比科技基于区块链技术优势，从供应链核心企业切入，深挖供应链金融领域。2016 年 11 月，布比科技与钢

管产业 B2B 平台壹钢网签署战略合作协议[55]，就双方采用布比区块链技术、整合社会资本及钢管产业资源共同打造以多中心信任为核心的钢管产业 B2B 平台和供应链金融体系达成战略合作。随后在 2017 年，布比推出了一个专为供应链金融打造的联盟链“布诺”[56]，将银行、核心企业、保理公司等都链接起来，布诺立足广州深圳，辐射东南区业务。在其实名验证、资产管理、在线融资、资金管控、数据溯源、账户系统六大功能的基础上，为用户提供供应链金融服务。通过释放并传递核心企业信用，为中小企业供应商带来融资的可行性、便利性，同时为金融机构提供更多投资场景，提高碎片化经济下资金流转效益。

33 复杂美以区块链底层平台为起点，帮助用户在供应链 - 票据融资、供应链 - 应收帐款融资、供应链 - 授信融资、资产数字化、商品生命周期跟踪、预付卡、区块链合同存证、积分联盟系统等细分领域，提供区块链技术方案，已在海航海平线、美的金融等企业正式上线区块链项目。2017 年 1 月，33 复杂美区块链与海航海平线就发布了国内首个基于区块链撮合系统的票据服务应用海票惠[57]。2017 年 4 月，33 复杂美与美的集团财务有限公司签署战略合作协议，共同打造美的金融区块链票据应用平台[58]。

2017 年 3 月，京东金融推出了基于区块链技术的资产云工厂底层资产管理系统[59]，帮助京东消费供应链金融服务公司落地到京东金融的资产云工厂业务中。京东金融的资产云工厂业务实现了区块链资产管理系统的部署，系统设置了三个验证节点，底层资产池中每笔贷款的申请、审批、放款等资金流转都将通过区块链由各个验证节点共识完成，通过其指定的支付通道将现金流信息直接入链，确保其底层资产的产生和流转与区块链之间的强耦合，保证了入链资产和链下资产之间的一致性和真实性。同时，各家机构间信息和资金通过分布式账本和共识机制保持实时同步，有效解决了机构间费时费力的对账清算问题。

腾讯区块链今年将重点发力供应链金融解决方案。2018 年 4 月 12 日，腾讯区块链正式发布了“腾讯区块链 + 供应链金融解决方案”[60]，基于供应链场景下的真实交易数据，通过腾讯区块链技术及运营资源，从根本上改善小微企业的融资困境，助力地方产业转型升级。该解决方案将以核心企业的应收账款为底层资产，通过腾讯区块链技术实现债权凭证的流转，以保证相关信息不可篡改、不可重复融资、可被追溯，帮助相关各方形成供应链金融领域的合作创新。

[55] 布比广州分公司成立 与壹钢网签署战略合作协议，http://www.bubi.cn/html/news/20161107/160.html.
[56] “布诺”于贵阳首次发布，“贵聚会”成果斐然，http://www.bubi.cn/html/news/20170526/175.html.
[57] 海航海平线 -33 复杂美区块链票据平台上线，http://www.fuzamei.com/newDetail?id=120.
[58] 美的金融涉足区块链与复杂美共同打造区块链票据项目，http://www.fuzamei.com/newDetail?id=121.
[59] 区块链技术首次落地资产证券化领域 京东金融 ABS 云平台再拓疆土，http://news.ifeng.com/a/20170322/50815368_0.shtml .
[60] 腾讯蔡弋戈：2018 年腾讯区块链将重点布局供应链金融，http://tech.qq.com/a/20180413/012603.htm

5.5 挑战与思考

区块链能帮助解决供应链金融的风控问题，并搭建产业链中企业间的信任桥梁，但在实际运行融资中，区块链供应链金融平台仍有很多问题需要突破。

首先，最需关注的就是合规问题。在将区块链技术融入到各行各业的供应链金融服务过程中，需要明确这种方案能否适应不同行业和法规的需求，要解决合规性的问题，解决法律的问题。比如在供应链金融实际操作中，银行非常关注应收账款债权“转让通知”的法律效应，都会要求一级供应商或核心企业签回“债权转让同意书”，如果无法签回，会造成银行不愿授信。因此，基于区块链的解决方案需要严格遵守供应链金融现行的法律规则开展研究应用。

其次，企业数据隐私安全管理也面临挑战。用于供应链金融的联盟链拓展了企业高效协作的边界，与此同时带来的问题就是，核心企业担忧数据泄露，以及担忧财务、税务、员工工资等核心数据共通之后，在同行竞争中失势。因此，基于区块链的供应链金融解决方案需要提升隐私管理技术手段，如增加分组、分层的访问控制，设置成员节点权威身份认证，避免贸易往来数据的泄露。

最后，供应链金融的主体模式其实并没有改变。区块链应用于供应链金融服务，是利用新兴的信息技术为供应链金融提供一种更为高效的解决思路，供应链金融现行的核心企业主导模式短期内不会发生改变。区块链技术本身不能解决道德风险等风控所面临的关键问题，这些风控所依赖的还是占据主导地位的核心企业。

CAICT 中国信通院

第六章 证券交易

证券领域也在积极探索区块链的创新应用，以期通过融入区块链的特性解决行业固有的问题与痛点。证券领域的区块链应用主要集中于私募证券的电子化与公募证券的发行交易，大多处在概念验证阶段。

6.1 证券行业的发展历程

电子信息技术是证券业发展的重要支撑。自 20 世纪 70 年代起，信息技术助力证券业逐渐实现电子化、网络化的交易结算体系，有力地推动了多层次资本市场的快速发展和市场各参与主体的信息化建设。近年来，证券业务逐步向移动互联网方向转移，进一步降低了证券机构的运营成本，提高了运行效率。

一是计算机的出现促进证券市场的无纸化。证券业务发展到今天，可以根据证券登记交易模式分为先后三个阶段：直接交易、托管交易、账本交易。17 世纪，在荷兰阿姆斯特丹出现了第一个证券交易所，证券市场登记发行的股票通过在实体纸质材料上记录相应权益，投资者直接持有纸质股票，交易时交易双方按照市场价格互换股票和货币。后来，托管业务的出现提高了证券市场效率，投资者不再直接持有纸质股票，由证券公司代为处理有关证券权益事务。1968 年，美国出现了纸上作业危机，大幅增长的交易量使证券公司陷入海量文件整理和数据核对计算工作，低效的手工操作制度造成大量经纪业务交易失败，给投资者带来不必要的成本，几乎使证券业陷入停顿。为了提高效率、降低风险，美国设立了中央证券存管机构美国存管信托和结算公司（DTCC），通过全国性清结算系统集中管理股票，证券登记和过户不需要任何物理上的移动工作，只需中央证券存管机构更新账本，股票所有者不再直接持有纸质股票，股票也不再是上市公司登记发行的纸质凭证，成为了上市公司在中央证券存管系统的电子账目，实现了证券登记与交易无纸化。

二是互联网、移动互联网提升证券行业服务能力。信息技术自从诞生以来就对证券行业产生了影响，从早期的以储存和信息传递为主到现代计算机技术、通信技术与证券业的全面结合。近年来，随着移动互联网、智能终端、大数据、云计算等一系列战略性 ICT 技术从趋势走向主流应用，使得移动互联网从一种技术演变为人们生活的环境，人们希望便捷、快速、无缝地获得针对自己的个性金融产品，享受全天候服务。越来越多的投资者有通过手机、平板电脑等移动终端随时随地接受金融理财服务的需要。如今，股民网上炒股、手机炒股普及率大幅提高，绝大多数证券公司网络开户占比超过九成，部分证券公司互联网平台佣金占比超过一半[61]。伴随移动互联网技术的发展和应用的普及，这一比例在全球范围内还将继续提高。客户资产的“碎片化”、交易的“高频化”、券商营销服务的“离散化”成为当前移动互联网证券业务呈现的新特征。

[61] http://www.sac.net.cn/hyfw/hydt/201708/t20170801_132435.html.

