中国通信学会
CHINA INSTITUTE
OF COMMUNICATIONS

区块链技术发展与应用创新白皮书

（2021年）

中国通信学会

2022 年 6 月

版权声明

专家组和撰写组名单

顾问(以姓氏笔画为序)：

邬江兴 中国工程院院士

张　平 中国工程院院士

陈世卿 美国国家工程院院士、美国艺术与科学院院士

陈清泉 中国工程院院士、英国皇家工程院院士、匈牙利工程院荣誉院士、乌克兰工程科学院院士、香港工程科学院院士

郑纬民 中国工程院院士

周孝信 中国科学院院士、美国国家工程院外籍院士

俞梦孙 中国工程院院士

董家鸿 中国工程院院士、法国国家外科科学院外籍院士

专家组：

组长：

郑志明 中国科学院院士，中国通信学会区块链委员会主任委员

成员(以姓氏笔画为序)：

姓名	单位	职务
王向东	中国通信学会区块链委员会	副主任委员
王栋	国网区块链科技公司	总经理
王焕然	深圳众联数字科技有限公司	董事长

亓峰	北京邮电大学	正教授
朱皞罡	北京航空航天大学	正教授
陈晓禾	中科院苏州医工所电子研究室	主任、正教授
邱望洁	北京航空航天大学	研究员
杨斌	清华大学网络行为研究所	副所长、研究员
金键	中国信息通信研究院工业互联网与物联网研究所	所长、正高工
侯锐	中科院信息工程研究所信息安全国家重点实验室	副主任、研究员
袁昱	深圳清华大学研究院 2022 IEEE SA	主任研究员 后任会长
黄河燕	北京理工大学计算机科学与技术学院	院长、正教授
曹源	湖南兆物信链科技集团有限公司	董事长
董进	北京微芯区块链与边缘计算研究院	院长、正高
褚晓文	香港浸会大学区块链与金融科技实验室	主任、正教授
魏丽红	中国移动通信集团有限公司信网部	总经理、正高工

撰写组(按单位排名)

单位	姓名
深圳众联数字科技有限公司	王焕然
深识全球创新科技（北京）	林道庄，王奇

有限公司	
苏州鸿链信息科技有限公司	邱望洁，章天乙

前　言

2019 年 10 月 24 日，习近平总书记在中央政治局第十八次集体学习时强调，“区块链技术的集成应用在新的技术革新和产业变革中起着重要作用。我们要把区块链作为核心技术自主创新的重要突破口，明确主攻方向，加大投入力度，着力攻克一批关键核心技术，加快推动区块链技术和产业创新发展”。

2021 年两会上李克强总理做的政府工作报告提出，加快数字化发展，打造数字经济新优势，协同推进数字产业化和产业数字化转型。作为数字经济的基石，区块链技术发挥着重要作用。此次两会正式发布的《中华人民共和国国民经济和社会发展第十四个五年规划和 2035 年远景目标纲要》中，“加快数字化发展建设数字中国”单设篇章，其中“区块链”被列为数字经济重点产业。

按照中国通信学会的部署，区块链委员会汇集国内外顶级专家近年实际科研、工作经验、成果、以及对国际部分国家区块链国家战略发布的洞察、分析，组织部分委员会专家委员，在国内外院士级专家的指导下，执笔撰写了本“2021 区块链技术发展与应用创新白皮书”。

本白皮书首先阐述区块链之战略地位，核心技术阐述涵盖区块链底层技术、跨链技术、交换技术、软硬协同技术、关键密码学技术、分布式账本的互联网数据库技术以及相关监管架构、系统脆弱性分析等，较全面、深入阐述区块链分布式数据存储、点对点传输、共识机制、加密算法等计算机技术的新型集成应用，具有去中心化、全程留痕、不可篡改、可追溯、集体维护等区块链本质特点，阐述区块链技

术在金融、智能制造、物联网、供应链管理、数字资产交易、社会治理和民生服务等多个领域发挥重要作用。此外，本白皮书还介绍了我们专家组构建的区块链全方位评测指标体系及测评方法，进一步加深对区块链核心技术和实际应用质量的认识和考核。本白皮书对于各级部门、机构、企业深刻理解习总书记关于区块链技术的高度战略定位、对于广泛培养各类区块链技术及应用人才都将发挥重要作用。报告内容丰富、真实、深厚，有战略高度，有覆盖全面和关键侧重，在“十四五”开启之年，可作为高校、研究机构以及金融、能源、政务服务、司法、医疗健康、产品溯源、智慧城市、物流等行业，落实国家“十四五”关于区块链行业应用发展和政府部门政策制定的参考。

中国通信学会区块链委员会

主任委员：郑志明

2021 年 12 月 10 日

内容摘要

区块链是人类历史上首次构建的可信互联系统，其核心功能将是提升国家在各个维度的治理能力。这是需要我们深刻理解和准确把握的，也是习近平总书记在十九届四中全会之前组织中共中央政治局集体学习区块链的重大意义。

从 2008 年比特币问世至今，区块链的发展大体可以分为三个时期，其应用范畴已经从最初的虚拟货币扩展至现今社会经济生活的方方面面。其中 1.0 阶段以比特币等虚拟资产为典型代表，2.0 阶段以智能合约的应用为典型特征，而 3.0 阶段以现实世界资产数字化为核心特征。然而，以比特币为代表的技术至上信仰具有典型的无政府主义色彩，无法与现实世界的法律与制度完美相融。从根本上还原区块链技术、经济特征，重新诠释区块链的哲学、社会意义，区块链将成为社会治理的基础性工具。基于规则的智慧社会治理体系将实现国家治理模式从基于传统信息化技术辅助的阶段进入基于区块链的法治与协同阶段。

本白皮书正文分成三个主要部分：区块链技术发展情况、区块链应用创新进展、以及区块链技术未来展望。在区块链技术发展情况部分，本白皮书从区块链的第一个应用——比特币——开始谈起，基于比特币解释区块链的技术特性：不可抵赖，不可篡改、分布式账本和智能合约。区块链技术的与众不同在于：每一个技术参数的改变都会引发经济甚至哲学上的变革与争论。本白皮书借用分叉这个技术术语，来讲述区块链技术发展过程中的各种理念延伸与冲突，帮助读者将区块链技术进行拆解与重构。

在区块链 1.0 阶段，可信公链技术的发展推进了数字货币领域的各种探索。在区块链 2.0 阶段，以太坊和智能合约推进了 ICO（代币发行融资）和通证经济的兴起。在区块链 3.0 阶段，区块链技术开始走向多链融合，区块链应用也开始与现实社会融合。

在第六章、第七章中，本白皮书一方面总结了区块链技术目前面临的挑战，另一方面，2020 年美国国家战略新兴技术报告将区块链技术列入其中，并禁止对华出口，因此研发自主可控的区块链底层技术迫在眉睫，本白皮书对当前国内自主可控区块链技术的发展情况进行了总结，并介绍了郑志明院士领导的中国通信学会区块链委员会构建的区块链全方位测评指标体系，更加深了对区块链核心技术、实际应用性能质量的认识和考核。

在区块链应用创新部分，本白皮书对 ICO 和通证经济中的各种现象进行经济和法律上的分析，指出 ICO 与通证经济中的违法违规现象和未来的发展方向。另外，本白皮书也分析了稳定币、STO、以及资产上链的经济与法律本质，以及市场上存在的各种典型项目。受比特币哲学的影响，区块链行业的原生发展都具有无政府主义的特征，与现行的社会运行机制难以有效融合。

在第四次产业革命和中国经济服务化转型的大背景下，区块链将实现数据生产要素的确权和分享机制，并在数字政务、数字金融、产业互联与社会治理等领域具有广泛的应用。

在《数据安全法》和《个人信息保护法》的背景下，隐私计算成为数据访问和计算的必须要求。本白皮书总结了目前各种隐私计算的研究方

向，并给出了区块链与各种隐私计算相互结合的建议。

在数字政务领域，区块链技术可以实现政务数据的协同，并利用其不可篡改的特性在政务的过程管理实现广泛的应用；在数字金融领域，本白皮书列举了区块链技术在银行、证券、保险等各个领域的应用案例，作为读者的启发和参考；在产业互联领域，本白皮书区块链技术在溯源领域的各种应用，以及区块链溯源面临的困境；在社会治理领域，本白皮书基于通证经济理论提出了基于区块链建设基层治理共同体的设想和方案。

在区块链技术未来展望部分，本白皮书指出公链技术架构于比特币的无政府主义哲学之上，将信任完全建立在算法与算力的基础上，不仅造成了能源的巨大浪费，也产生了事实上的霸权与不平等。现实中，真实社会的运行是构建在法律和制度基础上的。公众化联盟链将区块链技术与现实社会的法律与制度相结合，因此公众化联盟链才是区块链技术发展的未来。在具体判断某个场景是否适合区块链应用时，本白皮书提出了“强、弱、伪、非”四个标准供参考，并进一步提出区块链发展的法律、技术、政策方面的建议。从长远来看，“数字孪生、镜像世界”是数字化发展的目标和方向，将会不断推进新一次产业革命的进展；从短期看，在国际竞争格局重构的背景下，数字货币将颠覆现有的国际支付清算体系，进而带来国际贸易与金融体系的解构与重建。经历数字货币战争后建立的数字世界新秩序，才是全世界数字社会发展的牢固基石。

中国通信学会区块链委员会

王焕然 邱望洁 亓峰

目 录

第一篇 概述

第一章 研究背景

1.1 区块链技术之战略地位

人类社会的发展进程，与新技术的发明和应用有着密切关系。近代史上已经发生过三次产业革命，现在正迎来第四次产业革命。第一次产业革命跨越 19 世纪末期到 20 世纪初期，蒸汽机的发明带来了机械化，开启了工业生产时代。第二次产业革命从 20 世纪初期到 20 世纪 60 年代，电气化催生了大规模生产方式，推动了钢铁、机械等工业的崛起。第三次产业革命始于 20 世纪 70 年代，计算机技术促进生产自动化，使生产力得到了进一步提高。而第四次产业革命，则是在 21 世纪以后发展起来的，以区块链、云计算、物联网、大数据、移动通信及人工智能为代表的数字技术所驱动的社会生产方式变革[1]。第四次产业革命带来的自动化和数字化几乎将改变每一个行业。区块链实现可信任的数据协同，是第四次产业革命的核心技术之一。（如图 1-1 ）

区块链+物联网：基于区块链的分布式物联网结构可以实现大量设备可信联网、可信共享数据，以及自我治理，可避免多中心模式下物联网野蛮生长带来的基础设施建设和维护的巨额投入，释放物联网资源及数据共享进而实现数据节约的潜能。

区块链+云计算：将区块链与云计算融合，一方面区块链为云资源可信服务提供了简单有效的解决方案；另一方面，为区块链节点快速

[1] Klaus. Schwab，The Fourth Industrial Revolution [M]， World Economic Forum, 2016.

部署提供了网络和算力资源。

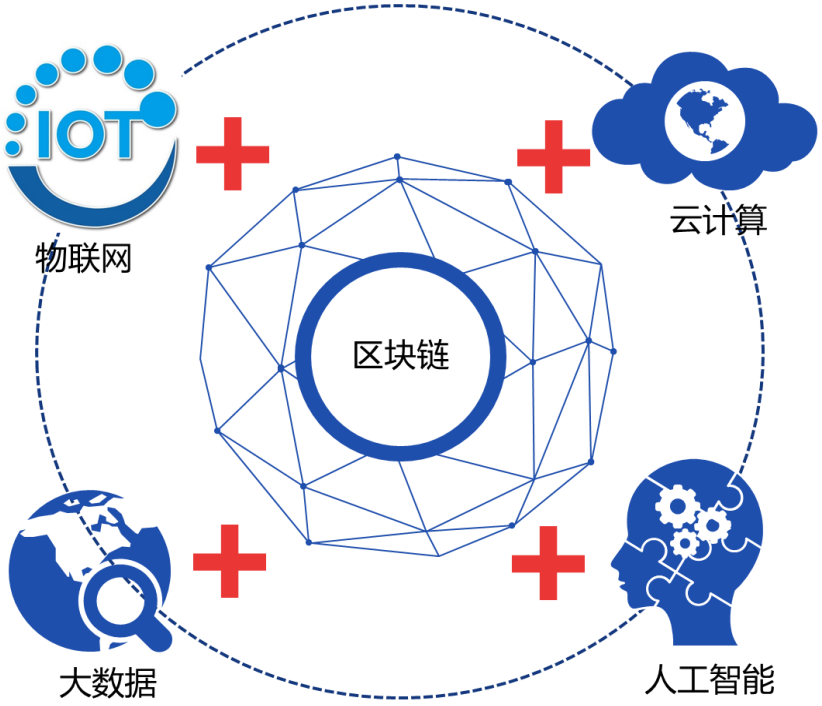

图 1-1 区块链技术是第四次产业革命的核心

区块链+大数据：区块链不仅为大数据的采集、确权、分享等全生命周期提供价值的可信传递，保护数据私密性；而且通过链上、链下数据协同存储，还可以提升数据共享效率，降低网络传输成本。

区块链+人工智能：二者的有机融合可以实现智能算力更可信、更广泛、更安全地分布与协同，并能够助力例如联邦计算、同态计算等服务模式的快速推广。

2019 年 10 月 24 日，在中央政治局集体学习中，习近平主席强调：区块链技术的集成应用在新的技术革命和产业变革中起着重要作用。发挥区块链促进数据共享、优化业务流程、提升协同效率、建设可信体系等方面的作用，推进区块链和实体经济深度融合，解决中小企业贷款难，银行风控难，部门监管难等问题。

在第四次产业革命和中国经济服务化转型的大背景下，区块链将实现数据生产要素的确权和可信分享机制，并在供应链创新、数字政务、社会治理、以及数字金融领域具有广泛的应用。

1.2 本文的研究目的和研究方法

1.2.1. 研究目的

从 2017 年开始，浙江、江苏、贵州、福建、广东、山东、江西、内蒙古、重庆等 9 个省份、自治区和直辖市就区块链发布了指导意见。2020 年，多个省份已经将区块链及数字经济建设列入本省“十四五”战略发展规划，如表 1-1 。

表 1-1 2020 年地方出台的区块链及数字经济政策

北京市	北京市区块链创新发展行动计划（2020-2022 年）
河北省	河北省区块链专项行动计划（2020-2022 年）
山东省	山东省传统产业智能化技术改造三年行动计划(2020-2022 年)
江苏省	江苏省区块链产业发展行动计划
上海市	上海市促进在线新经济发展行动方案（2020-2022 年）
浙江省	浙江省新型基础设施建设三年行动计划(2020—2022 年)
安徽省	安徽省“数字政府”建设规划（2020—2025 年）
福建省	福建省新型基础设施建设三年行动计划（2020—2022 年）2020 年数字福建工作要点
江西省	江西省数字经济发展三年行动计划(2020-2022 年)

广东省	广东省培育区块链与量子信息战略性新兴产业集群行动计划（2021-2025 年）
广西壮族自治区	广西壮族自治区区块链产业与应用发展规划（2020-2025 年） 《广西壮族自治区区块链产业与应用发展指导意见》
海南省	《海南省工业和信息化厅关于印发海南省加快区块链产业发展若干政策措施的通知》
湖南省	湖南省区块链发展总体规划（2020-2025 年）
内蒙古自治区	内蒙古自治区人民政府关于推进数字经济发展的意见
贵州省	关于加快区块链技术应用和产业发展的意见
云南省	云南省推进新型基础设施建设实施方案（2020—2022 年）
重庆市	重庆市新型基础设施重大项目建设行动方案(2020—2022 年)的通知

2020 年，中国人民银行采用了区块链思想构建的数字货币也已经进入试点阶段，在深圳、苏州、雄安新区、成都等地陆续开展了 DC/EP 的公众化应用试验。2021 年，第二批数字人民币面向公众的试点扩展到上海、海南、长沙、青岛、大连、西安等 6 个省市。DCEP 有望用好中国数字经济在全球视野下的相对优势，深度重塑货币政策体系，系统性地拓展政策空间、有效性和独立性，从而为中国经济“内循环”

进行长效化赋能。如图 1-2。

图 1-2 央行数字货币 DCEP 的意义

然而在现实中，区块链作为一项新兴技术，仍被社会以各种方式曲解，特别是一些别有用心的人打着区块链的名义行违法之实，不仅蒙蔽了普通大众，也误导了部分地方政府。结合国家与地方的政策，深入推进以区块链为核心的数字新基建，从哲学、技术、经济等多角度解析区块链技术及其应用，为区块链技术的合理应用提供指导，助力实体经济发展，是本研究最重要的目的。

1.2.2. 研究方法

本报告通过调查研究、数据分析、行业专家访谈以及案例分析等方法，对区块链技术及其应用进行研究和分析，旨在了解区块链技术的最新发展情况，分析区块链技术在哪些领域得到应用。

调查研究法，利用第三方的调查数据、访谈获得最新资料和信息，

并对此进行研究各行业企业布局区块链的现状分析。本文选择了全球知名的区块链行业数据库作为主要数据来源，同时梳理了行业内众多权威论文、研究报告作为研究参考。

数据分析法，主要针对行业内企业布局区块链的统计数据展开分析，从数据层面研究各个企业对区块链技术的应用积极度以及其所在发展阶段。

行业专家访谈法，通过对国内近 20 位区块链专家以及部分大型企业（华为、阿里、腾讯、平安等）员工进行了访谈，包括区块链学界研究人员、区块链项目技术开发人员、投资机构、法律专家等，获得了宝贵的意见和帮助。

案例分析法，通过行业内企业布局区块链的具体案例展开分析，对其布局区块链所遇到的问题进行深入探究，从而为其他企业布局区块链提供参考。

1.3 本研究对于现实的指导意义

区块链技术中蕴含的巨大经济、社会和科学价值正在被开发利用，其技术创新及多元应用超越了国家发展水平和意识形态差异限制，其应用场景与发展前景，对实体产业与互联网技术的进步，将产生重大的积极意义。

区块链技术将应用在数字社会建设的各个领域。但是，作为一种分布式技术，区块链有其天生的优点和劣势，不是所有场景都适合区块链。本报告提出了在具体判断某个场景是否适合区块链应用时使用的“强、弱、伪、非”四个标准。

要加快推动区块链技术和产业创新发展，积极推进区块链和经济社会融合发展，我们要加强人才队伍建设，建立完善人才培养体系，打造多种形式的高层次人才培养平台，培育一批领军人物和高水平创新团队。区块链作为集成性创新技术，对复合型人才需求巨大，要求从事者掌握涉及密码学、网络学、应用领域等多种专业知识。发展区块链，必须加强学科深度交叉融合的人才队伍建设，从基础研究、应用研发、产业融合等方面前瞻和系统性地建立人才培育体系。

本报告对区块链技术的发展与应用进行了系统分析，详细阐述了区块链技术在国家治理能力现代化中各个领域的应用，对于各级部门、机构、企业深刻理解习总书记关于区块链技术的高度战略定位、对于广泛培养各类区块链技术及应用人才都将发挥重要作用。

第二篇 区块链技术发展情况

第二章 区块链的定义与特征

2.1 区块链的起源与定义

区块链（Blockchain）的正式诞生源于两个标志性事件：

1）2008 年 11 月 Satoshi Nakamoto（中本聪）在密码学邮件组发布的一篇论文《Bitcoin: A Peer-to-Peer Electronic Cash System》，翻译名为《比特币：一种点对点的电子现金系统》[2]；

2）2009 年 1 月 3 日，中本聪公布比特币系统的第一个区块——创世区块，世界上第一个区块链数据诞生。

实质上，区块链的诞生是密码学、分布式技术、互联网治理、与数字经济发展融合的必然结果，是从信息互联网到信任互联网，再进展到价值互联网的必然进程。区块链技术目前并没有相关的规范和标准，参考《中国区块链技术和应用发展白皮书（2016）》给出的定义：

- 狭义的区块链：一种按照时间序列将数据区块以线性链表方式组合而成的特定数据结构，并借助密码技术确保交易信息数据的不可篡改和不可伪造。作为一种典型的分布式账本技术（Distributed Ledger Technology），区块链技术能够安全存储简单的、有先后关系的、在系统内可验证的数据。
- 广义的区块链：是利用加密链式区块结构来存储与验证数据、利用分布式共识算法来新增和更新数据、利用运行在区块链上

[2] Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System [OL], http://bitcoin.org/en/bitcoin-paper, 2008.

的代码(即智能合约) 来保证业务逻辑自动强制执行的一种全新的多中心化基础架构与分布式计算范式。

2013 年，程序员 Vitalik Buterin 受比特币启发后提出以太坊（Ethereum）的架构设计，并在 2014 年成立基金会开始研发以及运营。发展至今，比特币和以太坊已成为互联网上规模最大的区块链项目。区块链技术也被逐渐被社会接受，并尝试应用于各个领域中。

2.2 区块链的技术延伸与理念冲突

2.2.1 软分叉与硬分叉

分叉，是一个技术术语，用于描述区块链技术在软件更新过程中的版本不兼容问题。本报告借用分叉这个概念来描述区块链技术演进过程中的技术延伸与理念冲突。不同分叉代表了不同的技术路线选择，每一个技术细节的路线选择都将影响区块链的技术特征，以及基于技术之上的业务特征。

1）软分叉

- **技术上**是指软件升级向后兼容，即老节点不升级软件也可以运作，但无新功能；
- **理念上**是指在比特币技术哲学的基础上根据业务场景进行技术补充完善，是比特币技术的进一步应用延伸。
- 软分叉（技术延伸）主要体现在共识机制、记账方式、智能合约、加密算法、以及区块与链的具体技术实现上面。

2）硬分叉

- **技术上**是指软件升级不向后兼容，老节点不升级将不能正常运

作，新老节点将运行维护两条不同的区块链；

- **理念上**是指针对比特币技术哲学的认同发生严重冲突，进而导致两个完全不同的技术方向和使用场景。
- 硬分叉（理念冲突）主要体现在节点许可、去中心化、共识机制、激励机制、身份&隐私权、控制&主权等方面。

区块链的技术仍在不断发展中，因此区块链技术的分叉仍不断进行中……

2.2.2 软分叉——技术的延伸

2.2.2.1 共识机制（公链）

公链，也称非许可链，是指在无需许可或者第三方信任的分布式开放系统环境运作的区块链技术系统。共识机制是区块链技术的核心，不同的共识机制会生成不同的区块链系统，具有不同的技术特征。下面是几种常见公链共识机制的简单总结与对比。

1）工作证明 POW：基于哈希（Hash）函数计算的竞争机制，优胜者获得记账权和挖矿奖励。

- 优点：机制简单；挖矿即共识；作恶成本高 （51%攻击）；
- 缺点：耗费能源；效率低；矿场&专用芯片（ASIC）会导致算力寡头化。

2）权益证明 POS：在 POW 基础上加入节点权重，引入代币作为权重依据， 根据每个节点所占权重的比例和时间，等比例地降低权益证明（POS）难度，从而加快找随机数的速度。

- 优点：减少参与验证和记账节点的数量，可加快共识周期；

- 缺点：依赖代币，仍然会浪费计算资源，且使得“富者更富”。

3）委托权益证明 DPOS：在 POS 的基础上，每个节点根据权重，投票选出一定数量的“超级节点”，由这些节点轮流产生区块，代理它们进行验证和记账。

- 优点：不再需要通过“挖矿” 来产生区块， 可以大幅缩小交易确认的时间， 能够达到秒级的共识验证；
- 缺点：还是依赖代币，不适用于一般的商业应用。

4）其他混合机制（DPOW）：在上述机制的基础上混合。

2.2.2.2 记账方式

区块链技术也被称为分布式账本技术，账本的设计即每一个区块内交易记录内容。目前区块链应用中，交易记录内容主要为区块链系统上的交易及账户信息。实际上任何事物都可抽象成交易，区块链技术在更广泛行业应用设计的主要工作是定义行业交易行为及账本记录内容。

1）仅记录交易，以比特币 UTXO 模式为样板

- 优点：存储数据简单，量小，交易上链的先后次序不敏感；
- 缺点：每次计算帐户余额需要遍历所有交易汇总计算。

2）同时记录交易和账户余额，以以太坊 Ethereum 的模式为样板

- 优点：可以快速读取账户当前状态；账户状态与交易记录可以交叉验证；
- 缺点：同时处理交易与账户，效率较低；交易上链与账户更新需要同步操作确保一致性。

在数据隐私性方面，目前所有区块链技术系统的记录内容都是完全公开的，任何节点都可以查询所有交易记录。但是对于隐私敏感型数据和行业应用，需要设计账本的加密方式，信息公开的级别和访问权限要求。关于数据隐私管理，本报告中“自主权数据管理”相关部分将会予以详细论述。

2.2.2.3 智能合约

1995 年，计算机科学家尼克·萨博（Nick Szabo）给出了智能合约的定义：“一个智能合约是一套以数字形式定义的承诺(promises)，合约参与方可以在上面执行这些承诺。”

智能合约在区块链技术的逐步发展中变得越来越强大和完善。

- 智能合约 1.0：比特币在系统设计中引入了智能合约的理念，但是在系统实现过程中仅提供了基于函数调用方式的 API 接口，功能有限。这其实也是中本聪为代表的比特币开发者的初衷，过分强大的智能合约将给系统带来不可预知的安全隐患；
- 智能合约 2.0：以太坊 Ethereum 把智能合约发扬光大，首次实现了图灵完备的智能合约设计脚本语言，智能合约可以计算、存储、以及自动执行交易并修改账户约，智能合约一旦上链不可更改（Code is Law）。基于以太坊的智能合约应用，区块链进入了疯狂生长的 ICO 和通证经济时代；
- 智能合约 3.0：智能合约不仅限于交易及账户操作，Elastor、Qtum、Neo 等新兴的区块链项目实现了更为复杂的智能合约功能，几乎任何应用都可以使用智能合约实现。但是，上述区块

链项目市场影响有限，并未给区块链行业带来大的改变，其智能合约的安全性也没有得到大规模的验证。

2.2.2.4 加密及哈希算法

技术上，区块链系统上加密与哈希算法的升级主要源于已有算法的安全性受到威胁，如算法被破解等。

机制上，加密与哈希算法的选择直接影响了挖矿的实现方式和效率，进而影响了矿工的收益，从而决定了以矿工为代表的区块链社群生态的变化。

对于工作证明 POW 机制而言，利用专用芯片（ASIC）可以提高挖矿效率，造成矿工发展的不均衡，会导致事实上的中心生成。例如比特币的挖矿已经出现了几个事实上的寡头，从而引发了 2018 年“澳本聪大战吴忌寒”等寡头竞争的行业热门事件，导致比特币社群出现了一次大分裂。以太坊 Ethereum 和莱特币 LiteCoin 则分别选择了难以通过 ASIC 实现的哈希算法以保证挖矿收益的公平性和矿工社群发展的均衡性。

2.2.2.5 区块与链

比特币在社会上日渐流行，比特币网络处理和检验交易的压力加大，确认交易时间从 10 分钟到最长超过 40 小时。因此，提高比特币系统的处理能力成为区块链技术领域的核心议题之一。

1）区块扩容

比特币现金（BCH，一种比特币衍生出的虚拟货币）2017 年 8 月成立，将比特币的区块容量由 1M 升级为 8M，并计划进一步升级为 32M，

升级后，比特币现金的交易确认速度稳定为 10 分钟左右。但是，区块链扩容将增加矿工不均衡发展的机会，进一步导致矿工寡头崛起。因此在比特币社群中一直存在是否进行区块扩容的争议。

2）链与 DAG

区块链的名字中的“链”意味着所有区块通过链式结构连接在一起。链式结构可以确保区块上链的准确唯一性，但是链式结构的缺点是数据不能并行处理，导致系统效率较低。

有向无环图（Directed Acyclic Graph - DAG）原本是计算机领域的一种数据结构，因为独特的拓扑结构所带来的优异特性，被用来尝试优化区块链系统的效率。DAG 有向无环图协议使用 DAG 数据结构维护区块和系统状态，DAG 不要求节点线性方式处理交易，可以并行挖 DAG 区块，以实现更高的吞吐量和更快的交易处理时间。DAG 仍处于初级阶段，安全性和一致性尚待验证，还不能成为可行的扩展方案。

2.2.3 硬分叉——理念的冲突

2.2.3.1 节点许可

区块链系统是基于 P2P 分布式网络基础上的，基于 P2P 网络的节点加入网络是否需要许可机制，区块链系统分为许可链和非许可链。

1）非许可链：去中心化的分布式网络平台，任何节点可随时加入或者退出，节点可以通过挖矿获得奖励。

非许可链的应用场景要求

- 公开数据：链上任何节点都可以读写账本和交易信息，链上所

有数据都为公开数据；

- 数据溯源：链上保留所有数据历史，因此可追溯数据从产生至今的所有历史过程；
- 恶意节点：链上任何节点都可能故意提交错误数据，需要多节点交叉验证；
- 数据不可篡改：链上任何数据只能“读写”，不能“改删”，即使错误也不能补救；
- 交易延迟：交易信息需要所有节点同步，节点越多，延迟越大；

典型非许可链应用场景：

- 可信时间戳：任何节点可以将“时间+数据”哈希后发布上链，用以证明自己拥有某项数据；
- 能源互联网：上链记录任何节点的能源产出和消费，用于分布式智能电网的记账；

2）许可链：只有特定的节点才能加入并读写链上数据。

许可链与比特币理念的根本冲突点：

- 只有特定节点可以加入链 Vs. 任何节点可以随时加入和退出；
- 账本和交易数据读写权限 Vs. 账本和交易数据公开透明。

许可链与比特币理念的共同点：

- 基于分布式网络；
- 账户和交易数据可溯源。

许可链根据节点的可信程度可选择：

- 共识机制是否兼容恶意节点（或者只考虑故障节点）；

- 节点读写权限（读写、只读、只写）；
- 交易是否可回滚（修改、删除）。

许可链典型应用场景：

- 银行
  - 多家银行构建联盟链，共享分布账本；
  - 节点身份公开可信，无需挖矿；
  - 经协商一致，交易可回滚；
- 供应链
  - 生产商、中间商（物流）、销售商、客户；
  - 产品流程可追溯，增加消费信任；
  - 产品库存公开，增强库存管理；
- 医疗&保险
  - 个人、医院、药房、药厂、保险；
  - 分散数据上链，构建全面个人健康数据；
  - 为个人提供更好的医养、保险服务；
  - 医药研发、保险产品设计提供更具针对性数据支持。

2.2.3.2 去中心化

“去中心化”已经成为区块链技术被谈及最多的特性之一。实际上，去中心化包含两个层面：网络层面和信任层面。

从网络拓扑学的角度而言，网络拓扑结构包括三种（如图 2-1 ）。

- 中心化结构：所有信息的获取依赖于中心节点。这种结构的优点是效率很高，缺点是过于依赖中心节点，中心节点故障将导

致系统崩溃；

- 分布式结构：每一个节点都独立自主，互不依赖。这种结构的优点是系统健壮性很好，任何一个节点故障都不会影响网络运行，缺点是每个节点都是全功能节点，网络效率很低；
- 去中心化结构:介于中心化结构和分布式结构之间的一种结构。从拓扑结构上来说，又可称为多中心化结构。去中心化结构试图在系统健壮性和效率之间获得平衡。

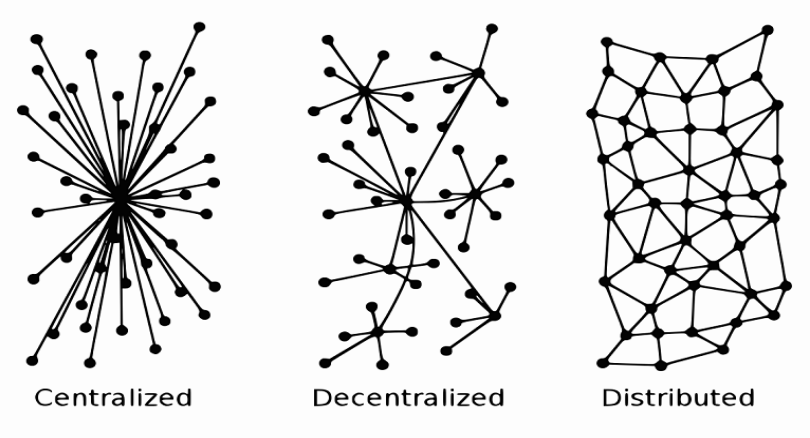

图 2-1 不同类型的网络拓扑结构

比特币和以太坊等公链项目属于完全的分布式结构。对于比特币原教旨主义者或者比特币的狂热信徒而言，完全分布式结构（他们口中的“去中心化”所指代的涵义）是一种信仰，任何变化都是对比特币精神的离经叛道。

在区块链技术的现实应用中，更需要根据应用的特性，设计一种介于中心化和分布式的网络和信任结构，安全而且高效地把区块链技术应用到现实场景中。

2.2.3.3 共识机制

如前所述，共识机制是区块链技术的核心，不同的共识机制会生成

不同的区块链系统，具有不同的技术特征。

针对在区块链系统中，应用场景是否考虑恶意节点（即主动数据造假节点）的存在，区块链分化为公链、联盟链和私链，共识机制和算法也随之不同，系统的效率也不同。（如图 2-2 ）

	公有链	联盟链	私有链
参与者	任何人自由进出	联盟成员	个体或公司内部
共识机制	PoW/PoS/DPoS	分布式一致性算法	分布式一致性算法
记账人	所有参与者	联盟成员协商确定	自定义
激励机制	需要	可选	不需要
中心化程度	去中心化	多中心化	（多）中心化
突出特点	信用的自建立	效率和成本优化	透明和可追溯
承载能力	3—20万笔/秒	1000—1万笔/秒	1000—10万笔/秒
典型场景	虚拟货币	支付、结算	审计、发行

图 2-2 公链、联盟链、私链的对比

- 公链，即非许可链，任何节点可以自由加入网络，这其中就包括恶意节点，公链的共识机制算法的容错率在 50%，只要恶意节点的算力不超过 50%，整个区块链网络都可以正常运转；
- 联盟链，许可链中的一种形式，节点要经过联盟许可才可以加入网络，但并不保证节点中不存在恶意节点，因此联盟链共识算法具有容错机制。目前常采用的拜占庭将军容错算法（BFT）及其相应的变种，容错率在 33%，只要恶意节点不超过 33%，整个区块链网络就可以正常运转；
- 私链，许可链中的一种形式。私链场景中完全不考虑恶意节点的存在，而仅仅考虑节点故障容错的情形。因此私链仅适用于

高可信任环境。

2.2.3.4 激励机制

激励机制是指关于通证（Token）发行和分配的制度设计，用于打造区块链系统的共建、共治、共享生态。基于对通证的认知和理解，区块链发展分化为“链圈”和“币圈”。传统传销诈骗手段和通证化混杂加剧了冲突的复杂性。

1）无币区块链：是指专注于分布式网络、共享账本、加密算法、智能合约等区块链技术在行业中的应用，视区块链为新一代 IT 基础设施，不在意基于通证（Token）的激励机制。

2）通证经济：针对区块链项目的社群自治模式，基于博弈论和产权理论设计社群经济模型、治理机制和自金融生态。其中通证(Token)是项目和社群价值的载体，其发行和分配制度设计是通证经济的核心关注问题。

