

区块链基础设施 研究报告 (2022 年)

中国信息通信研究院工业互联网与物联网研究所

2022 年 7 月

版权声明

本报告版权属于中国信息通信研究院，并受法律保护。
转载、摘编或利用其它方式使用本报告文字或者观点的，
应注明“来源：中国信息通信研究院”。违反上述声明者，本
院将追究其相关法律责任。

前 言

如果把以太坊主网上线时间界定为区块链基础设施启动的原点，那么这项历程已经过近七年时间。包括星火·链网、区块链服务网络 BSN、欧盟区块链基础设施 EBSI、印度国家区块链框架 NBF 等，多个国家和地区的重大工程先后启动节点建设和应用探索，其他各种公有链网络和跨链系统项目更是多达数百个，足可见全球各国和产业界都高度重视构建这一信任和价值的新基础设施。

中国信息通信研究院工业互联网与物联网研究所在去年首次编写并发布《区块链基础设施研究报告（2021 年）》。今年的蓝皮报告在上一版基础上，跟踪研究了全球区块链基础设施实践的最新进展，分析技术、应用、路径的发展态势，希望能够有助于产业界和学术界凝聚共识，更好地发挥区块链作为基础设施的作用和功能，为技术和产业变革提供创新动力及指导建议。

特别是过去的一年，全球范围对 Web3、元宇宙等数字原生空间的技术研究、产品研发、应用探索大幅加速。在新的网络空间内，从体系架构设计的初始阶段，就充分考虑信任底座的内生建设，更容易得到各方认可支持。同时，数字原生空间内部的经济理论模型已经发生改变，依赖于对数据要素的确权、交互、交易等基本支持和数字身份、数字资产等基本单元，也就迫切需要借助区块链基础设施在传递价值和管理信任等方面的功能。我们相信，随着区块链技术持续性改善，数据要素的市场化价值将不断得到发挥，区块链基础设施将有力支撑传统产业数字化转型和数字原生空间探索！

目 录

一、区块链基础设施概述	1
(一) 基础设施框架逐步稳定，部署与接入方式丰富	1
(二) 基础设施属性持续增强，政府与产业支持提升	5
(三) 基础设施能力拓展延伸，成为 Web3 核心底座	7
二、区块链基础设施发展路径的交织与演化	8
(一) 开源社区驱动的生态化路径：形成事实性标准规范	9
(二) 分域节点建设的网络化路径：规模网络需较长周期	12
(三) 行业应用优先的业务化路径：受业务场景影响较大	14
(四) 公共服务引导的平台化路径：跨链实际需求在改变	15
三、区块链基础设施技术创新	16
(一) 处理能力：单链交易的并发量取得突破	17
(二) 交互能力：服务平台的用户友好性提高	18
(三) 上链能力：接入终端的可信安全性增强	19
四、区块链基础设施应用实践	19
(一) 数字藏品	20
(二) 数据流通	21
(三) 双碳交易	23
(四) 供应链金融	24
(五) 产品溯源	25
五、总结与展望	27
(一) 网络信任底座是一项复杂的系统性工程	27
(二) 基础设施建设与应用创新趋于同步开展	28
(三) 数字原生空间将带来更直接的发展需求	28

图 目 录

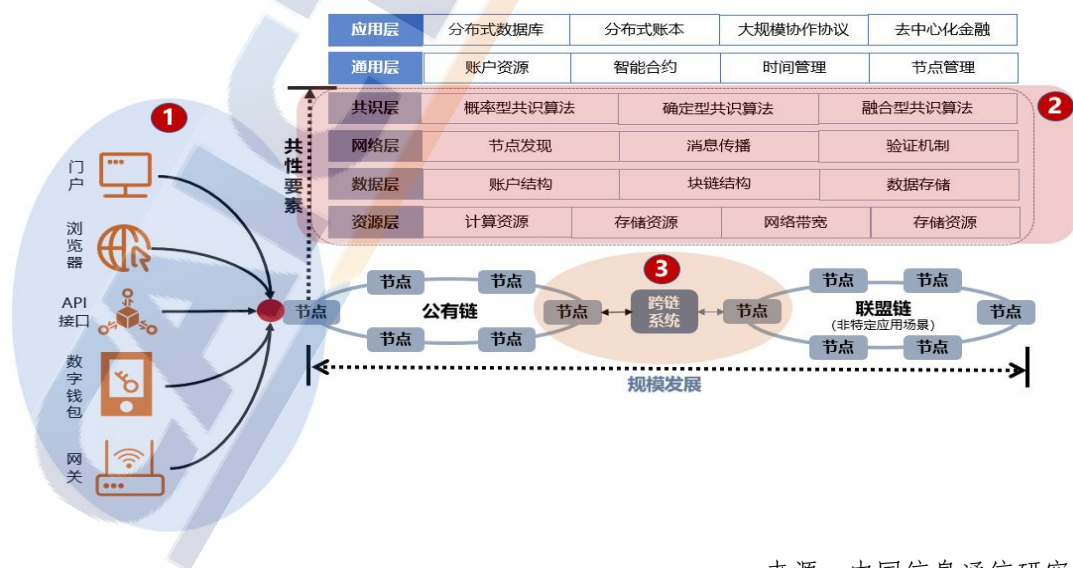
图 1 区块链基础设施框架	1
图 2 主要区块链基础设施的接入方式统计	2
图 3 区块链基础设施部署模式分类	3
图 4 区块链基础设施跨链发展历程	4
图 5 区块链基础设施项目投资占比	6
图 6 历年区块链基础设施项目投资数	6
图 7 历年区块链基础设施项目投资金额	6
图 8 区块链基础设施发展路径演进趋势	9
图 9 依托公有链模式的全球区块链基础设施数量增长趋势	10
图 10 区块链社区开发者月活跃人数增长趋势	11
图 11 区块链社区开发者新增人数增长趋势	11
图 12 区块链社区开发者新增人数增长趋势	11
图 13 星火·链网数字原生资产服务网络解决方案	21
图 14 RivTrust 数据要素确权流转平台的技术架构	22
图 15 Flowcarbon 技术架构及其解决方案	24
图 16 壹诺供应链金融平台技术架构	25
图 17 IBM Food Trust™的产品溯源功能模块与业务流程	26

一、区块链基础设施概述

区块链基础设施是由具有广泛接入能力、公共服务能力、可灵活部署的公共链网，及连接这些区块链的跨链系统组成的网络服务设施。狭义的区块链基础设施，是由遵循预定义共识机制的若干节点构成的分布式信任平台；广义的区块链基础设施，是面向数据这一新型生产要素，支持合规高效的数据要素流通和交易等市场化配置，从而推动构建大规模的可信协作网络。