三是在大数据分析、机器学习等创新技术应用的基础上，证券行业在客服、交易、咨询、风控等流程的智能化程度不断提升，智能投顾（Robo-Advisor）模式在国内外市场蓬勃兴起。除了字面意思上的投资建议功能之外，广义上的智能投顾还涉及投资组合管理服务，结合客户风险偏好和预期收益目标等信息，通过算法实现对客户资产的配置、管理和优化，部分智能投顾还可进行交易执行，是一种综合性、自动化、定制化的投资理财资产管理服务。智能投顾服务模式诞生于 2008 年，自 2011 年开始在美国等市场发展速度显著加快。通过智能投顾开展投资管理是财富管理市场的重大突破。与传统投顾模式相比，智能投顾具备透明度较高、投资门槛和管理费率较低、用户体验良好、个性化投资建议等独特优势，对于特定客户群体吸引力较高，呈现出用户数量和市场规模不断增长的趋势。

6.2 传统证券的行业痛点

由于私募证券登记、股权关系协议采用纸质文件或者依赖第三方机构，导致私募证券管理成本高、效率低。

一是证券登记一般采用第三方公信力机构和纸质文件。证券可以登记在具有公信力的第三方权威机构，例如政府部门、公共组织或大型企业等，这些机构能够保证登记或权益变更信息的真实性和一致性，利用自身公信力提供证券权属证明。在没有第三方公信力机构的情况下，由于纸质版文件不易被篡改更具有可信度，因此一般采用纸质文件而非电子文件。

二是非上市公司股权关系大都采用纸质协议。国内上市公司股份是登记在中国证券登记结算公司，能够保证整个系统交易后账目轧平而不会出现“双花”问题。而对于非上市公司的股权（股份）登记，是纸质文件与第三方公信机构结合的方式，一方面由公司自己置备股东名册来记载持股人，一般采用纸质文件形式，股东名册属于公司内部经营管理文件，针对公司内部发挥法律效力；另一方面，向公司登记机关（一般是工商部门）登记股东信息，在对抗公司以外第三人发生效力。除股东名册的股东外，其他股权关系一般采用纸质协议的形式。例如，对于公司股权代持的情况，实际与名义出资人之间往往仅通过股权代持协议确定存在代为持有股权或股份的事实。三是纸质证券管理繁琐、规范性较差。非上市股权管理需要通过人工处理纸质股权凭证。一方面，如果出现频繁的股权变更，股东名册的维护将变得繁琐，历史交易的维护和跟踪也变得困难。另一方面，由于在公司发展过程中存在股权私募、股权众筹、员工持股等多种股权关系，股权相关协议类型复杂多样，股权管理成本高，并且可能出现股权关系不明确的情况，容易出现股权纠纷。

在公募证券方面，交易结算过程涉及多个参与方，流程较长，同时有些环节需要人工参与，导致整体效率低、成本高。

一是证券交易结算效率低。传统证券交易需要经过资产托管人、证券经纪人、银行和中央登记结算机构才能完成，系统之间兼容性低、处理方式各异，整个流程效率低。例如，美国股票市场长期实行的是 T+3 清算结算周期（根据美国证监会发布的最新规定，已把 T+3 日的周期缩短为 T+2 日）[62]。目前，我国 A 股市场的交易的交收周期是 T+1。

[62] https://www.sec.gov/news/press-release/2017-68-0.

二是证券交易需要人工干预。当一笔交易涉及多个参与方时，每个参与方都须保存各自的交易记录，而各个不同交易记录版本可能会导致误差或不一致，如交易方向、头寸、到期日等等。为统一各个参与方对交易的确认意见，往往需要对交易记录进行人工核对和调整。

三是证券交易成本高。根据 SWIFT Institute 的研究，全球金融市场每年用于证券清算交收、担保品管理、托管业务的费用高达 400 亿至 450 亿美元[63]。借助区块链技术降低单位成本，将换来显著的规模效益。

6.3 区块链在证券领域的应用场景

当前证券体系结构最大特点是有中心化的第三方信用或信息中介机构作为担保，帮助人们实现价值交换。作为一种信息技术的新型模式，区块链技术具有共识机制、不可篡改等特性，能够实现互联网从中心化信任到弱中心化的转变，这给证券行业带来了新的可能。私募股权管理、公募证券发行交易可以通过区块链技术被重新设计和优化。

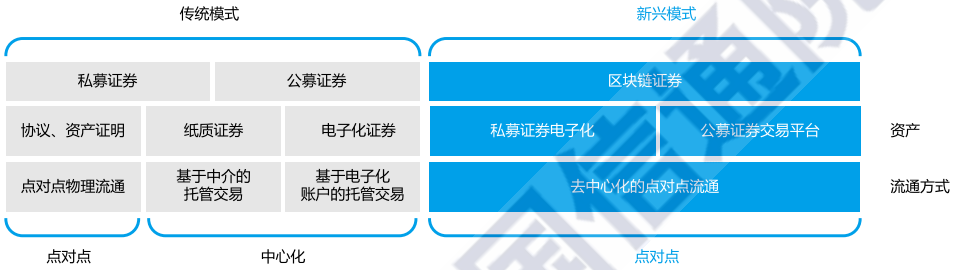

图 7 证券资产形式与流通方式的变迁

6.3.1 私募证券的电子化

未上市公司的股权，目前往往是通过协议（工商部门等第三方登记）、资产证明（例如股东名册、股权证等）或者纸质证券来证明资产的所有权。针对这一点，区块链可以在不改变私募证券流通规则的基础上，替代纸质文件作为证券资产的自治电子化载体，实现私募证券的登记和流通。

私募证券的电子化是未来发展趋势。证券登记是证券发行人建立和维护证券持有人名册的行为，具有确定或变更证券持有人及其权利的法律效力，是保障投资者合法权益的重要环节，也是规范证券发行和交易过户的关键。从历史发展的趋势来看，股东名册与记载其他类型信息数据的账本一样，只要技术手段允许，必然会朝着无纸化和非人工化的方向发展。例如公募证券登记的电子化，在 20 世纪 60 年代之前，在证券交易所上市发行的股票采用纸质股票和人工手动记账方式进行交易，后来随着上市公司的增多和股票发行交易频次的快速增加，上市公司在中央证券存管系统的电子账目，实现了证券登记的无纸化。区块链可以采用分布式账本记录股权信息，作为股权登记的电子凭证，在不依赖第三方公信机构的情况下实现证券登记的无纸化。同时，充分利用区块链账本的安全透明、不可篡改、易于跟踪等特点，记录公司股权及其变更历史，使股权登记证明更加高效可信，具有重要意义。可依托工商协会等组织采用区块链联盟链进行私募证券登记管理，例如美国纳斯达克交易所与区块链公司 Chain 合作建立的 Linq 区块链平台，为非上市公司提供私募股票管理服务。基于区块链的私募股权管理具有以下特点。

[63] The Impact and Potential of Blockchain of the Securities Transaction Lifecycle. SWIFT Institute Working Paper NO. 2015-007, May 2016.

一是具有合规性。无论是《公司法》还是其他法律法规，均没有对公司自行维护的股东名册的表现形式作出任何特定限制。公司可以自己选择采取任何有成文纪录的形式来创建并维护股东名册，因此采用区块链实现股东名册的电子化具有合规性。

二是更易实现规范化。公司证券通过区块链实现电子化之后，除了股东名册信息，公司股权私募、股权众筹、员工持股等多种股权关系也可以记录在区块链分布式账本中，同样具有不易篡改、可追溯的特点，可作为股权关系的唯一凭证，使公司证券管理更具完备性、规范性。

三是体现了公司自治精神。区块链对私募证券登记管理在本质上把削弱了提供公信力的第三方主体的功能，证券登记、交易不必经过特定的第三方主体，而是靠参与者全体来共同维护一套登记系统。而从所实现的功能上来看，区块链一方面将记录的权利交给了公司自己，体现了自治的精神，另一方面也能确保信息纪录的公开、透明及真实性，使权利争议最小化。

在具体应用方面，纳斯达克的 Nasdaq Linq 平台在业界具有一定代表性。纳斯达克在拉斯维加斯举办的 Money20/20 会议上，正式推出其基于区块链技术的产品 Nasdaq Linq。Linq 是一个私人股权管理工具，能够展示如何在区块链技术上实现资产交易，客户可以查看证券历史发行记录，并且能够转让证券。2015 年 12 月，纳斯达克公司的合作伙伴 Chain 成为了其 Linq 区块链技术的第一个用户[64]，并向一名私人投资者发售股份时使用了这项技术，ChangeTip、PeerNova 等企业也使用 Linq 平台参与股权交易。纳斯达克已在其全球超过 100 家市场运营商客户端开设了区块链服务器，以此作为纳斯达克金融框架的一部分。同时，Nasdaq 为“区块链交易记录系统和方法”申请了一项区块链应用专利，旨在作为一种方式用于简化交易后归档流程。

此外，全球资管巨头北方信托（Northern Trust）与 IBM 合作运行一个私募股权区块链平台，为瑞士资产管理公司 Unigestion 提供服务[65]，并于 2018 年 3 月与四大会计事务所之一的普华永道合作推出一项新工具，方便私募股权基金审计人员快速访问存储在其私人区块链上的数据[66]。