ICO（虚拟代币发行融资）的出现把通证经济推向社会前沿，但是通证经济理论和商业模式设计还未成熟，ICO 中“空气币”“传销币”等非法集资行为为通证经济的发展带来严重负面影响。

3）通证与区块链分离：试图把通证经济概念引入到传统（非区块链）领域，利用通证（Token）设计激活经济活力，其典型为“行为挖矿”机制。从目前已有的证链分离实践来看，大多项目走入非法集资的邪路。

2.2.3.5 身份与隐私

比特币具有伪匿名特征。比特币的匿名性是指用户能持有一个钱

包地址而不公开任何身份信息。但是，在比特币世界里的所有交易都是可追踪的，所有交易都保存在区块链里，基于社交大数据可以提炼追踪到真实用户身份。2015 年，国际刑警根据比特币交易流水追踪到暗网交易的非法人员，直接把全球最大的暗网丝绸之路（Silkroad）相关人员抓获。这加剧了人们对比特币匿名性的怀疑。

基于对匿名理念的认知和理解冲突，区块链发展分化为数字身份和完全匿名两条发展路径。

1）数字身份：完全实名制，在实名的基础上保护隐私数据的主权管理。

- 基于法律背书的实名认证，按照不同的授权等级采取人体生物识别特征（人脸、指纹、瞳孔、DNA 等），并通过哈希生成数字身份；
- 区块链数字身份的实施让用户成为自己信息的主人，任何对用户信息的访问和使用都需要用户的数字授权。

2）完全匿名：另有一部分区块链项目走向更深入的匿名机制，完全匿名的代价是交易信息完全不可追溯。

- 达世币 Dash：利用混币技术增加追踪难度；
- 门罗币 Monero：环签名技术隐藏交易者身份；
- 大零币 Zcash：使用零知识证明技术隐藏交易双方以及金额。

2.2.3.6 控制与主权

比特币的支持者宣称比特币网络无控制权和主权干预，即没有任何一个用户、国家、政府可以控制比特币系统。无政府主义是比特币

诞生的重要哲学理念。但实际上，比特币社区的核心开发者发布并上线的软件会影响系统的大部分节点和用户。因此，比特币社区的核心开发者实质上在控制着比特币系统，核心开发者的冲突和分裂会导致比特币网络的分叉，这在比特币的短暂历史上已经发生过很多次了。

因此，比特币系统无控制和主权的准确表述应该是：在现有比特币网络运行规则下，没人可以控制用户交易的时间和对手方。但是，无控制也意味着用户需要自负其责，即用户自己全权承担维护自己密钥的责任，一旦丢失无法找回。用户丢失密码导致其拥有的比特币永远无法找回的案例也数不胜数。

基于区块链本身的技术特性及其在社会治理中的应用潜力，中国贵阳市政府 2016 年发布的《贵阳区块链发展和应用》白皮书中提出了主权区块链的概念。

所谓主权区块链，是指将区块链技术发展纳入国家主权范畴下，在法律与监管下，从改进与完善自身架构入手，以分布式账本为基础，以规则与共识为核心，实现不同参与者的相互认同，进而形成公有价值的交付、流通、分享及增值，建立主权区块链。在主权区块链发展的基础上，不同经济体和各节点之间可以实现跨主权、跨中心、跨领域的共识价值的流通、分享和增值，进而形成在互联网社会的共同行为准则和价值规范。（如图 2-3 ）

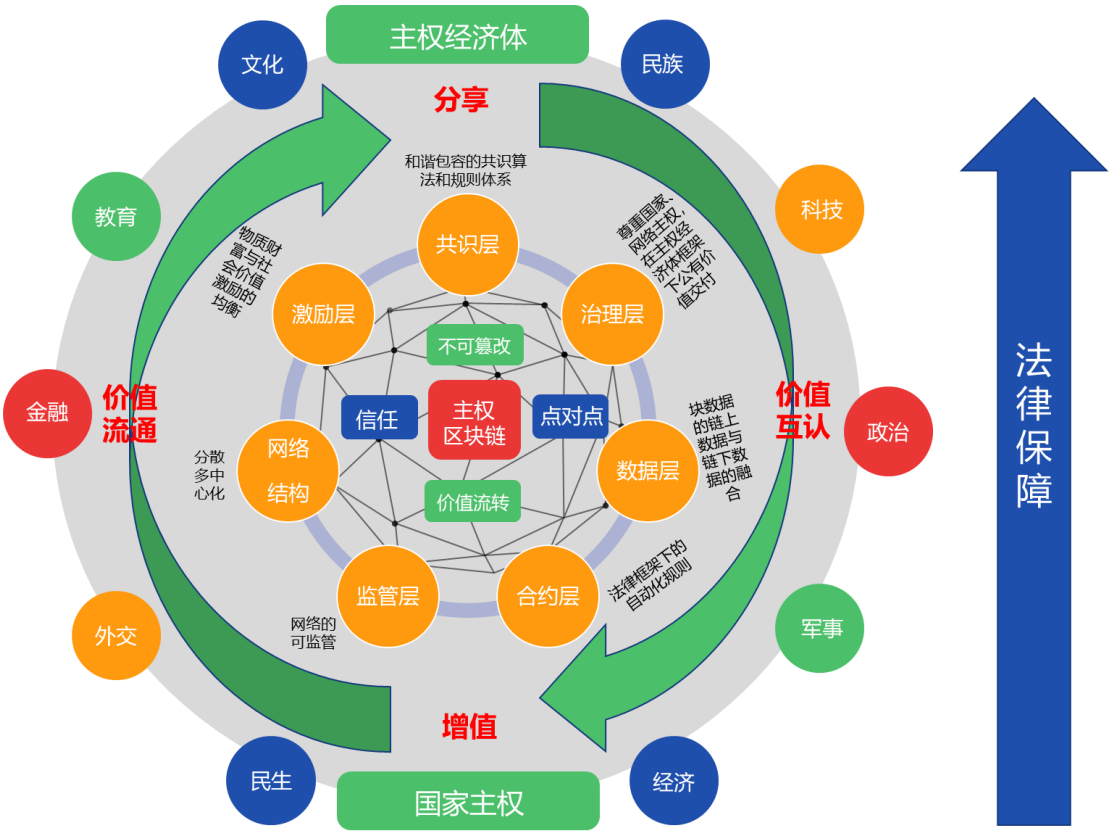

图 2-3 主权区块链示意图

第三章 可信公链与数字货币

3.1 基于比特币技术的衍生

比特币（BTC）用可信公链和数字货币开创了区块链时代。比特币对于诞生的时代和目标应用场景而言，是技术完备的，目前区块链领域的所有发展都可以在比特币的设计中找到影子。比特币的机制简述如下：

- POW 机制，使用 SHA256 哈希算法；
- 每 10 分钟产生一个新的区块，每个区块大小 1M；
- 挖矿发行机制，总数 2100 万，初始每次挖矿 50 枚，每四年减半；
- 每一个交易都附带脚本代码，可触发执行交易，构成智能合约的雏形；

比特币作为一个开源代码项目，其社区生态包括如下三个部分：

- 社区核心开发团队：核心开发团队来自世界各地，主要通过网络进行交流，主要任务是维护和更新比特币源代码，修复软件漏洞，保证网络的正常运行并不断提高网络的性能。
- 矿场：初期挖矿是基于个人电脑，随着挖矿设施逐渐升级（显卡、专用芯片 ASIC、数据中心、矿池），逐渐形成一批矿场寡头。矿场对比特币网络流畅运行有一定的影响，任何代码更新都需要矿场配合，因此矿场对比特币的开发具有一定程度上的发言权。
- 明星个人：比特币的早期拥护者，本身也持有大量的比特币，

具有很强个人号召力。

随着 BTC 用户的增加和应用场景的多元化，BTC 在性能和功能上都需要进一步扩展，比特币的子孙们基本复制了比特币的开源代码，并做了不同的扩展和分叉。

3.1.1 莱特币 LiteCoin（LTC）

莱特币 LTC 是比特币 BTC 比较早期产生的一个分支，目标是提供更快的交易确认时间。为此，莱特币在如下机制上做了升级与改进：

- POW 机制，使用 Scrypt 哈希算法，该算法使用更多内存，不易 ASIC 实现，避免了矿场算力的过度集中，同时也汇集了比特币生态中被 ASIC 算力挤出的显卡类矿工；
- 币总量升级为 8400 万枚；
- 实现了隔离见证（SegWit）功能，一方面从区块数据容量上实现了扩容，另一方面解决了交易延展性攻击问题，可以更好地支持闪电网络等链下交易技术。(隔离见证和交易延展性性攻击参加 3.2 节相关内容）

3.1.2 比特币现金 BitCoin Cash

比特币现金（国内简称 BCH，国外简称 BCC）的前世就是比特币，在 2017 年 8 月与比特币分叉之前，它存储的区块链中的数据以及运行的软件是和所有比特币节点兼容的，而到了分叉那一刻以后，它开始执行新的代码，形成新的公链。

比特币现金坚持链上扩容，解决了 BTC 中手续费高、确认慢、实用性差等问题，目前比特币现金由 8 个不同的开发团队维护；比特币

现金在比特币扩容方面，直接支持大区块（将区块大小从 1M 提升至 8M），不包含隔离见证 SegWit 功能。

比特币现金的诞生是比特币社区矛盾和冲突的一次爆发，以矿场为主的利益方支持了比特币现金 BCH 的诞生和发展。

3.1.3 其他衍生产品及机制对比

除上述影响力较大的比特币衍生产品外，还存在诸如比特币黄金（BitCoin Gold）等虚拟货币。各种不同货币的机制对比如下图 3-1 。

	Bitcoin 比特币	Bitcoin Gold 比特币黄金	Bitcoin Cash 比特币现金
货币发行上限	2100万	2100万	2100万
POW算法硬件支持	ASIC	GPU	ASIC
区块链生成时间间隔	10 分钟	10分钟	10分钟
难度调整时间间隔	2 周	每个区块	2周+EDA
Segwit隔离验证支持	是	是	否
中继保护	不适用	是	是
唯一地址格式	不适用	未来将支持	否

图 3-1 比特币衍生虚拟货币的对比

3.2 比特币的扩展方案

针对比特币的设计机制，直观上比特币性能的扩展方案可以从几个方面入手，比如增加区块大小，或者修改共识和记账机制。但是，这些直观的扩展方案会导致老系统无法兼容，因而将会硬分叉产生新的比特币网络，这对于比特币的信仰者是不可接受的。因此下面讨论

扩展方案都是不改变比特币基本机制下的扩展方案。

3.2.1 隔离见证（Segregated Witness ）

比特币的每一个交易记录的数据内容分成两个部分：交易数据和签名数据。其中签名数据占了交易记录的 65%。隔离见证 SegWit 机制约定链上区块只存储交易记录中的交易数据，而签名数据将存储在附加的见证（Witness）区块上。隔离见证机制实质上扩展了比特币区块的大小，并保持了与传统比特币网络的兼容性。

隔离见证机制同时也解决了比特币的交易延展性问题（Transaction Malleability)。

交易延展性 (Transaction Malleability)，是指当交易被签名时，签名并没有覆盖交易中所有的数据（即发送者的公钥和签名数据)，而交易中所有的数据又会被用来生成交易的哈希值作为该交易的唯一标识（transaction ID)。如此，比特币网络中的节点能够改变发送的交易内容（通过改变发送者中的签名，因为在椭圆曲线算法中可能存在两个有效的签名，攻击者可以将一个有效的签名改成另一个，但仍然是有效的签名)，导致该交易的哈希值，也即交易的唯一标识（transaction ID）发生变化。

注意，攻击者仅仅能够改变该哈希值（transaction ID)，但不能改变交易中的其他数据。然而，这确实意味着，在任何情况下，接收一系列未确认交易的链是不安全的。因为未确认交易的唯一标识可能会发生变化，而随后的交易中的发送者会依赖于先前交易的唯一标识来确认结算。即使交易得到了一个确认，也是不安全的，因为区块链

可能会被重新调整。

简单地说，交易延展性，或者叫做“交易可锻性”，指的是，比特币支付交易发出后、确认前可被修改（准确说是被伪造复制）。2014年，黑客利用了交易延展性，对当时最大的比特币交易所 MT.GOX 交易所（俗称“门头沟交易所”），导致交易所倒闭。本次攻击交易所丢失了 85 万个比特币，按当时的币价计算，这些损失的比特币价值近 4.54 亿美元。

黑客的攻击过程如下：

- Step1：黑客自己有 1 个账号，在交易所开了 1 个账号，把自己的比特币转进去。
- Step2：申请提现（withdraw），交易所发起 1 笔转账交易（Transaction）。
- Step3：这笔交易被广播到网络上，还未打包进区块链之前。黑客收到这笔交易，稍微更改了签名的格式，生成 1 笔新的交易广播出去，此时交易标识（Transaction id）已经变了。
- Step4：黑客的这笔新交易被区块链接收了。然后向交易所投诉，说它没收到钱。交易所根据自己生成的交易标识（Transaction id）查询该笔交易，发现在网络上查询不到， 会再次转账给黑客。导致同一笔钱，被黑客提现了 2 次，甚至多次。最终使交易所蒙受巨大损失。

隔离见证（SegWit）将签名数据与交易数据分离，使得交易标识（Transaction id）具有唯一性和稳定性，解决了交易延展性问题。

3.2.2 侧链技术（Side Chain）

侧链技术让用户可以在比特币和其他功能不同的区块链之间相互转移货币。在这个场景下，比特币被称为主链，其他的区块链则被称为侧链。侧链上可以使用价值来自主链的货币，与主链的功能和特性都可以不同，在一定程度上提高了主链的处理能力，扩展了主链的应用。围绕主链可以搭建起一个业务形态丰富的侧链生态。

主链向侧链转移货币时，将这些货币在主链上锁定的方式包括：

- 多方联合保管：在主链上创建一个多方共管地址，转移到侧链的虚拟货币用这个地址锁定，被锁定的虚拟货币需要多数同意才能使用；
- “矿工”保管：更容易围绕一个主链打造多个侧链应用，但是需要比特币的协议升级支持；
- 混合保管：主链使用多方共管，侧链使用矿工保管。

侧链技术的案例主要有三种：

- RootStock（RSK）：是一个建立在比特币区块链上的图灵完备的智能合约平台。
- Liquid:为用户提供一种从交易所安全、即时转移资金的方式。Liquid 将资金转移到一个共享的多重签名钱包地址，并通过一种拜占庭循环共识协议的区块链来处理交易。
- 扩展区块：是指在主链的区块之外并行地运行另一个侧链， 但是所有的矿工都要去验证这个侧链上的区块。因此可以将这些侧链区块看成主链的扩展区块。扩展区块可以提高交易处理能

力或者实现不容易在主链上推行的特性。

3.2.3 闪电网络（Lighting Networks）

闪电网络的设计思想则是将大量交易放到比特币区块链之外进行，只把关键环节放到链上进行确认。

闪电网络本质是使用了哈希时间锁定智能合约来安全地进行零确认交易的一种机制。闪电网络是由微支付通道演进而来，有两种类型的交易合约：序列到期可撤销合约 RSMC（Revocable Sequence Maturity Contract)，哈希时间锁定合约HTLC（Hashed Time Lock Contract)。

RSMC的设计思路是交易双方共同出资以创建一个双向微支付通道。交易双方先预存一部分资金到微支付通道里，初始情况下双方的分配方案等于预存的金额。每次发生交易，需要对交易后产生资金分配结果共同进行确认，同时签名把旧版本的分配方案作废。任何一方需要提现时，可以将他手里双方签署过的交易结果写到区块链网络中，从而被确认。

任何一方在任何时候都可以提现，提现时需要提供一个双方都签名过的资金分配方案。在一定时间内，如果另外一方拿出证明表明这个方案已经被作废了(非最新的交易结果)，则资金罚没给质疑方；否则按照提出方的结果进行分配。罚没机制可以确保没人会故意拿一个旧的交易结果来提现。

另外，即使双方都确认了某次提现，首先提出提现一方的资金到账时间要晚于对方，这就鼓励大家尽量都在链外完成交易。通过 RSMC，

可以实现大量中间交易发生在链外。

HTLC 可以保障任何两个人之间的转账都可以通过一条支付通道来完成。HTLC 简单理解就是限时转账，通过智能合约，双方约定转账方先冻结一笔钱，并提供一个哈希值，如果在一定时间内有人能提出一个字符串，使得它哈希后的值跟已知值匹配（实际上意味着转账方授权了接收方来提现），则这笔钱转给接收方。通过 HTLC 可以在闪电网络任意节点之间安全转移价值而无需信任中介节点。

闪电网络整合 RSMC 和 HTLC 两种机制，可以让任意两个节点之间的交易都在链下完成。在整个交易中，智能合约起到了中介的重要角色，而区块链网络则确保最终的交易结果被确认。闪电网络通过将大量的交易放在链下完成，大大降低了主链负荷，从而让主链快如闪电。然而，从其工作原理分析，闪电网络也会带来一些问题：

- 如果通道中任一节点反应迟钝，用户可能要等上几个小时才能关闭支付通道，并通过另一种途径重新发送资金；
- 没有离线支付：用户无法支付不在线的人；
- 不适合大额支付：即使一条经由各种支付通道的路线可能存在，但通道中其它节点多重签名钱包中的资金可能不足以转移大笔资金；
- 集中化：闪电网络可能会鼓励支付枢纽的集中化（类似于矿工集中化）。闪电网络包含百万级别的支付通道，通道内锁定了大量的资金，特别是大的中介人通道容易成为系统性攻击的目标。

没有一种技术可以解决所有问题，虽然闪电网络仍然存在一些问

题，但不可否认闪电网络是一个创新性的设计。对于闪电网络的研究仍在继续，相信未来闪电网络的应用会更加完善。

3.3 增强匿名的数字货币技术

3.3.1 达世币 Dash (DASH)

DASH 原名叫做暗黑币（Dark Coin），是在比特币的基础上做了技术上的改良，具有良好的匿名性和去中心化特性，是第一个以保护隐私为要旨的数字货币。听它的名字也能感觉出来 DASH 被黑市交易所喜欢。DASH 在 2014 年发布白皮书，发行总量为 1890 万个。DASH 问世之后，就被网友们奉为最能实现中本聪梦想的币种。

DASH 是在比特币代码的基础上创建的，但在代币总量、开采机制、出块速度、奖励分配等方面略有不同。（如图 3-2 ）

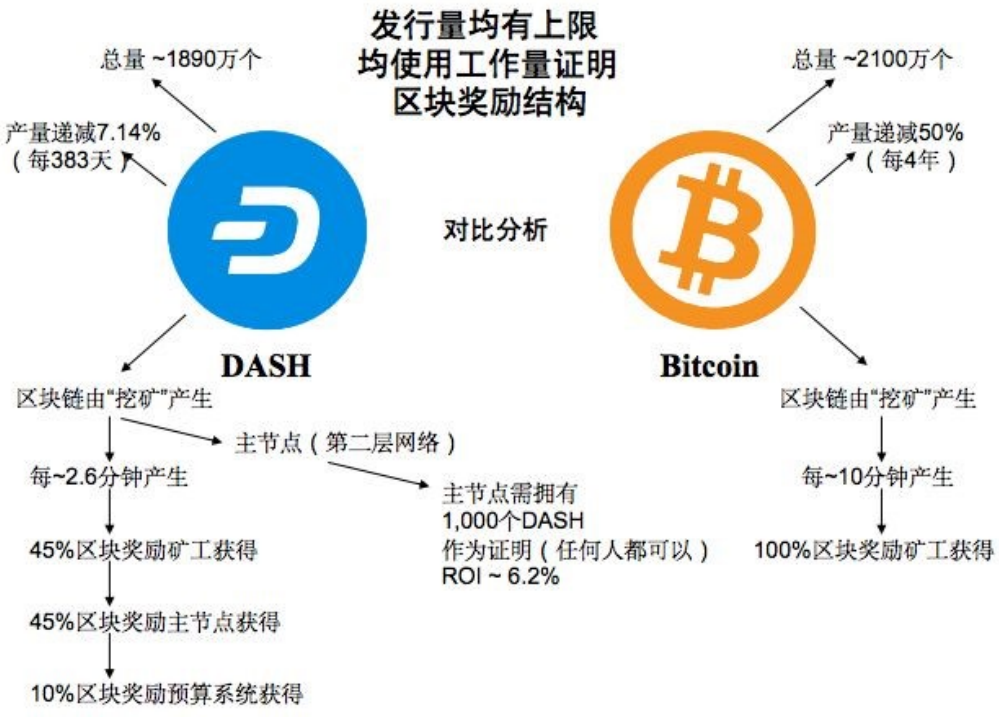

图 3-2 DASH 的机制设计对比

相比于比特币，DASH 主要有两点不同。

- 其一是 POW 矿工网络之上的主节点网络。主节点有四大职能，提供混币服务、即时支付、抵御 51% 攻击的链锁、和社区投票治理。该网络使用 POS 机制达成共识。
- 其二是独特的经济模型/治理机制。45% 区块奖励给矿工、45% 给主节点，另外 10% 给了“预算系统 DASH DAO”。

DASH 的去中心化自治组织 DASH DAO，它最重要的功能正如其名“预算系统”一样，能从区块奖励中抽取 10% 的费用，为网络发展提供激励和预算。DASH DAO 的预算资金任何人都可以申请，只不过提交议案有一定成本。此后主节点对提案投票，赞成票减去反对票的结果大于主节点总量的 10% 即可通过。（如图 3-3 ）

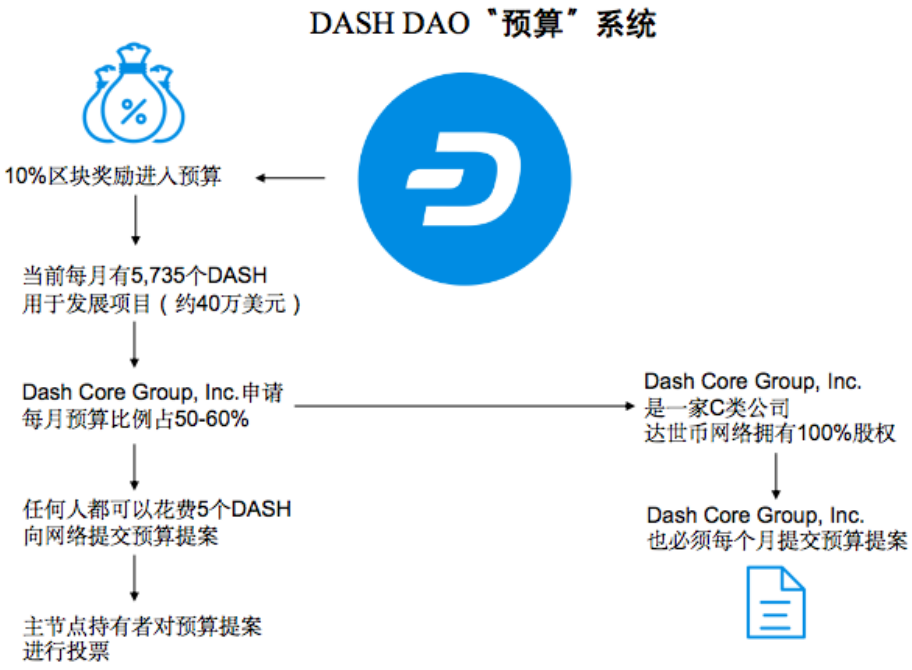

图 3-3 DASH DAO 预算系统工作原理

DASH 的开发团队 Dash Core Group（目前正式职员 20 余位），也需每月提交预算提案申请资金，可看作受雇于 DASH，一般每月可获得预算的 50-60%。DASH DAO 最早主要为了解决开发者的激励问题，后

来演变成重要的治理模式。

1）Dash 的双层网络实现即时支付

举例说明，Alice 向网络请求向 Bob 即时支付 1 枚 DASH。DASH 网络会随机选择 30 个（具体数量视金额大小而定）主节点，形成长效主节点仲裁链认证交易合法性，多数节点认证后该笔交易就被锁定，可视为到账了。此时，Bob 已经可以使用这枚 DASH 了。

而后，主节点将该交易向全网广播，就像比特币记账那样，矿工验证交易后写入最新的区块中。

通过随机选出的主节点“先斩后奏”的机制，实现即时交易。DASH 的主节点目前有 5000 余个，加上每个主节点均在网络中质押了 1000 DASH 作为保证金，也即一笔即时支付有百万美元资金作为担保。因此，DASH 的共识机制是“POW+POS”，DASH 称之为 Proof of Service，因为主节点和矿工都在为网络提供服务。

2）依靠“链锁”机制抵抗 51% 攻击

在矿工产生区块后，主节点网络还将随机选择 400 个主节点（时常在线的节点）生成长效仲裁链（Long-Living Masternode Quorums，LLMQs），对区块按照时间戳进行锁定。即便后来某位持有网络超过 51% 算力的大矿工释放出新区块，新链虽然是最长链，但其却无 LLMQs 的确认，由此将被网络拒绝，从而抛弃。

主节点的产生需要使用 1000 DASH 币做抵押，这提高了作恶成本和 51%攻击成本；DASH 的 POW 挖矿机制中使用 X11 哈希算法，即 11 种 SHA-3 算法的组合，因此 ASIC 挖矿基本不可行。

3）使用混币技术实现匿名

DASH 在默认情况下是即时支付，匿名支付作为一个可选项。DASH 采取名为“Coinjoin（混币）”的技术来实现匿名交易。该技术把属于不同人的 DASH 币（最低 3 笔一组）混在一起，拆分后再发送，从而割裂了交易双方的联系。多次混币、每次少量币，效果更好。混币服务将不同用户手中的币混合在一起，减少单笔份额，并分配给特定的接收者。这一过程会导致交易历史的随机化。成功的混币服务会聚合大量的随机交易进行再分配，这是一个需要协调的并且相当耗时的方法。（如图 3-4 ）

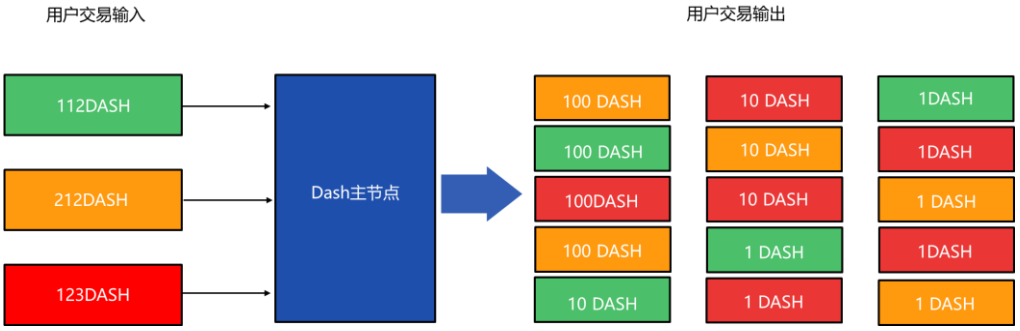

图 3-4 DASH 的混币技术示例

3.3.2 门罗币 Monero（XMR）

门罗币 Monero 于 2014 年 4 月 18 日推出。门罗币将自己定义为一种“Untraceable Digital Money”，采取的匿名方式也十分激进——交易地址、金额等交易信息都被隐藏起来。XMR 主要发行曲线为在约 8 年内发行约 1840 万枚币，其工作验证算法 CryptoNight 是 AES 密集型和很耗内存的操作，这显著降低了 GPU 对 CPU 的优势。

1）XMR 是如何成功地实现隐私加强的

环形签名(Ring signatures)和隐秘地址(Stealthy addresses)

是 XMR 实现隐私加强的关键技术。

环签名是一种简化的类群签名，它因为签名由一定的规则组成一个环而得名。在环签名方案中，环中一个成员利用他的私钥和其他成员的公钥进行签名，但却不需要征得其他成员的允许，而验证者只知道签名来自这个环，但不知谁是真正的签名者。环签名是 CryptoNote 协议的一部分，环签名策略就是“在人群中隐藏”，其成功与否取决于“人群”的规模以及成员的随机性。

隐秘地址有助于提供更高的隐私性。每一笔带有接收者姓名的交易都会随机生成隐秘地址，以隐藏其真实地址，从而隐藏收件人的身份。

2）XMR 面临的主要挑战

高隐私性和无法进行搜索回溯导致 XMR 可被用于毒品交易和赌博等非法活动中。事实上，在 Oasis 和 AlphaBay 等暗网市场中，门罗币的使用越来越多。虽然门罗币的高隐私性和逃避法律制裁带来了有益的结果，但同时也带来了极高的风险。

3）XMR 的优势

- XMR 拥有更好的挖矿算法：比特币算法在定制的挖矿芯片上（被称为 ASIC）的运行速度比在标准家庭电脑或者笔记本电脑上快得多，这会导致矿工相对集中在电力成本低的那些国家。相比之下，门罗币的挖矿算法是专门设计的，因此 ASIC 与普通公众的电脑设备相比不会拥有太大优势。
- XMR 的“自适应区块大小限制”：当交易广播到门罗币或者比

特币的网络时，它们将被打包到“区块”中。门罗币每两分钟出一个块，而比特币平均每十分钟出一个块。因为区块大小拥有上限，因此如果空间不足，交易会被延迟。门罗币从一开始就设置了自适应的区块大小。这意味着，它可以自动的根据交易量的多少来计算需要多大的区块。因此门罗币从设计上不存在需要通过硬分叉和共识来提高区块大小的问题。

3.3.3 大零币 Zcash（ZEC）

Zcash 是首个使用零知识证明机制的区块链系统，它可提供完全的支付保密性。与比特币相同的是，Zcash 代币（ZEC）的总量也是 2100 万，Zcash 出块和奖励机制类似比特币，不同之处在于，最初的 20,000 个块的奖励很少。这样做的目的是为防止早期的快速挖矿对 Zcash 系统造成伤害。

Zcash 交易自动隐藏区块链上所有交易的发送者、接受者及数额。只用那些拥有查看秘钥的人才能看到交易的内容。用户拥有完全的控制权，他们可自行选择向其他人提供查看秘钥。

零知识证明（ZKPs）： ZKP 是一种密码学技术，是一种在无需泄露数据本身情况下证明某些数据运算的一种零知识证明，允许两方（证明者和验证者）来证明某个提议是真实的，而且无需泄露除了它是真实的之外的任何信息。（如图 3-5）

Zk-SNARK 零知识证明：

A 要向 B 证明自己拥有某个房间的钥匙，假设该房间只能用钥匙打开锁，而其他任何方法都打不开。这时有 2 个方法：

一是，A 把钥匙出示给 B，B 用这把钥匙打开该房间的锁，从而证明 A 拥有该房间的正确的钥匙。

二是，B 确定该房间内有某一物体，A 用自己拥有的钥匙打开该房间的门，然后把物体拿出来出示给 B，从而证明自己确实拥有该房间的钥匙。

后面这个方法属于零知识证明。好处在于在整个证明的过程中，B 始终不能看到钥匙的样子，从而避免了钥匙的泄露。

图 3-5 零知识证明示例

使用 Zcash 零知识证明的用户能够在不泄露数据内容的情况下证明数据状态。这种方式用于加密数据的密码学验证，可以不公开发送方以及交易金额，但同时又能做到证明这笔交易的合理性。零知识证明的速度很慢。整个计算过程需要花费约 48 秒的时间。因此，这种方法不适合用在大流量交易中。

ZCash 的加密功能是可选项。大多数 ZCash 交易是没有保密功能的。这对那些担心隐私问题的 ZCash 用户是不利的，因为他们的活动只在一小部分启用了保密功能的用户群中处于隐藏状态。如果只能在一个非常小的群体中保持匿名性，而且这一小群人只有在需要隐藏某些东西的时候才会暂时出现，那么匿名也没有什么意义。

另外，Zcash 所涉及的加密概念对数学界来说也是全新的，可能要花上二十年的时间产业界才能真正有信心使用零知识证明解决安全问题。

第四章 以太坊（Ethereum）与智能合约技术

4.1 以太坊技术原理

以太坊（Ethereum） 致力于提供一个可编程的智能合约平台，相较于比特币脚本刻意追求简单的特点，以太坊的目标是提供一个带有内置的、成熟的、图灵完备语言的基础设施[3]。以太坊开创区块链 2.0 时代，不仅仅因为智能合约，在公链技术上也做了很多突破性创新。图 4-1 对比特币与以太坊的技术进行了简单对比。

BitCoin公链技术	Ethereum公链技术
哈希与Merkle树	使用Ethash反制ASIC；Merkle Patricia Tree数据结构，兼顾安全和效率
UTXO记账方式	使用基于账户的记账方式，包括用户账户和合约账户
区块与链	创新叔区块机制，提高效率；使用简化的DAG组织成链
P2P分布式网络	有自己的分布式系统， 包括文件服务（Swarm）、信息传输（Whisper） 和信用担保。
共识机制	当前使用POW，提出并准备启用POS
挖矿发行与激励机制	ICO发行7200万；每年挖矿发行1800万，目前不设上限；挖矿难度系数调整机制；创新合约执行的GAS消耗机制；
智能合约	图灵完备，虚拟机EVM及Solidity语言
治理机制	以太坊基金会制订了明确的发展路径和硬分叉升级计划

图 4-1 比特币与以太坊公链技术对比

4.1.1 账户机制

比特币使用 UTXO 记账，因此没有账户的概念。以太坊有两种类型的账户：**用户账户(EOA)和合约账户**。

- 用户账户由私钥控制，每个账户都有自己的余额。拥有者可以创建和签名一笔交易，如果账户余额足够支付交易费用，则交易有效，那么发起方账户会扣除相应金额，而接受方账户则计

[3] Buterin Vitalik, A Next-Generation Smart Contract and Decentralized Application Platform [OL], Ethereum White Paper, https://ethereum.org/, 2013.