（一）基础设施框架逐步稳定，部署与接入方式丰富

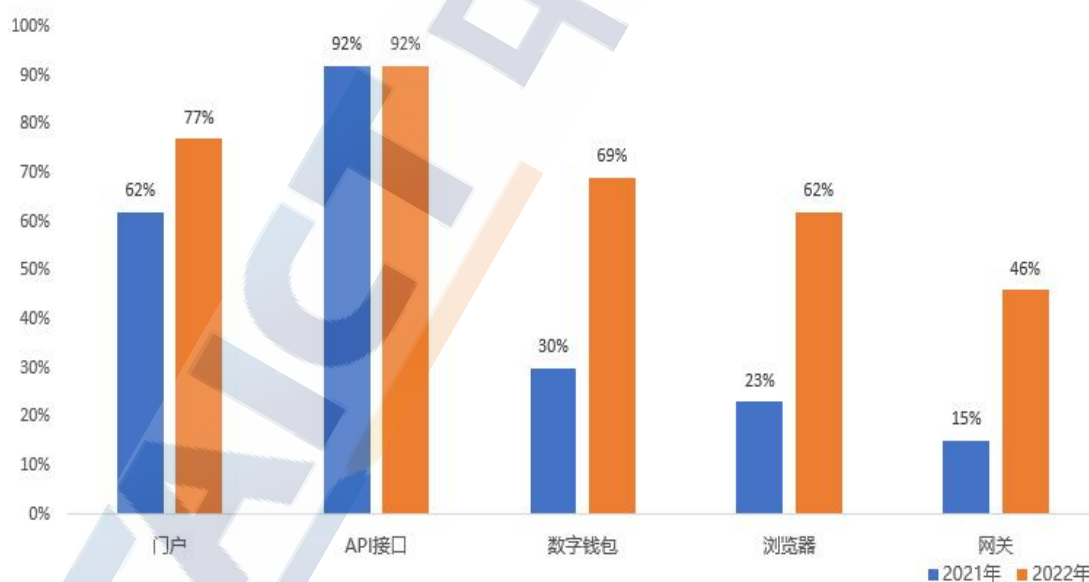
自《区块链基础设施研究报告（2021 年）》首次从垂直的“技术协议栈”和“水平的建设方案”两个维度梳理区块链基础设施组成要素以来，分布自治、跨链成网的区块链基础设施框架正趋于稳定。全球范围的区块链基础设施建设与运行实践普遍在节点接入方式上呈现多样化发展，在节点部署模式上重视简易化服务，在跨链系统建设中探索模块化方案。



来源：中国信息通信研究院

图 1 区块链基础设施框架

区块链基础设施接入方式多样化。**门户网站**为广大初级用户提供了解区块链资讯的渠道，同时可搭建区块链基础设施的信息集成入口；**API 接口**是众多资深用户及系统开发者构建去中心化应用的主要选择，通过提供程序调用的便利，仍然是区块链基础设施的系统开发入口；**数字钱包**逐渐脱离加密货币交易的单一功能属性，出现浏览器插件、手机 APP、硬件钱包等多种形态，正逐渐成为区块链基础设施的统一数字身份入口和一部分应用入口；**区块链浏览器**以其防止网络跟踪、避免恶意广告投放等特性发展迅速，被多数区块链基础设施的建设者和运行者作为重要的信息查询入口；**数据网关**通过融合多种通信协议、提供安全可信的数据缓存、计算、处理能力，成为区块链基础设施与企业信息化系统、实时数据采集设备以及其他网络数据源的连接器，未来有望成为区块链基础设施的数据连接入口。



来源：中国信息通信研究院

图 2 主要区块链基础设施的接入方式统计

区块链基础设施部署模式简易化。本地部署节点带来的成本问题，让众多开发者望而却步，一定程度限制了区块链应用发展和生态建设，因此简易化的节点部署方式受到社群高度关注。目前区块链基础设施部署模式主要分为集中托管和离散接入两类方式，均能够让开发者借助一系列通用功能组件和实用工具解决应用层问题，从而屏蔽底层的复杂度，快速搭建区块链应用。**集中托管方式**占比较多，如以太坊有超过 63% 的用户是通过统一的区块链开发平台 Infura 实现接入。该方式可以有效保障区块链节点运行的稳定性及可扩展性，通过提供 API 节点集群，让普通开发者无需在本地运行庞大的全节点就可快速接入区块链系统。**离散接入方式**则是为不同底层服务供应商制定接入标准并进行节点部署审核，帮助企业及开发者借助标准化的接口快速连接到不同区块链所对应的服务器，最终完成开发工作。因其统一的配置、统一的接口等标准化优势，逐渐得到众多服务厂商和用户认可。

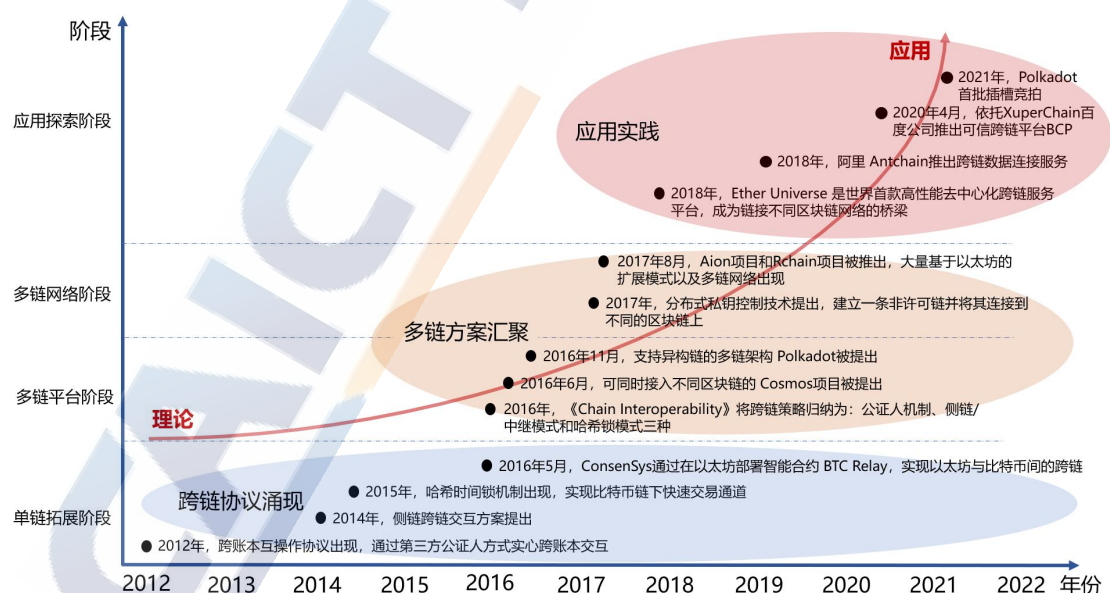


来源：中国信息通信研究院

图 3 区块链基础设施部署模式分类

区块链基础设施跨链系统模块化。跨链系统建设主要采用中心化或多重签名的公证人、侧链/中继、哈希锁、分布式私钥控制等四种技术方案，特别是中继技术已经逐渐发展成为最典型的跨链实现机制。随着跨链从技术研究走向产品化，并结合多链方案开展建设应用实践，逐渐形成了快速接入、平台接入、服务枢纽等三种常用的服务模式。

快速接入模式，通过构建三层跨链互操作架构（接入层、业务逻辑层、区块链层），基于可拆分、可流转的数字凭证，推动产业链企业开展合约化协同场景的跨域合作，提升跨链互操作效率；**平台接入模式**，借助侧链方案，将业务平台与区块链系统作为整体，通过跨链方式将平台交易信息存证到链上进行业务数据锚定，充分发挥基础设施提升业务数据可信度的作用；**服务枢纽模式**，基于可信跨链服务网关构建基础设施，可针对不同类型的链上业务参与方，以最小改动原则进行技术适配，满足各条异构链之间信息及资产跨链需求。