6.3.2 公募证券发行交易平台

与私募证券不同，公募证券登记、发行、交易、清结算业务发展比较成熟。但相关方在清结算环节存在多方对账的效率问题，区块链作为一种分布式账本技术，可以提供一种证券清结算的解决方案。在区块链分布式记账模式中，每个市场参与者都有一份完整的市场账本，共识机制保证证券登记在整个市场中同步更新，保证内容的真实性和一致性，在没有中央证券存管机构的情况下，实现交易结算。在区块链上通过建立智能合约让证券变为数字化智能资产，智能合约将规定参与者的权利和义务，以计算程序的方式实现执行自动化，再次降低人工操作成本。

一是货银对付降低违约风险。证券交割和资金交收被包含在一个不可分割的操作指令中，交易同时成功或失败，实现货银对付并降低因一方违约另一方受损的风险，违约风险的减少也会降低其他风险出现的可能。

---

[64] Nasdaq Linq enables first-ever private securities issuance documented with blockchain technology, http://ir.nasdaq.com/releasedetail.cfm?releaseid=948326

[65] Northern Trust and IBM pioneer use of blockchain technology to help transform private equity administration, https://www.northerntrust.com/about-us/news/press-release?c=70b5ba1adc9928f9977162844c34f57a

[66] Northern Trust strengthens private equity audit via blockchain technology with PwC, https://www.northerntrust.com/about-us/news/press-release?c=e2c653df01fd5f65cd9b42445ed7d5ef

二是增强分布式账本保障系统安全。证券结算不再完全依赖中央登记结算机构等中央对手方，每个结算参与人都有一份完整账单，任何交易可在短时间内传送至全网，分布式账本保证了系统安全性，可有效降低中央对手方单点失败的风险。

三是简化中介、简化结算流程。区块链技术将减少中介、简化结算流程，实现“交易即结算”模式。现有证券结算制度业务流程长，冗长的结算流程导致更久的资金占用和更多的风险敞口，基于区块链技术的分布式登记结算系统，可降低系统风险和成本，提高结算效率。

四是智能合约将证券变成智能资产。股票的分红派息、股东投票、禁售限制等可以程序化、自动化实现，尽最大可能地减少人工操作。

在具体应用方面，Overstock 公司开发出基于区块链股票交易平台 T0，于 2015 年 12 月获得美国证券交易委员会（SEC）批准，可以在区块链平台 T0 上公开出售股票，并于 2016 年 12 月利用区块链 T0 平台成功发行 190 万美元股票[67]。目前 T0 只能用来交易 Overstock 的股票，未来该平台可能会开放“定制功能”，上线其它公司的股票。与此同时，各大证券交易所在现有的证券平台基础上，积极探索区块链在证券交易结算中的应用。比如，澳大利亚证券交易所 ASX 与区块链技术初创公司 Digital Asset Holdings（DAH）合作，开发基于区块链技术的登记结算系统[68]。美国存管信托和结算公司 DTCC 也与 DAH 合作推进区块链解决方案，进一步改善回购市场清算流程[69]。2016 年 11 月，日本交易所集团 JPX 成立联盟，推进区块链技术在资本市场基础设施领域的概念验证测试[70]，联盟成员包括三菱 UFJ 银行、瑞穗银行、乐天证券、大和证券、日本证券存管中心等市场主体，以及日本银行、日本金融厅、日本证券业协会等相关机构[71]。

6.4 挑战与思考

证券区块链处于发展初期，具有一定的发展空间，但也存在诸多问题与风险。既有技术本身不成熟引发的风险，如区块链的安全性和不可变更性，也有现阶段应用可能导致的合规风险，如证券区块链新的模式可能不符合现有法律和监管规定。

一是区块链在证券领域的应用模式有待探究。在区块链上实现私募证券的电子化管理，虽然并没有改变对变私募证券流通规则，但与原有的纸质管理体系在管理流程、法律操作等方面还是存在很大差异。而利用区块链改造公募证券清结算流程后，证券清结算流程不需要经过中央存管机构，可能改变或削弱中介机构的部分作用。但美联储研究观点认为，清结算领域仍需必要的可信中介机构[72]。因此，不管是私募证券还是公募证券领域的应用，由于区块链弱中心化、多中心化的特点，在出现市场摩擦的情况下会产生由谁界定责权、如何界定等新问题。随着证券领域区块链项目不断尝试、问题和方案积累，将不断完善应用体系，实现真正的落地应用。

---

[67] Overstock.com Announces Rights Offering Including Blockchain Shares on t0 Platform, http://investors.overstock.com/mobile.view?c=131091&v=203&d=1&id=2215653

[68] ASX selects Digital Asset to develop distributed ledger technology for the Australian equity market, https://www.asx.com.au/documents/asx-news/ASXSelectsDigitalAssetHoldingsLLC.pdf

[69] DTCC and Digital Asset to Develop Distributed Ledger Solution to Drive Improvements in Repo Clearing, http://www.dtcc.com/news/2016/march/29/dtcc-and-digital-asset-to-develop-distributed-ledger-solution

[70] Launch of Consortium and Proof of Concept Testing for Capital Market Infrastructure Utilizing Blockchain Technology, https://www.jpx.co.jp/english/corporate/news-releases/0010/20161130-01.html

[71] Participants in Proof of Concept Testing for Utilization of Blockchain / Distributed Ledger Technology in Capital Market Infrastructure, https://www.jpx.co.jp/english/corporate/news-releases/0010/20170317-01.html

[72] 美联储发布研究报告《支付、清算与结算领域的分布式账本技术》，认为支付、清结算领域仍需必要的可信中介机构，以解决无法通过分布式账本技术解决的市场摩擦。现阶段，大部分机构倾向于将分布式账本技术整合进现有的系统和机制中 .

二是区块链不可变更性需要与证券市场进行调和。记入区块链的信息不能被删除更改，是区块链重要的技术优势，但绝对的不可变更性也有待商榷。证券业务活动中，由于行业、企业、个人的需求，在一些场景下需要变更，例如由于个人操作错误或监管司法要求需要撤回，个人执行被遗忘权删除数据。对此，也有一些区块链技术针对不可变更性进行了研究改进，例如埃森哲推出了 “可编辑”区块链原型，允许被授权方在不打断整个区块链的前提下编辑、重写或删除前面区块的信息[73]。未来，在不同领域的应用场景中，可能需要制定特定的可编辑规则来满足实际需要。

三是区块链弱中介化面临行业机制的大调整。传统模式下，证券中介服务机构承担着识别风险、防范风险的职能，维护市场的有序运行，因此被称为资本市场的“看门人”[74]。证券中介服务机构的职责包括但不限于：为发行人提供承销、保荐、财务顾问等服务，对发行人开展尽职调查、改制辅导等工作，帮助发行人建立公司治理制度，形成规范运作体系，督导发行人及时披露信息、揭示风险；为投资者提供经纪代理、投资顾问等服务，履行了解客户、投资者适当性管理、投资者教育与保护等义务；为交易各方提供证券登记保管、清算交收服务等。与传统模式有很大不同，区块链提供了市场参与方直接对接的技术基础，承销、经纪、登记、清算、交收等服务可能会被弱化，取代以其他差异化功能和能力。例如，券商投行业务转型方向是弱化承销和资源获取能力，强化为投融资客户提供专业证券咨询服务的能力。

[73] Accenture Debuts Prototype of ‘Editable’ Blockchain for Enterprise and Permissioned Systems, https://newsroom.accenture.com/news/accenture-debuts-prototype-of-editable-blockchain-for-enterprise-and-permissioned-systems.htm

[74] 刘志云，史欣媛 . 论证券市场中介机构“看门人”角色的理性归位 [J]. 现代法学 ,2017,39(04):94-106.