入该金额。

- 合约账户由代码控制。在一些情况下，当合约账户收到一条消息，合约内部的代码就会被激活，允许它对内部存储进行读取和写入、发送其它消息或者创建合约。

UTXO 与以太坊账户机制的对比如图 4-2 。

	UTXO	账户机制
优点	每个货币均可溯源；防止重放攻击；防止账户跟踪，保护隐私；	更高的货币通用性；账户操作简单；轻客户端；
缺点	每次计算地址余额需遍历UTXO	账户不可删除；账户可跟踪，隐私性差；为防止重放攻击，需要记录每笔交易的交易标识（nouce）

图 4-2 UTXO 与账户机制的对比

4.1.2 交易和消息

用户账户发起的签名数据称为**交易**；合约账户发起的签名数据称为**消息**。

- 交易记录的数据结构如下：
  - 1、交易标识（nouce）：随机数，用于确定每笔交易只能被处理一次的计数器，用于抵制重放攻击；
  - 2、接收方地址（receipt）：可以是用户地址或者合约地址；
  - 3、数值（value）：交易的以太币数量；
  - 4、数据（data）：可选填项，供智能合约接收方使用的数据；
  - 5、V/R/S：ECDSA 签名，用来恢复公钥；

- 6、GASPRICE：每一个 gas 的价格；
- 7、GAS：交易使用的最大 gas 数量

以太坊引进了“燃料（GAS)”的概念。两个数值 GAS 和 GASPRICE 的作用是为了对代码执行做出经济上的限制。这种经济上的举措就好比我们生活中的智能卡用电。为了防止滥用电资源（当然，还有其他的经济因素)，国家制定了用电成本，电价越贵，我们的用电成本就越高。我们能用多少电取决于花了多少钱买电，一旦用完，家里就停电了。

以太坊系统中，任何运算都是需要占用/消耗资源的，这包括计算资源、带宽资源、存储资源等。为了防止代码被恶意或不停地执行(如无限循环运算或其他无谓消耗资源的运算)，每笔交易需要对执行代码所引发的计算，包括初始消息和所有执行中引发的消息做出经济上的限制。GASPRICE 是每一计算步骤所需要支付的费用，好比电价。GAS 是交易执行时最大计算步骤数，好比电量。这两个值的作用就是用来限制交易中所能执行的代码计算步骤的。所以，在交易执行时，账户余额需要有足够多的“钱”来满足执行交易中代码的经济需求。

简单理解，就是以太坊中规避计算机恶意攻击占用资源的解决方案是经济制裁。既然执行交易需要预先设置花多少钱，那么就可能有下面这两种情况发生：钱用完了、钱剩余了。

- 1. 如果执行交易的过程中，用完了“燃料”（GAS)，那么所有状态将恢复到原状态，但是已经支付的交易费用不退。
- 2. 如果执行交易完结时还剩余燃料，那么这些燃料将退还给发

送者。

以太坊交易的具体步骤如下：

- 1. 检查交易的格式是否正确、签名是否有效和交易标识 nouce 是否与发送者账户的交易标识 nouce 匹配。如否，返回错误。
- 2. 计算交易费用：fee=GAS * GASPRICE，并从签名中确定发送者的地址。从发送者的账户中减去交易费用，增加发送者的 nouce。如果账户余额不足，返回错误。
- 3. 设定初值 GAS，并根据交易中的字节数减去一定量的燃料值。
- 4. 从发送者的账户转移货币价值到接收者账户。如果接收账户不存在，创建此账户。如果接收账户是一个合约，运行合约的代码，直到代码运行结束或者燃料用完。
- 5. 如果因为发送者账户没有足够的钱或者代码执行耗尽燃料导致价值转移失败，恢复原来的状态，但是还需要支付交易费用，交易费用加至矿工账户。
- 6. 否则，将所有剩余的燃料归还给发送者，消耗掉的燃料作为交易费用发送给矿工。

以太坊的消息跟交易在很多方面是相同的。不同点在于消息是从合约发出的，而不是从用户账户。这里需要注意的是，消息触发合约的执行同样也需要消耗燃料。

4.1.3 共识机制与挖矿

目前的以太坊的共识机制是工作量证明（POW)。效仿比特币，以太坊也通过挖矿的模式来产生系统中流通的货币——以太币。同时，

通过奖励的机制来激励那些处理交易并维护网络安全的矿工。虽然很多方面都与比特币系统相似，不过以太坊的挖矿机制也有其不同之处。

4.1.3.1 以太币的发行机制（永久线性增长模型）

与比特币累计发行总量固定为2100万不同，以太坊目前的设计是每年都会发行一定数量的货币，并且会一直发行下去。我们知道，比特币是通缩的，那么这是否意味着随着以太币的不断发放，会造成严重的通胀呢？按照以太坊的官方说法，其每年发行的货币有个数量上限，即1800万。随着时间的推移及货币的流失（如丢失、忘记私钥等），每年的通货膨胀率将递减，最终趋于零，达到平衡状态。

- 1. 预售期共发行了7,200万。其中6,000万用于募资，1200万归属开发团队及以太坊基金。
- 2. 每挖出一个区块奖励矿工5个以太币。在Byzantium版本中，奖励额降为3个。
- 3. 每年发行上限为1,800万。
- 4. 固定数额发行机制使实际通货膨胀率接近0。

4.1.3.2 挖矿算法设计与考量

以太坊的挖矿算法并未采用比特币所使用的 Sha256，而是在Hashimoto和Dagger基础上建立了自己的Ethash算法。算法设计概要如下：

- 与CPU无关，与内存大小及带宽相关；
- 抵御专门的矿机（ASIC）；
- Ethash使用了一种DAG的数据结构，每30,000个区块（约125

个小时）随机生成一个新的DAG，POW尝试基于给定的DAG和难度系数来解决一个约束问题，解决问题的过程难，验证答案的过程易。

目前主流以太坊挖矿采用GPU。实际挖矿操作，需要每个GPU最少具备1G以上的RAM用以加载DAG。另外，由于挖矿算法是通过OpenCL实现的，所以在同等价格下，AMD GPU相比较NVIDIA GPU有更好的表现。

需要注意的是，在规划的以太坊Serenity版本中，共识机制计划会变更为权益证明（POS）。

4.1.3.3 挖矿的奖励机制

奖励给成功挖出区块的矿工的金额如下：

- 每个区块奖励5个单位以太币，在Byzantium版本中调整为3个单位；
- 区块中的交易所花掉的费用（由GAS和GASPRICE决定，以以太币记账）；
- 如果区块中包含了叔区块，那么每收录一个叔区块将额外获得1/32的区块奖励（最多收录2个）；
- 奖励给被区块矿工收录的叔区块矿工：区块奖励的7/8（即4.375个以太币，Byzantium版本为2.625个以太币）。

4.1.4 幽灵协议GHOST与叔区块

“幽灵”协议（Greedy Heaviest Observed Subtree - GHOST Protocol）是由Yonatan Sompolinsky 和 Aviv Zohar在2013年12

月引入的创新。幽灵协议的提出是为了应对在确认时间较为快速的区块链中，由于生成区块的高作废率而受到安全性降低的困扰。

4.1.4.1 幽灵协议的动机

以太坊大概 15 秒就出一个块，出块速度提高，区块被打包之后，在这 10 多秒里尚未在全网播布完，如果矿工 A 挖出了一个区块然后矿工 B 碰巧在 A 的区块扩散至 B 之前挖出了另外一个区块，矿工 B 的区块就会作废且没有对网络安全做出任何贡献。

这种因出现分叉情况未能进入主链的区块成为“孤区块”。孤区块消耗了算力，但没为系统做出贡献，也没奖励。过高的孤区块作废率导致小矿工退出市场，进而导致：1、算力下降降低系统安全性；2、算力向大矿场集中导致系统中心化。

如果 A 是一个拥有全网 30%算力的矿池而 B 拥有 10%的算力，A 将面临 70%的时间都在产生作废区块的风险而 B 在 90%的时间里都在产生作废区块。如果作废率高，A 将简单地因为更高的算力份额而更有效率。因此，区块产生速度快的区块链很可能导致一个矿池拥有实际上能够控制挖矿过程的算力份额。

以太坊采用幽灵协议解决了降低网络安全性的问题。在计算哪条链“最长”的时候把作废区块也包含进来以计算哪一个区块拥有最大工作量证明。

4.1.4.2 叔区块

以太坊推出了叔区块的概念。叔区块是当前区块祖区块(爷爷辈，往前两个区块）及其之前祖先区块的废弃后代区块。这个祖先区块最

远可以到第七代。（如图 4-3 ）

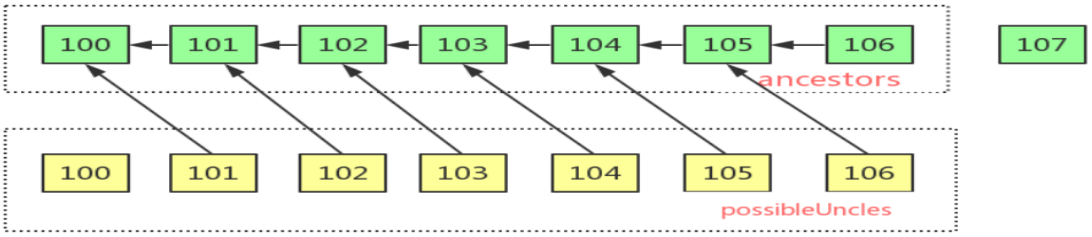

图 4-3 叔区块示意图

以太坊付给以“叔区块”身份为新区块确认做出贡献的作废区块87.5%的奖励,把它们纳入计算的“侄子区块”将获得奖励的12.5%。通过奖励引用叔块，给小矿工生存空间，保证算力的分散化，促进主链安全。在计算最长链时,将叔区块计算在内,使伪造长链攻击更难。叔区块仅有安全意义，内容无意义，因此叔区块奖励仅有挖矿奖励，没有交易费用奖励。

4.1.5 Merkle Patricia 树

Merkle Patricia 树（MPT）是一种经过改良的、融合了默克尔树和前缀树两种树结构优点的数据结构,是以太坊中用来组织管理账户数据、生成交易集合哈希的重要数据结构。在以太坊每个区块头中，存有三个根值。stateRoot（用于存储所有账户状态）、transactionsRoot（用于存储区块中的交易数据）、和 receiptsRoot（用于存储区块中的接收账户数据），他们都使用了 MPT 数据结构。所有在以太坊中使用的 Merkle 树实际上都是 MPT。

MPT 是 Merkle 树和 Patricia 树的结合，其结构具有以下特性：

- 高安全性：每个唯一键值对唯一映射到根的哈希值。难以破解（除非攻击者有 2^128 的算力）;

- 易修改性：增、删、改键值对的时间复杂度是对数级别。

MPT 树在以太坊数据结构中发挥的作用：

- 存储任意长度的 key-value 键值对数据；
- 提供了一种快速计算所维护数据集哈希标识的机制；
- 提供了快速状态回滚的机制；
- 提供了一种称为默克尔证明的证明方法，进行轻节点的扩展，实现简单支付验证；

4.1.5.1 快速状态回滚

在公链的环境下，采用 POW 算法是可能会造成分叉而导致区块链状态进行回滚的。在以太坊中，由于出块时间短，这种分叉的几率很大，区块链状态回滚的现象很频繁。所谓的状态回滚指的是：

- （1）区块链内容发生了重组织，链头发生切换；
- （2）区块链的全局状态（账户信息）需要进行回滚，即对之前的操作进行撤销。

MPT 树就提供了一种机制，可以当区块碰撞发生了，零延迟地完成全局状态的回滚。这种优势的代价就是需要浪费存储空间去冗余地存储每个节点的历史状态。

每个节点在数据库中的存储都是值驱动的。当一个节点的内容发生了变化，其哈希相应改变，而 MPT 将哈希作为数据库中的索引，也就实现了对于每一个值，在数据库中都有一条确定的记录。而 MPT 是根据节点哈希来关联父子节点的，因此每当一个节点的内容发生变化，最终对于父节点来说，改变的只是一个哈希索引值；父节点的内容也

由此改变,产生了一个新的父节点,递归地将这种影响传递到根节点。最终，一次改变对应创建了一条从被改节点到根节点的新路径，而旧节点依然可以根据旧根节点通过旧路径访问得到。

4.1.5.2 简单支付验证 SPV

简单支付认证，即 Simple Payment Verification，简称 SPV。SPV 的目标是为了不运行全节点也可以**验证支付**（交易的存在性检查和交易是否重花的检查）。

简单支付验证（SPV）充分利用了区块的结构信息及默克尔树（Merkle Tree）的强大搜索能力，从而能实现对交易信息的快速定位。 SPV 节点是一种轻节点，节点只需要维护链中所有的区块头信息（一个区块头的大小通常为几十个字节，普通的移动终端设备完全能够承受），在验证交易是否存在时不保存所有交易也不会下载整个区块，仅仅只是保存区块头。它使用认证路径或者 Merkle 路径来验证交易存在于区块中，而不必下载区块中所有的交易。

默克尔证明：一个轻节点向一个全节点发起一次证明请求，询问全节点完整的默克尔树中，是否存在一个指定的节点；全节点向轻节点返回一个默克尔证明路径，由轻节点进行计算，验证存在性。

SPV 强调的是验证支付，不是验证交易。这两个概念是不同的。验证支付，比较简单，只需要判断用于支付的那笔交易是否被验证过，以及得到网络多少次确认（即有多少个区块叠加）。而交易验证则复杂的多，需要验证账户余额是否足够支出、是否存在双重支付、交易脚本是否通过等问题，一般这个操作是由全节点的矿工来完成。

4.1.6 区块与链

同比特币区块链一样，以太坊的区块链也是一个有序后向链表。以太坊区块链与比特币区块链最大的不同在于区块结构。以太坊区块中除了包含有交易信息列表之外，还包括所有账户的状态信息、区块高度及当前系统难度系数。（如图 4-4 ）

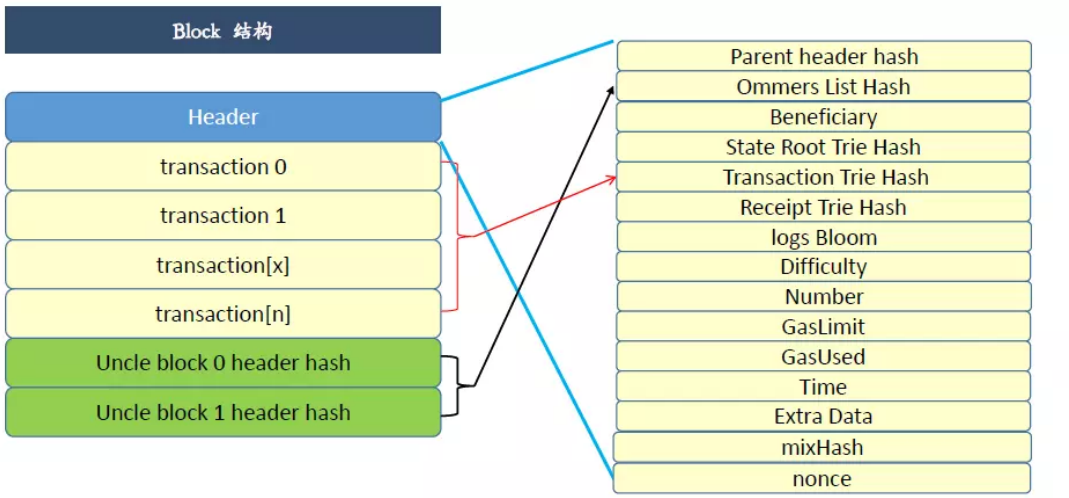

图 4-4 以太坊的区块数据结构

以太坊区块主要包括三部分：

- 区块头
- 交易列表
- 两个叔块的区块头哈希值。

区块头包括三个 MPT 根，保证了所有节点保存的状态一致、交易一致、交易结果一致，再通过对整个区块头进行哈希操作，保证历史一致。这样就保证了这个区块链的公信力：（如图 4-5 ）

- State Root Trie Hash，全局状态 MPT 树的哈希值
- Transaction Trie Hash，交易 MPT 树的哈希值
- Receipt Trie Hash，接收账户 MPT 树的哈希值。每一个交易都

有一个接收账户，主要包括交易执行后衍生出的信息。

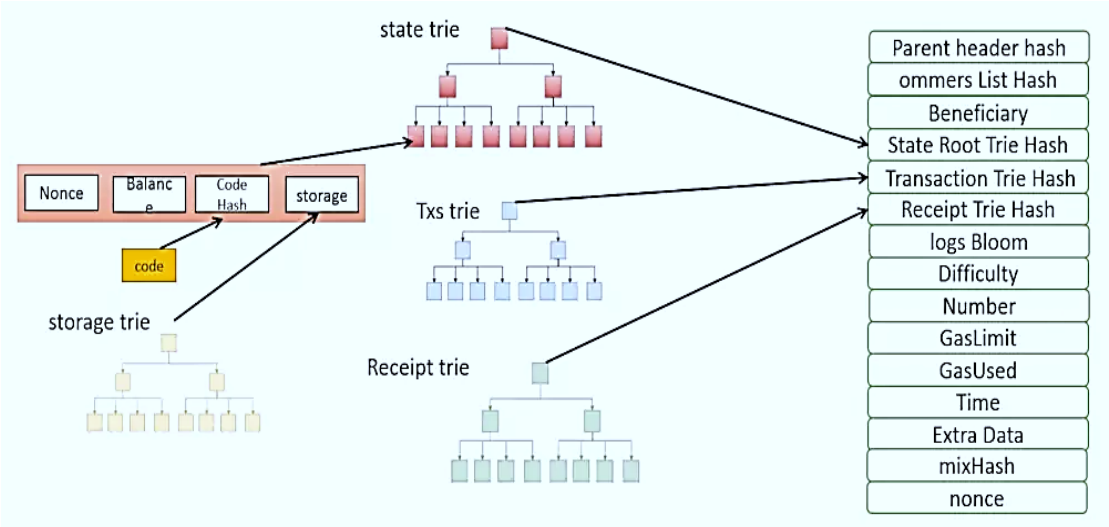

图 4-5 以太坊区块头数据结构

4.1.7 难度更新机制

以太坊中设有难度系数（Difficulty），用来度量挖出一个区块平均需要的运算次数，并需要在每生成一个区块时对区块难度做出调整。按照以太坊设计原则，其难度更新规则的设计目标是：简单、更新快速、波动性低、占用内存低且可以避免矿工利用篡改数据而获利。

挖矿本质上就是在求解一个数学问题，不同的公链设置了不同的问题。比如比特币使用 SHA-256、以太坊使用 Ethash。一个谜题的解的所有可能取值被称为解的空间，挖矿就是在这些可能的取值中寻找一个解。一般而言，这些谜题都有如下共同的特点：

- 没有比穷举法更有效的求解方法；
- 解在空间中均匀分布，从而使每一次穷举尝试找到一个解的概率基本一致；
- 解的空间足够大，保证一定能够找到解；

难度通过控制合格的解在空间中的数量来控制平均求解所需要尝

试的次数，也就可以间接的控制产生一个区块需要的时间，这样就可以使区块以一个合理而稳定的速度产生。

- 当挖矿的人很多，单位时间能够尝试更多次时，难度就会增大，当挖矿的人减少，单位时间能够尝试的次数变少时，难度就降低。
- 算法主要是让挖矿时间保持在 10-19s 这个区间内，如果挖矿时间在 0 到 9s 内，会增大挖矿难度；如果挖矿时间大于 20s，会减小难度。

4.1.7.1 以太坊难度特点

以太坊的区块难度以单个区块为单位进行调整，可以非常迅速的适应算力的变化，正是这种机制，使以太坊在硬分叉出以太坊经典(ETC)以后没有出现比特币分叉出比特币现金(BCC)后的算力“暴击”问题（如图 4-6 ）。

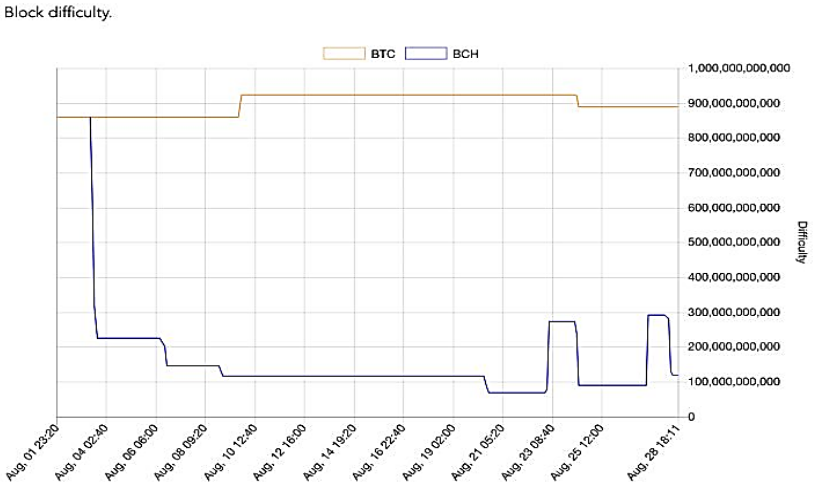

图 4-6 BTC 和 BCC 的难度变化

同时，以太坊的新区块难度在老区块的基础上有限调整的机制也使区块难度不会出现非常大的跳变。（如图 4-7 ）可以看出以太坊难

度的递增比较平滑，出现的几个跳变是由于难度炸弹造成的。

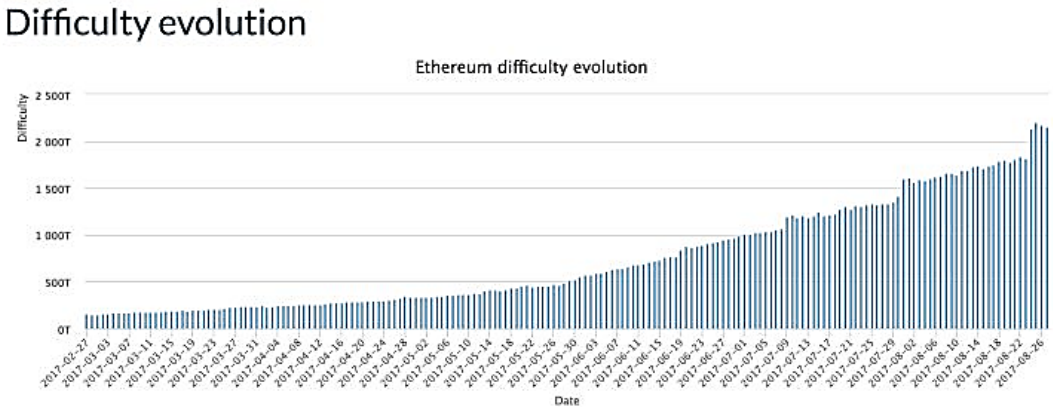

图 4-7 以太坊历史上的难度变化

4.1.7.2 难度炸弹

难度炸弹只是难度计算公式中的一部分而已，即如下公式：

INT(2**((block_number / 100000) - 2))

难度炸弹每100000个区块就会翻倍，目前只有1T左右。到5400000区块时，难度将达到4500T，会使挖矿变得极为困难，甚至不能收回电费成本。（如图 4-8）

图 4-8 以太坊的难度炸弹曲线

设置难度炸弹的原因是要降低以太坊未来迁移到 POS 协议时发生硬分叉的风险。假若矿工联合起来抵制 POS 协议模式，那就会导致以

太坊产生硬分叉；有了难度炸弹，挖矿难度越来越大，矿工就有意愿迁移到 POS 协议上了。

4.1.8 虚拟机 EVM

以太坊设计了自己的虚拟机（EVM），用于执行交易代码，这是以太坊与其他系统的核心区别。EVM 是图灵完备的，设计了一套指令集以及基于栈的虚拟机， 访存空间无限，嵌套深度最大为 1024 个元素，通过 Log 将 EVM 中的状态发送给外部，合约执行过程中会消耗 GAS，限制程序的复杂度。（如图 4-9 ）

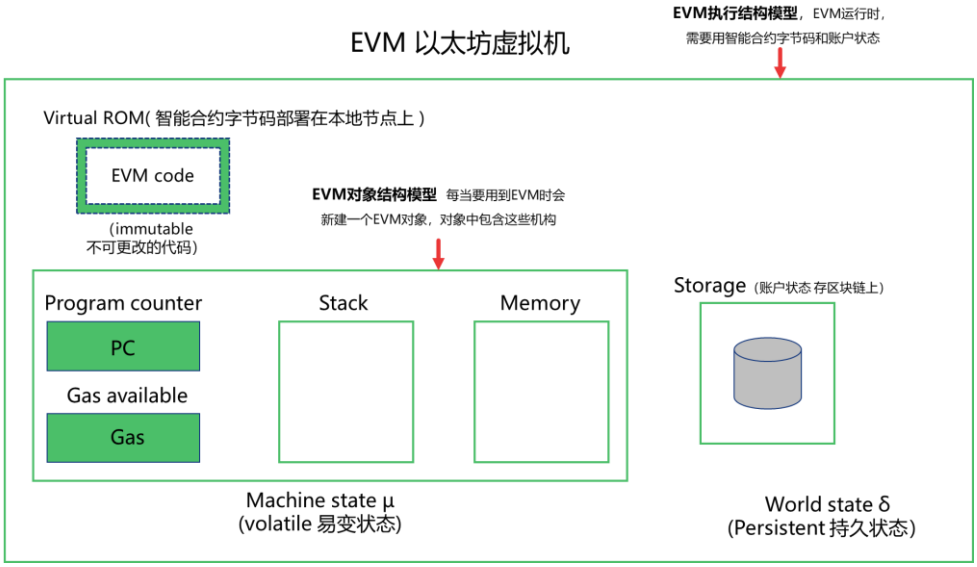

图 4-9 以太坊虚拟机 EVM

以太坊虚拟机 EVM 是智能合约的运行环境。它不仅是沙盒封装的，而且是完全隔离的，也就是说在 EVM 中运行代码是无法访问网络、文件系统和其他进程的。甚至智能合约之间的访问也是受限的。

EVM 程序用 Solidty 等语言编写，可以创建合约来编码任意状态转换功能， 用户只要简单地用几行代码来实现逻辑，就能够创建各种满足需求的系统。

合约自毁：合约代码从区块链上移除的唯一方式是合约在合约地址上的执行自毁操作。合约账户上剩余的以太币会发送给指定的目标，然后其存储和代码从状态中被移除。

4.1.9 智能合约与交易费用

以太坊编程语言是图灵完备的，交易理论上可以使用任意数量的宽带、存储和计算资源，如果没有引入交易费用，就可能被恶意攻击者通过没有任何成本的无限循环来进行 DoS 攻击，因此以太坊中引入交易费用的主要目的是为了防止此类恶意攻击行为。（如图 4-10 ）

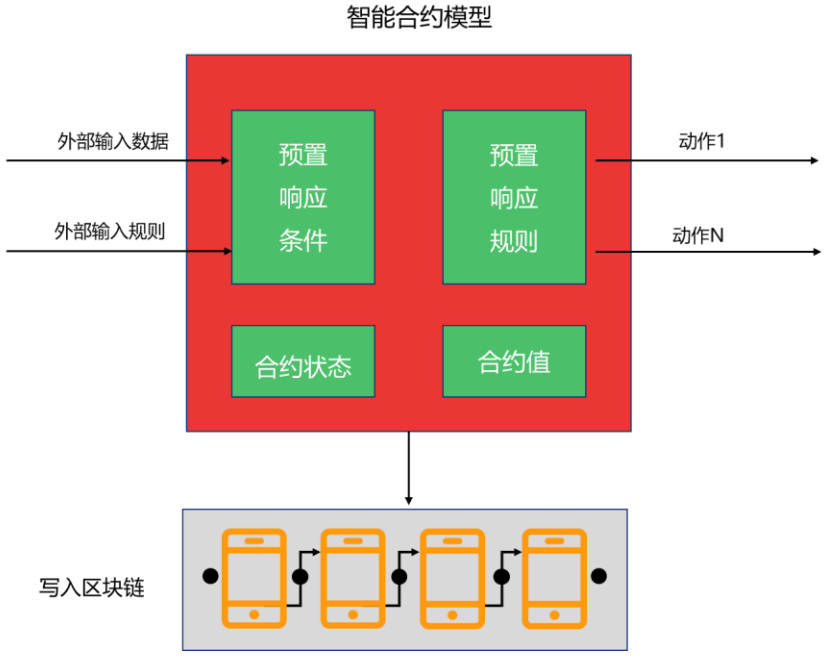

图 4-10 以太坊智能合约模型

以太币（ETH）是以太坊生态中使用的数字货币。以太坊交易中涉及的费用最终都是以 ETH 来结算的。每笔交易必须指明一定数量的 GAS（即指定 startgas 的值），以及支付每单元 GAS 所需费用（即 gasprice），在交易执行开始时，startgas * gasprice 价值的以太币会从发送者账户中扣除。交易执行期间的所有操作，包括读写数据

库、发送消息以及每一步的计算都会消耗一定数量的 GAS；如果交易执行完毕，消耗的 GAS 值小于指定的限制值，则交易执行正常，并将剩余的 GAS 值赋予变量 gas_rem ； 在交易完成后，发送者会收到返回的 gas_rem * gasprice 价值的以太币，而给矿工的奖励是（startgas - gas_rem）* gasprice 价值的以太币；如果交易执行中，GAS 消耗殆尽，则所有的执行恢复原样，但交易仍然有效，只是交易的唯一结果是将 startgas * gasprice 价值的以太币支付给矿工，其他不变；当一个合约发送消息给另一个合约，可以对这个消息引起的子执行设置一个 GAS 限制。如果子执行耗尽了 GAS，则子执行恢复原样，但 GAS 仍然消耗，无法退还。

- Gas price 的价格由交易者、矿工和智能合约设计者根据市场供求来决定。
- GAS 消耗数量如下：
  - 基本费用:21000gas。对于任何交易,都将收取这笔费用，用于支付运行椭圆曲线算法、交易存储所占用的磁盘空间和带宽。
  - 数据费用：每笔交易可以包括无限量的“数据”。固定费用为每个零字节 4 gas，非零字节 68 gas。
  - 账户存储费用：用于设置账户存储的费用，根据操作不同约需要 5000 至 20000gas。

4.1.10 基金会治理下的技术路线图

与比特币不同，以太坊有详细的升级发展规划，并有以太坊基金会

负责具体推进实施。以太坊发布之初，团队宣布将项目的发布分为四个阶段，即 Froniter、Homestead、Metropolis 和 Serenity；各阶段之间会以硬分叉的方式进行转换。（如图 4-11 ）

2015 年 7 月推出的 Froniter 实际上是以太坊的初期试验版本，仅有执行页面且存在某些待解决漏洞。

2016 年 3 月发布的 Homestead 则为以太坊正式产品的发行版，该版本中对部分协议进行相关优化改进，并为下一阶段的升级做好部署准备。

现阶段，以太坊网络已经进入第三阶段大都会（Metropolis）升级的第二版本君士坦丁堡阶段。

第四阶段 Serenity 期间，以太坊将专注于安全性、隐私性、扩展性及共识机制等等多方面的升级改善。

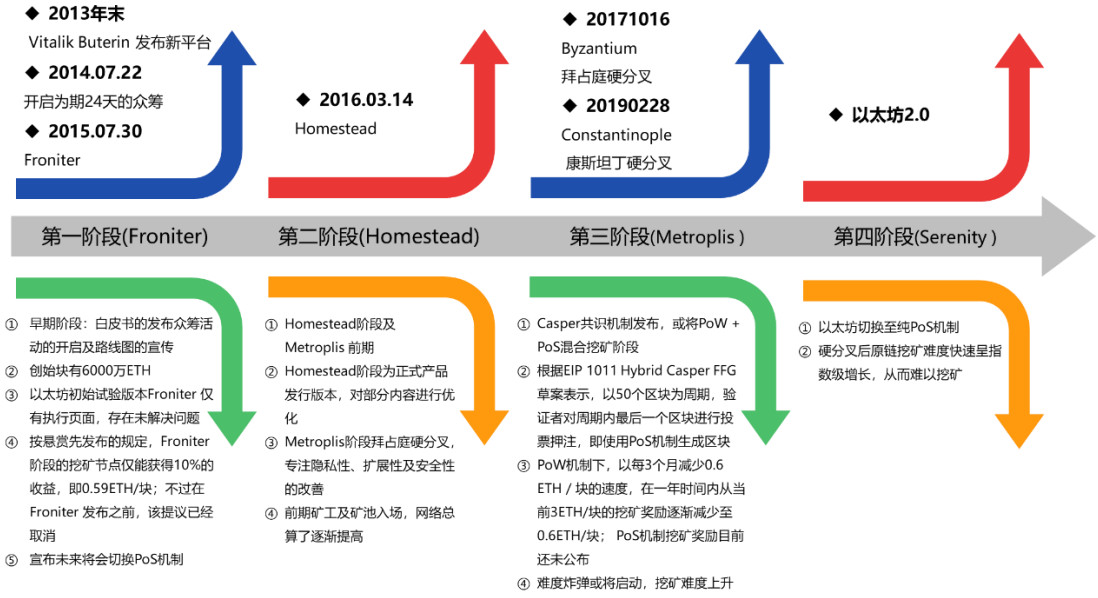

图 4-11 以太坊基金会公布的技术路线图

4.2 智能合约与区块链

4.2.1 什么是智能合约

1995 年，尼克·萨博（Nick Szabo）首次给出了智能合约的定义：“一个智能合约是一套以数字形式定义的承诺（promises），以及合约参与方可以执行这些承诺的协议。[4]

由此可以看出，尼克，萨博对于智能合约的理念即：将现实合约条款嵌入到计算机硬件和软件中，搭建赛博空间（虚拟空间）和物理空间（实体空间）之间的桥梁。

智能合约的形式，简单意义上，是一段计算机程序，满足可准确自动执行即可。因此自动售卖机也是智能合约的一种实现。系统角度上，智能合约不只是一个可以自动执行的计算机程序，它本身就是一个系统参与者，对接收到的信息进行回应，可以接收和储存价值，也可以向外发送信息和价值。智能合约就像一个可以被信任的人，可以临时保管资产，并总是按照事先的规则执行操作。

智能合约与传统合约相比具有许多优势：

- 不依赖第三方执行合约，消除中间人，大大减少了花费在合约上的成本；
- 消除第三方意味着合约验证和执行的整个过程随着用户间的直接交易而变得快速；
- 合约条款不能更改，不受各种人为干预，用户受骗的风险较小；
- 合约会永远保存在网络上，不存在放错或丢失的风险。

[4] Szabo Nick, Smart Contracts [J], Extropy, 1996.02.