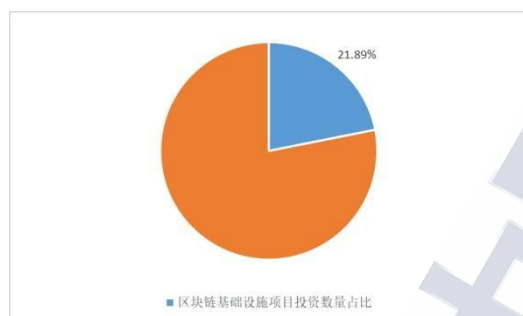
来源：中国信息通信研究院

图 4 区块链基础设施跨链发展历程

（二）基础设施属性持续增强，政府与产业支持提升

全球对区块链基础设施支持力度大幅提升。美国利用在全球金融和技术上的领先地位，希望继续引领全球区块链发展。美国拜登政府于 2022 年 3 月签发总统令，要求美国政府各部门研究区块链技术、数字资产发展与应用情况，分析其对美国金融、技术影响；美国国家科学技术委员会发布的《先进制造中的美国领导战略》和美国国防部发布的《国防部数字现代化战略》中均提到对区块链技术研究和基础设施建设的推动。欧洲注重区块链区域影响力和协同发展，重视数字身份的应用。欧洲区块链基础服务设施（European Blockchain Services Infrastructure, EBSI），已获得 30 个欧洲国家参与和支持，覆盖率超过 60%；2022 年 2 月，欧盟委员会发布《数字欧洲计划》”并宣布将继续推进 EBSI 服务创新、区块链标准和数字身份等。日本决心抓住 Web3 机遇，探索区块链基础设施建设带来的经济增长机会。日本首相岸田文雄于 2022 年 5 月发表声明,将区块链基础设施为技术支撑的新一代互联网框架 Web3 发展上升为国家战略，并于 6 月批准了日本《2022 年经济财政运营和改革的基本方针》，提出将努力为实现这样一个去中心化数字社会进行必要的环境改善。韩国政府则以元宇宙建设为起点，投资超过 1.77 亿美元启动元宇宙领域产业发展，韩国知名公有链 Klaytn 依托韩国最大科技公司 Kakao 转型成为全球领先的区块链基础设施。我国对区块链基础设施的支持力度持续增加，33 个省、市基于“十四五”规划中数字经济发展和区块链技术创新的指导方向，在资金、政策、产业、应用层面推出了一系列的政策支持。

面向区块链基础设施的投资规模持续加大。截止 2022 年 5 月，全球区块链投资机构累计投资 2897 个项目，投资金额达 658 亿美元。在投资数量方面，基础设施项目占全部区块链投资 22% 左右，其中 2021 年共有 285 次区块链基础设施项目投资，达到 2020 年三倍规模。在投资金额方面，2021 年投资为 75 亿美元，而 2022 年仅前 5 个月的投资就达到 90 亿美元，超过去年全年投资总额。在投资占比方面，a16z、Coinbase、Biance、Alameda Research、Multicoin Capital 等五家知名区块链投资机构都选择将基础设施视为重点投资领域。



来源：中国信息通信研究院

图 5 区块链基础设施项目投资占比



来源：中国信息通信研究院

图 6 历年区块链基础设施项目投资数



来源：中国信息通信研究院

图 7 历年区块链基础设施项目投资金额

（三）基础设施能力拓展延伸，成为 Web3 核心底座

随着全球区块链基础设施建设规模的不断扩展、运行能力的不断增强，其定位已经不仅局限于对原有互联网（包括产业数字化转型）在传递信任和管理价值等方面的能力补充，已经拓展延伸到 Web3、元宇宙等数字原生的新一代互联网探索。

Web3 是以太坊公有链和波卡跨链生态的创始人加文·伍德博士在 2014 年提出的新一代互联网框架。Web3 核心理念是通过新的协议和行动，让互联网更加去中心化、更加安全，让用户掌握自己的数字身份和数字资产，从而打破平台垄断，开启新的全球数字经济浪潮。目前，Web3 已初步形成包括设施层、协议层、能力层、应用层在内的四层功能框架。其核心是数字身份、数字资产、数字对象，底层将依托于区块链构建的分布式基础设施重塑存储、计算、通信、安全，以数字钱包为入口，接入网络并连接浏览、社交、媒体、游戏等不同领域的去中心化 Web3 应用。

元宇宙概念则是 1992 年诞生于科幻小说《雪崩》，被用于描绘一个庞大的虚拟现实世界。元宇宙的本质是在虚拟现实/增强现实、人工智能、区块链、物联网等多种技术推动下，与真实世界平行发展的虚拟数字世界。在当今数字经济重组全球要素资源、重塑全球经济结构、改变全球竞争格局的过程中，元宇宙作为一个扩展现实的数字原生空间，将会更加有利于发挥数据要素的价值、发挥数字技术的战略性变革作用。尽管元宇宙尚处于发展的初期阶段，但其核心技术、重要产品、典型应用、产业生态已经在形成。

一方面，区块链基础设施被视为构建 Web3、元宇宙的核心底座。Web3 提出对互联网架构去中心化和安全可信的变革创新，需要依赖区块链基础设施，以及在这样一个底层分布式框架上提供用户可自主管理的数字身份、可确权可交易的数字资产等共性能力。元宇宙未来所构建形成的虚拟数字空间中的各种虚拟数字人、虚拟土地和场所、虚拟服务和应用，也都需要依赖区块链提供对各种资源的存证。

另一方面，Web3、元宇宙加快促进区块链基础设施全方位发展。2021 年以来，全球 Web3 技术应用均呈现明显增长形势，Meta、谷歌、亚马逊、推特、eBay、奈飞、Paypal 等海外企业及阿里、腾讯等国内企业都在 Web3 领域开展了实际探索。Web3 应用规模快速发展，就对底层网络设施的服务性能、接口工具、交互方式、治理监管等提出了大量新需求，这也极大地促进了区块链基础设施的发展。

二、区块链基础设施发展路径的交织与演化

《区块链基础设施研究报告（2021 年）》总结提炼出四种发展路径以来，经过近一年多的发展，出现了一定程度的交织与新的演化。路径一是开源社区驱动的区块链基础设施生态化，得益于开源、开放等协作模式，吸引大批投资者和贡献者加入来共同促进社区生态繁荣，形成的标准规范得到全球事实性认可，为大多公众创新应用提供服务。路径二是分域节点建设的区块链基础设施网络化，多数由于整体规划庞大，前期容易受政策、资金、主体等方面较大影响，建设周期很长；但随着建设路径的逐渐清晰、网络规模的不断扩大，容易受到产业界的认可并与开展深度融合，在产业数字化转型中将发挥重要的作用。

路径三是行业应用优先的区块链基础设施业务化，大部分起点较高，但发展趋势受热点事件、热点场景的影响较大，容易受到业务局限性而无法清晰区分业务范畴，开始与路径一、路径二的项目形成整合。路径四是公共服务引导的区块链基础设施平台化，对跨链等共性技术的认识，容易受到其他已有设施实际运行的需求影响，所以多数跨链平台项目也在借助路径一发展方式加强主动话语权，同时部分路径二的实践在顶层架构设计中即与路径四开展了整合。