第七章 保险

保险领域中的区块链应用特点鲜明，基于区块链的智能合约特性研究开展智能保险产品，基于区块链的公开透明特性研究开展互助保险与再保险业务，通过技术手段解决保险信任问题。

7.1 保险的发展历程

保险是投保人根据合同约定，向保险人支付保险费，保险人对于合同约定的可能发生的事故因其发生所造成的财产损失承担赔偿保险金责任，或者被保险人死亡、伤残、疾病或者达到合同约定的年龄、期限等条件时承担给付保险金责任的商业保险行为。

按照保险标的的不同，保险可分为财产保险和人身保险两大类。按照与投保人有无直接法律关系，保险可分为原保险和再保险。发生在保险人和投保人之间的保险行为，称之为原保险。发生在保险人与保险人之间的保险行为，称之为再保险。我国保险业经历了开端、恢复、高速发展这三个阶段。

中国保险业的开端。1865 年我国第一家保险企业上海义和公司保险行成立，打破了外国保险公司对中国保险市场的垄断局面。1875 年李鸿章授意轮船招商局在上海创办我国第一家规模较大的保险招商局，成为我国保险业发展的里程碑。之后，我国的保险业才获得了一定的发展，到 1925 年，我国先后设立的保险公司达到 70 多家，但业务量中的 80% 以上又被外资在华保险公司所垄断。1949 年新中国成立后，中国人民保险公司成立，受中国人民银行领导和监管。从 20 世纪 50 年代后半期起，我国保险业进入长时间的低谷状态。

中国保险业的恢复阶段。1979 年国务院批准逐步恢复国内保险业务，保险业仍由中国人民银行监督管理。1992 年美国友邦保险公司把保险代理人制度引入中国，加快了保险业的步伐。1995 年，新中国颁布并实施了第一步《保险法》，使保险业终于拥有了法制保障。同年，中国人民银行成立保险司，专司对中资保险公司的监管。随着银行业、证券业、保险业分业经营的发展，国务院于 1998 年批准设立中国保监会，专司全国商业保险市场的监管职能。2000 年保费规模增加到 1595 亿元，保险行业成为中国发展最快的行业之一，保险的法制建设也逐步走向了正轨。

中国保险业的高速发展阶段。在加入世界贸易组织之后，2002 年保费收入与 2000 年相比翻了一番，达到了人民币 3053 亿元，中国保险业进入高速发展阶段[75]。近年来，得益于经济稳定增长、社会财富持续积累、人口结构变化和政策红利等因素，消费者购买保险的能力和投保意愿不断提升，我国保险市场业务规模保持快速增长。根据国家统计局的数据，2013-2017 年期间，我国国内生产总值（GDP）年均复合增长率为 8.57%，同期，根据保监会数据，我国保险行业原保险保费收入的年均复合增长率为 20.72%。单以保费收入规模计算，2016 年我国保险市场已经成为亚洲第二大、全球第三大保险市场，但从全球可比口径来看，我国 2016 年保险密度（人均保费）和保险深度（保费 /GDP）仍低于全球平均值[76]，仍有较大的发展空间。

[75] 王乐 . 浅析保险行业的发展历程及未来趋势 [J]. 商情 ,2014,(36):191.
[76] http://institute.swissre.com/research/overview/sigma/3_2017.html#tab_2.

7.2 区块链在保险业的应用场景

7.2.1 优化传统保险流程

当前，保险业内仍然存在着消费误导、理赔效率低、行业信息无法共享等问题，保险业外也存在骗保骗赔、对保险不信任等问题，成为制约保险行业可持续发展的瓶颈问题。

一是运营成本高昂。传统保险业是由一系列人为操作驱动的，从报价到投保申请、从承保到合规审核、从出单再到第一时间损失通知等等，每个环节都需要人的参与，导致成本高昂。此外，保险公司要接触大量用户，花费在用户身份认证上的成本也很高。

二是保险公司面临骗保的损失巨大。保险的基石是信用，保险业的痛点则是信息不对称，现代保险在审核费用上花的成本占总成本的 30% 甚至 40%，虽然在法律上规定了保险业诚实信用原则，并引入保险诈骗罪罪名，但骗保骗赔问题仍然是保险业的长期困扰。

区块链技术具有防篡改特点并且能够在此基础上实现智能合约，可以用来优化保险业务流程。一方面实现用户信息一致性管理。保险公司可提供用户信息区块链，经过审查验证的用户将信息写入区块链，购买不同保险时无须重复输入个人信息，在区块链上查询即可，缩短投保时间。另一方面实现自动理赔。将区块链与智能合约结合，一旦达到特定出险条件，即可快速理赔，一旦智能合约被触发，自动支付赔款，更好地保障保险消费者权益，增加客户满意度。此外，减少人为错误，节省劳动成本，为再保险业者节省 15% ~ 20% 营运费用[77]。

7.2.2 助力相互保险发展

相互保险组织内的投保人和保险人具有对等性特点，区块链在相互保险领域具有较大应用潜力。根据 2015 年发布的《相互保险组织监管试行办法》，相互保险是指具有同质风险保障需求的单位或个人，通过订立合同成为会员，并缴纳保费形成互助基金，由互助基金对合同约定的事故发生所造成的损失承担赔偿责任，或当被保险人死亡、伤残、疾病或达到合同约定条件时给付保险金。

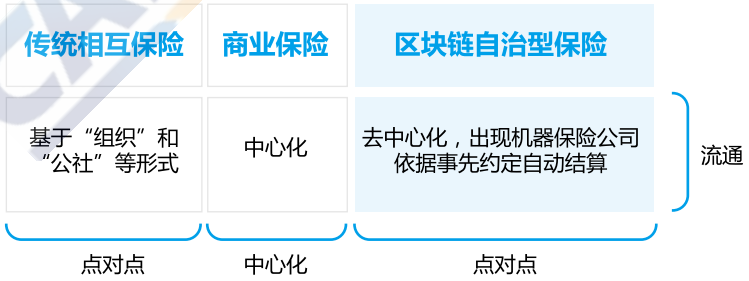

图 8 相互保险的发展变迁

[77] 曾于瑾 . 区块链在保险行业的应用现状与未来 [J]. 清华金融评论 ,2017(12):21-23.

从全球保险制度发展来看，相互保险是基于熟人社会的“组织”或“公社”的形式，是基于社交关系的信任模式，也是点对点（非中心化）的模式。后来随着陌生人社会的形成，逐渐发展成为公司模式的商业保险，这就需要依靠保险中介，用户需要预先向保险中介缴纳保费，再按照合同约定进行事后分摊，这是中心化模式，存在两方面的问题：运作不透明，可能存在平台虚构互助事件套取用户资金的问题；相互保险赔付流程缓慢，效率低下。

区块链技术的出现为解决上述问题提供了方案，为构建非中心化的信任模式提供了一种新的可能。基于区块链平台开发的网络互助应用，能够最大化地保证资金、协议、信息的绝对安全，提高风险控制能力。

首先，基于区块链的相互保险平台资金流向透明。所有资金流向明细都在区块链上记录，数据不可伪造和篡改确保了数据的真实有效，所有监管单位、公众媒体、普通用户都随时可以查看和监督。

其次，区块链网络规则执行高效。当保险事件发生并满足保险合同的赔付条件时，区块链上的智能合约将自动启动赔付程序完成理赔，确保保险合同在“代码即法律”的框架下自动执行，无法进行中途干预，大幅减少了人工操作，提高保险理赔业务效率，降低成本。所有的资金划转按照公开的、不可篡改的智能合约执行，一旦确定就能够精确无误的执行，无法人为挪用或干预，提升了规则执行效率。

第三，透明度提升。通过区块链的多方验证的交互式平台，能够促进保险平台提升内部监管和外部监管的透明度，交易参与者在各个节点都可以对保险业务并进行参与和审批，成为其中一个节点的监管者对相关技术和平台进行维护，进一步强化监管的技术能力。

7.3 区块链在保险业的应用现状

国际上，五大保险业巨头安联保险（Allianz）、荷兰全球人寿保险（Aegon）、慕尼黑再保险（Munich Re）、瑞士再保险（Swiss Re）和苏黎世保险（Zurich）联合组建区块链研究组织联盟 B3i [78]，旨在为保险公司提供交流平台，探讨区块链对提升保险行业效率的作用。

发达国家及大型企业纷纷布局区块链研究及应用。2017 年 7 月，以美国为基地的国际性跨国保险及金融服务机构巨头美国国际集团（AIG），与英国渣打银行、IBM 公司签订合作协议 [79]，完成了基于区块链和智能合约的跨国保险测试，将在英国、美国、肯尼亚、新加坡签订的保单整合进智能合约，实现保单信息实时共享 [80]。2016 年 9 月，日本最大的财产保险公司之一 Sompo 与 Soramitsu 公司联合开发一款针对自然灾害以及其他灾难事件相关的保险衍生品的区块链原型系统 [81]，该系统通过智能合约创建实现实时共享数据的服务，正确快速地执行保险流程中的每一个步骤，从衍生产品风险整合管理到决定是否支付索赔，以及执行程序支付赔偿金。普华永道推出针对伦敦保险市场目标运营模型（Target Operating Model /TOM）创新交易的区块链概念验证项目 [82]，通过区块链技术降低成本，加快专业保险业市场里的付款流程，该验证方案会在为期 6 周的时间里为伦敦保险市场加强索赔过程中参与各方之间的交互，包括第三方管理机构、理赔审批员和经纪人等。