4.2.2 智能合约与区块链

区块链技术和智能合约本身是无法分离的。区块链没有智能合约是无法有效运转，智能合约离开了区块链也无法实现。区块链和智能合约技术可以将信息流和资金流，做各种各样的排列组合。

尼克•萨博关于智能合约的工作理论迟迟没有实现，一个重要原因是因为缺乏能够支持可编程合约的数字系统和技术。区块链技术的出现解决了该问题。区块链不仅可以支持可编程合约，而且具有不可抵赖、不可篡改、过程可追踪等优点，为智能合约提供了公开、公正、透明的执行环境。

另一方面，区块链的链上资产需要通过某种途径流通。广义上讲，该类资产的任何操作都需要通过智能合约来进行，因为除了智能合约之外的其他任何形式对于资产的操作都是不透明的。因此，区块链上智能合约的首要需求就是：任何链上资产的操作只能通过智能合约完成。链上资产的特性由智能合约编写的规则来决定，比如说，发行的规则，流通的规则，回收的规则，持有的权益，这些都通过智能合约来决定。

4.3 预言机（Oracle）问题

预言机（Oracle），是指智能合约数据的提供者，它为数字世界里的智能合约提供关于物理世界中相对应问题的真实信息。预言机决定了智能合约的输入内容，从源头上控制了智能合约的运行。

预言机问题是指数字世界需要“了解”物理世界，需要解决数字世界和物理世界数据关联性的问题。这是一个双向的过程，物理世界

的状态要及时准确的传递给虚拟世界，而每当实体（比如说房产）的数字版本改变状态（权属），物理版本也必须相应改变。因此，必须需要一个可信的第三方来验证物理世界中事件的真实性。

4.3.1 去中心化预言机探索

真实性投票是去中心化预言机机制的尝试和探索。它利用区块链系统的通证持有者根据自己的认识对于物理世界的真实性进行投票，也可以对现有投票结果进行质疑。理论上说，经过大量的数据输入和不断优化，在数字世界里得到的结果会无限接近于物理世界的真实，但在实际操作中仍然困难重重。

- 首先，大量的个体放弃投票权是一个挑战，如何用共识和利益激励分散的个体去投票？如果样本量不够大，就无法得到趋近于真实的结果。
- 其次，如果社群内部没有“自律意识”，这种方案仍然无法从根本上杜绝中心化倾向，利益相关方会有动力去“贿选”，收买大量投票权，仍然可以去控制结果。
- 最后，去中心化的决策机制也会导致决策的效率极其地下，在应对变化的重要关头缺乏行动能力。

4.4 智能合约的技术安全

区块链智能合约系统都被设计成无须信任的环境，这意味着无法改正出现的错误。这是由区块链的不可逆特性决定的。如果与诈骗犯进行交易或者已经将货币发送到错误的地址中，那么很不幸，金钱损失是无法挽回的。在现实生活中，这些事情可以通过中心化的系统来

撤销，但是在智能合约中不行。同样，在合约代码的设计过程中也有欺诈的问题：某人需要设计（编程）合约，在合约设计时就会需要确保没有欺诈的问题发生。

技术上，智能合约的安全风险包括：

- 隐私泄露：智能合约对区块链上的所有用户可见，包括标记为 private 的资源，存在隐私信息泄露风险。
- 交易溢出与异常:由于智能合约本身的约束条件,如条件竞争、交易顺序依赖等，可能会造成交易溢出与异常。
- 合约故障：由于智能合约代码中可能存在不合理的故障处理机制，从而导致异常行为。
- 拒绝服务：由于各种原因导致的拒绝服务风险。

在漏洞扫描领域，可以大致分为黑盒扫描和白盒扫描两种主流方式，黑盒扫描工具主要是通过发送模拟攻击数据包给线上业务，通过返回数据包中的特征发现漏洞;白盒扫描则是通过扫描程序源代码中的漏洞代码特征，进行针对性的漏洞查找。相对于黑盒扫描，白盒代码扫描可以从代码层面准确发现隐藏较深的安全漏洞,但是白盒代码扫描相对来说技术门槛和成本都比较高。

智能合约白盒审计和形式化验证是应对智能合约技术风险的手段。

智能合约白盒审计包括：

- 函数可见性审核，包括：敏感函数继承权限检测和函数调用权限检测。
- 合约限制绕过审核，包括：使合约失效，删除地址字节码和将

所有合约资金发送到一个目标地址。

- 调用栈耗尽审核，包括：检测栈高度限制，是否出现栈耗尽情况。
- 拒绝服务审核，包括：过多货币交易发生异常，导致交易回滚，最终导致合约拒绝服务。

形式化验证(Formal Verification)是智能合约工程的重要环节，它可以成为对合约进行确定性验证的一种技术，通过形式化语言把合约中的概念、判断、推理转化成智能合约模型，可以消除自然语言的歧义性、不通用性，进而采用形式化工具对智能合约建模、分析和验证，进行一致性测试，最后自动生成验证过的合约代码，形成智能合约生产的可信全生命周期。

形式化验证是一种基于数学和逻辑学的方法，在智能合约部署之前，对其代码和文档进行形式化建模，然后通过数学的手段对代码的安全性和功能正确性进行严格的证明，可有效检测出智能合约是否存在安全漏洞和逻辑漏洞。该方法可以有效弥补传统的靠人工经验查找代码逻辑漏洞的缺陷。形式化验证技术的优势在于，用传统的测试等手段无法穷举所有可能输入，而我们用数学证明的角度，就能克服这一问题，提供更加完备的安全审计。

随着区块链平台级应用的普遍化，智能合约涉及的金额呈指数级别增长，智能合约的安全问题也成为投资者和开发者共同关注的焦点。今年以来有数个区块链应用项目因为智能合约代码出现漏洞而遭到黑客攻击，导致投资者巨额的损失。为了防止类似事件的发生，交易

所、钱包、项目方等都在智能合约安全上加大投入，同时围绕着智能合约安全的周边生态成为目前投资的热点。

形式化验证技术已经在军工、航天等高系统安全要求领域的取得了相当成功的应用，将形式化方法应用于智能合约，使得合约的生成和执行有了规范性约束，保证了合约的可信性，使人们可以信任智能合约的生产过程和执行效力。通过形式化语言，把合约中的概念、判断、推理转化成智能合约模型，可以消除自然语言的歧义性、不通用性，进而采用形式化工具对智能合约建模、分析和验证，进行一致性测试。合约的形式化验证保证了合约的正确属性，自动化代码生成提高了合约的生成效率，合约的一致性测试保证了合约代码与合约文本的一致性。

模型检测是对有穷状态系统的一种形式化确认方法，其理论逻辑为：给定一个合约和规约，按照规约生成对应的合约模型，通过证明合约在模型中成立，以此证明合约满足约定规则。有穷状态模型在建模时有一定难度，需要采集大量样本，并在其中提取逻辑，但因为状态是可穷的，可以保证搜索过程及时终止，因此，在工程上是实际的。

形式化验证理论过去一直服务于集成电路的功能验证，发展多年，已经非常成熟。智能合约是区块链系统发展应用的重要内容，也是目前传统网络安全公司尚未触及的安全盲区。市场已经发现了形式化验证对于智能合约安全的重要性。然而，安全机制的建立从数学理论变成现实，仍然需要时间。

智能合约重大安全事件

TheDAO 是 2016 年世界上基于以太坊区块链平台最大的众筹项目。其目的是让持有 TheDAO 代币的参与者通过投票的方式共同决定被投资项目，整个社区完全自制，并且通过代码编写的智能合约来实现。于 2016 年 5 月 28 日完成众筹，共募集 1150 万以太币，在当时的价值达到 1.49 亿美元。

TheDAO 事件是指 2016 年 6 月 17 日，DAO 因为编写智能合约时不谨慎，存在漏洞，而黑客则利用该漏洞盗取了 DAO，造成 360 多万个 ETH 被盗，按照当时的以太币价格，损失达到了 6000 万美元。

被黑客攻击后，为了找回被盗的巨额数量以太币，以太坊基金会商讨了方案，首个提议方案为进行一次软分叉，不会有回滚，不会有任何交易或者区块被撤销。软分叉将与 The DAO 相关的交易认作无效交易，以此阻止攻击者在 27 天之后提现被盗的以太币。但由于软分叉产生的争议与负面影响，并没有实施。最终通过一次硬分叉找回了被盗的以太币，但也导致以太坊分裂出 ETH 和 ETC（旧版）。

TheDAO 事件在币圈引起了巨大争议，ETH 市场价格从记录高位 21.50 美元跌至 15.28 美元，其影响延续至今。

第五章 多链融合技术进展

5.1 区块链基础设施 BAAS/BTAAS

5.1.1 BAAS 与 BTAAS

区块链云服务（BaaS - Blockchain As A Service）提供公链的实例服务。把区块链的节点和应用，比如比特币、以太坊等这类型公链，直接部署在云平台。节点提供查询，交易、区块生成等操作。底层使用云计算资源和云存储空间，并支持公链的延伸应用。例如存证型区块链应用公证通(Factom),数字身份型区块链应用优端口(uPort)等。利用云平台提供的容错、网络的多链路负载、计算资源的动态调整等技术,节省了节点的运行成本,提高了整个系统之间交互的效率。同时也为区块链浏览器、数字货币交易平台以及一些现有的区块链系统提供开放的服务。

区块链技术云服务（BTaaS - Blockchiain Technology As A Service）提供的是区块链技术架构接口，需要基于 BTaaS 开发部署个性化的区块链应用。云平台的区块链技术多指与云平台技术结合后的区块链架构或者区块链操作系统，主要是指 Hyper Ledger，Multichain，以太坊私有链等多个技术框架。使用这些框架去结合应用业务需求，开发出适合业务的应用。这种方式称为区块链技术云服务。

BaaS 与 BTaaS 的区别如图 5-1 。现实中提及 BaaS 的时候，通常既包括 BaaS 的涵义，也包括 BTaaS 的涵义，需要根据实际情况明确其内容。

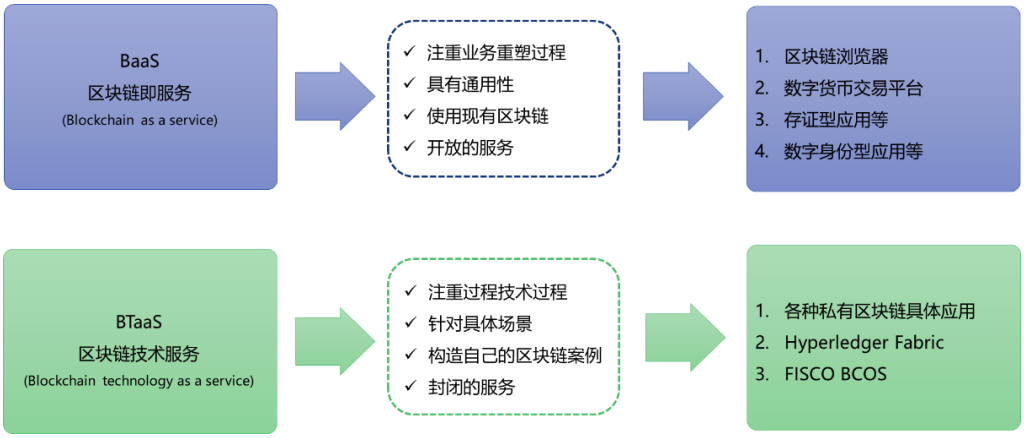

图 5-1 BaaS 与 BTaaS 的区别

BaaS 平台综合了云和区块链的优势，作为用户或开发者，只需要通过平台或者开放 API 等进行自己的需求管理和开发，底层技术能力均作为可插拔选项供其使用。简单说，BaaS 就是一个结合云和区块链的强大工具集。

在底层基础资源层，BaaS 通常依托云计算的能力，结合容器引擎、镜像仓库等提供统一的接口层，支持云端托管、安全监管、账户权限、一键部署等能力，并且底层云基础设施和服务对用户透明；

在网络层，比如 Ethereum、Fabric、EOS 等托管区块链的典型网络，用户可以按需选择对应的网络应用；

在框架层，BaaS 平台支持账本、合约、鉴权以及共识机制全能力，提供丰富的可插拔定制的区块链场景参数；

在业务层，用户可以通过开放平台或者客户端、SDK、开放 API 等进行快速开发使用。

BaaS 在供应链金融、票据、跨境支付、信贷、物流和医药溯源等领域已经开始探索和逐步应用，市场的反应和接受程度远远超出预期。

5.1.2 区块链服务网络 BSN[5]

区块链在中国进入快速发展期。但在这个过程中，造链建设成本高、底层平台异构、数据无法交互、应用推广难等问题都阻碍着区块链的大规模应用。区块链服务网络（Blockchain-based Service Network，以下称为 BSN）正是一个针对这些问题的解决方案。BSN 是一个构建于通信网络之上可以实现数据可信共享的层网络，是用来快速部署和运行区块链的基础设施。BSN 由国家信息中心、中国移动通信集团公司、中国银联股份有限公司共同发起。BSN 从 2019 年 12 月开始内测，到 2020 年 4 月正式商用。

BSN 的顶层设计的特点可以用“1 基 1 核 6 跨 7 性”概括：1 基——以联盟链架构为基础；1 核——以支撑智慧城市和数字经济为核心；6 跨——跨云服务、跨门户、跨底层架构、跨公网、跨地域、跨机构；7 性——开放性、公用性、扩展性、开源性、多门户性、低成本性和自主性。

BSN 与其他 BAAS 服务不同，BSN 以互联网理念为开发者提供公共区块链资源环境，极大降低区块链应用的开发、部署、运维、互通和监管成本，从而使区块链技术得到快速普及和发展。如图 5-2。

[5] 本小节资料来源：BSN 官网 https://www.bsnbase.com/

	BSN	区块链云服务
开发	不需要懂区块链编程语言，不需要聘请专业区块链开发人员	开发者必须懂得区块链编程语言
部署	每个虚拟机可管理超过40个应用，合理调配，让资源得到了充分的使用	每个虚机只能安装一个应用的peer节点，资源基本闲置或不饱和运营状态
运维	统一运维机制，在网关以内的系统，不需要开发者进行任何维护	开发者必须自行维护区块链环境，必须要有区块链网络管理员
互通	统一的密钥体系，只要授权，链与链的数据即可互通，并相互调用	每个区块链应用均使用不同的架构和不同的密钥体系，互通成本非常高
监管	监管部门可以进行一站式监管	众多孤立局域网，监管成本非常高

图 5-2 BSN 与区块链云服务对比

从参与方的角度来看，BSN 的基本生态主要由五类企业参与组成：云服务商、底层框架商、门户商、开发者和 BSN 运维体系。生态内各类企业的具体分工如图 5-3。

图 5-3 BSN 生态及其分工

从网络架构的角度来看，BSN 核心架构由公共城市节点、共识排序集群服务、权限管理链、智能网关和预制链码机制组成。如图 5-

4。

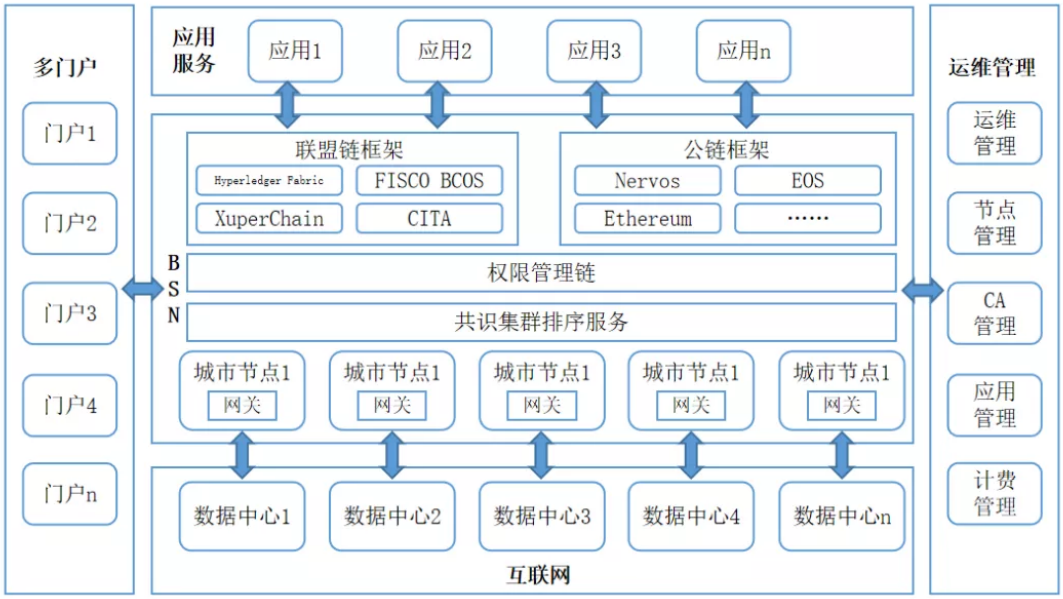

图 5-4 BSN 核心架构

BSN 城市节点是一个部署在每个地级市的 IDC 机房或云资源内的公共区块链环境系统。截至 2020 年 12 月 1 日，BSN 已经在全国范围内 26 个省（含直辖市、自治区、特别行政区）80 个城市建成了 99 个 BSN 公共城市节点，在北美洲、欧洲等 6 个大洲建立加利福尼亚、巴黎等 7 个海外节点，所有城市节点均支持同城专线接入。从技术角度来看，BSN 已经适配 Hyperledger Fabric（及国密）、FISCO BCOS（及国密）、XuperChain（及国密）、CITA（及国密）等联盟链框架，并已集成 Nervos、Tezos、NEO、EOS、IRISnet、Ethereum、ShareRing、Solana 和 Alogrand 等公有链。

5.1.3 其他国内外 BAAS 平台案例

1）国外产品

微软 Azure：2015 年 11 月，与 ConsenSys 达成合作，在其 Azure 环境里面提供 Ethereum BaaS。2016 年 4 月，与由 43 家银行组成的 R3 联盟结成合作伙伴，在 R3 成员当中推广 Hyper Ledger。

IBM Bluemix Garage：2016 年 2 月宣布基于 Fabric 推出 BaaS，开发人员就可以访问完全集成的开发运维工具，用于在 IBM 云上创建、部署、运行和监控区块链应用程序。

亚马逊 AWS：在 2016 年 5 月宣布与 Digital Currency Group 合作，向 DCG 投资的公司提供区块链云服务。2018 年 4 月，亚马逊 AWS 正式发布了基于 Fabric 的 AWS 区块链模板。

2）国内产品

2016 年 6 月，微众银行开发的金融行业联盟链云 BaaS 发布，作为位于腾讯金融云 IaaS 平台与应用场景的中间层。

2017 年 11 月，沿用联盟链的思路，腾讯云正式发布金融级解决方案 TBaaS，TBaaS 构建于金融云之上。

2017 年 7 月，百度推出区块链开放平台“BaaS”，主要是帮助企业联盟构建属于自己的区块链网络平台。平台依托于百度 Trust 区块链技术框架，适用于支付清算、数字票据、银行征信管理、权益证明和交易所证券交易、保险管理、金融审计等领域。

2018 年 8 月，阿里云宣布发布企业级 BaaS 平台，支持一键快速部署区块链环境，实现跨企业、跨区域的区块链应用。适用于商品溯源、供应链金融、数据资产交易、数字内容版权保护等领域。

2018 年 8 月，“京东区块链防伪追溯平台” BaaS 正式上线，参

与企业可直接使用自有区块链节点加入主链共同运营，将商品从原料、生产加工、物流运输、零售交易等数据上链。

5.1.4 BAAS 面临的挑战

1）安全风险较大

BaaS 采用云的分布式架构来支撑业务扩展，数据存储和输出服务涉及客户权益保护，在信息互联网向价值互联网的过渡中，需要高度关注监管适应性和风险控制等问题。

2）技术存在难点

服务提供方搭建一套功能完善、性能稳定的 BaaS 平台可能会面临诸多技术挑战：包括安全性、可扩展性、可感知性、负载均衡、底层资源普适性等。

3）落地应用受限

BaaS 平台的推出，某种程度上讲是区块链技术落地应用的里程碑，但目前仍处于研究阶段，真正实现区块链提升和改善商业的应用仍然乏善可陈。互联网巨头发布 BaaS 平台，都是基于自身已有的云服务，这与数据库相差无几，真正落地应用非常有限。

4）马太效应明显

BaaS 不仅需要花费高额的研发费用和大量硬件费用，还对技术的更新具有较强的依赖性，只有大型公司和高收入公司有能力负担，不管是国内还是国外，BaaS 几乎都是由商业巨头把控。另外，BaaS 供应商都在摸索阶段，产品存在较高的同质化问题。

5.2 星际文件系统 IPFS

5.2.1 IPFS 的目标与特点

星际文件系统（IPFS －InterPlanetary File System）本质上是一种基于内容寻址、支持文件多版本管理、点对点的超媒体分布式存储和传输协议，目标是补充甚至取代过去 20 年里使用的超文本媒体传输协议（HTTP），希望构建更快、更安全、更自由的互联网时代。从技术层面，IPFS 借鉴了区块链技术的经验，但与区块链技术没有直接关联。

对互联网而言，HTTP 是一场革命，在过去数十年时间里将发布信息的成本降到了最低，瓦解了经济、政治、文化管理机构对信息（音乐、思想、视频、新闻、游戏等等）传播的控制，使获取信息的渠道变得更加平等，过程变得更为简单。

但是，由于基于 HTTP 运行的 Web 内容是中心化的，数据中心的运作十分依赖 Internet 的主干网络，而且 HTTP 分发内容的方式从根本上讲是有缺陷的，特别缺乏可分布性和可持久性，难以成为人类知识总和的永久载体。

1）HTTP 的中心化是低效的，并且成本很高

使用 HTTP 协议每次需要从中心化的服务器下载完整的文件，包括网页，视频，图片等，速度慢，效率低。如果改用 P2P 协议的方式下载，可以节省近 60%的带宽。P2P 网络将文件分割为小的块，从多个服务器同时下载，速度非常快。

2）Web 文件经常被删除

当使用 HTTP 进行网络查找的时候，寻找的是文件在网络上的位置，但这个位置取决于服务器管理者，用户只能寄希望于服务器没有关闭，文件维持在原来的地方没有被移动。但实际上，HTTP 的页面平均生存周期大约只有 100 天。Web 文件经常由于存储成本太高而被删除，无法永久保存。IPFS 提供了文件的历史版本回溯功能，可以很容易地查看文件的历史版本，数据可以得到永久保存。

3）中心化限制了 Web 的成长

现有互联网是一个高度中心化的网络。互联网是人类的伟大发明，也是科技创新的加速器。各种管制将对互联网的功能造成威胁，例如：互联网封锁，管制， 监控等等。这些都源于互联网的中心化。而分布式的 IPFS 可以克服这些 Web 的缺点。

4）互联网应用高度依赖互联网主干网

互联网主干网受制于诸多因素的影响，战争、自然灾害、互联网管制、中心化服务器宕机等等，都可能使互联网应用中断服务。IPFS 可以极大地降低互联网应用对主干网的依赖。

针对 HTTP 的功能特性，IPFS 的特点描述如下：

- IPFS 是一个点对点超媒体传输协议，类似 HTTP 协议。IPFS 定义了基于内容的寻址文件系统和分布式网络上的内容分发协议，包括分布式哈希算法、P2P 文件传输、和文件版本管理协议；
- IPFS 是一个文件系统。用户将文件上传后，IPFS 将其转换成专门的数据格式进行存储，有文件夹和文件，可挂载本地文件系统；

- IPFS 是一个 Web 协议，可以像 HTTP 那样查看互联网页面，未来浏览器可以直接支持 ipfs:/ 或者 fs:/ 协议；
- IPFS 是模块化的系统，具有 8 层协议栈。典型协议层包括：连接层，通过其他任何网络协议连接；路由层，寻找定位文件所在位置；数据块交换，采用 BitTorrent 技术传输文件；
- IPFS 是一个 P2P 系统，支持世界范围内的 P2P 文件传输网络，分布式网络结构没有单点失效问题；
- IPFS 天生是一个内容分发网络(CDN)，文件添加到 IPFS 网络，将会在全世界进行 CDN 加速；
- IPFS 拥有命名服务（IPNS），实现基于自认证系统（SFS）的命名体系，可以和现有域名系统绑定。

5.2.2 IPFS 技术架构

IPFS 协议栈模型定义了八层子协议栈，从下至上为身份、网络、路由、交换、对象、文件、命名、应用，每个协议栈各司其职，又互相搭配。(如图 5-5)

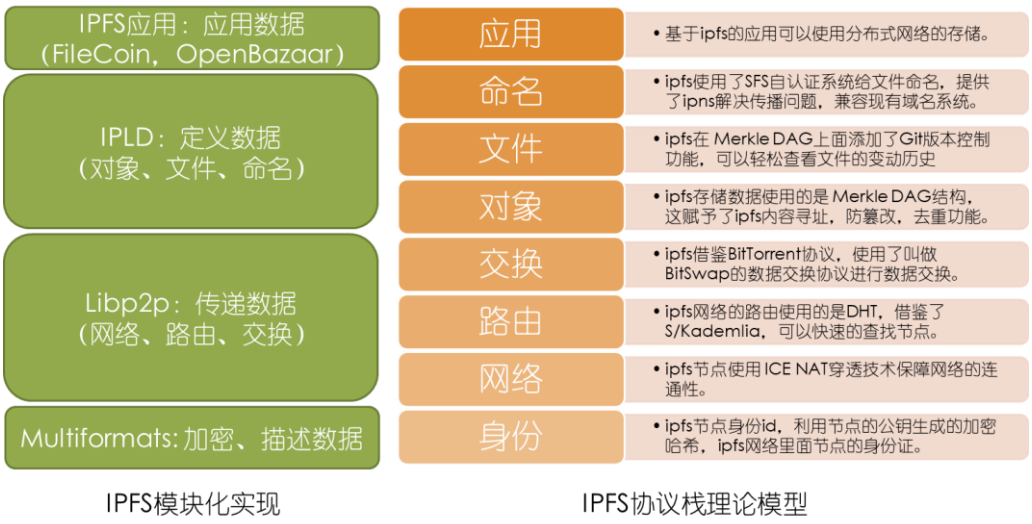

图 5-5　IPFS 协议栈模型

身份层和路由层共同定义了对等网络（P2P 网络）的寻址功能。对等节点身份信息的生成以及路由规则是通过 Kademlia（KAD）协议生成制定，KAD 协议实质是构建了一个分布式松散哈希表，简称 DHT（Distributed Hash Table），每个加入这个 DHT 网络的人都要生成自己的身份信息，然后才能通过这个身份信息去负责存储这个网络里的资源信息和其他成员的联系信息。

网络层使用 ICE NAT 穿透技术来保障网络的连通性，使得 IPFS 节点可以和网络里面成百上千的其它节点通讯。

交换层，IPFS 借鉴 BitTorrent 协议进行了创新，叫做数据交换协议（Bitswap），它增加了信用和账单体系来激励节点去分享，用户在 Bitswap 里增加数据会增加信用分，分享得越多信用分越高。如果用户只去检索数据而不存数据，信用分会越来越低。这一设计可以解决女巫攻击[6]。

对象层和文件层管理了 IPFS 上 80%的数据结构，大部分数据对象都是以 MerkleDag 的结构存在，这为内容寻址和去重提供了便利。文件层是一个新的数据结构，和 DAG 并列，采用 Git（ Git 是一个开源的分布式版本控制系统）一样的数据结构来支持版本控制功能，这使得 IPFS 文件拥有了时光机功能，可以轻松查看文件的变动历史。

命名层具有自我验证的特性，当其他用户获取该对象时，使用指纹公钥进行验签，这验证了用户发布对象的真实性，同时也获取到了

[6] 女巫攻击模型是指在 P2P 网络中，一个网络节点伪装成多重身份，并且在网络中其他网络节点对于它的每一次伪装都认为是不同的节点，就像一个特工频繁的换衣服化妆以达到特定目的。当这些伪装节点达到一定数量时，那么就成功发起了一次女巫攻击。

可变状态。IPFS 加入了 IPNS 这个巧妙的设计来使得加密后的 DAG 对象名可定义，增强可阅读性。

应用层，IPFS 核心价值就在于上面运行的应用程序。可以利用 IPFS 类似 CDN 的功能，在成本很低的带宽下，去获得想要的数据，从而提升整个应用程序的效率。

IPFS 的团队在开发时，采用高度模块集成化的方式，像搭积木一样去开发整个项目。基于 IPLD、LibP2P、Multiformats 这三个模块，实现了除应用外的七层协议栈功能，参见图 。

Mutiformats 是一系列哈希加密算法和自描述方式的集合，它具有 SHA1 \ SHA256 \ SHA512 \ Blake3B 等 6 种主流的加密方式，用以加密和描述节点以及指纹数据的生成。

LibP2P 是 IPFS 实现模块的核心，面对各式各样的传输层协议以及复杂的网络设备，它可以帮助开发者迅速建立一个可用 P2P 网络层，快速且节约成本。

IPLD 其实是一个转换中间件，将现有的异构数据结构统一成一种格式，方便不同系统之间的数据交换和互操作。现在 IPLD 支持的数据结构，包括比特币、以太坊的区块数据。这也是 IPFS 为什么受到区块链系统欢迎的原因，它的 IPLD 中间件可以把不同的区块结构统一成一个标准进行传递，不用担心性能和稳定性。 IPFS 应用了这几个模块的功能，集成为一种容器化的应用程序，运行在独立节点上，以 Web 服务的形式，供用户使用访问。

5.2.3 IPFS 与 FileCoin

FileCoin 是一个基于 IPFS 的区块链公链项目，用于搭建一个分布式存储网络。Filecoin 为用户提供的数据存储功能如下：

- 存储：付费存储，用户付费，矿工和 Filecoin 网络保证存储的安全性；
- 下载：付费下载，用户付费，矿工负责发送数据；
- 用户：不需要自己提供存储，也不需要自己提供节点；
- 存储内容：收费存储一切 。

FileCoin 是运行在 IPFS 上面的一个激励性应用。IPFS 有巨大存储需求和节点需求，如果没有激励机制，无法解决分布式的节点和存储来源问题；Filecoin 把存储数据价值化，通过类似比特币的激励政策和经济模型，让更多的人去创建节点，去让更多的人使用 IPFS。FileCoin 可以为 IPFS 贡献很多节点，同时带着一个巨大的分布式存储空间，解决了 IPFS 的需求问题。

FileCoin 代币（简称 FIL）是沟通资源使用者（用户）和资源提供者（矿工）的中介桥梁。FileCoin 协议拥有两个交易市场，数据检索和数据存储，双方在市场里面提交自己的需求，达成交易。

1）FileCoin 机制设计

FileCoin 市场分为两大类：

存储市场是把文件输入进去，存储起来。在链上撮合客户和矿工之间的订单，给出全球市场的报价，使存储供应商们（矿工）进行竞争记账，选出最优的矿工来为客户服务。矿工的硬盘容量和收益成正比。

检索市场是把客户的文件找出来。在链下进行订单的撮合，使用链下支付通道，力图将请求的延迟最小化。容量小但是带宽高的矿工有可能获得较好的回报

FileCoin 中存储文件的生命周期包括四个阶段：

- PUT 阶段：由客户端发起文件存储请求，并以 FIL 为单位出价，同时系统会撮合矿工和用户的订单，一旦撮合成功，交易便存储在区块链上。
- SEND 阶段：上一步订单撮合完成后，客户端发送要存储的文件给矿工，矿工接收到这个文件将它让放入到数据单元里，同时加密文件数据，并且验证之后发送到链上。
- 管理阶段：矿工不断以复制证明的方式和规则来证明他们在工作，客户端支付的金额是分期付款进行的，随着存储时间进程线性像前推进给矿工进行支付。
- GET 文件：客户请求文件并支付 FIL 到检索市场之后，相应速度最快的矿工拿到这个文件的分发权。

矿工挖矿获取收益主要体现在两个方面：一、需要不断的证明他在复制用户的数据、打包交易；二、打包区块，这和比特币、以太坊类似。在速度方面也有考量，谁能快速分发内容给用户，谁便能获取更高的收益。所以拥有带宽、拥有高速硬盘而不是传统的机械硬盘的矿工将具有一定的优势。拥有硬盘容量将在共识机制上扮演比较重要的角色，创建有价值的存储服务和网络是挖矿的目的和结果。

2）FileCoin 共识机制

Filecoin 共识机制抛弃了以往区块链的高度依赖计算资源和能源消耗形成的共识机制，重新利用有意义的工作来形成共识机制，这就是 PFT（power fault tolerance），进化版的拜占庭容错机制。将矿工当前在网中使用的存储量和生成的时空证明转化为投票的权重，然后节点利用这个权重进行选举产生一个或者多个领导节点，领导节点创建新的区块并把它们传播到网络。

因此，FileCoin 的共识机制使用复制证明（Porep）作为核心工作函数，并在时空证明（Post）中进行汇总，使用秘密领导人（Sle）选举产生领导者，最后达成预期共识。（如图 5-6 ）

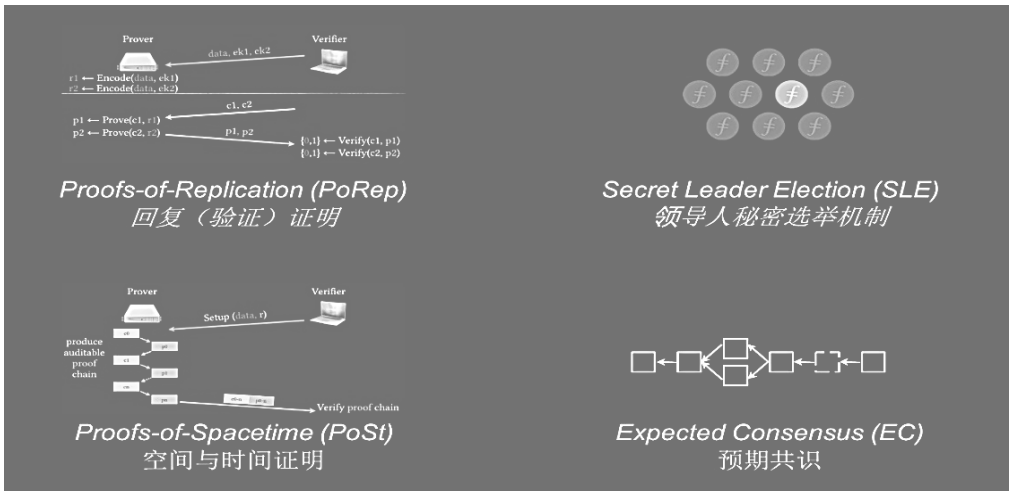

图 5-6　FileCoin 的共识机制

复制证明（Porep），是这样一份协议：

- 证明者 P 可以向验证者证明，P 自身存储了数据 D 的一个特定副本，并且副本不会被重复地存储到同一个物理存储器中。

时空证明（Post），是这样一份证明协议：

- 允许证明方 P 随着时间的推移，将空间证明（或存储证明）集中到可审查的记录中，这证明 P 确实消耗了空间 S（或存储数

据 D)，并且维持了一段明确的时间 T。

基于时空证明的矿工投票权重，FileCoin 按照如下方式达成预期共识（EC）：

- Filecoin 的共识协议策略是每一轮里面选举出来一名或多名矿工来创建新的区块，矿工赢得选举的可能性跟矿工当前的有效存储成比例。
- Filecoin 把矿工在网络中的当前存储数据相对于整个网络的存储比例转变为矿工投票权（voting power of the miner)。
- FileCoin 共识采用秘密领导人选举 SLE 确定记账者。预期每轮都只选出 1 个记账者，但一些轮内可能会出现 0 个或者多个记账者。记账者通过创建一个区块并将其传播到网络的方式来拓展区块链条。在每一个轮次，区块链将被延伸一个或多个区块。在没有记账者的轮次里，一个空的区块将被添加到区块链中。虽然区块链中的区块可以线性排序，但它的数据结构是一个有向无环图。
- 预期共识 EC 是一个概率共识，每个轮次都比前面的区块更加确定。如果绝大部分的参与者通过扩展链或签名区块的方式将他们的权重添加到区块所属的链上，那么这个区块就被确定了。
- Filecoin 有抵押机制，强制参与者选择一条链，通过巧妙地结合抵押机制，对同时挖多个链的矿工进行惩罚，这样可以非常快速地进行管理。

预期共识机制的缺点：

- 预期共识机制具有公平性、保密性、公开可验证性等特性，而它并非是完美的，它的问题在于出块的不稳定性；在每一个周期里面，预期选举出来的记账者是 1 个，但是在某些特殊情况下也会选举出来多个记账者。
- 每个周期内出现空块轮次的比例高达 36.78%，符合预期出现且仅出现 1 个区块的轮次比例也仅有 36.78%。

3）FileCoin 存在的问题

FileCoin 为 IPFS 协议的使用带来了分布式节点和存储空间，是推广 IPFS 的巧妙手段。但是 FileCoin 的机制设计中存在导致攻击的缺陷。

第一，外包攻击与时空证明。

空间和时间证明（PoST）：矿工需要证明他们将用户的数据存储在自己独立的物理存储空间中，在与用户商定的时间段内。存储矿工需要不断计算散列值，而散列值则需要用户数据来计算散列值。如果矿工不能持续访问用户的数据，他们将无法提供他们获得奖励所需的证据。每计算 10 亿次，哈希结果将被发布到 FileCoin 区块链中进行验证。如果结果不正确，矿工将无法获得奖励。如果一个矿工被认为是一个错误的节点，那么矿工甚至可能失去作为矿工的代币存款。