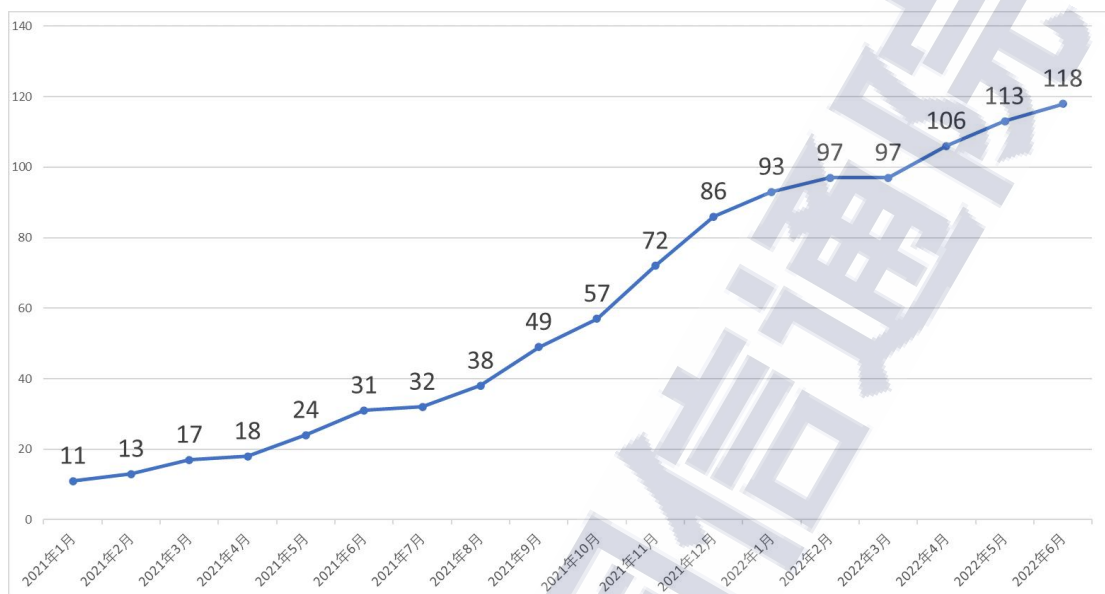
来源：中国信息通信研究院

图 8 区块链基础设施发展路径演进趋势

（一）开源社区驱动的生态化路径：形成事实性标准规范

一是开源社区扩展形成了多个阵营，多链共存成为趋势。大部分开源社区致力于依托公有链模式建设基础设施（例如以太坊社区）。截止 2022 年 6 月，全球公有链数量已达 118 条，较 2021 年初仅有 11 条主要公有链，数量超过 10 倍。少部分开源社区致力于依托联盟链模式建设基础设施（例如超级账本社区）或聚焦跨链公共服务模式开展建设（例如 Web3 基金会）。整体看，开源社区发展多元化，以太坊市场份额从 96% 下降至 62%，逐渐形成新的四大社区阵营，即包

括侧重生态兼容性的以太坊兼容链、侧重处理性能的技术创新链、侧重区块空间的二层扩容链及侧重互联互通的跨链协议生态链等。



来源：中国信息通信研究院根据 Footprint Analysis 数据整理

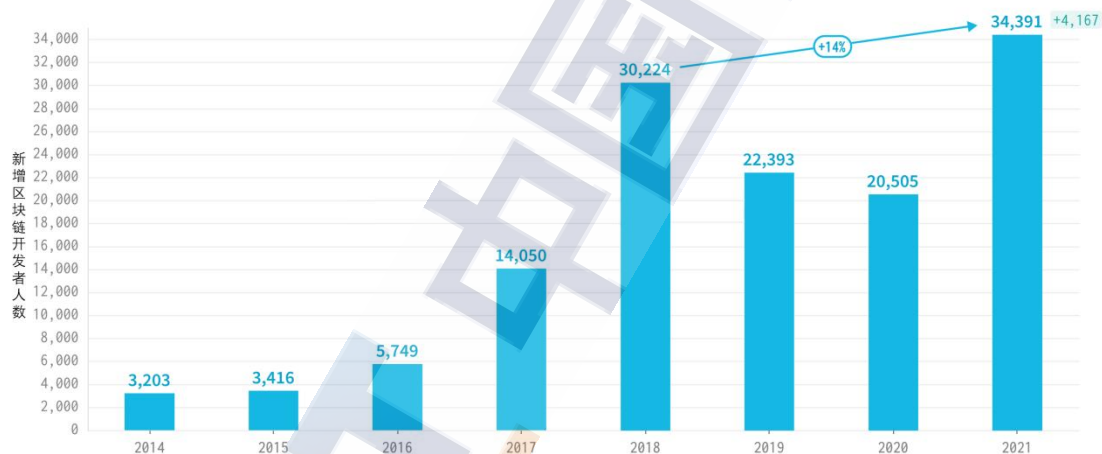
图 9 依托公有链模式的全球区块链基础设施数量增长趋势

二是开源社区开发者人数显著增加，活跃度保持新高度。不同于传统企业雇佣专职研发人员和运维团队的集中式项目建设方式，开源社区的组织协作模式天然契合了区块链去中心化的思想和基于共识算法的信任机制，更符合区块链基础设施项目的建设需求。根据全球最知名开源社区 GitHub 的数据统计，2021 年区块链社区开发人数和活跃度均达到了历史之最，新增 34391 名区块链开发者，月均活跃达到 18416 名（占比 53.5%），区块链基础设施项目开发活跃度增幅达到 68.6%，为全球区块链技术和产业发展形成了重要贡献。



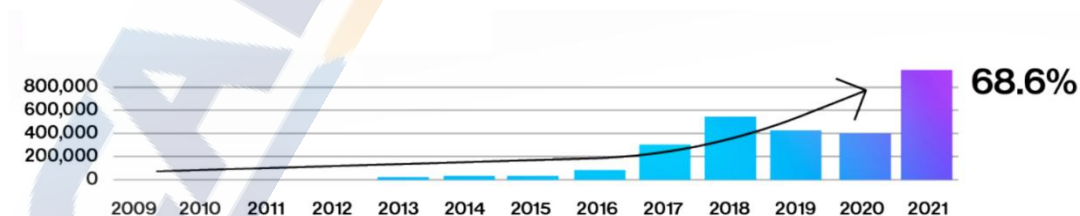
来源：Electric Capital《2021 区块链开发者报告》

图 10 区块链社区开发者月活跃人数增长趋势



来源：Electric Capital《2021 区块链开发者报告》

图 11 区块链社区开发者新增人数增长趋势



来源：a16z crypto

图 12 区块链社区开发者新增人数增长趋势

三是开源社区治理方案在逐步成熟，提案成为事实标准。大多数区块链基础设施项目已逐步形成开源社区治理机制，可通过提案投票等形式推行改进方案，来持续提升基础设施服务能力。如以太坊开源社区的改进提案（Ethereum Improvement Proposals, EIP）已评议超过四千多条标准提案，其中同质化通证标准（ERC20）和非同质化通证标准（ERC721）被很多开源社区广泛使用，成为事实性标准。