[78] https://b3i.tech/about-us.html
[79] https://cointelegraph.com/news/aig-issues-first-insurance-policy-based-on-blockchain-technology.
[80] AIG, IBM, Standard Chartered Deliver First Multinational Insurance Policy Powered by Blockchain , https://www-03.ibm.com/press/us/en/pressrelease/52607.wss
[81] Sompo Embarks on Use of Blockchain Technology for Derivative Products, https://www.sompo-hd.com/~/media/hd/en/files/news/2016/e_20160926_1.pdf
[82] PwC blockchain prototype reduces costs for London insurance market claims, https://www.pwc.co.uk/press-room/press-releases/pwc-blockchain-prototype-reduces-costs-for-london-insurance-market-claims.html

我国保险业也在积极布局区块链技术，联盟、传统保险机构、互联网公司纷纷踊跃开展区块链的研究和应用。

上海保交所 2017 年联合 9 家保险机构搭建 10 个节点，组成了小型联盟链，开展区块链数据交易技术验证[83]。其中，各家保险机构分别作为交易及验证节点，保交所作为管理节点。在验证过程中，保交所选取了 3 套主流区块链底层框架，并着重对性能和安全两方面进行了定性定量的测试。其中 1 套区块链方案在保交所云平台的处理能力可达每秒 300 次交易 (300TPS)，基本满足了商用化系统对于性能的要求。在安全方面，通过数据存储加密、数据传输加密和许可型授权的区块链方案，确保了商业交易中对数据安全性的要求。

各个保险公司陆续推出区块链保险应用。阳光保险于 2016 年推出具备区块链特性的微信保险卡单“飞常惠”[84]，将区块链应用在航意险这样的小众险种上。众安科技于 2017 年 5 月开发了基于区块链技术的“安链云”平台[85]，并在云端搭建了保险核心系统，将保单、客户及理赔等信息放到去中心化的区块链上。

总体来看，传统保险行业因为渠道费用高，更看重区块链技术带来的流通属性提升。而新型的互助保障行业，因为缺乏监管机构，行业公信力不足，更注重区块链不可篡改带来的存证作用。

7.4 挑战与思考

在保险领域，区块链应用面临用户隐私、行业共享机制不完善、标准缺失和监管政策风险等问题。

一是用户隐私和数据安全问题。保险行业数据包括健康、财富、家庭等各个方面信息，涉及个人隐私，是在利用区块链开展传统保险业务优化以及相互保险创新的过程必须要关注的问题。

二是需要建立保险行业共享机制。保险行业相关机构的数据共享是未来需要解决的关键问题，通过探索保险行业信息共享机制，利用区块链技术建立健全风险评估、信息、信用体系，整合行业资源，增强反保险欺诈能力，切实维护保险消费者合法权益。

三是面临标准缺失问题和监管风险。一方面区块链保险标准处于探索阶段，保险行业的区块链标准是属于“真空地带”。另一方面，二是区块链保险面临政策监管挑战。区块链将改变传统保险的商业模式，不仅给保险监管带来全新的方法和工具，也将改变监管环境，带来新的挑战。同时，创新模式如互助保险还没有得到官方机构的认可，保监会称相关的互助计划没有政策的监管，在财务稳定性和赔偿给付能力上没有充分保证。

[83] 保交所 + 区块链 首攻“保险征信” ——上海保交所“联盟链”成功通过技术验证，https://www.shie.com.cn/art/2017/3/31/art_19_482.html
[84] 阳光保险应用区块链技术打造全新保险卡用户体验，http://xw.sinoins.com/2016-08/02/content_203894.htm?bsh_bid=1468473650
[85] 众安科技发布“安链云” 构建区块链经济模型，http://cases.anlink.com/?p=91

第八章 征信

现代金融体系的运转，离不开信用的支撑。征信作为信用体系中的关键环节，奠定了金融信用风险管理的基础。大数据时代来临，互联网金融兴起，面临新形势，传统征信业中信用信息不对称、数据采集渠道受限、数据隐私保护不力的问题愈加严峻。区块链以分布式存储、点对点传输、共识机制与加密算法等技术，屏蔽了底层复杂的连接建立机制，通过上层的对等直联、安全通信和匿名保护，加速打破“信息孤岛”的行业坚冰，加快各行业信用数据的汇聚沉淀，加强用户数据的隐私保护，以低成本建立共识信任，以新模式激发行业新业态、新动力，在征信领域有着广阔的发展前景。但是，区块链也存在私钥丢失或泄漏、对用户数据“被遗忘”、现有信息系统管理建设条例和征信监管体系等不适应的问题，区块链应用于征信领域的实践之路任重而道远。

8.1 用户征信的发展历程

我国征信业以企业征信为主，个人征信有待发展，整体市场前景广阔。我国企业征信发展较早，市场较为成熟，截止到 2017 年 10 月，我国完成备案的企业征信机构为 137 家[86]。2018 年 1 月 4 日，中国人民银行受理了百行征信有限公司（筹）（以下简称“信联”）的个人征信业务申请，百行征信由中国互金协会和腾讯征信、芝麻信用、前海征信、拉卡拉征信、中智诚征信、中诚信征信、鹏元征信和华道征信等 8 家征信公司共同筹建。截至 2017 年 5 月底，央行征信中心金融信用信息基础数据库收录了 9.26 亿自然人、2371 万户企业和其他组织的相关信息[87]。但央行征信中心仅覆盖个人在银行机构的信用记录，个人征信维度相对单一，存在巨大的市场需求和发展空间。

大数据融入传统征信正成为趋势。2015 年 7 月国务院印发《促进大数据发展行动纲要》，2015 年 9 月国务院办公厅印发《关于运用大数据加强对市场主体服务和监管的若干意见》，从国家政策方面鼓励大数据在征信业的应用和发展。大数据征信具备覆盖群体广泛、信息维度多元、解决方案丰富和评估全面四个创新特点，以大数据为依托和支撑构建征信体系，可提高信用评价的全面性、实时性和授信效率。信联的成立有望化解各家征信机构的信息孤岛困局，促进构建社会信用体系建设，用户的负债数据可以在各个机构之间共享，互金平台和企业依托这些数据与自身的原有数据进行融合分析，更容易形成完备的大数据风控系统，为用户提供更加全面、清晰、安全的金融业务，提升整个互金行业安全，意义重大。

[86] https://www.creditchina.gov.cn/xinxigongshi/jinronglingyu/201710/t20171021_74625.html
[87] 中国人民银行：金融信用信息基础数据库已收录 9.26 亿自然人信息，http://www.gov.cn/shuju/2017-06/20/content_5204079.htm

8.2 传统征信的行业痛点

数据缺乏共享，征信机构与用户信息不对称。征信机构与征信机构、征信机构与其他机构等缺乏有效的共享合作，信息孤岛问题严重，无法实现征信业内高质量的数据流通及交易，造成征信机构与用户信息不对称。征信机构间信息孤岛问题严重，金融业内信贷机构、消费金融公司、电商金融公司等机构的海量信用数据尚未发挥其应有的价值，金融业外信用信息割裂在法院、政府部门、电信运营商等机构手中。究其原因，主要是我国数据归属权尚未确立，处于隐私保护的顾虑，各机构宁愿握紧手中的数据画地为牢，没有额外的积极性进行数据交换共享。除体制机制原因外，传统征信业也由于技术架构的问题无法在各机构、行业间安全地共享数据，使得传统征信工作中数据孤岛障碍的问题迟迟得不到解决。

正规市场化数据采集渠道有限，数据源争夺战耗费大量成本。信用数据不同于其他行业数据，所属用户是最为重要的数据标签，涉及到企业和个人的切身利益，因而无法通过传统数据交易平台进行共享交换，导致正规市场化采集信用数据渠道极其有限。传统征信机构通过自爬、合作、购买等方式，主动对接相关的部门与机构，从有限的场景中整合数据，抢占征信业发展的高地与先机。因此关于数据源的竞争尤为激烈，这也直接使得传统征信机构在采集数据上耗费了大量成本，导致用于数据分析及征信产品研发的资金比例缩水，征信机构无法过多关注征信产品的质量，继而影响了征信机构的水平与信誉。