外包攻击是指矿工可能将数据转移到其他地方，而不是存储在自己的硬盘上。其他矿工可能会做同样的事情。 结果是多个矿工可能最终将数据存储在同一个硬盘中。

其次，价格波动可能会导致矿工的不正当行为。

在 FileCoin 网络中，自由市场决定存储/检索数据的价格。ICO 市场的历史证明，代币价格具有很强的波动性。为追求最大利润，矿工也可能违反与客户的合同，并在波动的市场中接受新的报价。这对于存储服务来说是不可接受的。

5.2.4 多区块链浏览器与桥接系统

将数据添加入 IPFS 中，就可以使用 IPFS 来浏览交易，同时可以直接在网络中浏览文件。IPFS 多区块链浏览器试图以与网络将所有这些网站连接在一起的方式，将所有这些不同的区块链联系起来。比如可以在以太坊中嵌入能够连接到 Zcash 的链接，而 IPFS 能够解决这之中的所有问题。

FileCoin 桥接系统（Bridges）是旨在连接不同区块链的工具，计划支持跨链交互，以便能将 Filecoin 存储带入其他基于区块链的平台，同时也将其他平台的功能带入 Filecoin。

- Filecoin 进入其他平台：其他的区块链系统，如比特币，Zcash，特别是 Ethereum，这些平台只提供很少的存储能力和非常高的成本。桥将存储和检索支持带入这些平台。桥的支持将允许这些系统以交换 Filecoin 代币的方式来保证 IPFS 存储内容。
- 其他平台进入 Filecoin：计划提供 Filecoin 连接其他区块链服务的桥。例如，与 Zcash 的集成将支持发送隐私数据的存储请求。

5.3 跨链技术与区块链互联网 IoB

区块链互联网（IOB - Internet of Blockchains）旨在实现高

性能、去中心化的通用跨链基础设施，并接入各种跨链应用。

5.3.1 Polkadot

Polkadot 技术是由以太坊核心开发团队(Ethcore)推出的公开无需授权的区块链互联技术。Polkadot 计划将私有链/联盟链融入到公有链的共识网络中去，同时又能保有私有链/联盟链的隐私和许可的防护措施。它建设了一个全新的交易层，并有机会将数百个区块链互相连接。

Polkadot 的核心思想是区分交易方发起和执行交易的方式，以及交易方统一记录的方式。Polkadot 提供基础的中继链(relay-chain)，很多可验证的、全球动态同步的数据架构都建立在这个基础上，这些数据架构为平行链或者互为侧链。区块链应用可以将以太坊分叉链，按照各自需求调整，通过 Polkadot 与以太坊公有链连接，或者给不同的链设置不同的功能，实现更好的扩展性和效率。

在 Polkadot 看来，其它区块链都是平行链，Polkadot 为通过中继链技术能够将原有链上的代币转入类似多重签名控制的原链地址中，对其进行暂时锁定，在中继链上的交易结果将由这些签名人投票决定其是否生效。它还引入了钓鱼人角色对交易进行举报监督。通过 Polkadot 可以将比特币、以太币等都链接到 Polkadot 上，从而实现跨链通信。(如图 5-7)

Polkadot 目前还是以以太坊为主，实现其与私链的互连，并以连接其他公有链网络为升级目标，最终让以太坊直接与任何链进行通讯。

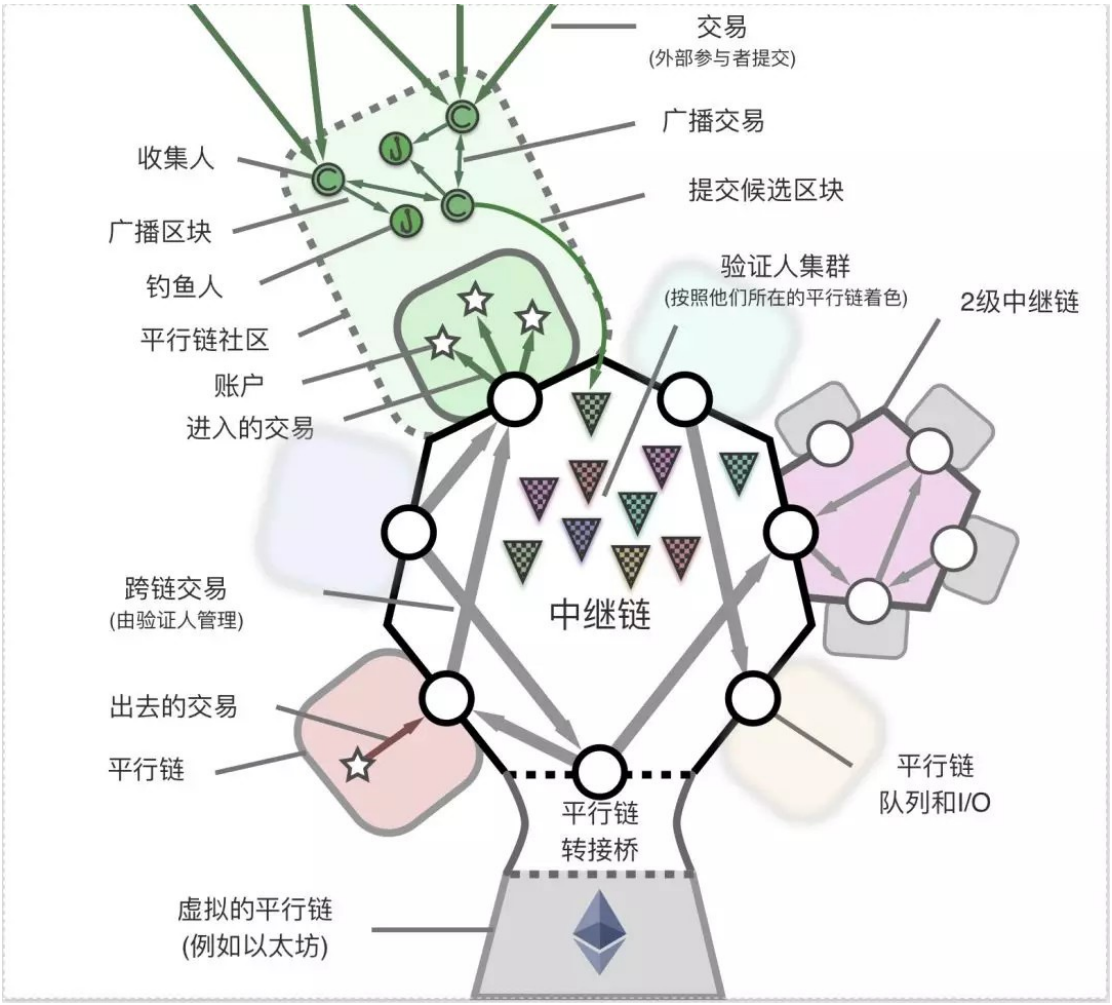

图 5-7 Polkadot 工作原理

5.3.2 Cosmos

Cosmos 是 Tendermint 团队推出的一个支持跨链交互的异构网络。Cosmos 采用的 Tendermint 共识算法，是一个类似实用拜占庭容错共识引擎，具有高性能、一致性等特点，而且在其严格的分叉责任制保证下，能够防止怀有恶意的参与者做出不当操作。

Cosmos 上的第一个空间叫做"Cosmos Hub"。Cosmos Hub 中心是一种多资产权益证明加密货币网络，它通过简单的管理机制来实现网络的改动与更新，还可以通过连接其他空间来实现扩展。

Cosmos 网络的中心及各个空间可以通过区块链间通信（IBC）协

议进行沟通，这种协议是针对区块链网络的，类似 UDP 或 TCP 网络协议。 加密货币可以安全快速地从一个空间传递到另一个空间，两者之间无需体现汇兑流动性。相反，空间内部所有代币的转移都会通过 Cosmos Hub 中心，它会记录每个空间所持有的代币总量。这个中心会将每个空间与其他故障空间隔离开。因为每个人都可以将新空间连接到 Cosmos Hub 中心，所以 Cosmos 也可以兼容未来新的区块链。（如图 5-8 ）

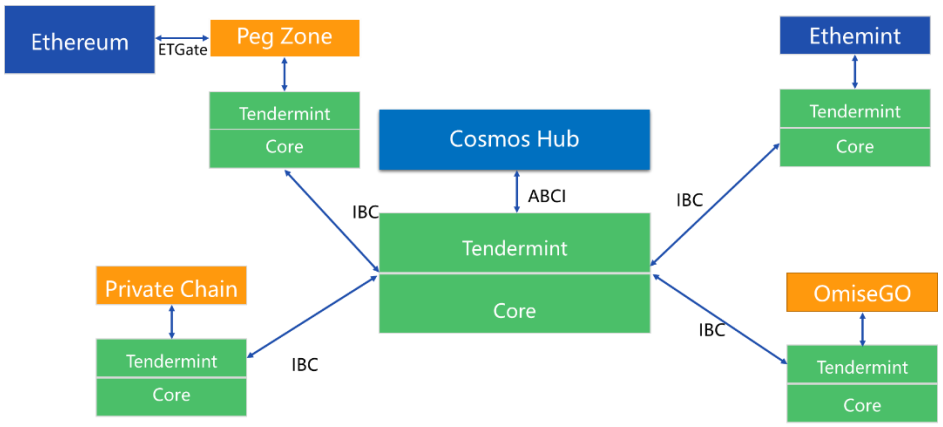

图 5-8 COSMOS 生态系统

5.3.3 链网的设计原则

现在的区块链互联网（简称链网）项目只考虑到了互通性，而没有考虑到完备性。中间链（或中继链），无论是 Polkadot 还是 Cosmos，都是一个中心化的架构。虽然中间链可以由一条分布式的链来完成，但是以整个系统来看，中间链还是一个中心化的组织。中间链的计算及通讯量容易成为链网的瓶颈。

一个理想的链网项目，需要下面的特性[7]：

[7] 蔡维德，从大数据时代走向区块链时代，互链网新思维和新架构，https://www.8btc.com/article/359033，2020.01.28.

支持多链式架构(Multi-chain structure)：异构网络是由多条不同的类型的并行的链所构成的；同质网络是由一群相同类型的并行的链所构成的。理想的链网项目需要支持异构网络互联的多链式架构，而不是同构网络连通的单链式架构。

互通性（Interoperability)：在异构网络上，每一对不同的链都需要有互通的协议。假设有 100 种链参加链网，如果采用点对点的数据互通，则需要 100x99＝9,900 种互通协议。

可延伸性(Extensibility)：一个理想的链网可以像互联网一样，随时的、无限制的到处延伸。

可更改性(Modifiability)：一个理想的链网可以让任何机构或个人随时加入或离开，但是区块链架构不能改变，链网的架构也不能改变。

可复制性(Duplicability)：每个链可以很快地复制。如果链的复制很慢，链网需要很长的时间才能搭建起来，高可复制性可以迅速地搭建链网。

可管理性、非对称结构（Asymmetric structure)：链网必须具有可管理性。正因为管理机制的存在，链网具有非对称结构。有些节点或链会比其他的节点或链更加重要，并拥有非对称的信息，例如监管机构、域名服务商、控制节点等。

层次性（Hierarchical structure)：成为一个大型网络，链网必须具有层次性，高层次的链和节点具有不对称的权利。

一致性(Consistency)：每一条链都必须有自己的一致性，链与链

之间也要有一致性的协议。

高可靠性（Integrity）：链网既然是一个价值网络，就必须具有高可靠性。

完备性（Integrity）：每一条链与每一条链的共识机制及消息的来源与可靠性是不一样的，因此不同的链的完备性是不一样的。低完备性的链不可以输送数据到高完备性的链，而高完备性的链可以输送数据到低完备性的链。如果高完备链收了低完备链的数据，高完备链的数据就会被污染（contaminate）。

第六章 区块链面临的技术挑战

6.1 区块链技术的不可能三角

6.1.1 CAP 理论

计算机科学家埃里克.布鲁尔针提出了关于分布式计算系统的一致性(Consistency)、可用性(Availability)、分区容错性(Partition-tolerant)的 CAP 定理。CAP 定理证明，当网络存在分区时，一致性，可用性和分区性之间只能三取二。

先来解释三个名词：

- ① 一致性：统一的记录；
- ② 可用性：正常节点响应；
- ③ 分区容错性:指的是网络中允许丢失从一个节点发送到另一个节点的任意数量的消息。

在网络分区发生时，两个分布式节点之间无法进行通信，那么我们对一个节点进行的修改操作将无法同步到另外一个节点,所以数据的「一致性」将无法满足,因为两个分布式节点的数据不再保持一致。除非我们牺牲「可用性」，也就是暂停分布式节点服务，在网络分区发生时，不再提供修改数据的功能，直到网络状况完全恢复正常再继续对外提供服务。或者为了保证可用性，而牺牲数据一致性。

所谓的“**区块链技术的不可能三角**”是指在区块链公链中，很难同时做到既有很好的“去中心化”，又有良好的系统“安全性”，同时还能有很高的“交易处理性能”。其中“交易处理性能”也就是经常说的 TPS—每秒处理交易的笔数。(如图 6-1)

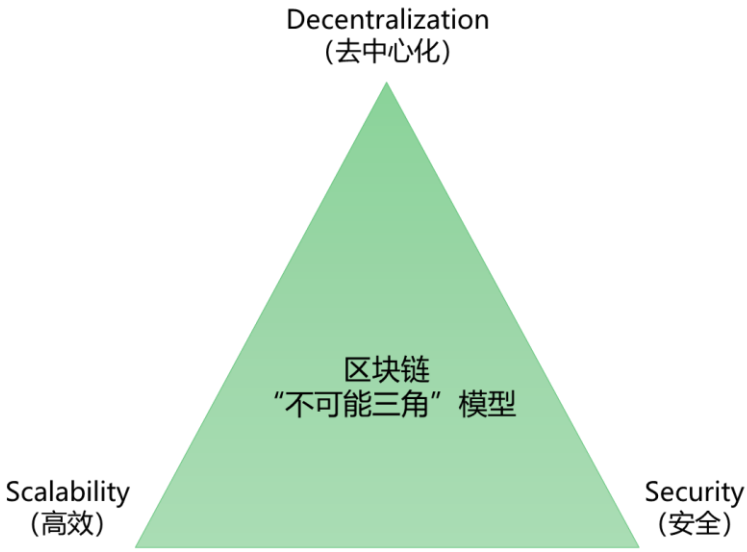

图 6-1 区块链技术的“不可能三角”

接下来用 CAP 理论，来解释区块链不可能三角为什么不可突破。

1）一致性是安全性的必要条件

当系统中出现不一致时（两个节点记录的数据不一致），我们认定这样的区块链系统是不安全的。在这样的定义下，一致性是区块链系统安全的基本前提，区块链的安全性是比分布式系统的一致性更加严格的需求。

2）可用性是可扩展性的必要条件

可扩展性指的是，每秒可以处理的交易量，高可扩展性即是实现每秒高频次的可读可写操作。在逻辑上，可用性是比可扩展性更基础的网络要求，不能实现可用性的区块链系统，是不能实现可扩展性的，即是可用性是可扩展性的前提。

3）分区容错性是去中心化的必要条件

在真实分布式环境中，分区是分布式系统必然存在的，不可能保证系统中的每个节点，都不会出现任何故障。也就是说去中心化必定

导致发生分区的可能，也就意味着分区容错性是实现去中心化的前提。

6.1.2 公链技术现状

目前最著名的三大公链是比特币，以太坊和 EOS。其它公链要么是模仿三大公链，要么是从三大公链分叉出来，在各方面都和三大公链很类似。因此我们主要观察三大公链就可以看到公链技术的现状。

1）比特币

比特币采用的是基于工作量证明（POW）的共识机制。在比特币发展初期，一台普通电脑就可以参与挖矿。但后来，随着币价的猛涨，挖矿变得有利可图，于是显卡挖矿出现，再后来，算力更强的 ASIC 矿机出现，并最终成为主要挖矿手段。普通电脑和显卡挖矿彻底成为历史。现在 ASIC 矿机的制造和生产几乎被比特大陆所垄断，而比特币全网的算力也几乎被几大矿池所垄断。因此比特币的“去中心化”在很多人看来已经名不符实。

在“交易处理性能”方面，比特币的 TPS 大概只有每秒 7 笔，已经完全不适合作为日常高频，小额转账使用。正是如此低下的交易性能导致比特币社区对比特币未来的发展产生了分歧。而这个分歧并没有得到妥善的解决，最终导致 2017 年比特币硬分叉出了比特币现金。

在安全性方面，比特币目前来说无疑是最好的。其全网算力一方面随着 ASIC 矿机自身的更新换代在不断提高，另一方面新矿机源源不断地加入也在持续增强全网算力。据测算，目前攻击比特币所需的代价是所有 POW 公链中最高的。

2）以太坊

以太坊也是基于工作量证明的共识机制。但它仍然可以采用显卡挖矿，因此算力垄断的情况没有比特币那么严重，所以在“去中心化”方面比比特币要好一些。以太坊未来将彻底转向 POS 共识以解决算力垄断的问题。

以太坊的 TPS 比比特币稍微高一点，每秒大概 7 到 15 笔左右。但由于以太坊是智能合约平台，它的应用场景更复杂，相对比特币更容易发生拥堵。因此以太坊爆出的性能问题所受的关注度更高。也正因为如此，才有了后来备受期望和关注的 EOS 诞生。

以太坊在安全性方面仅次于比特币。据测算，目前攻击以太坊所需的代价仅次于比特币。

3）EOS

EOS 一出现时，最大的卖点就是 TPS 高，交易性能强。现在 EOS 的真实性能虽然没有达到官方曾经宣扬的百万级，但在三大公链中是最高的，达到了 3000 到 4000TPS 左右。这个性能远远抛开了比特币和以太坊。

但 EOS 为了达到这样的 TPS，在“去中心化”方面做出了巨大的牺牲。相对于比特币和以太坊全网上万个节点，它全网只有 21 个节点。因此在“去中心化”方面是三大公链中最受质疑的。

在安全性方面，由于 EOS 全网只有 21 个节点，因此比起攻击比特币或以太坊的几千个节点，攻击 21 个节点对黑客来说相对容易很多。所以在安全性方面 EOS 也是三者中最差的。

图 6-2 对三大公链的“不可能三角”进行了总结对比：

		安全性	扩展性	去中心化
Bitcoin	POW	√	×	√
以太坊	POS	√	√	×
EOS	Dpos	×	√	×

图 6-2 三大公链技术的对比总结

6.2 可扩展性及探索方向

公链在保证去中心化机制和安全的前提下，隐藏了两个结果

1. 低吞吐量：单位时间只能处理有限的交易数量；

2. 缓慢的交易处理时间：全链形成共识导致区块生成时间缓慢。

随着公链规模的增大，对存储、带宽、节点算力的要求提高，导致系统效率更低。目前解决可扩展性的探索方向包括：

- 链下交易通道：例如闪电网络，使用链下微支付通道快速处理交易，链上结算阶段性交易总和；
- 分片：类似传统数据库的分区，将区块链分成不同的片，片间可以并行处理；
- 链下计算扩展：例如侧链技术，因为主链升级代价非常高，将特殊的计算和验证过程转移到链下，并将结果上链；
- DAG：基于有向无环图组织区块，提高出块和成链的并行处理能力。

6.3 隐私保护及探索方向

对于交易的匿名和隐私保护对于方面，达世币（DASH）、门罗币（XMR）、大零币（ZEC）分别在混币技术、环签名、和零知识证明技术上进行了尝试和探索。

隐私保护的另外一个领域是智能合约的隐私保护，以防止针对智

能合约的攻击。目前有几个方向的探索：

- 代码混淆（Code Obfuscation）：隐藏程序中的私有数据，降低攻击风险。不可分辨性混淆（indistinguishability obfuscation）是正在努力的方向；
- 预言机（Oracles）：智能合约与链外数据源之间的信息载体，有助于隐私信息的保护；
- 可信执行环境（Trusted Execution Environment）：保证内部加载的代码和数据在保密性和完整性上得到保护。

代码混淆(Code Obfuscation)亦称花指令，是将计算机程序的代码，转换成一种功能上等价，但是难于阅读和理解的形式的行为。代码混淆可以用于程序源代码，也可以用于程序编译而成的中间代码。执行代码混淆的程序被称作代码混淆器。目前已经存在许多种功能各异的代码混淆器。

黑箱混淆器（black box obfuscator）是理论上非常理想的混淆器，但早在十多年前就被证明是不可能的。2013 年，美国加州大学洛杉矶分校的 Sahai 教授及其合作者们提出了一种不可分辨性混淆技术（indistinguishability obfuscation），其基本思想是把一个程序转换为一种称为多线性拼图的游戏（multilinear jigsaw puzzle），从而将混淆技术的安全性转化为一类与格（lattice）有关的数学难题。与理想的黑箱混淆器相比，这种混淆技术具备了黑箱混淆器的大多数特性。不仅如此，这一技术自提出以来，已经经受住了领域内一大批专家（包括提出者）的第一轮攻击。

代码混淆器也会带来一些问题。主要的问题包括：

- 被混淆的代码难于理解，因此调试以及除错也变得困难起来。开发人员通常需要保留原始的未混淆的代码用于调试。
- 代码混淆并不能真正阻止反向工程，只能增大其难度。因此，对于对安全性要求很高的场合，仅仅使用代码混淆并不能保证源代码的安全。

6.4 智能合约形式化验证

软件的形式化验证用于确定程序是否按照规范行事。一般使用一个具体的规范语言来描述函数的输入输出应该如何相关，并基于此证明程序的输入输出的相关性。

智能合约需要形式化验证。第一，智能合约一旦上链不可改变，因此编程漏洞变得不可接受；第二，智能合约是完全公开访问的，这提供了开放性和透明度，也使其成为黑客攻击目标。形式化验证是减少软件漏洞和攻击风险的强有效的方法，与传统方法（测试、同行评审等）相比提供了更高的正确性保证。

目前以太坊智能合约形式化验证较难实现，因为以太坊虚拟机EVM不针对第三方提供测试，目前以太坊基金会仅使用机器辅助逻辑推理验证合约所需的工作量。如果要实现以太坊智能合约的形式化验证，需要彻底改革以太坊虚拟机EVM使其更容易进行形式化验证，或者建立全新的语言和虚拟机系统来支持形式化验证。但无论哪种选择，都需要制定形式化验证库和标准。

6.5 数据存储的探索方向

数据信息上链意味着：第一、数据在区块链上的每个节点都要进行存储；第二，数据仅可读写，不可改删，因此数据被永久存储。因此，区块链数据存储的成本巨大，任何构建在链上的现实应用，都需要优化存储解决方案。“分片”是目前区块链数据存储的主要探索方向。

1）分片的种类

分片是一种水平分区，是一种广泛使用的数据库设计原则，将大型数据库中的数据划分成很多数据分片（shard），再将这些数据分片分别存放在不同的服务器中，以减小每个服务器的数据访问压力，从而提高整个数据库系统的性能。区块链引入芬片技术是为了解决可扩展性和交易确认延迟问题。

区块链分片按技术划分为网络分片（Network Sharding），交易分片（Transaction Sharding），状态分片（State Sharding）。

- 网络分片：将整个区块链网络划分成多个子网络，也就是一个分片。网络中的所有分片并行处理网络中不同的交易。在区块链中实现分片，网络被分成不同的团队（分片）。分片可以并行处理事务。每个节点只拥有区块链上的部分数据，而不是全部信息。因此，可以同时处理更多的事务。例如，想象一个有 1000 个节点的网络;可以将网络分成 10 个分片，每个分片由 100 个节点组成。速度应该增加 10 倍。
- 交易分片：由于网络分片是其他所有分片的基础，因此交易分

片的前提是先进行网路分片。交易分片主要涉及的问题是哪些交易应该按照特定的属性被分配到哪些分片当中。

- 状态分片：状态分片的关键是将整个存储区分开，让不同的分片存储不同的部分，每个节点只负责托管自己的分片数据，而不是存储完整的区块链状态。状态分片可以减少状态的冗余存储，使得整个区块链网络具有存储的可扩展性。

2）分片面临的挑战

在私有区块链部署中，分片可能是有效策略，但在公共区块链网络使用区块链分片并不容易。最大的挑战之一是分片间的通信。 当节点分配给分片时，与该节点相关的用户和应用程序会将分片视为独立的区块链系统，而不是大型系统的一部分。分片之间的通信可能难以建立，并且需要特定的开发工作来部署通信机制。即使有这种机制，分片间通信也会导致更大的开销，这会让分片的优势大打折扣。

分片也可能破坏更传统的区块链接带来的制衡。通过分片，用户不再下载和验证整个交易历史记录，因此他们无法确定数据的可靠性和不变性，这通常是根据交易块的链式序列来确定。如果没有这些安全机制，黑客就可更容易操纵或控制分片，这种情况被称为单一分片攻击，可能导致数据丢失或受损。

区块链分片的另一个挑战是共识和验证。不同的区块链方法依赖于不同的算法来跨节点达成共识。两种常见的算法是工作量证明(POW)和权益证明（POS)。这两者都可确定如何在分布式网络中验证交易，但它们是以不同方式完成验证。一般来说，POS 被认为比 POW 更适合

分片。

对于如何部署分片，缺乏标准化。可以通过不同的方法来进行分片，并且很多方法仍然在研究、开发或测试中。每种分片方法都有其优点和缺点，这使得难以确定行业标准。

3）分片的未来

对于公共区块链部署，可扩展性仍然是重大挑战，而分片正在成为解决此问题的主要方法之一。必须谨慎应用分片技术，以确保它不会对区块链过程产生负面影响或使数据置于风险之中。事实证明，区块链分片必须与其他技术结合使用以提供必要的可扩展性，例如支持分片通信的新协议。在此之前，公共区块链存储可能仍然保持目前的整体性，直到随着它变得越来越大，性能逐渐下降。

4）现有数据存储与分片的案例

Swarm 是以太坊采用的点对点文件共享协议，允许用户将数据存在链下的 Swarm 节点，并在主链上交换数据。Storj 是一种数据分片解决方案，将数据分片、加密、分散多个节点，使用 SCJX 币支付激励节点的存储操作。IPFS 是一种 P2P 超媒体协议，是以内容寻址超链接为基础的、提供高吞吐量和内容寻址的块存储模型。

6.6 共识机制的困境和创新

共识是一切交易的基础，是区块链技术的核心。达成共识越分散（参与度越高），其效率就越低，但安全性越高，因此也越稳定；达成共识越集中（参与度越低），效率越高，也越容易出现独裁和腐败现象，安全性越低。

目前为止，工作证明 POW 仍是最安全的共识机制，但是存在如下缺陷：

- ASIC 矿机和矿池的形成促使挖矿算力集中化，前五大矿池占据挖矿算力的 70%，已经形成了算力寡头格局；
- 能源浪费：2017 年比特币“挖矿” 电量超过 29.05 太瓦时，超过了全球 159 个国家的年均用电量,2018 年则超过 59 太瓦时；

权益证明 POS，完全不需要进行计算，但在提升性能的同时，很难保证其安全性，目前存在 POS 攻击方式如下：

- 权益无关问题（Nothing at stake）：如果攻击者分叉了当前的链，挖矿节点的保证金已经押在了两条链上，它不需要去判断哪条是正确的链，而是都支持，从而导致攻击者得逞；
- 长链攻击风险（Long range attack）：攻击者不分叉现有的链，而是回到初始阶段的链，造一条更长的新的链，让网络误以为是主链。目前长链攻击（long range attack）还没有很好的解决方案。

6.7 去中心化的治理难题

公链的理想是不需要任何中心机构或者组织进行决策，但这面临了一个两难境地：

- 构建一个完全不需要任何信任和许可的开源系统；
- 实现安全一致的协议升级方式，并有专人负责制定并维护标准。

目前各家公链都采用了开放社区或者基金会的方式来运作公链系统，比如比特币社区和以太坊基金会。但是，比特币的数次分叉已经

证明，完全开放的社区治理模式是失效的；以太坊基金会的运作也证明，在没有明确领导力的情况下，制定标准会造成一片混乱，也不能在紧要问题上迅速达成共识。

总之，区块链公链治理是一个棘手难题，探索合理的区块链治理机制和标准，在中心化和分布式管控之间寻找平衡是公链治理步入正轨的关键。

第七章 国内自主可控区块链技术

7.1 自主可控区块链技术

2020 年 10 月 15 日，美国正式宣布区块链技术作为战略性核心技术，禁止对华出口。国内研发自主可控的区块链核心技术迫在眉睫。就区块链本体技术而言更多表现为数据库、密码、网络等技术的集成，并形成不断进化的软件和数据生态。因此，其所谓的核心技术主要表现为以下几个方面：

1）数据库、密码、网络等计算机技术，这也是我国长期以来一直未解决的技术。如果这些卡脖子的基础技术不解决，区块链的发展基本上还是重蹈沙滩上建高楼的过程。

2）数据库、密码、网络等进行有效组合而构建为高性能区块链的区块链体系结构技术。在这一方面，各方处于同等发展机会，关键是新型区块链体系结构能否快速得到验证和推广应用。

3）区块链的平台化、服务化、生态化构建能力。正如操作系统有服务端的 Linux、桌面端的 Windows、手机端的 Andirod 等构建自己的生态并各领风骚一样，区块链生态中也不可能一种系统独揽天下，需要踏踏实实凝练出针对不同应用领域的区块链平台，并在本领域构建相应的生态。

实际上，国内的学术界和产业界一直都在进行自主可控区块链技术的研发，本文以北航郑志明院士和清华郑纬民院士的区块链项目为代表，介绍国内原始创新的自主可控区块链技术的进展与情况。

7.1.1 鸿链系统[8]

苏州鸿链是由北京航空航天大学郑志明院士团队的科研成果转化而来，团队在分布式可信系统、区块链、密码学、隐私保护等领域具备扎实的产学研用的理论和实践基础。目前郑志明院士担任工信部区块链与安全技术重点实验室学术委员会主任、北京市区块链专班首席顾问、雄安区块链实验室学术引领委员会主任、 国家电网区块链实验室主任、鹏城实验室（国家实验室）区块链技术牵头人、中国通信学会区块链委员会主任/金融委员会主任、可信区块链联盟战略指导委员会主任委员。

鸿链主要面向电力行业、金融行业、国际贸易行业、产业物联网等领域提供区块链可信智能整体解决方案。鸿链从异构理论交互理论、运筹与并行理论、密码学安全理论、分布式计算理论以及软件可信性理论出发，遵循理论-技术-工程一体化路线，原始创新了自主安全可控的区块链底层操作系统——鸿链区块链底层操作系统 NSCHAIN，实现了强兼容、强安可、强隐私、强扩展、快收敛、松耦合、轻量级、易监管等八大核心技术特征。团队首次提出了区块链抗量子身份识别系统、基于状态通道的全态隐私保护技术、海量物联网终端身份即标识的区块链轻量级接入技术等理论和技术创新点。

鸿链区块链操作系统 NSCHAIN 是一套理论-技术-工程多维度原始创新的区块链基础平台，其八大设计理念如图 7-1 所示。

[8] 本小节内容由鸿链科技提供 http://www.hongchain.cn/

图 7-1 鸿链区块链操作系统 NSCHAIN 核心技术特征

鸿链系统的特点是在技术上实现了国密账本和安可链双核心引擎支持，如图 7-2。

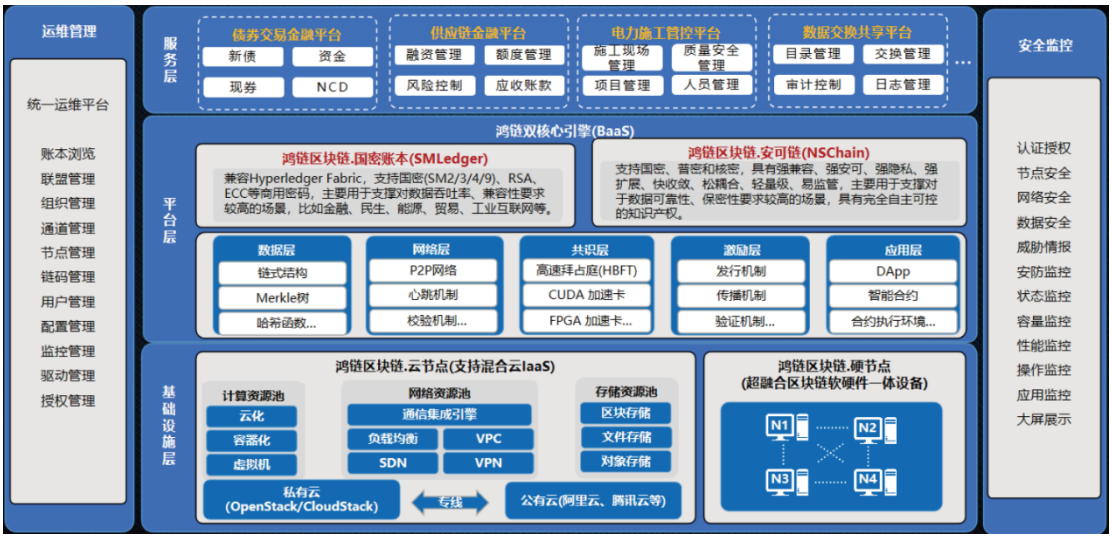

图 7-2 鸿链技术架构

鸿链区块链国密账本（英文:SMLedger，简称:SML）是由鸿链科技研发的先进的、高性能的、高安全的国密区块链系统，可支持丰富的业务场景，具备国密安全、共识插拔、低延迟、高 TPS 的特性，已在多个领域中实现落地应用。鸿链区块链国密账本一体化管理平台（英文:SMLedger Admin）是提供操作鸿链区块链国密账本的管理工具，

其功能包括账本浏览、联盟管理、组织管理、通道管理、节点管理、链码管理、用户管理、配置管理、监控管理、驱动管理和授权管理，共 11 个功能模块。SMLedger 主要用于支撑对数据吞吐率、兼容性要求较高的场景，比如金融、贸易、工业互联网等。

鸿链区块链底层操作系统 NSCHAIN(也称：鸿链.安可链)，实现了强兼容、强安可、强隐私、强扩展、快收敛、松耦合、轻量级、易监管等八大核心技术特征。团队首次提出了区块链抗量子身份识别系统、基于状态通道的全态隐私保护技术、海量物联网终端身份即标识的区块链轻量级接入技术等理论和技术创新点。鸿链区块链操作系统 NSCHAIN 是一套理论-技术-工程多维度原始创新的区块链基础平台，主要用于支撑对于数据可靠性、保密性要求较高的场景，比如军事生态体系。

7.1.2 清华自主链系统

清华自主链（暂定名）系统由清华大学计算机系郑纬民院士领衔研发，团队历时三年，已基本完成主体系统的设计和开发工作，具有完全的自主知识产权。该平台系统的整体架构如图 7-3。