四是开源社区可稳定运行基础设施，部署模式存在差异。自 2015 年上线以来，在以太坊社区的努力维护下，以太坊区块链基础设施已稳定运行近 7 年，社区运行模式得到业界认可。但考虑到去中心化、安全性和性能之间的平衡问题，开源社区部署网络节点数量差异较大。如以去中心化和网络安全性为重心、致力于广泛服务的以太坊区块链基础设施，目前已建设记账节点 2048 个，验证节点超过 20 万个。而侧重交易性能、致力于为用户提供高效快捷服务的币安智能链，由于牺牲部分去中心化特性以换取更高的性能，目前只有 21 个验证节点。

（二）分域节点建设的网络化路径：规模网络需较长周期

一是分域节点建设重视顶层规划，工程建设周期较长。各国政府高度重视区块链基础设施对推动传统产业数字化转型和打造新型数字原生空间的战略意义，积极组织推动可覆盖本国或本地区的区块链节点网络，但此类重大工程的建设通常会被划分为若干阶段分步实施。例如“星火·链网”是在中国工业和信息化部指导与支持下，采用许可公有链模式建设的区块链基础设施，自 2020 年正式启动以来，目前完成部分超级节点、骨干节点的建设任务，初步覆盖了京津冀、长

三角等国内经济发展较快、信息化水平较高的区域。此外，欧盟委员会和 29 个国家（包括所有欧盟成员国、挪威和列支敦士登）共同推动建设的欧洲区块链服务基础设施 EBSI，自 2018 年正式启动以来，目前完成 36 个公共服务节点部署，覆盖超过 60% 欧洲地区，尚有节点处于建设阶段。

二是分域节点建设预期目标较高，多数需要追加投资。采用此类路径建设的区块链基础设施，多数由政府主导或委托专业研究机构和企业作为建设运营者，通常被定位于国家级重大工程项目，并在政府主管部门的组织下参与支撑产业数字化转型等经济社会的重要发展和科技革命的重要创新。但随着项目的实施和任务的调整，投资规模往往会不断增加。例如欧洲区块链服务基础设施 EBSI 的启动，是在 2019 年由欧盟委员会通过“欧洲互联设施”项目提供的 400 万欧元初始资金支持，随后欧盟委员会再次通过“欧洲地平线 2020”计划为 EBSI 技术供应商提供 620 万欧元资金支持。到 2021 年 11 月，欧盟委员会通过“数字欧洲计划”为 EBSI 提供 3800 万欧元资金支持，其中 EBSI 节点建设和区块链监管试验占 2200 万欧元，区块链应用服务占 1500 万欧元，区块链标准化工作占 100 万欧元。

三是分域节点建设能力不断外溢，跨境部署成为热点。受到全球新冠肺炎疫情和局部地缘政治冲突影响，跨境贸易成为支持经济复苏的重要动力，世界各国普遍希望发挥区块链基础设施在促进数据要素市场化配置、跨境数据流通等方面的能力。例如“星火·链网”在泰国、马来西亚等地部署境外节点，推动“一带一路”国家间跨境数据流通、

跨境贸易溯源等新模式。此外，乌克兰成为继挪威和列支敦士登之后，第三个除欧盟成员以外，加入欧洲区块链合作伙伴关系的国家，希望通过 EBSI 为战争冲突中的难民提供跨境庇护登记和援助等服务。

（三）行业应用优先的业务化路径：受业务场景影响较大

一是行业应用市场难以支持通用设施，缺少业务规模。在能源、通信等信息化水平高、基础条件好、应用场景多、市场规模大的领域，部分领军企业或第三方机构牵头建设区块链基础设施，以服务本行业为起点，逐步扩展至其它行业形成通用设施，已经取得了一些进展。例如国家电网公司已建成国内电力能源领域最大的区块链基础设施“国网链”，可实现绿电生产、交易、消纳等全过程信息上链，建立了安全共识、互信高效的绿电交易通道与绿电溯源机制，为电力数据安全流通和外部协同提供可信支撑。但在其他一些细分领域内，由于数字化转型的进程原因，急需传递信任和管理价值的应用场景并不多，使得独立建设和推动区块链基础设施的探索难以得到足够资源支持。

二是行业应用范畴受到原有业务限制，影响业务辨识。以区块链基础设施建设运营主体原先所在的优势业务领域逐步拓展到其他业务领域的设想，可能面临来自组织协作层面的信任危机。例如美国脸谱公司是全球知名的互联网社交巨头企业，但其试图以社交为起点，为全球金融交易构建统一的区块链基础设施 Diem，为超过 20 亿用户提供方便、快捷、安全跨境支付服务，打破现有金融体系格局的理想过于宏大。2022 年 1 月底，在金融监管和伙伴质疑的多重压力下，Diem 项目以被美国加州特许银行低价收购而宣告失败。

三是行业应用方向受到热点场景牵引，发生业务转移。相较于传统产业数字化转型面临的诸多实际挑战，构建全新的数字原生空间、探索轻量级的应用更容易取得快速进展。不仅选择行业应用优先路径推动区块链基础设施建设的主体，包括很多其他的建设运营主体，也纷纷开始投入更大力量支持数字资产、数字藏品等新的热点场景。如 2022 年 1 月，区块链服务网络 BSN 推出了分布式数字凭证基础网络 BSN-DDC，为数字藏品业务方和平台方提供安全可信、价格低廉的环境，用于数字藏品的生成和管理。2022 年 6 月，“星火·链网”也上线推出数字原生资产服务网络（Digital Native Asset, DNA），为不同的数字藏品平台提供统一的数字藏品注册、认证和查询等功能。

（四）公共服务引导的平台化路径：跨链实际需求在改变

一是跨链系统首先服务资产交易场景，稳定运行值得关注。跨链技术最早是美国瑞波公司于 2012 年首次提出的跨链转账方案。随后，Cosmos、Polkadot 等明星级跨链项目启动，使得跨链目标由资产扩展到数据和业务等深层次互操作。但由于加密数字货币应用占极高比重，实际上多数跨链系统和产品仍然是首先被应用于资产交易场景。例如知名跨链系统 Multichain 主要是针对支持以太坊虚拟机的区块链之间提供跨链服务，目前可支持近 40 条区块链超过 1721 种加密数字货币的资产转移。但服务于多条区块链的跨链系统通常由第三方运营，其基础设施属性和稳定运行能力没有得到足够重视，例如 2022 年 1 月 Multichain 跨链系统因安全漏洞被盗超 450 枚以太币，价值约 143 万美元；2022 年 6 月，Horizon 跨链桥系统被盗，损失超过 1 亿美元。

二是跨链技术可有效支持异构链接入，概念扩展值得认可。随着区块链应用探索的加快，全球各国都在积极开展区块链基础设施建设。考虑到技术、运营、治理等多方面的因素，多数基础设施的建设主体都认识到任何一条单链不可能完全满足全部业务需求，同时单链架构也难以同时满足高安全、高性能、高扩展等特点，很难在全球范围内保持区块链基础设施建设底层的单一性。因此，分布自治、跨链成网是现阶段构建基础设施的必然趋势，一大批项目实践都在架构设计中希望支持对多种不同底层技术框架的异构链接入。尽管“接入”强调南北向对接，而“跨链”强调东西向互通，但其技术本质十分相似。例如“星火·链网”正是基于对数字身份标识和数字原生资产的跨链服务，通过骨干节点，实现蜀信链、云洲链等不同异构底层链的接入。