数据隐私保护问题突出，传统技术架构难以满足新要求。大数据时代下的征信业对隐私保护和数据安全的要求更高。此外，“暗网”中的个人信息交易灰色产业链，以其多样性、隐蔽性与复杂性成为监管部门查处的痛点与难点。为此，中国人民银行征信管理局明确指示要加强隐私保护，要求征信机构采集使用用户信息应当经信息主体同意，并明确告知可能产生的影响等事项，信息主体有权要求征信机构将其纳入拒绝用于营销的范围内。然而，传统征信系统技术架构对用户的关注度较低，并没有从技术底层保证用户的数据主权，难以达到数据隐私保护的新要求。

8.3 区块链在征信领域的应用场景

区块链具有去中心化、去信任、时间戳、非对称加密和智能合约等特征，在技术层面保证了可以在有效保护数据隐私的基础上实现有限度、可管控的信用数据共享和验证。针对目前我国传统征信行业现状与痛点，区块链可以在征信的数据共享交易领域着重发力，例如面向征信相关各行各业的数据共享交易，构建基于区块链的一条联盟链，搭建征信数据共享交易平台，促进参与交易方最小化风险和成本，加速信用数据的存储、转让和交易。

平台节点成员包括征信机构、用户、其他机构（互联网金融企业、银行、保险、政府部门等），平台主要的共享交易模式有两种：一是征信机构与征信机构共享部分用户信用数据，二是征信机构从其他机构获取用户信用数据并形成相应信用产品，如下图所示。

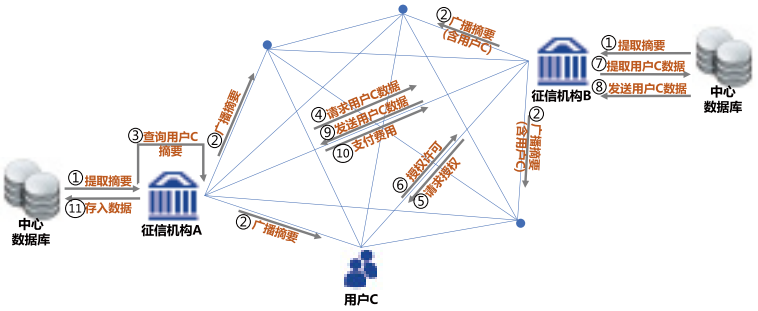

图 9 征信机构间共享用户信用数据

第一种模式下，征信机构各方参与者是主要参与节点，既作为数据查询使用方，也作为数据提供方。征信机构 A、B 原始数据均保存在自己的中心数据库，①从中提取少量摘要信息，②通过区块链广播，保存在区块链中。征信机构 A 对用户 C 的信用数据有查询需求时，③首先查询自己所在节点中公开透明的摘要信息，匹配到征信机构 B 的摘要信息含用户 C，④则查询请求可通过区块链转发到征信机构 B。⑤征信机构 B 向用户 C 请求授权，⑥用户 C 向征信机构 B 许可授权后，⑦征信机构 B 向中心数据库申请用户 C 的信用数据。⑧中心数据库返回用户 C 的信用数据，⑨征信机构 B 向征信机构 A 发送用户 C 的信用数据。⑩征信机构 A 向 B 支付费用后，⑾将用户 C 的信用数据存入自己的中心数据库。这样征信机构各方既可以查询到外部征信机构的信用数据，又不泄漏自身核心信用数据。

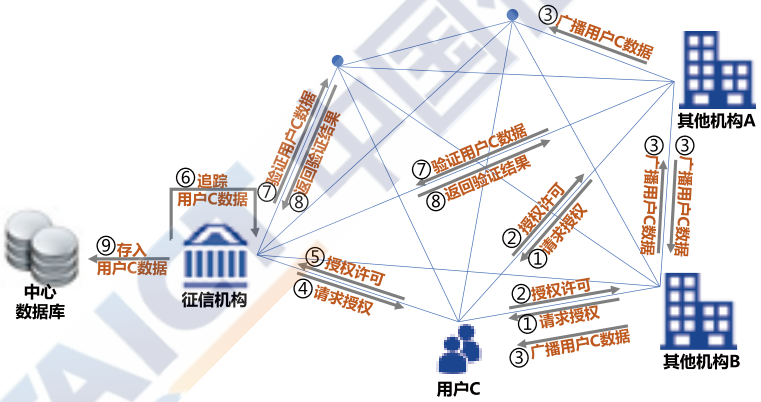

图 10 征信机构从其他机构获取用户信用数据

第二种模式下，①其他机构 A、B 向用户 C 请求授权，②经过用户 C 授权许可后，③将各个环节关于用户 C 的数据进行广播添加到区块链中，在链上显示的这些数据只有用户 C 的地址属性，并不会泄露用户隐私。④征信机构向用户 C 请求授权，⑤经用户 C 授权许可后，在自身节点中对这些数据进行追踪，获知用户 C 过往的贷款记录、还款记录、逾期记录、当下大致的债务情况等数据。⑦⑧征信机构在区块链中验证得到数据的真实性，⑨存入中心数据库，继而对其信用状况进行分析判断。该模式中信用数据是可以多源交叉验证的，因此数据真实性有所保证，且无法被企业或者个人篡改。

基于区块链的征信数据共享交易平台，解决了传统征信业的痛点，是征信业革命性的创新。场景中区块链可以帮助多家征信机构实现数据资源不泄露前提下的数据多源交叉验证与共享，信贷客户多头负债的问题得到了根本的解决，数据交易成本、组织协作成本也将大大降低且有利于打破行业坚冰。不仅如此，场景中区块链基于数据确权，重构了现有的征信系统架构，将信用数据作为区块链中的数字资产，有效遏制数据共享交易中的造假问题，保障了

信用数据的真实性。

实现数据共享与协作，打破“信用数据孤岛”。该平台能帮助用户确立自身的数据主权，生成自己的信用资产。在信用确权的基础上，以用户作为数据聚合点，该平台可连接各个企业及公共部门，进而开展用户数据授权，就可以解决数据孤岛的问题，同时又确保用户隐私安全及各方源数据不对外泄露。该平台有助于征信机构作为一个网络节点，以加密的形式存储及共享用户在本机构的信用状况，从而实现信用资源的共享共通、共建共用。

实现系统维护与业务拓展，大大降低征信运营成本。该平台有助于征信机构以低成本方式拓宽数据采集渠道，并消除冗余数据，规模化地解决数据有效性问题，还可去除不必要的中介环节，提升整个行业的运行效率。另外，区块链可以使信用评估、定价、交易与合约执行的全过程自动化运行与管理，从而降低人工与柜台等实体运营成本，并能大幅提高银行信用业务处理规模。

保障系统安全，实现数据隐私保护。该平台中每一个完整的节点都参与了系统的维护，不会由于系统中的某一个组件发生问题而影响全局。只要不超过51%的节点出现问题或是遭遇恶意袭击，系统就可继续稳定运行下去。另外，并不是所有的数据都要跑在“链”上，也并不是所有的数据都是公开透明的，除了数据共享交易参与的各方，不会有任何第三方可以获得数据。

8.4 区块链在征信领域的应用现状

目前，我国正积极将区块链技术探索应用于征信领域，包括新兴金融科技、新兴民营征信及保险在内的金融行业企业与机构，探索测试基于区块链的征信系统，意在解决传统征信业的痛点。整体来看，区块链的实践应用集中在解决信用数据的交易问题。

公信宝于2016年将区块链技术结合到征信行业中，深度研发基于区块链技术的“公信宝数据交易所”。公信宝数据交易所是一个通用的数据交换平台，底层是基于区块链（公链）打造的一条联盟链，面向的典型客户为互联网金融企业、政府部门、银行、保险等。公信宝主要通过数据爬虫产品负责在用户授权下抓取用户数据，覆盖泛金融、泛电商、泛社交、个人身份等多种维度数据，为各大银行、互联网金融公司等机构提供征信基础数据服务，交易过程中公信宝会对交易双方进行匿名处理，并实现数字资产的所有权认证以及有效遏制数据交换中的造假问题[88]。

同样地，区块链技术服务商布比于2016年与征信企业甜橙信用达到战略合作[89]，旨在通过区块链去中心化的互助协作、全网记账体系，构建普惠式的征信体系，利用区块链的共识机制建立开放式的信用。双方设计的区块链征信解决方案是，存入区块链的数据部分公开可见，有需要的用户可以通过搜索找到需要的数据并向数据所有商购买。该方案将解决数据提供商之间信任难和交易难的问题，减少数据交易的程序和成本。

总体来看，目前区块链在征信业的实际应用还较少，主要还是浅层的概念性探究。已有探索的案例以信用数据的交易共享为切入点，不过这种技术层面的设计与现有的征信业体制机制及从业者观念不甚一致，区块链在征信业的落地应用长途漫漫。