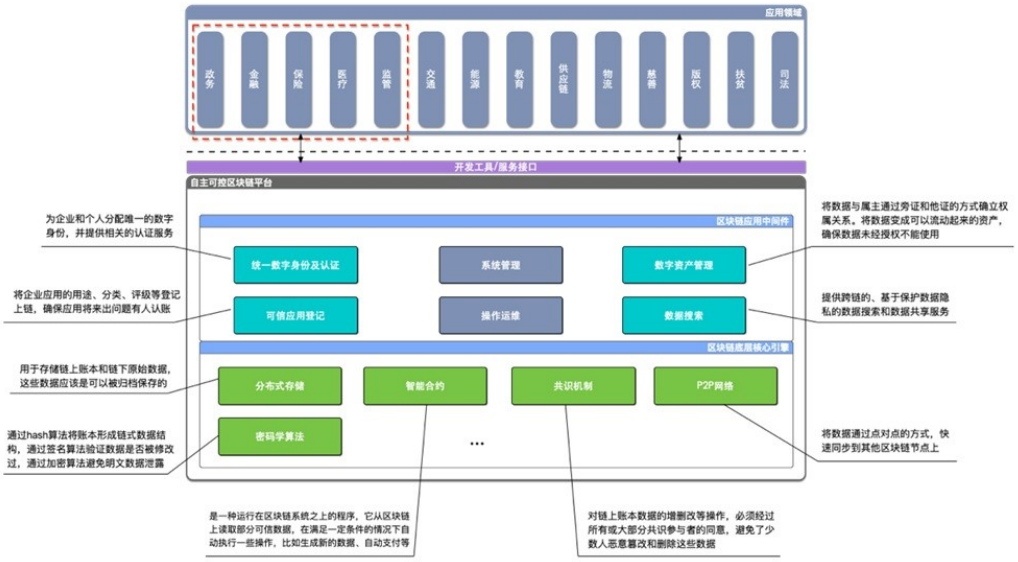

图 7-3 清华自主链系统架构图

该平台系统包含三个主要组成部分：（1）区块链底层核心引擎，（2）区块链应用中间件，（3）区块链海量数据存储系统。

1）区块链底层核心引擎（自主联盟链系统）

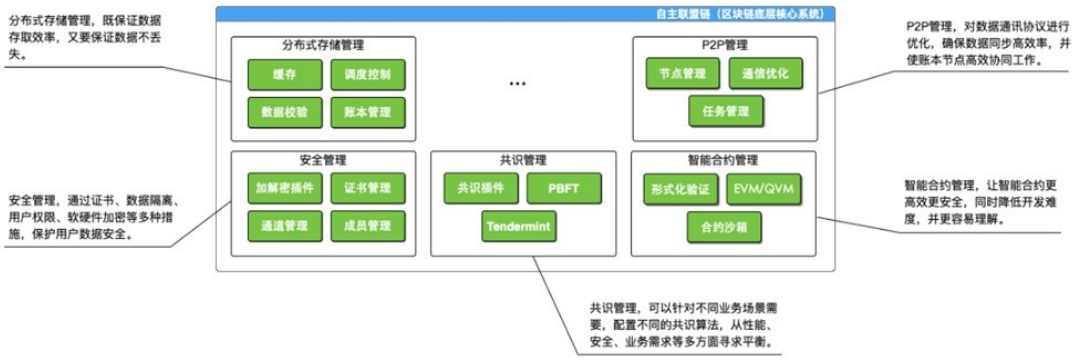

图 7-4 清华自主链核心引擎

该联盟链核心引擎（如图 7-4）的核心技术路线如下：

- 对国产加密算法原生支持：不仅对目前通用的椭圆曲线加密算法能够很好地支持，而且对国密算法的支持有了更进一步的优化，结合软硬件加速等措施，使数据在加解密、签名、验签的效率和性能方面有了极大提升。

- 共识算法：对 Tendermint 算法进行改进，在确保了安全性的前提下，减少了交互确认的次数，提升了性能。
- 智能合约管理：建立智能合约沙箱机制，使智能合约在部署到生产网络之前进行全面的验证，提高了安全性，同时降低了开发和验证难度。

后续将会通过优化 P2P 网络通讯协议，提升数据传输、数据同步的效率；引入智能合约形式化验证，加强安全检测，减少漏洞；提供零知识证明及隐私计算模块，确保数据安全。

2）区块链应用中间件

区块链应用中间件系统的主要目标是让应用开发与具体的区块链底层技术，以及系统部署、运维、数据维护等复杂技术工作相隔离，从而大幅度简化区块链应用的开发难度和成本，让项目具备快速迭代、易维护、易扩展、高可用等能力，并支持对接各种不同异构区块链底层核心技术。如图 7-5。

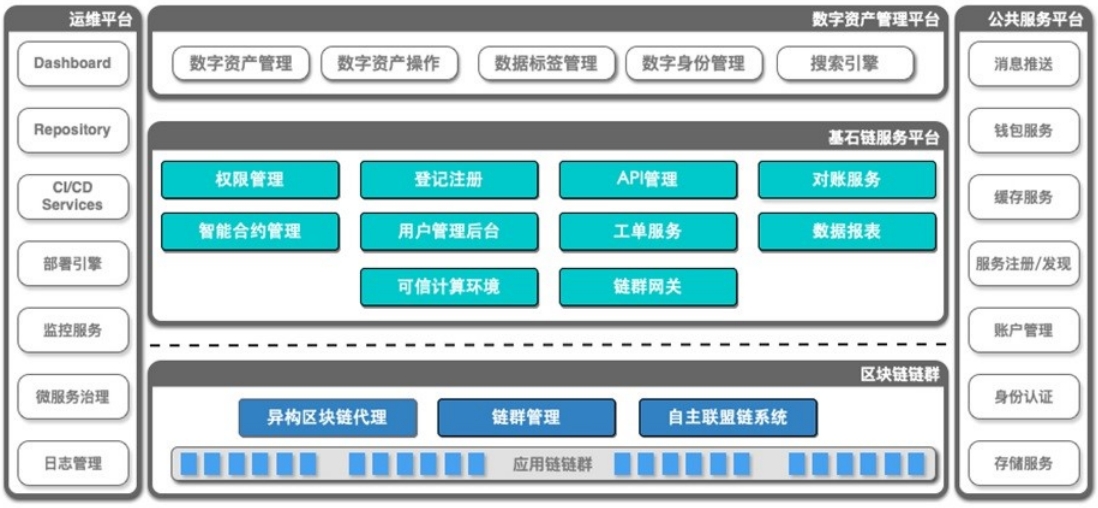

图 7-5　清华自主链区块链中间件系统

3）区块链海量数据存储系统

区块链海量数据存储系统有别于数据的单纯哈希值上链，该系统解决的是数据本身上链的问题（与 IPFS 类似），其核心技术路线如下（如图 7-6）：

- 支持多种异构数据源：借鉴 Hadoop、Spark 等现有大数据系统的成熟方案，可以接入多种异构数据源。
- 对数据分类算法进行优化：使用基于内容+地址寻址算法，对数据进行智能化目录和标签分类，建立树形索引来对数据进行分类存储。
- 对数据的存储结构进行优化：结合 DAG 技术优化存储结构，使存入分布式存储系统中的数据分块、分版本，带时间戳、校验码和签名，能够让存储的数据既具备了不可随意篡改的属性，又确保了读写的性能和多副本的安全性。

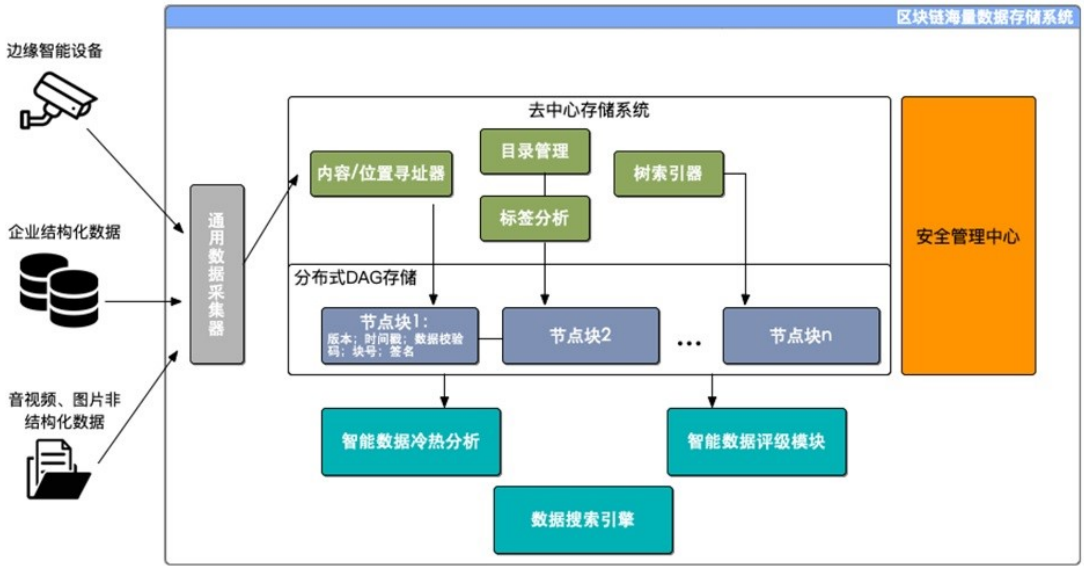

图 7-6 区块链海量数据存储系统

后续将结合人工智能、图数据库等技术，实现历史数据的智能冷热分析和智能数据质量评级，结合硬件芯片，对数据分类、压缩解压

缩、编解码、校验、加解密等进行性能优化，并开发基于可信数据源的搜索引擎。

7.2 区块链技术生态联盟

区块链技术诞生于开源社区。以开源社区为代表的技术生态联盟在区块链技术的发展过程中一直扮演着重要作用。在国际上，公链技术主要是比特币、以太坊、和 EOS。根据赛迪区块链研究院与天德科技 2018 年 12 月 6 日发布的公链技术评测报告[9]，其他大部分公链开源项目的代码都与上述三大公链其中之一的代码重合度极高，不具自主创新性，可以视为上述三大公链项目的衍生项目。

国际上的联盟链技术生态联盟主要是企业以太坊联盟（EEA - Enterprise Ethereum Alliance）和超级账本（Hyper Ledger）联合项目。

EEA 致力于将以太坊开发成企业级区块链，2017 年 2 月 28 日，由一批代表着石油天然气行业，金融行业和软件开发公司的全球性企业正式推出，这些企业包括英国石油巨头 BP、华尔街投资银行摩根大通、软件开发商微软、印度 IT 咨询公司 Wipro 以 30 多家其他不同的公司。

超级账本（Hyper Ledger）联合项目，于 2015 年 12 月，由 Linux 基金会牵头，IBM、Intel、Cisco 等共同宣布了成立。超级账本项目为透明、公开、去中心化的企业级分布式账本技术提供开源参考实现。

对应 EEA 和 Hyper Ledger，国内联盟链也存在两个比较有影响力

[9] 天德科技，全球公链项目技术评估与分析蓝皮书，http://www.tdchain.cn/tdchain/publicchain.html

的区块链技术生态联盟：FISCO BCOS 和长安链。需要说明的是，根据公开资料，上述两个项目虽然最初基于 EEA 和 Hyper Ledger 项目，但是已经各自完成了代码重构与自主化，成为国内自主可控区块链技术生态联盟的代表。

7.2.1 FISCO BCOS

金融区块链合作联盟（简称金链盟）是由深圳市金融科技协会、深圳前海微众银行、深证通等二十余家金融机构和科技企业于 2016 年 5 月 31 日共同发起成立的非营利性组织。金链盟作为一个开放式组织，自愿遵守章程的金融机构及向金融机构提供科技服务的企业等均可申请加入。至今，金链盟成员已涵括银行、基金、证券、保险、地方股权交易所、科技公司等六大类行业的八十余家机构。如图 7-7。

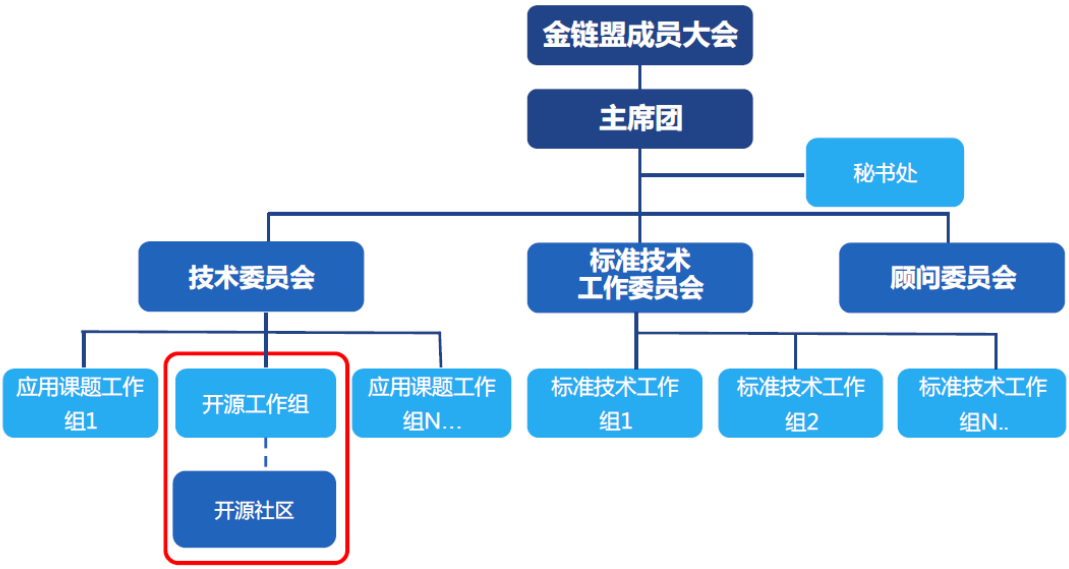

图 7-7 金链盟的组织结构

FISCO BCOS 初衷是设计一个国内企业主导研发、自主可控、对外开源的满足金融行业需求的企业级区块链底层平台，并逐渐扩展至其他领域、适用于广泛的分布式商业场景。所以进行了自底向上的完整

设计，并考虑了较多国内的特殊需求。FISCO BCOS 扎根金融行业，由金链盟管理。

根据 FISCO BCOS 白皮书，FISCO BCOS 旨在解决传统行业，特别是金融行业，IT 基础设施的不足与痛点，包含操作风险、道德风险、信用风险、信息保护风险等方面。

FISCO BCOS 引入了多个特性，包含基于区块链网络的消息通信协议（AMOP）、合约命名服务（CNS）、并行共识与并行计算、极强维护性和可视化的浏览器与监控。

在监管方面，FISCO BCOS 引入如下标准：风险数据整合；风险建模，分析和预测；实时交易监控，汇报和拦截；身份识别等。

FISCO BCOS 还在安全及隐私保护方面有重大突破，包括支持了多 CA 认证、国密算法、同态加密、零知识证明、群签名环签名等。同时，FISCO BCOS 即将在腾讯云上线区块链云服务，向企业及开发者提供便捷易用的区块链云服务，配合开源运营与生态建设，让 FISCO BCOS 成为更佳更完备的联盟链系统。如图 7-8。

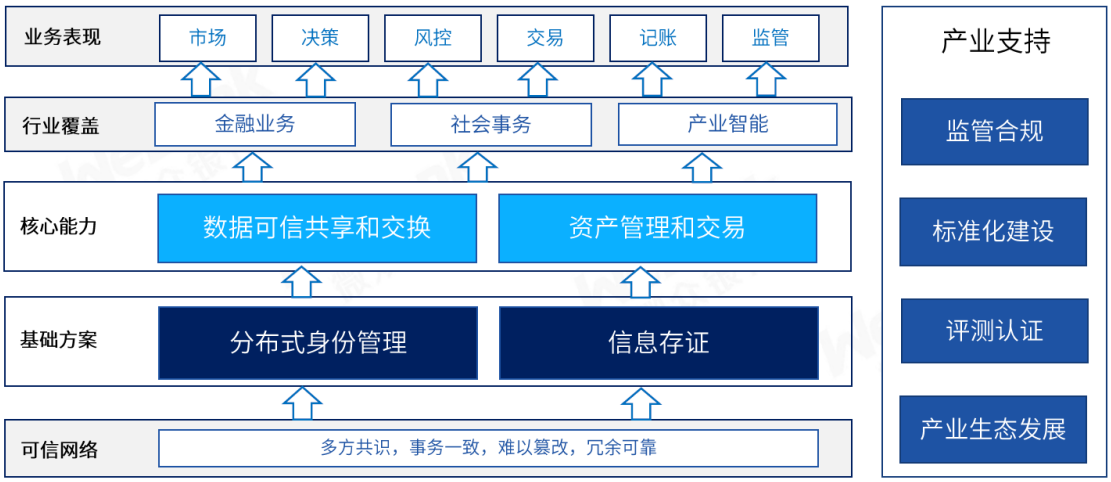

图 7-8 FISCO BCOS 的系统结构

7.2.2 长安链

为加快推动区块链技术和产业创新发展，北京市联合央企、头部企业等优势力量，着力推动自主可控区块链技术体系研发，建设可信数字基础设施，组建长安链生态联盟，推进区块链产业创新生态建设。

2021 年 1 月 27 日，由国家电网、建设银行、北京微芯研究院等 27 家单位共同发起的长安链生态联盟工作在北京成立。27 家联盟成员共同签订倡议书，共建长安链生态联盟，并发布长安链·ChainMaker 软硬件技术体系和联盟首批重点应用场景。

长安链具备自主可控、灵活装配、软硬一体、开源开放等特点，由北京微芯研究院、清华大学、北京航空航天大学、腾讯和百度等知名高校、企业共同研发。长安链面向大规模节点组网、高交易处理性能、强数据安全隐私等下一代区块链技术需求，融合区块链专用加速芯片硬件和可装配底层软件平台，为构建高性能、高可信、高安全的数字基础设施提供新的解决方案。

软件方面，长安链独创深度模块化、可装配、高性能并行执行的区块链底层技术架构，实现抗量子加密算法、可治理流水线共识、混合式分片存储等十余个核心模块全部自主研发，交易处理能力达到 10 万 TPS，位居全球领先水平。长安链软件平台可实现根据不同的业务场景自动选取和装配适当组件，满足资产交易、数据共享、可信存证等不同需求。

硬件方面，全球首创基于 RISC-V 开源指令集的 96 核区块链芯片架构，构建物理安全隔离的高效可信运行环境，实现智能合约的并行

加速处理，大幅提升超大规模区块链网络交易性能。

长安链生态联盟将致力于共建国家战略科技力量，推动长安链技术体系不断迭代优化，为我国区块链核心技术自主创新突破创造有利环境；共谋驱动经济发展，协同布局产业场景，打造可信数字基础设施，助力区块链技术赋能实体经济，推动经济高质量发展；共推服务社会民生，遵循以人为本的理念，探索自发、内生的区块链治理服务体系，赋能社会治理共同体建设。

7.2.3 能源电力领域技术生态联盟

2020 年 10 月 24 日，国家电网公司联合航天科技、兵器工业集团、中国石油、中国石化等 20 余家中央企业共同发起成立中央企业区块链合作创新平台，致力于搭建中央企业区块链服务网络，构筑区块链产业新业态。成立中央企业区块链合作创新平台是中央企业落实区块链国家战略和适应区块链行业转型发展之需，平台将以突破区块链核心技术自主创新、推动“区块链+”多元化赋能、培育区块链产业新业态、构建区块链行业标准体系、探索区块链应用技术引导和规范为重点建设内容，依托中央企业资源优势和强大影响力，引领创新区块链产业发展新模式，加速我国区块链产业化、规模化进程，助力我国抢占区块链国际话语权和规则制定权。

2020 年 11 月 27 日国家电网公司牵头成立 IEEE PES 信息通信与网络安全技术委员会（中国）电力信息通信区块链技术分委会，承担分委会秘书处工作，致力于搭建中国与世界各国在信息通信技术领域的学术交流和国际合作平台，推动 IEEE PES 电力系统通信与网络安

全技术委员会在中国的健康发展，加快中国信息通信企业的国际化进程。

2021 年 1 月 27 日，国家电网公司携手 8 家中央企业区块链合作创新平台成员单位参与“长安链”生态联盟建设。为全面贯彻落实国家 “碳达峰、碳中和”战略目标，国家电网公司牵头发布“区块链+碳交易”生态网络场景，助力北京建设全球区块链科技创新和产业发展高地。深入融入“长安链”，推动清洁能源消纳、冬奥绿电溯源等典型应用场景落地北京，进一步拓展虚拟电厂、共享充电桩、能源大数据中心、综合能源、共享储能、需求侧响应等场景，全面落实北京市与国务院国资委共谋央地合作工作部署，打造央地合作典范。

7.3 金融行业区块链标准

鉴于区块链在金融行业的巨大应用潜力，我国在金融行业的区块链应用标准制定方面走在前列。2020 年，由中国人民银行牵头起草，并由全国金融标准化技术委员会正式发布两项区块链金融应用标准，分别是 2020 年 2 月发布的《金融分布式账本技术安全规范》（JR/T0184-2020），和 2020 年 7 月发布的《区块链技术金融应用 评估规则》（JR/T 0193-2020）。这两个标准（以下简称《标准》）是国内甚至国际的首个区块链金融应用标准。

《标准》中规定了区块链技术金融应用的具体实现要求、评估办法、判定标准等，适用于金融机构开展区块链技术金融应用的产品设计、软件开发、系统评估。《标准》的编制，旨在规范分布式技术在金融领域的应用，提升分布式账本信息安全保障能力。“标准”中提到

的分布式账本技术是密码算法、共识机制、点对点通信协议，分布式存储和其他核心技术高度集成的一种分布式基础架构与计算范式。“金融分布式账本技术安全规范”对分布式账本技术提出了通用的安全规范，作为一个行业标准，其适用范围也相当广泛，会对数字货币，供应链金融等业务应用的安全起到规范的作用。

《标准》从区块链必要的技术要素出发，提出了相关要求和评估方法。从区块链层次架构上总的来说可以分为两个层次：接口层和平台层。接口层主要从对外交互的角度，定义了四种接口的相关要求和测评方法，共涉及 18 个评估子项。平台层划分了 9 个区块链平台核心功能，共包含 207 个评估项。划分在一定程度的参照目前的 ISO、国标等在制定的参考架构的一些思路。在具体内容上，也针对金融行业提出具体要求。如图 7-9。

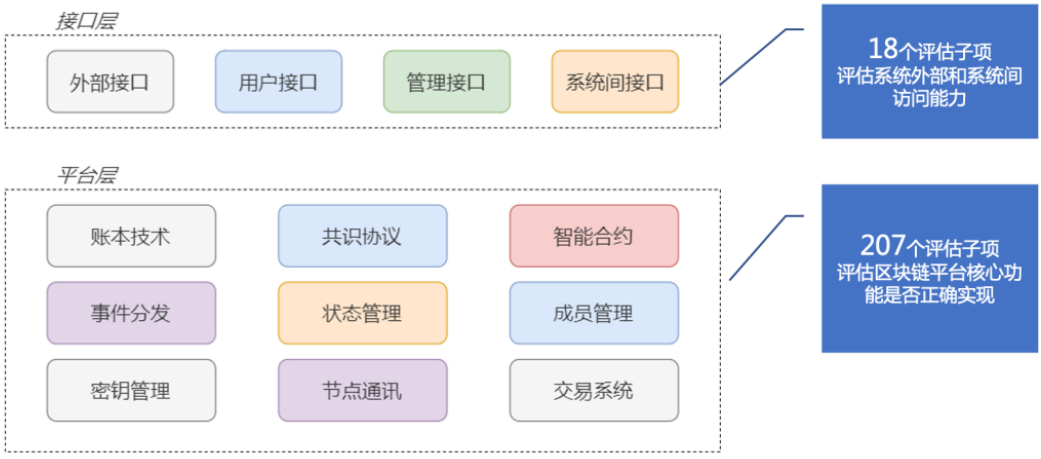

图 7-9 区块链金融应用基本评估

由于行业特殊性，金融行业一直将安全风险视为重中之重。《标准》提出的一套区块链安全架构。如图 7-10。

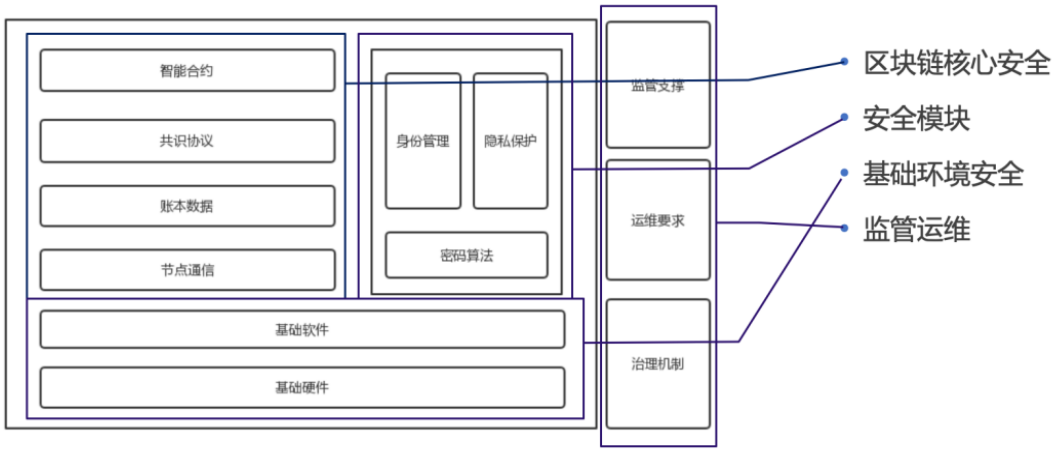

图 7-10 区块链金融应用安全架构

央行牵头发布这份《标准》，对整个行业来说是一个里程碑式的标志事件。可以说，这份标准的发布，不仅在区块链标准制定和应用研究方面分析确定领先技术优势，也是国内企业金融服务行业、区块链行业从业者们的新机遇，有了标准的区块链，将不再野蛮生长，将有更多的共识和协作基础，这对于区块链进一步连接数字化去更好的管理世界、并实现彼此互联互通，具有非常重要的指导实践意义。

2020 年 12 月，深圳市市场监督管理局批准发布地方标准《金融行业区块链平台技术规范》，并于 2021 年 1 月 1 日实施。该标准由深圳市地方金融监督管理局提出并归口，起草单位包括深圳证券交易所、深圳前海微众银行股份有限公司、深圳证券通信有限公司、深圳市互联网金融协会等。该标准为国内首部地方版金融行业区块链平台技术规范，规定了金融行业区块链平台的基本原则、分层框架、功能组件及其技术要求，并适用于深圳市企业建设金融区块链和分布式账本系统、开展金融区块链和分布式账本服务。

只有标准得到更稳固搭建和运行之后，才能谈上层的区块链产品

应用，技术标准是产品应用的根基和土壤，是底层建筑。区块链技术的真正作用，是在产业数字化过程中破解各方协同的痛点，利用自身的技术特性助力效率提升，促进信任经济发展。

7.4 其他区块链领域标准进展

早在 2016 年，区块链就已经开始了标准化的历程。国际标准化组织 ISO 在 2016 年成立了 TC307 分布式账本技术委员会，同年，国内区块链技术和产业发展论坛成立，并开始一系列区块链团体标准的实施计划。

国际标准化组织、全球最大专业技术学会 IEEE（电子电气工程师协会）于 2018 年 12 月正式批准成立区块链标准委员会。迄今为止，该委员会已成立了数字资产、区块链电子票据、加密货币、互助自治以及可信物联网数据管理等 13 个工作组。2020 年 3 月，IEEE 批准成立了数字金融与经济标准委员会，在短短的半年内快速发展并成立了涵盖区块链技术及应用的联盟链、证据收集等 5 个工作组。

在 IEEE 的标准活动中，我国的技术专家积极活跃，引领了很多委员会和工作组的标准活动，并于近一年获得了丰硕的果实。2020 年 6 月 12 日，全 IEEE 的第一个区块链标准 *IEEE 2143.1-2020 - IEEE Standard for General Process of Cryptocurrency Payment* 正式发布，成为了国际标准组织中的第一个发布的加密货币领域标准，为数字货币支付在商业场景下的应用奠定了坚实的基础规范。同年的 7 月至 2021 年 1 月，以下的四个区块链标准/推荐实践也正式发布/获批：

- *IEEE 2140.5-2020 - IEEE Standard for a Custodian Framework of Cryptocurrency*
- *IEEE 2140.1-2020 - IEEE Standard for General Requirements for Cryptocurrency Exchanges*
- *IEEE 2144.1-2020 - IEEE Standard for Framework of Blockchain-based Internet of Things (IoT) Data Management*
- *IEEE P2142.1 Recommended Practice for E-Invoice Business Using Blockchain Technology*

可以看出，在大量的区块链国际标准活动里，我国的技术专家都引领并参与了制定工作，也取得了一定的成果，但在垂直应用方面的标准还需要进一步的加强，区块链金融、区块链能源、区块链医疗、区块链农业、区块链政务等场景将作为 2021 开始的近三年国际、国内标准的重点突破领域。

我国国标也很早开始开展区块链标准工作，目前有三项标准正在起草中，分别是:《信息技术 区块链和分布式账本技术 参考架构》、《信息技术 区块链和分布式记账技术 存证应用指南》、《信息技术 区块链和分布式记账技术 智能合约实施规范》。区块链和分布式账本技术标准体系如图 7-11。

图 7-11 区块链和分布式账本标准体系表

7.5 区块链指标体系与评测

对区块链进行性能测试越来越受到业界的广泛关注。新加坡国立大学的 TTA Dinh 等人开发的 Blockbench 是第一个分析私有区块链性能的测试工具,他们将区块链抽象为四个层,即共识层、数据层、执行层，分别从吞吐量、延迟、可扩展性和容错性四个维度对区块链系统进行了评估，比较了以太坊、Hyperledger Fabric 以及 Parity 的性能；华为公司于 2017 年 5 月推出了一款区块链基准测试工具 Calipe，它可以持续跟踪不同区块链系统的性能特征，用户可以选择负载来测试区块链的性能,并获得相应的结果,目前支持Hyperledger的多种解决方案；印度国立理工学院 Thakkar 等人对 Hyperledger Fabric v1.0 进行了一些研究，通过调整配置参数对 Fabric 进行了测试，并根据测试结果提出了一些优化方案；滑铁卢大学的 Gorenflo 等人通过改变 Hyperledger Fabric 的系统架构，将其吞

吐量从 3000 TPS 提高到了 20000 TPS；泰国国家电子和计算机技术中心的 Pongnumkul 等人比较了以太坊和 Hyperledger Fabric 的性能，但选择的工作负载种类有些单一。

目前，关于区块链性能测试方法及测试流程的国际标准尚处于空白阶段。为此，在 2021 年 4 月 19 日至 2021 年 4 月 30 日国际电信联盟第十六研究组召开的全体会议中，中国人民银行数字货币研究所和中国信息通信研究院携手合作，针对区块链平台的性能测评的痛点，提出“分布式账本技术平台性能测评方法”的标准作为现有国际标准 ITU-T F.751 系列标准的补充，对区块链的性能测试方法进行规范。上述标准作为国际上首批聚焦于区块链测试方法的标准，填补了区块链国际标准在测试方法方面的空白，进一步完善区块链国际标准体系，提升我国在区块链国际标准方面的贡献度，促进国内区块链技术和相关产业健康发展。

郑志明院士领导的中国通信学会（CIC）区块链委员会专家团队在国内外多位院士级专家的支持和指导下，提出 CIC 区块链全方位测评体系，着重区块链系统的性能效率测试和安全性测试。

7.5.1 区块链性能指标体系

2021 CIC 区块链性能指标体系包括六（5+1）大方面评测，即：数据层指标、网络层指标、共识层指标、合约层指标、扩展层指标和应用测评体系。评测的性能包括：账本同步延时，网络中各个独立部署的节点完成账本状态同步所需要的时间；数据读写吞吐量，节点每秒钟读写的数据数量；账本存储效率；网络节点延时，区块链网络中节

点状态变化产生的延时；网络传输效率，节点之间数据传输效率；网络数据丢包率；一致性吞吐量；出块时间：区块链产生新旧区块的时间间隔；交易吞吐量；交易验证效率；交易确认延时；合约执行延时；有效交易吞吐量，以及跨链交易吞吐量和跨链交易验证效率等。

7.5.2 区块链安全测评指标体系

区块链技术作为一种新兴技术，安全性威胁已是其面临的最重要的问题之一。根据腾讯发布的《2017 年数字加密货币安全报告》显示，近年来区块链系统爆发的安全漏洞超过 14000 多个。根据白帽汇安全研究院发布的《区块链产业安全分析报告》，从 2011 年至 2018 年 4 月，全球范围内因区块链安全事件造成的损失高达 28.64 亿美元，其损失额度从 2017 年开始呈现指数上升趋势，仅 2018 年前 4 个月，损失的金额就高达 19 亿美元。

造成重大影响的安全事件层出不穷，包括 2016 年 6 月 17 日，分布式自治组织 THE DAO 项目因其合约代码中存在的漏洞遭受黑客攻击，导致项目失败，最终导致以太坊硬分叉出以太经典。2016 年 8 月 2 日，香港比特币交易所 Bitfines 因为多重签名漏洞被黑客攻击，大约价值 7000 万美元的比特币被盗。2018 年 1 月 25 日，日本最大的比特币交易所 Coincheck 遭到黑客攻击，丢失了市值多达 5.3 亿美元的数字货币。发生被盗的主要原因是交易所的绝大部分资金被保存在缺乏多重签名、低安全性的热钱包中，其安全性非常脆弱。同时，2018 年 3 月 7 日，币安交易所的 API Key 被盗，黑客利用盗取的可以在 VIA/BTC 交易市场通过程序化下市价买单，配合 31 个预先充值

VIA 币的账号高价卖 VIA。通过利用盗取的币拉高 VIA 的价格的同时做空，造成交易市场的恐慌。今年 3 月份，安全研究团队检测到以太坊 RPC/API 存在鉴权不当漏洞，导致黑客自 2016 年 2 月 14 日起持续偷取以太币长达 2 年之久，直到研究报告发布之时，被监视的 3 个黑客钱包收款地址中的账户余额高达 2220 万美金。2018 年 5 月 29 日，360 公司 Vulcan 团队发现了区块链平台 EOS 的一系列高危安全漏洞，经验证，其中部分漏洞是由于代码实现不当造成的内存越界写缺陷，可以在 EOS 节点上远程执行任意代码，实现远程攻击，直接控制和接管 EOS 上运行的所有节点。

区块链的安全问题越来越受到业界的广泛关注。国家信息技术安全研究中心在区块链安全高峰论坛上表示，安全是区块链未来的生命。区块链还处在初级阶段，存在密码算法安全性、智能合约安全等诸多挑战，其安全风险不仅来自外部实体，也来自内部的区块链参与者的攻击。如何围绕物理基础设施、交易数据、应用系统、加密、风险控制等构建安全体系，是目前面临的重要问题。

本安全指标体系对于基于密码学算法的区块链天然的具有可追踪性和不可篡改性，实现区块链系统中交易数据的保密性、算法的完整性、节点代码与合约代码的执行的完整性、系统服务的可用性等方面是其主要的安全目标。

本安全指标体系方案中所阐述的区块链系统的安全目标是确保其保密性、完整性、可用性、可审计性和不可抵赖性，构建区块链安全测评指标体系旨在为区块链的安全检验检测提供测评标准和依据。

2021 CIC 区块链安全测评指标包括 5 个方面的测评，即：数据安全风险分析、网络层风险分析、共识算法风险分析、智能合约风险分析、应用层风险分析，并设计了安全测评 BSAIS 方法和安全测评综合指数计算方法，包括：数据层安全测评，即：数据存储方式指标测试、密钥管理体系指标测试、密码算法标准指标测试、信道安全指标测试、硬件安全指标测试、区块安全指标测试；网络层安全测评，即：节点安全指标测试、文件配置指标测试、P2P 网络指标测试、通信过程指标测试；共识层安全测评，即：共识算法指标测试、账本安全指标测试、分叉管理指标测试；合约层安全测评，即：智能合约完备性指标测试、合约环境指标测试；应用层安全测评，即：账户体系指标测试、集成插件安全指标测试、区块链应急响应指标测试，以及设计采用同行评议法、特尔斐法和层次分析法进行安全测评。

第三篇 区块链技术应用创新进展

第八章 区块链发展过程中的应用及其分析

8.1 ICO：总结与反思

8.1.1 ICO 的起源与现状

ICO 定义：ICO 是从加密货币及区块链行业衍生出的众筹概念，是一种区块链创业项目的融资方式，创业团队将一定比例他们所发行的数字代币出售给项目支持者，以换取法币或者其他数字代币的行为。随着 ICO 的发展，ICO 代表的字面从货币发行（Initial Coin Offering）逐渐演变成加密通证发行（Initial Crypto-Token Offering）。[10]

ICO 起源于 2013 年，在 2017 年至 2018 年到达高峰，ICO 的简单发展历史如图 8-1 。

时间	事件
2013年7月	Mastercoin（现更名为Omni）：可查的最早ICO项目，通过meta-protocol拓展比特币功能，募集5000 BTC。
2013年12月	NXT（未来币）：首个完整的PoS区块链，募集21 BTC（约等于当时6000美元），市值峰值曾到达过1亿美元。对投资者来说最成功的ICO项目之一。
2014年7月	Ethereum（以太坊）募集3万余个比特币（超过1800万美元）创下纪录，也被视作迄今为止最成功的ICO项目。
2015年3月	Factom（公正通）：双代币设计，首提存在性证明的区块链商业化以及由此导出的基金会与公司双机构设置。
2016年5月	TheDAO等值1.5亿美元破世界纪录的ICO众筹，非典型ICO（其本身不是区块链），向世界大声宣告智能合约时代到来后一个月即被黑客攻克。
2017年3月21日	日本内阁会议通过《关于虚拟货币交换业者的内阁府令》，其中规定，从事虚拟货币买卖和虚拟货币间交换业务的公司，需要在政府网登录申请，在申请时需要提供包括3年内的收支预算、公司结构等各种信息。
2017年7月25日	美国证券交易委员会（SEC）发表通告称，虚拟组织发行和销售的数字资产，将被纳入联邦证券法监管范围。
2017年7月	Autonomous NEXT报告，2017年上半年全球ICO融资近13亿美元，已经超过区块链行业的VC投资额，是2016全年ICO融资额的六倍多。
2017年8月	爱沙尼亚共和国公开了以国家名义发起ICO并推出国家虚拟货币Estcoin的计划（后来被欧盟阻止）
2017年8月	新加坡央行与加拿大证券管理局先后表达了对ICO监管的态度，前者发通知称，数字代币的提供或发行将由MAS监管，为ICO代币提供交易兑换服务的公司同样需要被管理；后者表示，根据代币销售的特殊性，某些ICO将被要求遵守加拿大的证券法。
2017年9月4日	中国央行、银监会、证监会等七部委联合发布了《关于防范代币发行融资风险》的公告，ICO不仅被定性为非法公开融资，相关的代币发行活动和平台也均被叫停。
2017年底	研究数据显示全年ICO募资总额超过40亿美元
2018年3月	Telegram是一家拥有超过2亿月活跃用户的社交应用巨头，放弃IPO选择通过ICO的方式筹集了17亿美元，成为继EOS之后第二最大融资项目。（随后根据监管要求成为首单STO）
2018年6月	EOS长达一年的ICO结束，募集资金总额42亿美元
2018年6月	Fcoin创新了"交易挖矿"模式，以另类方式实现ICO。开启了"行为挖矿"时代。
2018年8月	研究数据显示上半年ICO募资超过2017年全年，截至8月底，ICO募资超过190亿美元

图 8-1 ICO 发展历程

[10] Chod Jiri, Evgeny Lyandres, A Theory of ICOs: Diversification, Agency, and Information Asymmetry [J], SSRN Electronic Journal, 2019.12.