三是跨链架构影响多数基础设施设计，运营模式值得思考。跨链技术的不断成熟、跨链产品的不断丰富、跨链理念与“接入”等需求的交织重叠，使得更多区块链基础设施运行主体开始关注跨链系统的建设，逐渐形成了跨链系统提供商模式和公有链自建等两种典型模式。例如波卡作为知名的跨链系统提供商，通过 Web3 基金会等社区组织，设计研发了可提供跨链互操作服务的平行链插槽，但实际应用有限，是否以产品形式交付其他区块链基础设施部署和运营值得思考。

三、区块链基础设施技术创新

垂直维度的区块链基础设施功能协议栈框架趋于稳定，技术创新的热点方向主要是进一步提高服务性能、加强交互友好性、增强可信安全性等。

（一）处理能力：单链交易的并发量取得突破

随着区块链应用逐渐扩展，不再局限于加密数字货币领域，而是向制造、服务、文化、能源等更多行业领域延伸，对基础设施底层链的处理能力也提出了更高的要求。单条区块链的并发性能通常用每秒传输的交易处理个数（Transactions Per Second, TPS）进行衡量，主要取决于共识算法及处理交易所涉及的全网广播和节点验证环节，这两个过程又与广播的传输效率和节点的处理能力有关。其中广播的传输效率由各个节点网络带宽决定，受限于通信技术；而节点的处理能力通常和节点计算性能有关。因此，可通过提高节点的计算性能和分割网络进行并行交易处理来提高单链交易的性能。

$$TPS = \frac{\text{区块交易数量}}{\text{区块产生时间}} = \frac{\text{区块链交易数量}}{\text{全网广播时间} + \text{节点验证时间}}$$

创新点一：采用硬件加速或者链外计算技术，提升高并发场景下区块链节点的计算性能。如蚂蚁链、长安链、万向链、“星火·链网”等相继推出区块链节点硬件加速器，通过软硬件深度融合，提高节点计算性能，其中蚂蚁一体机可实现每秒 10 万笔交易的处理能力。

创新点二：采用网络分片(Network Sharding)和有向无环图(Directed Acyclic Graph, DAG)技术，提高网络并行处理能力。如以太坊 2.0 最终目标是通过分片来解决性能不足问题，希望可实现每秒 100 万笔上链交易。此外，IOTA、Nano 等项目都采用 DAG 技术并行打包区块的方式来提高并发量。

（二）交互能力：服务平台的用户友好性提高

技术门槛、运营成本等问题长期影响区块链基础设施规模化发展。对于大部分来自开源社区的上层应用开发者而言，无法承担本地部署基础设施节点的计算、存储、通信等成本，也不具备长期运行节点的能力，迫切希望借助第三方提供的通用服务平台在本地分布式应用和远端区块链节点之间建立连接，从而屏蔽底层链复杂度，降低开销，提高开发效率。

创新点三：采用区块链即服务平台（Blockchain as a Service, BaaS）技术，提供快速搭建区块链基础设施节点的能力。从参与的主体看，互联网平台企业、云服务商、独立区块链技术提供商及大型金融企业、通信企业等都在加入此类技术竞争。特别是云服务商依托广泛分布的计算设施、扎实的技术产品、雄厚的市场渠道，在竞争中呈现显著优势。例如微软 Azure 云平台可提供以太坊区块链即服务 EBaaS，华为云区块链服务 BCS 同时支持自主研发的区块链引擎和超级账本。

创新点四：采用区块链通用接口平台技术，提高系统的开放性与节点的远程托管能力。就类似于云计算中把计算存储等 IT 基础设施虚拟化作为一种服务通过网络对外提供的 IaaS 模式，以太坊选择 Infura 系统来托管区块链节点集群，从而开放通用功能的程序接口，便于开发者高效快速接入。此外，微众、腾讯等发起成立开源联盟链生态圈“金联盟”，致力于打造面向金融级区块链基础设施 FISCO-BCOS，基于中间件平台，提供了数据治理通用组件、多方治理协作组件等，以及区块链应用开发工具和节点托管服务。

（三）上链能力：接入终端的可信安全性增强

随着区块链基础设施与实体经济深度融合，芯片安全可控及数据隐私保护越来越受到重视，对各种安全算法协议的硬件化成为区块链端侧领域发展的重要方向。一方面物联网和区块链之间的交互主要在云端，物联网终端源头产生的数据存在被篡改风险，难以实现区块链信任机制的商业闭环；另一方面私钥作为用户访问区块链系统和控制数字资产、数字身份的“钥匙”，其安全存储问题就至关重要。

创新点五：采用终端设备硬件底层部署可信数据上链技术，打通“物联网+区块链”关键一环。紫光展锐携手万向区块链、摩联科技、广和通推出全球首款 Cat.1 区块链模组 L610，使基于春藤 8910DM 的物联网设备具备访问区块链和调用智能合约能力，实现数据可信上链。

创新点六：采用数字钱包私钥加密存储与恢复技术保障秘钥安全。“星火·链网”区块链基础设施结合其 S1 芯片，可以为用户提供区块链密钥安全存储解决方案，满足密钥不可读取、复制、导出等安全要求。蚂蚁链使用其 T1 安全芯片，通过区块链对关键数据进行数字签名和完整性验证，实现“区块链+安全芯片”的软硬件技术创新。

四、区块链基础设施应用实践

随着全球区块链基础设施建设规模的不断扩展、运行能力的不断增强，已经不仅应用于加密数字货币等场景，而是在制造业、服务业等不同的领域开展应用实践，涌现出数字藏品、数据流通、双碳交易、供应链金融、产品溯源等一批典型的去中心化多方信任应用模式。

（一）数字藏品

需求分析：数字藏品是使用区块链技术，对作品、艺术品生成的唯一数字凭证，在保护其数字版权的基础上，实现真实可信的数字化发行、购买、收藏和使用。目前国内数字藏品市场处于各平台分别自选区块链进行发行的阶段，用户无法通过个人信息查询名下所有数字藏品情况，数字藏品在流转过程中的平台安全性问题也有待于解决。

解决方案：大多数文化产业从业者，如艺术品的版权所有方等，不一定有深厚的区块链专业技术知识，依托第三方区块链服务商建设、部署、运营专用区块链系统成本高且难维护，利用区块链基础设施的公共服务能力和灵活部署能力，有利于降低数字藏品发行管理成本。此外，区块链基础设施为数字藏品的铸造和认证，可提供统一的数字凭证注册和认证等一站式服务，从而形成长期稳定的服务能力。

典型案例：DNA——基于“星火·链网”的数字原生资产网络

数字原生资产（Digital Native Assets, DNA）服务网络，基于“星火·链网”区块链基础设施，可以为数字藏品平台提供便捷的、安全的、低成本的服务。数字藏品平台可通过 DNA 服务网络完成其数字藏品注册，并获得认证。同时，基于 DNA 服务网络直接发行的数字藏品均可通过“星火·链网”提供的唯一分布式标识符，进行数字藏品查询。