[88] 公信宝数据交易所产品白皮书，https://github.com/gxchain/whitepaper/blob/master/zh/dataExchange-whitepaper.md
[89] 甜橙信用与布比达成战略合作 共同打造区块链征信平台，http://www.01caijing.com/article/4709.htm

8.5 挑战与思考

重构的征信系统直击传统征信业的痛点，虽然目前的应用场景主要集中在数据交易共享、打破数据孤岛方面，但是区块链在征信领域的应用前景值得期待。值得关注的是，传统征信业在征信系统和基础设施方面耗费了大量资源，传统系统与新系统的过渡和衔接存在较大的成本替代风险，区块链在征信业的实际应用也将遭遇较大的挑战。

用户“被遗忘”的权利与区块链无法篡改的特性存在本质矛盾。根据我国 2013 年 3 月 15 日实施的《征信业管理条例》第十六条，“征信机构对个人不良信息的保存期限，自不良行为或者事件终止之日起为 5 年；超过 5 年的，应当予以删除。”也就是说，如果采用区块链来记录个人的征信记录，也同样需要保存 5 年以内的信用信息，同时删除超过 5 年的不良信用信息。然而，区块链的结构就是依托密码学算法，实现一个环环相扣、无法删除的数据结构，这就导致了用户“被遗忘”的权利在实施过程中将遇到较大的技术挑战。因此，如何在区块链系统中确保用户不良信用信息的及时删除，仍需重点研究和实践证明。

CAICT 中国信通院

第九章 区块链金融应用的挑战与监管

9.1 金融领域区块链应用所面临的挑战

金融行业目前处于区块链技术研发的早期阶段，在技术成为金融领域实际应用的解决方案之前，仍有来自以下几方面的挑战需业界共同探讨解决。

9.1.1 商业挑战

一是成本收益。区块链应用中挑战之一是如何确定适当的应用场景，实现投资成本和潜在收益之间的平衡。此外，与现有或其他替代技术相比，区块链运营的长期成本是否具有比较优势，需结合具体应用案例进行对比评估。

二是网络效应。网络效应是指网络中每一个新增用户都将提升现有用户的效益。由于缺乏足够数量的参与者，网络中早期应用者的净收益往往是负的，导致应用率较低。区块链能否在金融领域有广泛应用，取决于是否有足够数量的参与者采用该技术，许多参与者将网络效应作为影响技术应用和普及的关键因素。成立行业联盟，推动相关领域沟通合作，有助于解决网络效应带来的挑战。

9.1.2 技术挑战

一是可行的技术解决方案。在开发和应用中，区块链需实现足够的处理规模和互联互通性，以满足金融市场的需求。（1）可扩展性：美国的支付、清结算系统每天需处理数亿笔交易，共识算法和加密验证带来的延迟和处理笔数上的限制对系统运行效率带来一定挑战。此外，账本中不断添加的交易数据也对系统存储能力提出更高的要求。这些问题部分可通过共识算法等机制的设计得以缓解。另外，电子支付技术也应具备可扩展性，以提供快速、可靠的服务。（2）互联互通性：行业主体普遍认为，未来市场中可能同时存在多个区块链方案，而部分原有系统可能也将继续运行。随着不同系统之间的连接和应用的复杂程度的不断提升，新旧系统并存客观上也增加了复杂性和碎片化程度，系统之间的互联互通性，将成为决定技术应用和普及中的重要因素。系统运营商之间的协调、沟通有助于解决这些挑战，而标准化的 API 和互联互通协议也可作为新旧系统衔接的桥梁。

二是标准化。标准对于建立不同系统的底层互联互通性而言是重要因素，开放的行业标准有助于降低应用和整合成本，并确保区块链构建和访问方式的一致性。由于目前区块链应用仍处于开发和测试阶段，行业缺乏充分信息以建立适当的通用标准。此外，通过 API 的应用，机构可以在不进行大幅改变 IT 结构的前提下，实现区块链方案的运营，建立行业通用的开放 API 标准语言，有助于降低进入区块链领域的门槛。

三是密钥和访问数据管理。在区块链方案中，对密钥和访问证书的有效管理是尤为重要的问题。与其他加密技术的应用不同，对于区块链技术而言，如果密钥或访问证书遗失或损坏，用户将遭受即刻无法挽回的财产损失，且没有救济和追索措施。维护私钥的私密性并实现公钥加密的安全性，是较为复杂并具有挑战性的任务。在密钥的使用和密钥管理系统的设计方面，标准制定组织和监管机构出台了指引和最低要求。将这些指引和要求应用于区块链方案，是技术推广和应用中的重要环节。除密钥管理问题之外，部署区块链的市场主体还需考虑信息安全问题。

四是信息管理。区块链的参与者在账本中共享信息，且几乎不可能对信息进行更改，因此确保共享信息的正确性是系统运行的重要基础。如果许多参与者都可以在账本中进行记录，则很难确保信息的正确性。此外，区块链设

计者还需决定如何处理和解决错误和欺诈问题。另一个挑战来自于确定哪些信息可以在账本中共享，特别是当参与者之间存在竞争关系时。参与者需就信息共享范围形成一致意见，并确定是否需中心化机构保管账本完整信息。此外，信息管理还需符合隐私方面法律法规的要求。

9.1.3 金融设计挑战

区块链的应用可能带来金融工具模式的转变，以及在某些情况下引发对金融中介功能定位和必要性的探讨。

一是金融工具。一些市场主体正考虑将区块链引入证券交易流程中。在设计模式上，需确定证券是否直接向最终持有者发行，或是通过中介机构持有和交易证券。区块链应用可能对传统证券的设计、持有和流通带来新的问题，比如“代币化”概念的出现，以编码数据代表证券资产，实现账本中的证券交易。证券仍为最终发行人的负债，而代币不等同于证券，也不代表证券所承载的债权债务关系，因此代币的定位成为了新的问题。另外，在区块链中，各银行维护自己的账本，实现客户之间直接支付，无需通过银行发送支付指令。当交易涉及多个银行，客户需进行跨行支付时，需建立机构间的交易结算机制，而传统的跨行结算需通过专业化金融中介实现。

二是金融中介。传统监管框架规定了哪些机构可以发行债务，哪些机构可以作为中介机构，并为发行和交易体系的安全、高效运行，设计了相关机制和规则。部分观点认为区块链可能淘汰金融中介机构。长远来看，金融市场中中介机构的作用、职能和需求将会发生变化，但金融中介在资金供需双方的匹配、提供安全金融工具等方面，仍发挥着重要作用。金融中介的职能和作用是否会随着新兴技术的应用而逐步淘汰，从目前的市场结构来看仍存在较大不确定性。

9.1.4 风险管理挑战

区块链的应用也对原有的风险管理框架带来了新的问题。根据目前金融市场结构，这些风险集中于银行、金融市场基础设施等中介机构。因此，中介机构成为风险管理和控制中的核心主体，通过中心化治理结构建立有效风控措施。对任何区块链方案的应用和评估，需考虑其是否会带来风险在市场主体间的传导，或导致市场整体风险的提高。

一是法律问题。在未来的区块链应用场景中，应充分考虑法律框架可能发生的变化。

（1）区块链中各要素的法律基础：随着区块链的日益成熟，部分技术构成要素的法律基础，尚未涵盖在目前的金融法律框架中，需市场主体仔细考量。一是账本中同步并向参与者公布的记录，其法律效力如何认定，是否可以作为确定基本义务和履行义务的依据；二是与数字代币和数字资产相关的权利义务关系，在现行法律框架中并未明确界定，需通过详细分析确定法律适用问题；三是智能合约的执行需具备健全的法律基础。合同法确立了合同订立、修改、终止和争议处理等领域的基本原则，其中一些经典原则与智能合约的自动执行相冲突。

（2）牌照问题：区块链的出现可能引入新的市场主体，进一步扩展现有市场结构。部分新兴市场主体是技术或软件公司，一些通过与金融中介机构开展合作，开发区块链；另一些则可能取代金融中介的部分业务。对于从事传统金融中介业务的新兴企业，可能需获得某些类型的牌照或许可，才能从事资产交易相关业务。牌照或许可的性质和形式仍未明确，是沿用现有金融机构牌照类型，或是发放新的牌照类型。在加密货币领域，纽约州金融服务管理局颁发的比特币牌照是为提供比特币服务的机构发放新牌照的例子。在区块链方案中，中介机构从事金融资产的存储、记录和交易业务，不涉及贷款等传统银行业务，可考虑对这类机构发放特殊银行牌照。