8.1.1.1 ICO 的性质

ICO 是一种介于 IPO 和众筹之间的融资方式。ICO 通常发生在公司开发出实际产品或服务之前，性质类似产品重筹，但通证（Token）具有更高的流动性。IPO 和股权重筹的参与者可以获得发行公司的股权或者某种所有权，未来还可以对企业决策和项目进行投票；相对而言，ICO 向公众出售的加密通证却并不默认这种所有权。ICO、IPO、股权众筹的对比如图 8-2 。

	ICO	IPO	股权众筹
融资资金	比特币、以太币或其他数字代币	法定货币	法定货币
法律地位	尚不明确，监管处于空白	已有相关监管法律法规	已有相关监管法律法规
发行主体	不一定为实体企业，可能是非企业团队	企业	企业
投资主体	范围没有限定	面向大众，但在监管上对投资者提出相关限制	面向大众，但在监管上对投资者提出相关限制
服务中介	没有相关服务中介，去中心化的网络上开展	证券经纪商	众筹平台
流通渠道	代币交易所	证券交易所等二级市场	场外交易

图 8-2 ICO、IPO、股权众筹的对比

在真正高技术的项目方眼里 ICO 只是一种为自己筹集技术研发资金的方式。在投资者眼中 ICO 是一种以小博大的投资手段。在传销团伙眼里，ICO 是漂亮的谎言。

8.1.1.2 ICO 与区块链

ICO 作为一种融资方式源起于区块链社区并服务于区块链项目。ICO 发行的加密通证（Token）主要基于以太坊、比特股等区块链基础平台实现。

区块链技术对项目融资带来了革命性的变化：

- 1、信任：区块链技术实现了一个第三方公证的机制，以保证一旦参与众筹交了钱，就一定能拿到对应的电子加密货币。这解决了 ICO 的底层信任问题，降低了 ICO 的制度门槛；
- 2、成本：区块链技术让项目通证（Token）代表的权益所属确认成本无限逼近于 0。(相对于 IPO 环节,机构需要花很多人力，物力，财力，时间去确认股份的所属权益)；
- 3、流通：区块链技术能够大幅降低通证（Token）点对点流通成本，并存在众多数字资产交易所提供集中化交易；
- 4、参与：区块链技术让通证（Token）代表的股/债权无限拆分变成可能，让投资的门槛和地域限制无限逼近于 0；

在上述技术特征下，项目融资不再需要投行、VC/PE 投资机构等非必要性的信息和信任中介，项目方可以直接面对最终投资人寻求投资。

8.1.2 ICO 的价值逻辑

8.1.2.1 社群众筹逻辑

ICO 兼具产品众筹和股权众筹的特征：

1）产品众筹特征

社群因为项目的愿景而被吸引和聚集，社群的 ICO 出资人都将成为项目的第一批试用者，提升了用户的参与度和反馈性。这样协作出来的产品更容易受到欢迎。虽然没有法律强制执行，但产品众筹具有明显的债权债务属性，项目团队的愿景被视为承诺，需要履行和实现。

2）股权众筹

社群的 ICO 出资人对项目的盈利预期感到乐观，愿意出资参与持

有项目的权益以获得未来回报，而项目团队也承诺用分红或者回购的方式为投资人提供预期回报实现途径。众筹融资方式保持了团队的独立性和控制权。团队虽然需要考虑到 ICO 投资人的权益，但他们对于一个项目有 100%的控制力。（大多数情况）他们可以去做任何自己想要做的，也许短期无法获得回报，但长期来看是有益的事情。

以太坊为代表的早期 ICO 项目产品众筹属性多一些，2017 年之后的 ICO 项目股权众筹属性多一些。

8.1.2.2 货币逻辑

货币逻辑，是指在一个区块链项目中，特别是分布式社区组织（DAO）项目中，发行社区通证（Token），并在使用该项目提供的服务时会被要求使用通证（Token）支付一定的费用。本质上通证（Token）承担了网络社区内流通货币的角色。

每一个 DAO 可视为一个封闭经济体，经济体内人口越多，价值交换活动越多，经济体越繁荣，经济体内部货币对外升值越多。

货币方式的出现，让基于区块链技术的开源软件的开发者和投资者盈利，只不过不同于传统的卖软件或许可证的方式，而是必须以让更多的人使用和价值交换为前提，驱动最初的开发者有动力不断地提升整个系统的质量，而投资者也有动力成为一个义务的销售者，努力扩大该系统的使用范围。这完全构成了一个正向循环的盈利模式。

以太坊是货币逻辑的典型代表。（如图 8-3 ）

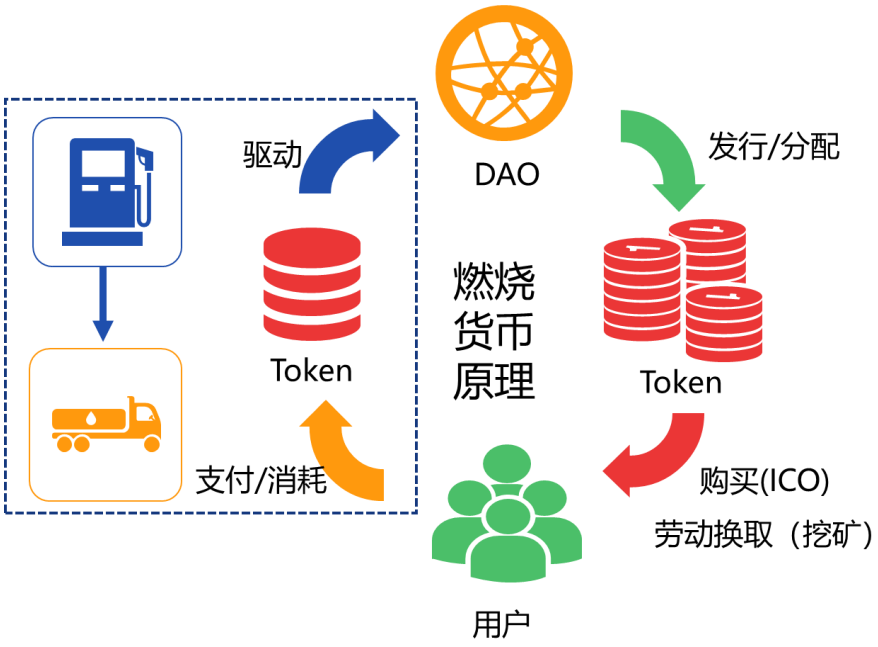

图 8-3 ICO 的货币价值逻辑

8.1.2.3 资产逻辑

随着区块链项目的推广，对区块链项目关注人增多，就会对这些通证（Token）有更多的需求。当通证供不应求时，价格随之上升。

开发团队和早期投资人有动力把项目推广吸引更多的人使用和持有 Token。越多的人使用该项目，通证需求越多，升值越多，从而使开发者和早期投资者获利。

比特币具有比较明显的资产价值逻辑。（如图 8-4）

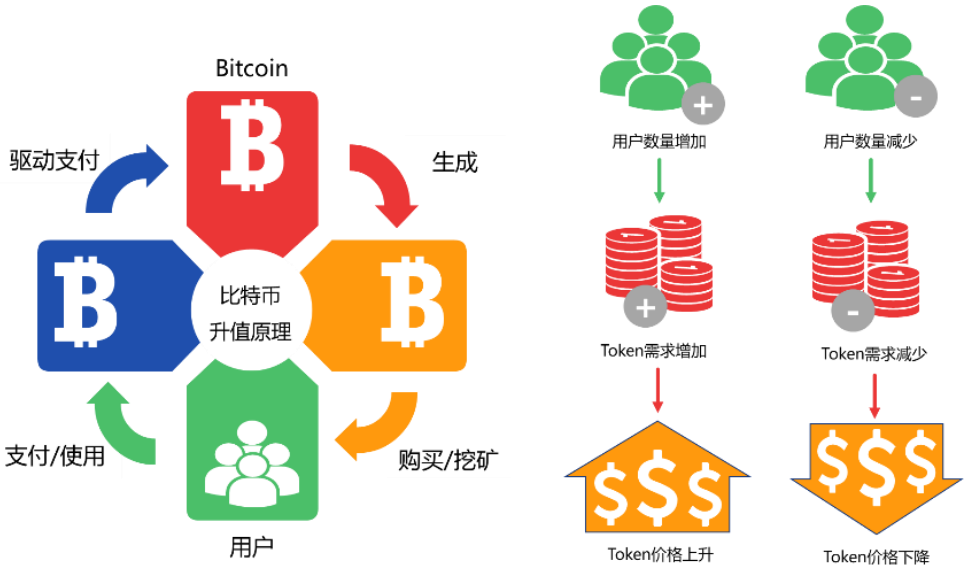

图 8-4 ICO 的资产价值逻辑

8.1.3 ICO 的法律认定与监管

8.1.3.1 比特币和以太币的法律认定

对于比特币、以太坊等主流虚拟数字货币，法律上还未有明确认定。但从已有的司法案例中，比特币、以太坊等曾被定为虚拟商品或者数字资产，因此可作为一般法律意义上的财产受到法律保护。

将比特币和以太币视为财产，意味着 ICO 过程使用其认购加密通证（Token）的发行，如果存在虚假信息披露则可以做诈骗行为认定。

因目前各国法律均不认可比特币和以太坊等虚拟数字货币作为货币的属性和地位，ICO 暂时无法做非法集资认定。

8.1.3.2 美国对于 ICO 的认定和监管

在美国法律框架下，倾向于使用证券法来监管 ICO 行为。针对加密通证的特征，一般使用哈威测试（Howey Test）来判断加密通证是否属于证券，以及 ICO 行为是否属于证券发行。一旦 ICO 被认定为证券发行，就必须去美国证监会（SEC）办理注册登记，除非符合条件

可以申请豁免。

哈威测试（Howey Test），用来判断一项交易是否符合证券法下的投资性合同的要件，判断的要素主要包括：

- 1. 投资人是否需要支付一定资本投入，这里的投入可以是货币、资本、物资等。
- 2. 是否投资于一个共同的事业？即是否所有投资人与发起人一样追求同一个事业的收益，换句话说投资人是否还有与发起人不一致的目标也能实现其投资收益。
- 3. 是否有获得收益的预期，并且该收益主要通过其他人的努力实现。

如果满足上述三个条件，就会被认定为是证券。

2017 年 7 月，在 SEC 经过调查后认为所有加密通证都是证券。所以针对 ICO 的监管变成了是否办理 SEC 登记，不办理登记的话选择哪种方式申请豁免。

豁免登记有三种选择，分别是：监管条款 D，监管条款 A+和监管条款 CF。

监管条款 D 是由 SEC 制定，并于 1982 年开始实施的关于私募证券发售的规则，又称为“避风港”条款。目前发行加密通证多数用到的是 Rule 506(c)，其规定如果投资人为合格投资人，且发行人采取合理措施来确认投资者是否符合合格投资人的条件，发行人可以申请豁免 SEC 登记要求。这里的合格投资人指在前两年每年年收入超过 20 万美金（或者与其配偶合计超过 30 万美金）。监管条款 D 的优势在于

针对合格投资人没有融资限制，低合规需求，低花费，速度比较快。缺点是发行人对投资人有审查义务，需要审查合格投资人的银行和税务文件，这增加了发行人的负担。同时投资人取得的是限制性证券有6-12 个月的限售期，会影响取得的证券的流动性。此外监管条款 D 还要求如果企业资产超过 1000 万美金，且投资人数超过 2000 人，企业就需要向 SEC 办理登记。也就是说资产规模在 1000 万美金以上的企业，投资人数的限制是 2000 人。

监管条款 A+有两种发行方式：第一类是在 12 个月内，发行融资上限为 2000 万美元，发行给关联方的数额不超过 600 万美元；第二类是在 12 个月内发行融资上限为 5000 万美元，发行给关联方的数额不超过 1500 万美元。监管条款 A+是一个合规要求高很多的方式，所以很少有通过这个方式 ICO 的实例。这个方式的优点是加密通证的流通不受限制，可以拥有最多 500 个非认证投资人。但是他有最高融资额的限制，并且发行人注册地需要在美国或者加拿大。另外很高的合规要求使得这个方式比较耗时，花费也非常高。

监管条款 CF (Crowdfunding) 即众筹条款，众筹对于小额的 ICO 融资也是一个选择，《初创期企业推动法案》（JOBS 法案）为众筹行业提供了监管框架。它的优点是由于众筹的特殊性，众筹不受投资者人数限制。但由于众筹针对小额融资的特性，所以有较多的投资金额限制：(i) 发行人在 12 个月期间内，众筹总金额不得超过 107 万美金；(ii) 如投资人的年收入或净资产低于 10.7 万美金，则投资额不得超过 2200 美金或者年收入与净资产两者取低的 5%；如投资人

的年收入及净资产均超过 10.7 万美金，则投资额不得超过年收入与净资产两者取低的 10%；(iii) 交易需通过中介平台进行，且该中介平台应在 SEC 或者 FINRA（美国金融业监管局）登记注册。

8.1.3.3 中国对于 ICO 的认定和监管

2013 年，中国人民银行就联合五部委发布《关于防范比特币风险的通知》，明确了比特币的性质，认定比特币不是真正意义的货币。

2017 年 9 月 4 日下午，央行、银监会、证监会等七部委联合发布了《关于防范代币发行融资风险》的公告。ICO 不仅被定性为非法公开融资，相关的加密通证发行活动和平台也均被叫停。ICO 被认定为未经批准的非法公开融资行为，涉嫌非法发售代币票券、非法发行证券以及非法集资、金融诈骗、传销等违法犯罪活动。根据公告，任何所谓的代币融资交易平台不得从事法定货币与代币、“虚拟货币”相互之间的兑换业务，不得买卖或作为中央对手方买卖代币或“虚拟货币”，不得为代币或“虚拟货币”提供定价、信息中介等服务。（如图 8-5 ）

对于存在违法违规问题的代币融资交易平台，金融管理部门将提请电信主管部门依法关闭其网站平台及移动 APP，提请网信部门对移动 APP 在应用商店做下架处置，并提请工商管理部门依法吊销其营业执照。

图 8-5 央行公告防范代币发行融资风险

8.1.3.4 香港对 ICO 的认定和监管

香港证监会 2018 年 3 月 19 日关于 Black Cell 的公告代表了相关金融监管机构对于 ICO 的态度。

香港证券及期货事务监察委员会（香港证监会）关注到 ICO 发行人 Black Cell Technology Limited（Black Cell）可能进行未获认可的推销活动及无牌进行受监管的活动，要求 Black Cell 停止向香港公众进行加密通证发行（ICO），将相关的募资归还予香港投资者，并取消有关的 ICO 交易。

香港证监会认为 Black Cell 的融资行为构成集体投资计划，而集体投资计划中的权益被视为《证券及期货条例》所界定的“证券”。证券发行行为须根据《证券及期货条例》事先获得认可或符合监管规定。香港证监会再次提醒投资者，在决定参与投资 ICO 前须审慎考虑。

为响应香港证监会的监管关注事项，Black Cell 亦承诺，除非符

合《证券及期货条例》下的有关规定，否则不会设计、订立或推广任何构成“集体投资计划”的产品或行为。

8.2 稳定币及其意义

8.2.1 稳定币的历史与现状

“稳定币”（Stable Coin）只是一个习惯的说法，没有任何官方和个人曾给出“稳定币”的确切说法和解释。所以从通俗地说法中提炼信息,可以把“稳定币”简单地理解成“汇率价格波动微小的货币”。[11]

实用货币的职能有三：交换媒介、价值尺度和价值存储。如果货币价格在一天内波动 20%，它就无法有效履行其价值尺度与价值存储的职能。实际上，以比特币、以太坊、EOS 为代表的各类加密货币都经历过市值的剧烈波动,这也是造成加密货币难以成为有效的交易和储值货币的原因之一。因此，便有了对稳定币的需求。

截至 2018 年底，稳定币市值约 30 亿美元，仅占数字货币市值不到 2%，但日均交易量也接近 30 亿美元，超过数字货币市场日均交易 20%;其中锚定美元的稳定币 USDT 市值超过稳定币市场总市值的 90%。

8.2.1.1 第一个稳定币 USDT

泰达（Tether）公司 2014 年推出世界第一个稳定币 USDT。USDT 的诞生为加密货币投资的风险规避提供了一条重要思路，USDT 由此竖立起了稳定币的第一杆大旗。通过 1：1 锚定美元，确保了其价值的相对稳定，从 2015 至 2019 年底，在近四年的漫长市场征途中，

[11] Eichengreen, Barry, The Stable-Coin Myth [M], Project Syndicate, 2018.

USDT 仅出现过为数不多的几次较大幅度波动，且很快就恢复稳定。

图 8-6 显示了以美元计价的 USDT 的价格趋势。图 8-7 显示了 2018 年全年以美元计价的比特币、以太坊、瑞波币、以及 USDT 的相对于美元的价格波动情况。

图 8-6 以美元计价的 USDT 的价格趋势

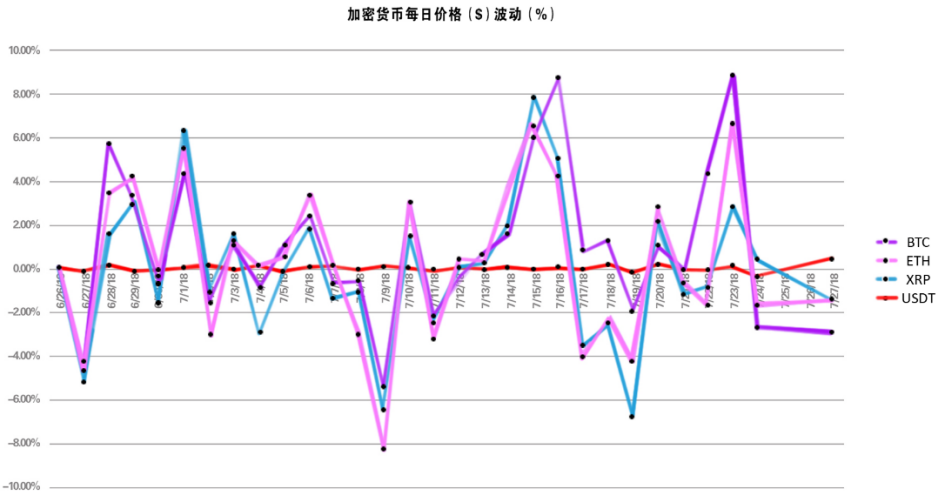

图 8-7 以美元计价的加密货币的价格波动对比

从图表中可以看出，以美元计价的 USDT 价格非常稳定，这应该也就是“稳定币”名称的来源。但实际上，USDT 的设计机制就是锚定美元，所以它的价格相对美元稳定本身是一个“循环论证”。无论如何，

USDT 开创了稳定币的先河，并在接近 2 年的时间内，没有任何竞争对手出现。

USDT 诞生之初，由于法币与加密货币的交易通道顺畅，以及用户习惯等原因，USDT 的交易量表现一直平平无奇，其日交易量在 2017 年之前甚至从来没突破 400 万美元。（如图 8-8 ）

图 8-8　2017 年 USDT 的交易量走势

2017 年 9 月 4 日，中国人民银行等七部委发布《关于防范代币发行融资风险的公告》（以下简称《九四公告》）。九四公告将比特币定性为不具法偿性和强制性的非法定货币（简称“法币”）的商品，并认为：“代币发行融资是指融资主体通过代币的违规发售、流通，向投资者筹集比特币、以太币等所谓‘虚拟货币’，本质上是一种未经批准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、金融诈骗、传销等违法犯罪活动。” 《九四公告》将境内的 ICO 定性为涉嫌非法活动，等于否定了发行虚拟货币的融资行为。

《九四公告》为 USDT 的崛起带来契机。由于法币与虚拟货币的直接交易通道被禁，基于 USDT 与 BTC、ETH 等虚拟货币的交易相继在各个虚拟货币交易所上线。伴随着 2017 年底加密货币市场的暴涨，USDT

的日交易量最高达到 63 亿美元，至 2019 年底，日均交易量仍在 20 亿美元以上，比排名第二的稳定币高出 40 倍以上。

8.2.1.2 第一个合规稳定币 GUSD/PAX

从 2014 年到 2018 年，市场上共发行了 7 种锚定美元的稳定币。（如图 8-9）

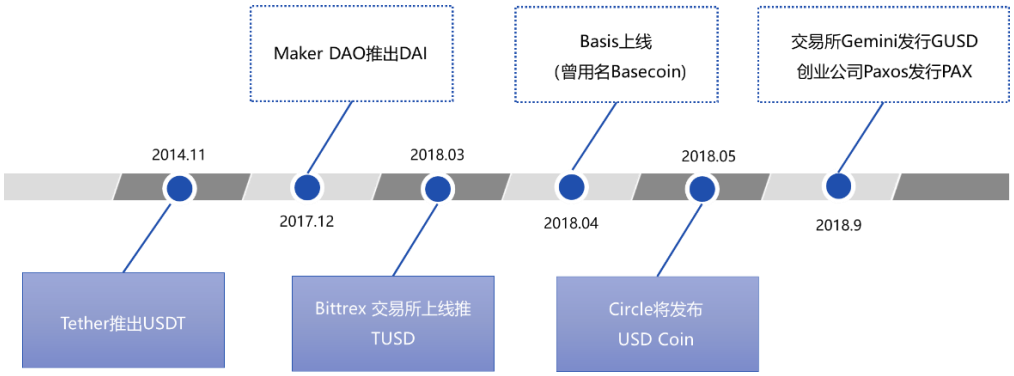

图 8-9 锚定美元的稳定币发展

2018 年 9 月 10 日，纽约金融服务部（NYDFS）同时批准了两种基于以太坊发行的稳定币，分别是 Gemini 公司发行的稳定币 Gemini Dollar（简称 GUSD），Paxos 公司发行的稳定币 Paxos Standard（简称 PAXOS），每个数字货币有 1 美元真实货币支撑，旨在提供具有法币的稳定性，以及加密货币流通便捷性和无国界性质的数字货币 。

Gemini 与 Paxos 的美元稳定设计如图 8-10 和图 8-11 。

图 8-10 GUSD 的制度设计

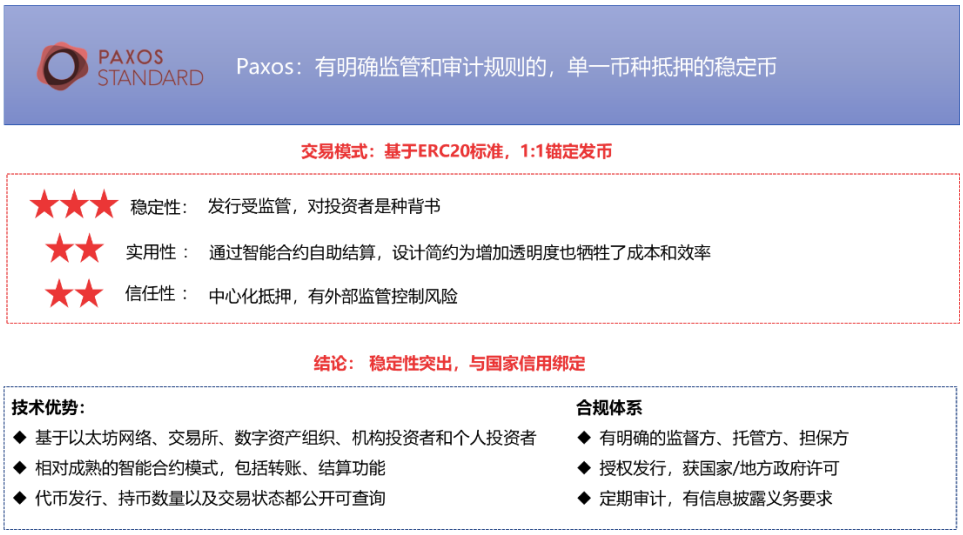

图 8-11 PAXOS 的制度设计

GUSD 和 PAXOS 都符合纽约国家金融服务部 （NYDFS） 的严格要求：

- 实施，监督和更新有效的基于风险的控制措施以及适当的银行保密制度（BSA）和反洗钱制度（AML），并接受美国财政部海外资产控制办公室（OFAC）控制条款；
- 实施，监督和更新有效的基于风险的控制措施，以防止和应对任何潜在或实际错误使用稳定币，包括但不限于其在非法活动，

市场操纵或其他类似不当行为中的使用；

- 警告消费者：“如果稳定币已经或正在被用于非法活动，任何稳定币和/或兑现任何稳定币时可获得的法定货币可能会被没收”；
- 警告消费者：“如果存在法律秩序或其他法律程序，任何稳定币可能会被执法机构没收或扣押”；
- 警告消费者：“在交易使用已被执法机构冻结，没收或扣押，和/或受其使用限制的稳定币时可获得的任何稳定币或法定货币可能完全永久无法收回，无法使用，并可能在适当的情况下被销毁“；
- 由 NYDFS 备案的信托公司发行；
- 在联邦存款保险协会（FDIC）保险的美国银行账户中以 1：1 完全抵押美元，这意味着流通中的此类代币数量将始终与预留的美元数量完全匹配，并且每月审计（外部）美元余额；
- 建立在以太坊区块链(设计为根据 ERC-20 标准编写的以太坊令牌）上，这意味着它们可以存储在任何以太坊钱包中；
- 主要适用于对冲其他加密数字货币的波动性，在银行营业时间之外结算交易，或用于降低跨境交易费用；
- 智能合约开源，让公众查看智能合约代码。

GUSD 和 PAXOS 的出现，意味着美元开始进行数字化尝试，在区块链数字法币领域布局。数字化美元有利于美元借助以太坊的全球公链网络穿透不同国家的外汇管制，增强美元的全球霸权地位。

8.2.2 稳定币的种类和运行机制

8.2.2.1 稳定币的种类

目前稳定币的实现模式根据抵押物、中介方、合规性、稳定机制、盈利方式的不同分类有三种:（如图 8-12 ）

- 法定资产抵押模式，基于中心信任和集中发行。目前市场上存在的各种锚定法币的稳定币，以及委内瑞拉的石油币是此类模式的典型案例;
- 数字资产抵押模式,以去中心化的方式通过链上抵押资产发行。典型案例如 MakerDAO 的 Dai;
- 算法央行调节模式，与世界各地的央行一样，依托相同的经济学原理，利用类似于“公开市场操作”以及“准备金政策”之类的工具来谋求货币价格的稳定。典型如 Basecoin，它以“货币数量论”为理论基础,通过借助 “Base 债券”与“Base 股份”来实现对稳定币供给的调节来使 Basecoin 与所锚定的目标价格相吻合。

	代表项目及发行方	抵押资产	监管机构	合规监管	稳定机制	盈利手段
法定资产抵押（中心化发行）	Tether (USDT)	美元	会计师审计,目前已停止	无	无	利差+兑换手续费
	比特股 (Bitcny)	人民币	无	无	无	利差+兑换手续费
	TRUST (TUSD)	美元	第三方存管并审计	KYC/AML	无	利差+兑换手续费
	Gemini (GUSD)	美元	监管部门	有	存款保险	利差+交易手续费
	Paxos (PAX)	美元	监管部门	有	存款保险	利差+交易手续费
	DigixDAO (DGD)	黄金	第三方存管审计	无	无	交易/兑换手续费
	委内瑞拉石油币	石油	委内瑞拉政府	无	每个币一桶油	
数字资产链上抵押	Maker (DAI)	以太坊	智能合约	无	简单算法	交易/兑换手续费
无抵押算法发行	Basecoin (Basis)	无	智能合约	无	复杂算法	交易/兑换手续费

图 8-12 稳定币的分类与案例

8.2.2.2 稳定币的运行机制分析

1）法定资产抵押的稳定币

这是最简单的稳定币设计方案。它是中心化的，必须信任托管人，托管人也必须值得信赖。还需要审计师定期对托管人进行审查。

根据法定资产的不同，可以分为法币抵押和实物抵押：

- 法币抵押：在合规的方式中，有存款保险，接受监管，更像是法币的数字化表示；
- 实物抵押：DGX 数字黄金，通过第三方托管，没有保险，兑付风险较高。

在法币抵押中，稳定币的设计机制是发行的数字货币与某种法定货币挂钩。任何挂钩都面临以下四重问题：

- 挂钩能承受多大的波动性？（即下行抛压）
- 维持挂钩的费用是多少？

- 挂钩可自行恢复的市场行为区间及难度有多大？
- 交易者可观察真实市场状况的透明度如何？

上述中最后两点很重要，因为货币挂钩与谢林点（Schelling Points）有关。如果市场参与者无法确定挂钩何时会疲软，就很容易引起虚假新闻散播或造成市场恐慌，最终引发进一步的抛售——从根本上说，就是一个死亡螺旋。透明的挂钩对于操控和舆论波动反应会更加稳健。

现实情况是，任何挂钩都可以维持，但只有在一定的市场行为区间内才能实现。对于不同的挂钩，其市场行为区间可能要比其它的更广。不过可以确定的是，至少在某些市场条件下，挂钩机制还是可以维持下去的。而每个挂钩机制所面临的问题是：它能支持多大的市场行为区间？

理想的稳定币应能承受大量的市场波动，无需过高的成本来维持，且易于分析稳定参数，并对交易者和套利者透明。这些特点可最大限度地提高其实际稳定性。

实物抵押要复杂很多。超额抵押（over-collateralization）是一种可行且在金融市场广泛运用的方式。超额抵押创造流动性并不是一件新鲜事，最早起源于中国古代的当铺，当铺使得流动性的需求者与提供者无需进行价格发现过程，快速的获得流动性。比如有人有意愿出售收藏的名画获得流动性，但是名画的准确估值是一件成本很高的事情，与其讨价还价，当铺不如直接给与名画持有者一笔明显低于其价值的贷款，然后双方协定在规定的时间清偿贷款和利息，名画物归

原主。这种古老但是十分有效的手段一直延续到现代金融的回购市场。

超额抵押品在常规时期有助于维持稳定币评价和信心；但在市场信心崩溃时，市场连续下跌，稳定币持有者卖出挤兑，抵押者则会趁机打压市场，低价回购稳定币套利。因此抵押品管理策略，包括合格抵押品的范围、价格、折扣率等对于实物资产抵押稳定币运行至关重要。

法定资产抵押稳定币的特性总结：

- 优点：1. 百分百价格稳定；2. 最简单；3. 由于在区块链上无抵押品，所以不易受到黑客攻击；
- 缺点：1. 中心化，需要一个值得信任的托管人来储存法定资产（否则容易被盗）；2. 成本高、清算慢；3. 被高度监管；4. 需要定期审查，以确保透明度。