（二）数据流通

需求分析：数据要素市场化配置的流通过程中，面临的问题主要在于以下几个方面，一是数据确权，即数据要产生价值，必须解决数据所有权问题；二是数据可信，如溯源数据没有得到充分利用，多数源于无法证明数据是否造假；三是数据互通，如各种信息系统相互独立而形成孤岛，则难以支持数据充分的流通。

解决方案：利用区块链基础设施的广泛接入能力和灵活部署能力，数据流通过程中所涉及的数据所有者、数据使用者等多种角色主体，可以通过更简易的操作实现数据上链存证，对数据开放、数据交易、数据共享等不同行为，进行数据权限的配置、数据版本的管理、数据使用的记录。特别是针对不同行业、不同领域的数字空间，区块链基础设施均可通过唯一的分布式标识进行覆盖范围内的全网统一检索和认证。

典型案例：RivTrust——数据要素确权流转平台

RivTrust 平台为政企数据资源提供价值流转载体，是基于区块链基础设施的数据协同平台。在保证数据隐私的前提下，助力不同机构进行产业协同，完成数据资产的全生命周期管理，实现数据资产的确权、保护和价值转移。RivTrust 平台主要是基于万维网分布式标识符 DID 技术和点对点传输协议 DIDcomm 技术，实现身份所有者自管理和分布式授权。通过凭证的上链存证帮助数据共享和安全可见，无惧信息孤岛。目前可支持供应链、金融、能源、工商、税务等多种领域的凭证申领和使用。



来源：网络公开资料

图 14 RivTrust 数据要素确权流转平台的技术架构

（三）双碳交易

需求分析：碳交易将碳排放权视作以气候环境资源使用权为实质的发展权，以市场化机制的效率原则解决环境治理问题，能以较低成本解决环境治理。碳交易市场存在交易主体间信息不对称、交易市场信息不透明等问题。低透明度使得交易者对市场缺乏信心，也妨碍了碳排放企业对自身碳资产进行有效评估和管理。

解决方案：针对碳交易中碳资产认证和交易市场多主体信任问题，出现了一批初创项目利用区块链技术探索构建碳交易市场，但由于应用场景和应用模式尚未成熟，市场风险大，单独建设区块链成本较高。利用区块链基础设施提供的公共服务能力，能快速低成本构建高效可信的碳交易平台，提供应用场景和应用模式验证基础，有效降低应用风险，加速打造碳交易主体、交易机构、第三方认证机构、政府机构等多方参与、灵活互动的碳资产交易模式。

典型案例：Flowcarbon——通证化碳信用交易平台

Flowcarbon是基于Celo协议建立的碳信用发行交易平台，通过将碳信用通证化，打通碳信用链上和链下的双向流通，来提升流动性，一定程度提升了透明性和交易效率。一是Flowcarbon发行GCO₂通证，供给方可以将自己多余的碳信用上链变成通证，用户根据自身需要购买；反之，用户也可以将购买的通证赎回为链下对应的碳信用。其二是Flowcarbon引入GNT捆绑通证，为碳信用市场引入流动性。每个GNT通证也都由储备的碳信用额所支撑，这种一对一的碳信用挂钩机制，实现GNT价格与碳信用市场定价保持一致。

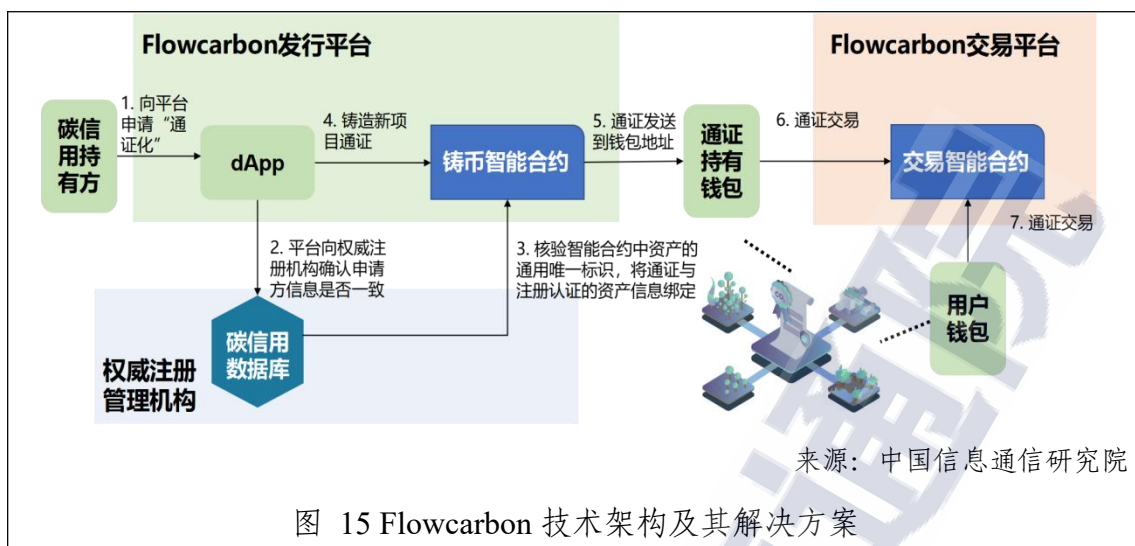


图 15 Flowcarbon 技术架构及其解决方案

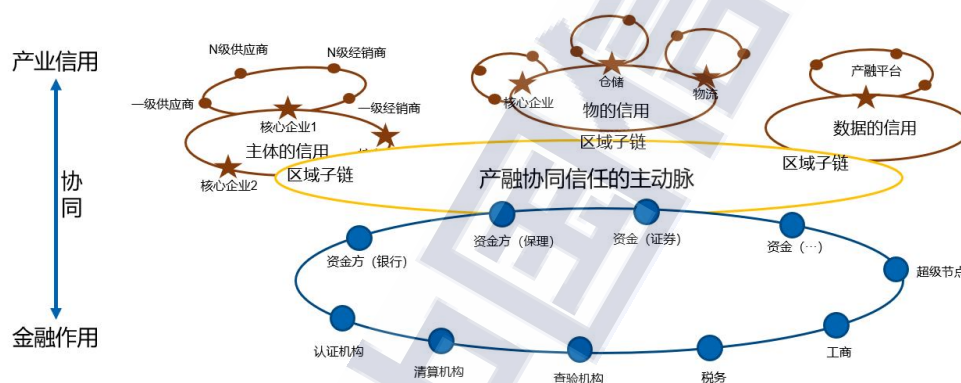
（四）供应链金融

需求分析：供应链金融以供应链上下游的真实贸易为基础，强调成员企业间竞争与协作的特殊关系，是中小企业重要融资渠道，主要分为应收账款融资、仓单融资和订单融资等三种类型。其中应收账款融资占供应链金融业务 60% 左右，主要围绕核心企业展开。企业信用资质，核心企业的配合度决定了应收账款融资规模和风险程度。金融机构、保理公司依托核心企业来为供应链上的中小企业提供服务，信息的不透明严重影响整个链条效率，也不利于构建供应链信用体系。

解决方案：针对供应链金融中，供应商、核心企业、银行和金融机构等多方参与跨地域交易场景下的流程复杂，监管效率低等问题，结合区块链基础设施广泛接入能力，帮助更多中小企业上链，为所有参与方提供了便捷的访问途径，简化审批认证流程，便于银行和金融机构低成本高效地做出放贷决策；结合区块链基础设施公共服务能力，借助数据存证严防票据作假、重复质押等风险问题，降低了交易信用风险，提升供应链金融交易流转透明度，增强其整体监管水平。