（3）反洗钱（AML）合规：遵守反洗钱（AML）要求是银行、货币服务商和券商等各类金融中介机构的义务。

反洗钱合规包括交易监控、了解你的客户（KYC）要求。随着区块链的发展，以及金融中介类型的变化，相关政府机构需就法律适用问题提供指引。FinCEN 曾就虚拟货币交易所适用银行保密法的相关问题发布指引。

二是治理问题。为确定功能、风险管理、网络接入方面的规则，以及由哪些主体负责维护和修改协议，区块链方案中仍需健全的治理机制。治理机制根据区块链的设计而有所不同。开放和“无需许可”系统可能需要分布式治理模式，使用共识算法确定网络协议或功能的更改。但目前仍不清楚这种治理模式能解决多少重大问题，或是否需要对重要规则进行调整。缺乏明确性、透明度和可预见性的治理机制，尤其在开放和“无需许可”的区块链中，将会对网络以及金融系统稳定性产生负面影响。

9.2 金融领域区块链应用整体监管状况

在后比特币时代，大多数国家和地区对区块链技术的其他应用呈现开放态度。但区块链技术的不确定性和变革性对金融体系的冲击后果更难预测，尤其需要引导和规范。如何把握平衡，是每个监管者面临的难题。面对区块链金融的发展趋势，各国政府也积极的调整监管策略，与时俱进地摸索出适应本国金融科技发展的监管方式。主要有三大类：

（1）以英国、新加坡、香港等为代表的主动型监管

这些国家或地区金融体系成熟，有完善的征信体系、较为专业的金融人才队伍，但技术和市场处于相对劣势。为了发展区块链技术，形成后发优势，政府挺身而出成为主导力量。英国对区块链实行宽松的监管政策，鼓励深入研究区块链金融应用。英国金融业务监管局（Financial Conduct Authority，FCA）针对区块链金融的监管问题，提出“监管沙盒”（Regulatory Sandbox）项目，企业家们可以利用这一工具以及使用客户的“知情同意书”，在一个可监管的环境中实验他们的想法，进而鼓励初创公司进行该领域的创新。此外，英国即将推出区块链监管指引，进一步消除市场的担忧，鼓励创新。新加坡金融管理局（MAS）同样采取了开放的、鼓励创新的区块链金融监管政策。政府官方推出了“沙盒机制”，允许在沙盒注册的公司事先报备后开展与目前法律相冲突的业务，并保证未来不追究法律责任。香港金融管理局（HKMA）同样也致力于探索区块链技术，2016 年 11 月就分布式账簿技术发布白皮书并成立了一个配有高性能的计算资源和专业人才的金融科技创新中心。银行、支付服务供应商、金融科技企业和 HKMA 都能在此创新中心集思广益，以一种安全高效的方式测试及评估新的金融科技解决方案。

（2）以美国、澳大利亚等为代表的限制性监管

美国的人才优势和优越的资本环境，构建了良好的以技术创新为主要驱动力的金融生态。针对这样的特性，美国实行功能性监管，即不论区块链金融以何种形态出现，抓其金融本质，厘清该金融业务的实质，按照其功能纳入现有金融监管体系。美国银行监管机构货币监理署（OCC）发布了联邦宪章的“责任创新框架”，并将区块链科技纳入银行风险评估报告中。总体来说，美国对区块链金融的应用监管是相对比较严格的，监管以稳定为主。澳大利亚政府同样密切关注金融领域区块链行业的发展，官方组建了一个国际技术委员会，旨在创建区块链国际标准。但为了防止垄断，政府机构严格审查国内四大银行的区块链活动，大型银行在参与区块链项目之前必须先获得澳大利亚竞争与消费者委员会（ACCC）的批准，接受详细审查。

（3）以我国等为代表的适应性监管

和美国相反，我国的金融科技以市场和商业模式为驱动。国内巨大的市场需求和有待完善的现有金融服务体系，为区块链技术的发展提供了广阔的应用空间。但是，我国法律属于大陆法体系，对金融的监管需依靠成文的法律法规，故灵活性和时效性相对不足。目前，在没有建立适应金融科技特点的风险防范和监管体系情况下，我国针对区块链等金融科技的监管主要纳入互联网金融的监管框架下进行，采用适应性监管的策略。2015 年 7 月，国务院出台的《关于促进互联网金融健康发展的指导意见》，对我国互联网金融监管进行了基本规划，明确了鼓励创新和加强监管并行的监管思路。既提出了“鼓励创新、防范风险、趋利避害、健康发展”的总体要求，又强调了“依法监管、适度监管、分类监管、协同监管、创新监管”的监管原则。2016 年 10 月，国务院办公厅下发的《互联网金融风险专项整治工作实施方案》中要求，互联网金融应透过表面判定业务本质属性、监管职责和应遵循的行为规则与监管要求，实施“穿透式”监管办法，避免因监管规则不统一导致监管套利。

虽然互联网金融整体处于严厉整治阶段，但由于新一届政府鼓励创新的整体战略，我国监管当局对区块链金融发展整体还是比较包容的，监管初期采取较为宽松的“黑名单”策略。总体而言，我国的监管者更多的是处于观望的态度，属于被动型监管。

CAICT 中国信通院

第十章 结论与建议

总体来说，区块链技术在金融行业的应用仍处于逐步发展和演进过程中。区块链在金融领域的应用只是提供一种新角度下的、适用于资产权益证明的发放与流通环节的新型解决方案，目前来看区块链并未对金融领域生产关系产生颠覆性影响。目前，世界各国在区块链、分布式账本技术领域的研发进程持续推进，在金融市场中的概念验证项目不断涌现，结合我国相关领域的研究进展，提出以下建议。

（一）立足实际，扎实推进区块链技术应用型研究

区块链技术与金融市场的结合，现阶段还存在较多不确定性，有待于市场主体通过持续、深入的实践验证和分析研究加以论证。推进区块链技术应用研究，应关注以下三个层面的问题：一是突破技术自身瓶颈，包括数据处理和存储规模、系统之间的互联互通、技术标准化、信息安全和隐私保护等问题。二是与各类金融场景结合，将技术创新成果转化为实实在在的产业活动，真正为金融市场的提质增效和改革创新提供服务和支持。三是加强技术与金融复合型人才培养，鼓励相关企业设立高校实习和培训基地等，形成产学研相结合的联合培养机制。此外，在区块链应用发展过程中，应将“币”与“链”区分对待，区块链产业主体应增强自律意识，坚决杜绝如部分 ICO 项目打着“区块链金融创新”旗号，从事非法金融活动的行为。

（二）优势互补，着力促进产业主体的协调与合作

从技术研发到实际应用过程中，区块链产业容纳了大量不同类型的市场主体。主体类型的多样化，客观上增加了产业链的复杂性和协调难度，需探索建立顺畅、高效的沟通和协调机制。一是探索搭建政府与市场之间的政策传导和信息反馈桥梁，深化政府和企业多层面合作机制。部分中央银行的概念验证项目的成功部署，正是得益于技术联盟、金融机构、系统运营者、监管部门之间的密切合作。二是可通过行业协会、联盟等平台，推动产业链上下游主体联动与合作，加快产业整体的自主研发和创新能力，进一步解决网络外部性、互联互通、标准化等方面的问题。三是加强与国外产业主体的交流，探索开展多形式、多领域的双边或多边示范性项目合作，提升国际标准制定的话语权，实现我国金融科技创新的价值输出。

（三）及时跟踪，密切关注新兴技术对金融监管体系带来的挑战

作为金融科技的细分业态，区块链在金融领域的应用也应遵循金融业的核心原则与规则。“守住不发生系统性金融风险的底线”是金融领域的永恒主题，也是习近平新时代中国特色社会主义思想在金融领域的根本要求。现阶段，由于缺乏先例、长期实践不多，区块链技术可能对金融体系带来的风险和挑战，仍具有较大的不确定性，难以预判。因此，一方面，应结合相关产业实践，深入研究新兴技术对现有金融市场结构、风险管理模式、监管及法律框架产生的影响。另一方面，适时为区块链技术的应用提供必要的法律基础，明确现有法律和监管规则的适用性问题。此外，金融科技全球化发展的趋势，对建立一致的监管体系提出了全新的要求[90]。我国应加强与各国金融监管主体及国际组织的协调，积极开展合作，在区块链技术的国际监管协调领域发挥积极作用。

[90] 徐忠，孙国峰，姚前，等．金融科技：发展趋势与监管 [M]. 北京：中国金融出版社，2017:355-356.

CAICT 中国信通院

金融区块链研究报告

CAICT 中国信通院

中国信息通信研究院 腾讯研究院
联合课题组