典型案例：壹诺——供应链金融平台

壹诺供应链金融平台，通过布比底层链与“星火·链网”区块链基础设施的对接，发挥区块链技术驱动供应链金融的创新效应。该平台核心功能主要包括实名认证、凭证管理、在线融资、资金管理等。通过跨链互操作等关键技术，可促进全链条信息共享，实现供应链金融可视化，降低中小企业融资成本，提高资金流转效率，间接降低整体生产成本。



来源：布比(北京)网络技术有限公司

图 16 壹诺供应链金融平台技术架构

（五）产品溯源

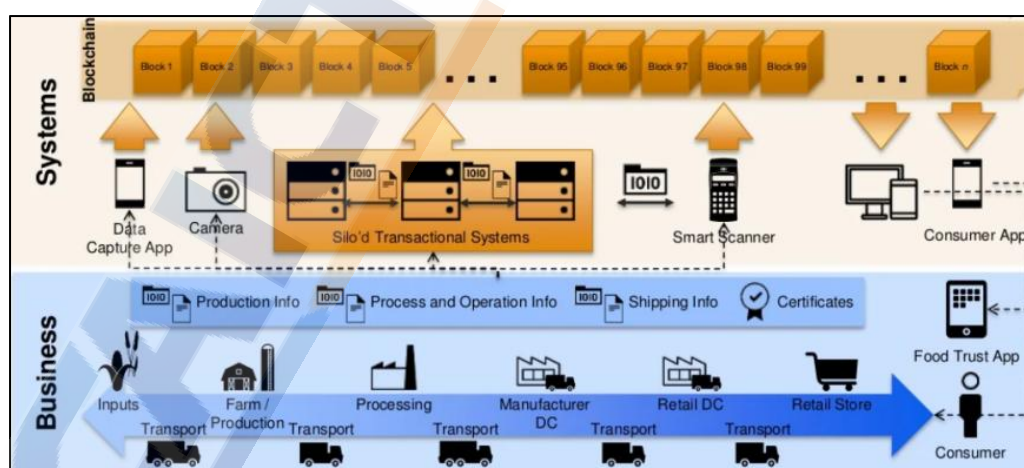
需求分析：溯源是在产品流通过程中回溯对象来源、用途、位置、参与方等信息的活动，以实现对象来源可查、去向可追、责任可究、风险可控。由于往往溯源涉及生产、流通、使用等多种不同的环节，存在链条长、业务复杂、参与主体多等问题，因此需要跨领域协同，打破上下游信息共享壁垒。

解决方案：利用区块链基础设施广泛接入能力，有利于全产业链上下游的各种协作主体，在无需复杂系统改造和新平台建设的情况下，

参与产品溯源应用。同时，利用区块链基础设施公共服务能力，可以减少消费品、工业品等各种行业为产品溯源单独建设区块链系统并且运营信任体系所造成的重复建设和成本问题。

典型案例：IBM Food trust——食品溯源与供应链管理

IBM Food Trust™ 通过建立更安全、更智慧和更可持续发展的食品生态系统使所有供应链网络参与方受益。通过使交易和数据实现数字化，提高了整个供应链（包括种植者、加工商、运输商、零售商、监管者、消费者）的工作效率。同时，该解决方案支持授权用户即时访问涵盖从农场到商店再到消费者的整个供应链数据。在区块链基础设施灵活部署基础上，IBM Food Trust™ 集成了物品编码的 GS1 标识体系和 EPCglobal 网络服务系统架构，可为参与方提供便捷的产品链管理和溯源服务。目前，该系统已经成为市场上规模最大且最活跃的非加密数字货币区块链基础设施应用，已开展交易服务 900 多万笔。包括家乐福、沃尔玛等零售巨头都是 IBM Food Trust™ 成员。



来源：网络公开资料

图 17 IBM Food Trust™ 的产品溯源功能模块与业务流程

五、总结与展望

比特币网络作为区块链技术的首个系统性实践，主要应用于加密数字货币。而以太坊作为全球第一个推出智能合约功能的区块链平台，则更加符合区块链基础设施支持跨行业、跨领域开展大规模可信协作网络建设的需求。自 2015 年 7 月 30 日，以太坊主网正式上线以来，经过七年时间的发展，包括“星火·链网”、区块链服务网络 BSN、欧盟区块链基础设施 EBSI、印度国家区块链框架 NBF 等国家级重大工程先后启动节点建设和应用探索，其他各种公有链网络和跨链系统项目更是多达数百个，足可见全球各国和产业界都高度重视构建这一信任和价值新型基础设施。我们相信，随着区块链技术的持续性改善，数据要素的市场化价值将不断得到发挥，区块链基础设施将有力支撑传统产业的数字化转型和数字原生空间的探索！

（一）网络信任底座是一项复杂的系统性工程

互联网的核心精神是包容、开放、简单，通过采用数据分组交换等技术提供了“尽力而为”的服务，计算、存储、通信被视作互联网的基本要素，但安全可信未被纳入互联网体系架构最初的设计考虑，只有通过持续的各种安全补丁来弥补。通过区块链基础设施的建设，为网络构建信任底座，将有助于从根本上解决这一问题。但随着全球互联网近五十年的发展演进，已成为影响社会治理和经济发展的基石，任何变革都将牵一发而动全身。因此，重新构建基于机器的信任体系，不仅需要完善区块链基础设施自身的建设，还需要充分考虑其对网络基础资源管理、网络底层协议的影响，以及对网络应用生态的适配。

（二）基础设施建设与应用创新趋于同步开展

“优先完成设施的全面建设”，还是“同步开展规模性应用实践”，是任何基础设施发展都会面临的艰难选择。过去几年时间内，大部分区块链基础设施的关注重点都是前者，而目前更多主体开始选择后者。例如许多开源社区驱动的区块链基础设施生态化发展，已经不再局限于加密数字货币应用，而是在制造、能源、文化等领域积极探索应用。在政府支持下采用分域节点建设的区块链基础设施网络化发展，更是格外重视与产业的深度融合，通过顶层设计、资金和政策引导等多重方式，组织大规模的多方信任建立与数据价值发挥等应用实践。

（三）数字原生空间将带来更直接的发展需求

在现有互联网体系架构内建设网络信任底座的复杂程度和成本很高，这也在一定程度上限制了区块链基础设施的发展，容易引发对发展模式和路径的争议。但在过去的一年里，全球范围内对 Web3、元宇宙等数字原生空间的技术研究、产品研发、应用探索大幅加速。一方面，在这样一些新的网络空间内，从体系架构设计的初始阶段，就充分考虑信任底座的内生建设，更容易得到全球各方的认可和支持；另一方面，数字原生空间内部的经济理论模型已经发生改变，依赖于对数据要素的确权、交互、交易等基本支持和数字身份、数字资产等基本单元，也就迫切需要借助区块链基础设施在传递价值和管理信任等方面的功能。

中国信息通信研究院 工业互联网与物联网研究所

地址：北京市海淀区花园北路 52 号

邮编：100191

电话：010-62300566

传真：010-62304980

网址：www.caict.ac.cn