2）加密资产抵押的稳定币

如果放弃法定资产，用另一种加密货币的储备金来抵押稳定币。这样一来，一切都是在区块链上进行的，并不涉及法定资产。

但加密货币是不稳定的，这就意味着抵押品的价值会波动。因此加密资产抵押稳定币与实物资产抵押稳定币一样，都需要超额资产抵押确保稳定币有足够的抵押品，以应对抵押品的价格波动。

基于这种模式并且目前来看最成功的，是 MakerDAO 项目发行的稳定币 Dai。 Dai 创新之处在于其抵押物为以太坊等链上资产，基于智能合约可以低成本地提供流动性。链上资产抵押的发行模式激励了人们自发抵押配资、丰富了流动性的来源，并无需中心化网关和托管，

消除了人们对中心机构的质疑。

假设用户存入 200 美元的以太币作为抵押，然后发行 100 个 1 美元的稳定币。那么稳定币现在拥有 2 倍的抵押物。这就是说当以太币的价格下降 25%时，稳定币仍有 150 美元以太币作为抵押品。每个稳定币的价格仍然可以是 1 美元。一旦发生清算，向稳定币的持有者提供 100 美元以太币，剩余的 50 美元以太币还给原储户。

但人们为何会愿意用 200 美元的以太币来创造一些稳定币呢？这里有提供两种激励措施：首先，可以给发行者支付利息，有些方案中也有这种做法。或者，发行人可以选择创造额外的稳定币作为一种杠杆。具体操作原理如下：如果储户储备了 200 美元以太币，那么他们就可以创造 100 美元的稳定币。如果他们用 100 美元稳定币再购买 100 美元以太币，就有了 300 美元以太币的杠杆头寸，实际由 200 美元的抵押品作为价值支撑。

在上述过程中存在的一个问题是如何实时获得以太坊等抵押物的价格以调整稳定币的抵押率数据，因为是链上加密资产抵押，其价格获取比实物资产价格要方便的多。对实物资产抵押，这是一个不可解决的问题。

加密资产抵押稳定币是一个不错的想法，但有几个缺点。加密资产抵押的稳定币比法定资产抵押的稳定币更易受到价格不稳定的影响，极端情况下会导致自动清算。如果用以太币抵押稳定币，而以太币价格暴跌，那么稳定币会自动清算赎回以太币。防止这种情况发生的唯一方法是尽量多的抵押，这使加密资产抵押的稳定币的资本更加密集。

加密资产抵押稳定币的特性总结：

- 优点：1. 更加去中心化；2. 可以快速、低价清算为基础的加密资产抵押品（只是一种区块链交易而已）；3. 非常透明——便于每个人查看稳定币的抵押率；4. 可以用来创建杠杆；
- 缺点：1. 在价格暴跌时可自动清算为基础抵押品；2. 相比法定资产抵押币，价格不够稳定；3. 受特定加密货币的影响；4. 资本使用效率低。

首个使用该方案的稳定币是由 Dan Larimer 在 2013 年创造的 BitUSD（用 BitShares 作为抵押品）。目前，MakerDAO 的 Dai 就被广泛认为是最有前景的加密资产抵押的稳定币（以太币作为抵押品）。

3）无抵押的稳定币

根据上世纪 70 年代 F.A.哈耶克的观点：私人发行、无抵押、价格稳定的货币可能会对法定货币的主导地位构成极大的挑战。但是如何确保其保持稳定呢？

铸币税股权（Seignorage Shares）是由 Robert Sams 在 2014 年提出的一种方案。其基本逻辑很简单：将智能合约模拟为中央银行，智能合约的货币政策将只有一项任务：发行交易价格为 1 美元的货币。通过控制货币发行量来调整市场供需，进而稳定发行货币的价格。

假设货币的交易价格为 2 美元，这意味着价格过高，或者说，发行量过低。为了解决这一问题，智能合约可以铸造新币，然后在市场上拍卖以增加供应量，直到其价格回到 1 美元，这将为智能合约带来一些额外的利润。从历史来看，当政府铸造新币为其运营提供资金时，

所得的利润被称为 seignorage（铸币税）。

假设其交易价格为 0.5 美元。智能合约买进市场上的货币来降低其循环供应量。但如果储存的铸币税不够全部买进货币呢？智能合约将发行股份，让股东享有未来的铸币税。

这是铸币税股权（Seignorage Shares）的核心理念。铸币税股权方法类似现实世界的平准基金运作方式。它可以暂时缓解下行压力，但如果抛售压力持续的时间过长，交易者将不再相信持有铸币税股权最终会获得回报。这将进一步压低价格，并引发死亡螺旋。

无抵押稳定币的特性总结：

- 优点：1. 无需抵押品；2. 最去中心化、最独立（不受限于任何其他加密货币或法定货币）；
- 缺点：1. 依赖持续增长；2. 大部分易受加密资产下跌或崩盘的影响，并无法被清算；3. 很难分析安全界限或健康状况；4. 复杂性最高。

8.2.3 搅动世界的天秤币（Libra）

2019 年 6 月 18 日，由全球社交网络巨头脸书（Facebook）主导的数字货币天秤币（Libra）测试网上线并发布白皮书[12]。

Libra 的使命是建立一套简单的、无国界的货币和为数十亿人服务的金融基础设施。加入 Facebook Libra 计划的基本都是支付或互联网领域的头部玩家，包括信用卡清算巨头 MasterCard 和 VISA、线上支付系统 Paypal、线上旅游预订公司 BookingHoldings、电商平台

[12] The Libra Association, Libra Whitepaper, https://libra.org, 2019.

Ebay 和 Mercado、线上打车平台 Left 和 Uber、流媒体音乐平台 Spotify、线上奢侈品平台 Farfetch 以及电信运营商 Vodaf one 等。

Libra 体系有三个核心。据白皮书描述,Libra 是以区块链为基础、有真实的资产担保、有独立的协会治理的全球货币,货币单位为 Libra。Libra 将由真实资产储备作为担保，每 Libra 数字货币都会有对应价值的一篮子货币和资产做信任背书，受 Libra 协会的创始成员监督，每位创始成员负责运行一个验证者节点。

Libra 的出现引发了全球的关注与讨论，在定位上它是全球性的数字货币；在技术上则是结合了脸书技术与区块链技术；从协会创始成员结构来看,则是强化了这种数字货币的支付功能与交换媒介的作用；从它的储备基础来看，它则是 IMF 特别提款权（SDR）的拓展版。

Libra 白皮书表明，Libra 的发展是一个过程，起点是支付，短期内可能颠覆全球支付体系；中点是重塑国际货币体系，中期内可能颠覆全球货币体系和全球货币政策体系；终点是再造全球金融生态，长期内最终颠覆和重塑全球金融市场生态和全球金融稳定体系。

8.2.3.1 Libra 对金融体系的潜在影响

1）颠覆传统的电子支付

Libra 是以区块链联盟链为基础的点对点和去中心化的新一代支付系统,而不是目前 SWIFT 和支付宝等所采用的银行账簿式的电子支付。区块链的架构使其天然具有直接跨境支付的功能，速度快、成本低、效率高，从而解决了传统跨境支付账本复杂、认证时间长、商业机构手续费高的痛点。因此，Libra 将首先挑战和颠覆现有的支付系

统，直接和 SWIFT、VISA、PayPal、IBM World wide 等跨境支付系统竞争。而 Libra 一旦从跨境进入当地市场，也会以其效率和低成本的优势，颠覆像中国的网银、支付宝和微信支付等以本地市场为主的支付系统，或者阻止这些以本地支付市场为主的科技支付企业进入全球跨境支付市场。

2）开创全新自金融生态

Libra 开创了一个线上线下结合的、用户自主性的、点对点支付的自金融模式。

Libra 从个人私钥本地生成，再到基于公钥生成钱包，最后基于钱包地址生成账户，整个过程都不需要中介机构，直接代替了原有商业银行的账户系统。

Libra 天然具有银行加资本市场的金融属性，可以承担直接融资和间接融资的金融功能。Libra 本身也是一种证券，是由传统资产抵押产生的凭证。一旦 Libra 开始使用，就会自然通过交叉产品销售进入细分市场。只要交易采用 Libra 定价，Libra 就会自动进入贸易融资、消费信贷、存款吸收、支付发起、资产管理等金融领域。另外，它还可以嫁接的存贷款、证券发行、数字资产发行、去中心化资产交易、激活第三类边缘资产交易等金融业务，形成一个线上线下，银行、股市、债市、金融衍生产品集合的新金融生态。Libra 也由此几乎集央行和商业银行于一身，同时具有直接发行货币和信用扩张的能力。

Libra 的金融属性广泛，其未来的金融服务可能涉及支付、跨境支付，将纳入央行第三方支付监管范围；Libra 作为资产，将受到证券

监管机构基于众筹、证券发行、消费者保护等一系列的监管；而 Libra 可能涉及的贷款、资产管理等，也将涉及这些领域的金融监管。

Libra 未来可能的发展和可能的对各国法定货币和国际金融系统的冲击，包括对中国的支付系统、资本管制以及金融系统、人民币国际化和金融经济安全的挑战。鉴于目前 Libra 协会会员大都是美国企业，美国监管层对 Libra 保持较高程度的影响，预计美元资产占比也会高于 60%。从储备资产维度，Libra 和美元互相支持。在目前中美经贸摩擦大背景下， Libra 实际上是加强了美元的霸权地位。

3）推动形成新的国际秩序

以 Libra 为代表的数字货币和支付系统合一的构想很可能推动第三次国际货币体系的变革。这将是线上和线下结合、自下而上的自由跨境流动的货币。

如果 Libra 能大规模应用，全球货币竞争格局将被分为线上和线下两个部分并相互影响。Libra 一篮子货币的构成也将影响各国货币的竞争力，被大比例纳入篮子的货币，比如美元，其全球地位将被加强，而未被纳入该篮子的货币将会进一步被边缘化，对弱势货币形成贬值压力，一些小国的主权货币甚至存在消失的可能。

Libra 作为存款凭证进行支付的工具，就自然会有货币创造和货币乘数，Libra 协会就可能成为数字世界的中央银行，这将颠覆现有的全球货币金融体系。Libra 也可能有对金融风险蔓延起推波助澜作用。如果一篮子货币中的某一种货币出现危机，持有该货币的民众就会倾向于将本币兑换成 Libra，从而引发该货币进一步的贬值，加剧

风险蔓延。

Libra 也可能会加大货币波动。被纳入 Libra 篮子的货币，会有通过发行货币兑换 Libra 的冲动，这可能导致竞争性印钞局面出现。而由于自下而上和同时同步的技术特性，以及 Libra 跨境流动时的不规则性，也会对现行跨境资本流动和管理形成挑战和冲击。

Libra 在现有主权货币竞争上增加了一个电子层面上的竞争，由于电子竞争的技术和规模垄断优势，“赢者通吃”现象普遍。篮子货币通过 Libra 载体，增加它的法定货币的竞争优势，造成新的竞争不公。由此，Libra 的运营会侵蚀相当一批主权货币，实际上是要求一些主权国家的主权让渡。

8.2.3.2 Libra 的进展情况

Libra 对传统金融体系的潜在影响引发了全世界的强烈关注。

2019 年 7 月 16 日，美国参议院银行、住房和城市事务委员会就 Facebook 的新加密货币 Libra 举办听证会。

2019 年 7 月 17 日，美国众议院金融服务委员会举行有关 Facebook 虚拟货币的听证会。

Facebook Libra 项目团队负责人 David A. Marcus（前 PayPal 总裁）出席听证会，并就数据隐私、监管、反洗钱、纳税等美国国会议员关心的问题做了陈述。在听证会上，Marcus 强调在监管问题完全解决前不会急于发行 Libra 货币，但同时也指出虚拟货币是全球重要的发展趋势，由 Facebook 牵头推进更加符合美国国家利益。

议员们多次打断前来作证的 Libra 项目负责人马库斯（David

Marcus）的发言，来自两党的成员们也全程对 Libra 表现出非常一致的质疑和反对意见。多位议员表示，他们担心 Facebook 通过 Libra 进入金融界为全球金融带来风险，同时也担心 Facebook 如何保护用户的支付数据信息。

听证会后，美国众议院金融服务委员会表示，将会讨论起草一项法案《Keep Big Tech Out of Finance Act（让大型科技公司远离金融领域)》，它将阻止类似 Facebook 的科技巨头成为金融机构，阻止它们创建数字货币。

欧洲方面也同样对 Libra 反映强烈。

2019 年 9 月 13 日，法新社报道，法国经济和财政部长 Bruno Le Maire 表示，他们将阻止社交媒体巨头 Facebook 的加密货币 Libra 在欧洲发展。德国财政部长 Olaf Scholz 表示，政府必须否决 Facebook 的 Libra 项目。

2019 年 10 月 13 日，七国集团（美英法德日意加）发表的一份报告，列举了加密货币的 9 大问题，包括确保不能用来洗钱、不能用来资助恐怖分子、不能对全球金融体系构成风险等。而且即便解决了这 9 大问题，Libra 项目也不会得到监管机构的批准。各国官方的态度非常明确，尽一切可能封杀 Libra。

Libra 的发起机构方面，在政治和舆论的压力下，几个全球性金融机构退出了发起机构会员。

美国财政部致函 Visa（维萨）、Mastercard（万事达）、PayPal、Stripe 等机构，要求他们全面概述其合规计划以及 Libra 项目将如

何适应这些计划。这使得 Libra 项目的合作伙伴面临的压力骤增。

2019 年 10 月 5 日，国际支付巨头 PayPal 宣布退出 Facebook 牵头的 Libra 项目。10 月 11 日，信用卡巨头 Visa（维萨）和 Mastercard（万事达）、数字支付初创公司 Stripe Inc.、电商巨头 eBay Inc.、以及拉丁美洲支付应用公司 Mercado Pago 宣布将退出 Libra 项目。这意味着 Libra 项目在两周内失去了 5 家重要机构的支持。失去全球最大的四家支付公司，意味着 Facebook 损失了此前为 Libra 集结的大部分力量，而 Facebook 原本希望通过 Libra 这种数字货币使自己成为电子商务和全球汇款的参与者。

2019 年 10 月 14 日，作为 Libra 的构建和管理机构，天秤币协会（The Libra Association）正式成立。这家位于瑞士的非营利组织由包括 Facebook、Uber、Spotify 和 Coinbase 在内的 21 家公司组成。该协会是一个新的管理机构，它将负责对 Libra 的运行进行监督。

2019 年 10 月 24 日，Facebook 创始人扎克伯格作为唯一证人出席关于 Libra 的又一次听证会。扎克伯格表示：Libra 不想与任何主权货币竞争，也不想进入货币政策领域，仅是一个数字支付系统。中国有一部分金融基础设施比美国要先进的多，美国必须要在现有基础上建立更现代化的支付基础设施。扎克伯格同时强调：不会在没获得美国政府许可的情况下，强行推出 Libra 数字货币。

2019 年 11 月 12 日，Facebook 宣布推出移动支付应用 Facebook Pay。Facebook Pay 与微信支付和支付宝非常相似。Facebook Pay 是基于法币（美元）交易，需要绑定银行卡使用，之

后可以在 Facebook 上购物、捐款以及购买游戏或者票务类产品；可以在 Facebook 聊天应用中进行转账。Facebook Pay 与 Libra 相比，产品中没有过多的理想化色彩地宣传和前沿技术的运用，是一个朴实而实用的支付工具。

2019 年 12 月 19 日，美国《财富》杂志发表文章称，Facebook 内部的员工已经开始使用天秤币，而天秤币协会目前仍由 Facebook 资助，天秤币协会的创始成员尚未缴纳最初承诺的 1000 万美元的会员费。

2020 年 12 月 1 日，Facebook 官网更新的信息显示，其提出的超主权数字货币 Libra 已更名为 Diem。Diem 已经确认是一种稳定币，Diem 代币将完全由美元支持，并与美元锚定。

8.2.4 稳定币的作用与风险

“稳定币”的发展将能大幅减少区块链资产和以法币为基础的金融资产间的隔阂，为区块链资产打开众多新的应用场景。稳定币在区块链领域的重要性越来越突出。

8.2.4.1 稳定币的作用

避险资产（Store of Value）：充当避险资产是稳定币诞生的最初愿景，规避市场下跌风险。在市场行情大幅下行情况下，把其他数字货币换为 USDT 等稳定币可以规避市场下跌风险。

除了虚拟世界中作为避险资产外，稳定币也可以作为现实世界的避险资产。在面临经济和货币危机的国家，如伊朗、土耳其、委内瑞拉、阿根廷和津巴布韦，比特币 BTC 的交易活动都曾经大幅度增加。

当具有强信任的稳定币出现时，有理由相信上述情形下，比特币的交易会转化为稳定币的交易。

交易媒介（Medium of Exchange）：在强监管的区域和环境中，稳定币可以作为比特币等虚拟数字货币的交易与结算媒介。

价值尺度（Measure of value）：加密数字货币波动性很大，无法作为尺度实现对其他资产的定价职能。锚定法币的稳定币，则可以实现对现实世界物理资产以及虚拟资产的定价。

短期借贷需求（Pegged Lending）：稳定币可以解决短期流动性问题，用户可以把自己的虚拟数字货币换成稳定币并且随时兑换成所需的法币。

稳定币要实现两个“跳跃”，才能达到实用性的目标，成为一个流行的稳定币。如图 8-13。

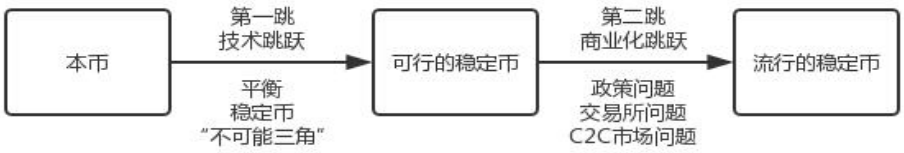

图 8-13 稳定币走向实用的两个跳跃

第一个跳跃是稳定币在技术层面实现与法币或者现实中锚定的资产相锚定。第二个跳跃是稳定币获得人们的广泛使用。

第一个跳跃的技术路线在前面稳定运行机制分析中已经描述，技术上主要围绕“可信任”、“易用性”、“稳定性”等特质进行平衡。

第二个跳跃是商业跳跃，稳定币被更多的人使用才有价值。目前

稳定币主要面临政府政策、虚拟货币交易的接受程度、个人交易市场繁荣程度等商业因素影响。

首先是政策因素。稳定币本质上也是发行一种区块链数字货币，同样面临着各个国家法律的监管。稳定币商用某种程度上侵犯了所在区域的货币主权，需要得到相应国家和地区的授权或认可才是合法的。

其次是虚拟货币交易所的接受程度。交易所的接受程度代表一个稳定币在虚拟数字世界的认知和接受程度，做一个优秀的稳定币一定要尽可能地在更多交易所使用。

最后是个人交易市场的繁荣程度。区块链数字货币与电子货币的不同，区块链数字货币的货币即支付，交易即结算。稳定币一定要得到承兑商和商业场景的认可才能方便的被大家购买和使用。

8.2.4.2 稳定币的风险

稳定币本身存在很多风险，以目前最大的稳定币 USDT 为例，其发行方 Tether 已经很长时间没有公布过账户资产的审计报告，公众无从得知 Tether 发行的 20 多亿枚 USDT 是否有相应的美元储备，也几乎没有用户从 Tether 官网上将手中的 USDT 成功兑换过美元。时至今日，USDT 超发几乎已经成为公认的「事实」。

从 USDT 的案例看稳定币存在的风险如下：

法律风险：稳定币面临发行方欺诈、虚拟数字货币交易所非法经营、卷款跑路、洗钱等数字货币领域常见风险；

技术风险：黑客攻击智能合约，导致货币超发的风险；

集中风险：稳定币市场很可能出现赢者通吃局面，目前 USDT 市场

占有率过高，USDT 的自身信用风险可能引发市场整体动荡；

金融稳定风险：在法定数字货币缺位的情况下，私人发行数字货币相当于获得铸币权，将冲击目前世界上以央行为主构建的全球信用体系；

国际货币体系和主权风险：美元稳定币的发展将增强美元国际主导地位，形成对经济不稳定和通胀国家的实质性货币替代；

资本管制风险：基于区块链公链的稳定币穿透了主权国家的资本项目管制，模糊了“离岸”和“在岸”货币市场的边界，对居民、非居民为主的跨境资本管理框架带来冲击，提高打击非法跨境资本流动的难度。

8.3 通证证券化与证券通证化 – STO

8.3.1 证券通证的法律含义与认定

证券通证（ST - Security Token）是各国政府将以 ICO 为代表的融资行为纳入监管后的结果或者“应激反应”，是各国政府（特别是美国政府）在不出台新的监管政策的情况下，将现有加密通证发行市场纳入传统金融监管的尝试。

8.3.1.1 美国关于证券的法律含义

为了实现对日益泛滥的各种各样证券的发行进行有效监管，在多种政治原因的影响下，1911 年，美国堪萨斯州通过了第一个蓝天法案（Blue Sky Law），将所有股票、债券或证券的销售（除某些政府相关债券和票据外），都纳入了其规制范围，以此对投资银行及各种证券发行的监管提供合法性依据，从此证券发行需要接受实质审查

（Merit Review）以减少投机证券的泛滥。

美国 1933 年《证券法》在制定的过程中，深受各州蓝天法的影响，《证券法》第 77b 条对证券进行了定义，力图将所有证券都纳入其中："包括任何票据，股票，库藏股，债券，信用债券，债务凭证，息票或任何利润分享协议，担保信托证券，公司成立前的认股证书，可转换股份，投资合同，表决权信托证书，任何有形或无形财产权益证书，通常称之为的'证券'的任何权益或权益工具，任何与上述项目相关权益证书、认权证书、暂时或临时的证书、收据、权证（Warrant）、认购权、购买枚"。

如此详细列举且比较周详的定义条款，直接将所有的非豁免的证券全部纳入其中，目的即在于实现对证券市场的充分、全面监管。此后，在 1934 年、1982 年、2000 年和 2010 年，该条款先后进行的四次修订不断结合当时的经济发展情况与证券市场监管要求，对证券的外延进行扩充。

1982 年的修订将"与证券、存托凭证、一组证券或证券指数相关的任何卖出权、买入权、跨式套利权（Straddle）、期权或优先权（包括其中或以其价值为基础的任何权益），与全国性证券交易所中外币相关的任何卖出权、买入权、跨式套利权、期权或优先权"纳入了证券的定义；

2000 年的修订将"证券期权"纳入证券定义；

2008 年金融危机之后，基于对繁杂的资产证券化相关证券产品的监管需求，美国又对"互换"产品（Swap）的监管权进行了划分，将

“基于证券的互换”（Security-based Swap）纳入了证券定义之中。[13]

美国证监会(SEC)关于证券监管的核心理念:合格投资人管理 KYC、反贪污洗钱制度 AML、信息披露要求、以及投资人锁定期限。

8.3.1.2 美国关于证券的认定标准

1933 年以后，美国的州和联邦法院也在解释证券的定义上下足了功夫，特别是通过对 SEC v. W. J. Howey Co. 案、Landreth Timber Co. v. Landreth 案、Reves v. Ernst& Young 案等案件的解释，逐渐明晰了“投资合同”、“股票”和“票据”的检验标准，为法院参与证券市场治理提供了相对明确的边界。

在适用该标准时，法院采用“实质重于形式”的原则，即法院看中的投资行为的实质，而不论表面称谓上是否叫做“股票”、“证券”、“债券”。

实务操作中，测试由具备资质的律所进行，并出具法律意见书，然而测试结论的弹性却非常大。

1）股权类证券

股权类证券是最为典型的证券产品，其一般包括股票、认股权证、新股认购证书、证券类期货产品等。在美国 1933 年《证券法》的证券定义中，其还包括了库藏股，息票或任何利润分享协议，公司成立前的认股证书，可转换股份，表决权信托证书，存托凭证，石油、天然气或其它矿产权的小额未分割权益，与证券、存托凭证、一组证券

[13] 吕成龙，我国<证券法>需要什么样的证券定义[J]，政治与法律，2017.02.

或证券指数相关的任何卖出权、买入权、跨式套利权、期权或优先权，通常称之为的“证券”的任何权益或权益工具，任何与上述项目相关权益证书、认权证书、暂时或临时的证书、收据、权证等。此外，美国有法院裁判甚至将有限责任公司（Limited Liability Company）的份额亦作为股权类安排下的证券。

在 1985 年 Landreth 案的审判中，美国最高院司法解释把股权类证券的特征认定为：

- 1、根据利益的分配获得股息的权利；
- 2、可流通性；
- 3、能够被抵押或者质押；
- 4、根据持股比例拥有相应的投票权；
- 5、增值功能；

作为一种新兴的融资方式，股权众筹产品是否属于美国 1933 年《证券法》第 77b 条定义的范畴、发行监管方式、是否应该豁免等问题也曾不明朗，并困扰行业多年。直到 2012 年，美国《创业企业促进法案》（Jumpstart Our Business Startups - JOBS Act）通过后才有初步定论——该法对募集金额、发售方式、门户网站身份定位、披露义务进行了规定。

2）投资合同类证券

在美国，投资合同是否属于证券是各州及联邦法院长期争论的问题。作为一种类似兜底条款的存在，以期为投资者提供证券法的保护，投资合同出现在美国 1933 年《证券法》的证券定义中。虽然从蓝天

法案到现在的联邦证券法、各级判例法，一直难以就该问题得出明确的结论，但在漫长的司法实践中，美国的法院逐渐创制了一些检验标准来判断某种投资合同是否属于证券。

直到 1946 年，Howey 测试成为了检验性质模糊、罕见的投资计划是否属于证券的重要标准，联邦及各州法院也自此有了一个相对统一的判断标准。Howey 测试的内容如下：

- 1、是金钱（money）的投资；
- 2、该投资期待利益（profits）的产生；
- 3、该投资是针对特定事业（common enterprise）的；
- 4、利益的产生源自发行人或第三人的努力。

该定义中的“金钱”的概念不断扩大，可延伸为资产的投资。特定事业的定义可以是对项目的投资。如果投资者自身的行为将决定盈利是否产生，则该等投资将不构成证券。实际上，美国司法上的“投资合同”具有一定兜底的功能，目的是尽量将各种各样的证券纳入监管范围。

3）债权类证券

一般来说，债务类安排的证券产品包括票据、债券、信用债券、债务凭证等在这些产品中，债券不难理解，票据（Note）则争议颇多。1990 年 Reves 案，法院提出了“家族类似性”（Family Resemblance Test）的判断标准，以甄别某种票据是否是证券。

票据的判定首先需要与七种特定的非证券的票据进行比较，这七种票据包括消费融资票据、家庭房屋作为抵押担保的票据、以小型营

业或某些资产作为质押的短期票据、银行因融资而给付的票据、应收账款让与权作为担保的短期票据、日常经营业务范围内所产生的账上债务的票据和公司因经营需要而向银行融资所得的票据。如果某种票据与这七种票据没有很强的相似性，则极有可能被认定为证券，否则，就可能被作为商业消费票据，而不受证券法律的监管。

法院需要审查票据的动机、分配计划、预期及其它规制方式的可能性，以此来最终判定有关票据是否为美国 1933 年《证券法》的证券。

4）资产支持证券 ABS

资产支持证券没有被明确列举在美国 1933 年《证券法》第 77b 条中，但 2008 年金融危机却凸显了资产证券化监管的必要性。根据美国《多德弗兰克法案》第 943 条，SEC 有责任对资产支持证券市场进行一定的监管，鉴于资产支持证券的具体操作情况，Howey 测试与 Reves 测试都需要相应地加以适用。

上述测试只是美国证监会（SEC）和法院使用的工具，最终是否认定为证券，美国证监会有最后的解释权。

8.3.2 证券化的通证—Securitized Token

证券通证（ST - Security Token）从本质上来说，有两重涵义。一是证券化的通证（Securitized Token）。证券化的通证是 ICO 在证券法监管要求下的延续。在证券法监管下的加密通证发行被简称为 STO（Security Token Offing）。相比 ICO，STO 在证券法的要求下具有如下合规性限制：

- 投资者资质限制：美国的非合格投资者将不能再投资 STO 项目，

在美国发行和出售证券的 STO 发行人必须在美国证券交易委员会(SEC)注册或获得豁免权。这也意味着根据 SEC 的监管要求，STO 项目将只能向合格投资者或者非常富有的人发行；

- 二级市场交易限制：由于合规门槛的存在，证券化的通证只能够在持牌的交易所进行交易（拥有所在国的证券交易牌照）。此外，在一定的时间段内证券化的通证也只能在合格投资人之间交易；
- 相比 ICO 成本更高：STO 平台服务提供商（例如承销商）可以提供服务来确保 STO 活动遵守了 SEC 的监管要求，但是成本会增加很多，融资金额也会降低很多。

合规监管是 STO 的重点关注事项。目前，只有美国明确了 STO 的监管框架，证券化的通证需要接受 SEC 及其他相关机构的监管，发行证券化的通证的主体也将受到联邦法律的约束。证券化的通证需要在 SEC 注册，并需遵守证券法的种种规定。

根据美国 1933 年颁布的证券法，任何证券（股票，债券，各类票据）的出售都需要在 SEC 注册。但当发行方在满足证券法规定的特定条件时，可以豁免 SEC 注册（仍然需要接受监管），仅需要 SEC 备案，如 Reg A+，Reg D，Reg S 等。条款 D 是主要的私募融资法规；条款 S 是监管面向海外投资人的法规；条款 A+相当于小 IPO，需要提供 2 年经审计的财务信息。通过选择以上三个条款之一发行证券类通证，发行方将节约巨大的成本，但同时符合监管机构的合规规定。（如图 8-14 ）

主要条款	Reg D		Reg S	Reg A	
	506 (b)	506 (c)		第一层	第二层
募集金额限制	无	无	无	2000万美金	5000万美金
证券类型限制	无	无	无	不允许资产支持证券	不允许资产支持证券
是否需要SEC审核	否	否	否	是	是
是否需要所在州注册	免除	免除	-	需要	免除
禁售期	有	有	有	无	无

图 8-14 豁免 SEC 注册的证券发行条件

8.3.3 通证化的证券—Tokenized Security

证券通证（ST - Security Token）的另一个涵义是通证化的证券（Tokenized Security），是指利用区块链技术改造传统金融的技术和业务逻辑，这将会引发传统金融的巨大变革。

通证化的证券具有极大的应用空间和发展潜力。从市场规模上看，全球有超过 70 万亿美元的股票资产，超过 100 万亿美元的债券资产，超过 230 万亿美元的不动产资产（住宅约 180 万亿美元，商业 32 万亿美元等），上述各类资产都可以进行通证化，以提高效率，减低交易成本。

具体而言，通证化的证券具有如下好处：

1）降低监管摩擦

交易摩擦的产生很大原因是因为监管的复杂性。比如，监管规则可以在资产类型、投资者类型、买方管辖权、卖方管辖权和券商管辖权等多个维度上发生变化，每一个维度都有众多的监管组合和管理交易的多个监管机构；此外，监管合规通常需要通过一系列独立的交易实体记录，来验证交易的所有权和合规性，因而保持合规性增加了交易的延迟和成本，分割了市场，降低了流动性。

通证化的证券是合规的代码化体现，交易的监管从一个个割裂的平台审批变成写入程序的自动化行为。监管要素将被系统化地硬连接

到证券的体系结构中，市场参与者的合规成本也因为规模化和自动化而大幅降低。

监管的无摩擦(frictionless)甚至可能会让监管机构主动要求市场主体『通证化』。

2）交易全球化、提高市场效率

通过将监管程序化的方式，降低监管成本与难度，打破监管机构之间、国家之间的壁垒，使资产在不同国家和地区之间的交易更加便捷，基于区块链的跨国证券交易，甚至去中心化市场的合规证券交易将成为非常普遍的市场选择。因为这些通证可以在世界范围内销售和交易（只要符合规定），资产的定价将更加公平，价格发现机制更有效率，因此对投资人具有吸引力。

3）降低成本、拓展金融服务能力

传统的 IPO 发行费用和时间成本极高，占到募资额的 4-7%（根据普华永道 PWC 的数据统计）。而采用 STO 的方式，减少中介的参与，成本将大大降低。

STO 将扩大中小企业融资渠道。仅在美国，每年就创建了超过 65 万家公司，但是华尔街，硅谷和天使投资者没有为创业公司提供足够的资金。因此，受监管且符合要求的 STO 可以帮助中小型企业获得新的融资渠道。

4）金融创新的巨大空间

通证化的证券提供的可编程监管和交易逻辑，或为证券的设计开拓出新的道路，证券及其衍生品未来将会被更形式化和数学的语言重

新定义与拓展。

从经济学的理论来审视，可编程的证券是一种对有限理性（Bounded Rationality）的扩张，它将允许我们构建以前不可能执行的契约特性，从而更接近完全契约（Complete Contract）的新经济形态。

- **公司治理：**企业治理结构表现为一系列契约的集合，当契约以通证的形式存在时，持有公司发行的通证化的证券的投资者名义上应该是公司的「股东」。公司治理结构将以可编程的形式存在，为治理形式的创新留下了空间。比如，创设公司治理通证，持有股票的时间越长，获得的选票就越多，相当于创始人在产品上市时创造了一种拥有 10 倍投票权的股票。
- **新的金融产品形态：**除了现有金融产品的各类形态（ABS、MBS、各类权证等等，不管多复杂）都可以通证化之外，新的金融产品形态一定会被创造出来，比如持有通证化的证券的投票权和股息权被分拆出来进行抵押，去偿还房屋的贷款（资产拆分和信贷交叉）。信贷在多个维度上实现扩张。
- **增强资产流动性：**比如一个封闭期为 10 年的私募基金，投资人只能在 10 年后才能收回自己的投资，但如果将基金通证化，那么投资人可以随时买卖基金份额，实现资产的流动。

8.3.4 STO 的监管与未来

基于区块链公链的 STO 为金融监管带来极大的挑战：

- **国家和法律边界：**在区块链公链上，发行人的注册地址、发行

地点、交易地点可以完全不同，给跨区域监管带来很大困难。

- **流动性泡沫风险：**当资产的流动性增强，资产的价格往往会出现流动性溢价的情况，从而衍生出资产价格泡沫，增加了巨大的波动性和不确定性。
- **技术安全漏洞：**任何技术都没有绝对安全，当 KYC/AML 流程或者通证底层协议被修改或者利用，投资者将面临巨大的损失。

总结而言，证券化的通证是 ICO 在法律与合规基础上的延续。区块链、DAO 基础上创新的 ICO 融资和激励方式的探索仍将继续下去。对通证经济而言，深入研究如何区分证券型通证、应用型通证（货币型通证）、资产型通证和治理型通证在不同场景下的用途和使用方式，并综合各种类型通证来实现共识机制和激励机制，是未来通证经济理论完善和应用的重要课题。

而通证化的证券则潜藏了一个大的机遇，现有的证券类型资产可能会选择区块链作为资产的底层支撑技术工具，也即实现现实社会的资产上链。这一方面为区块链技术的落地提供了一个巨大的应用场景，另一方面也为传统金融行业注入了新的活力，传统金融的监管、产品、和市场结构将被颠覆。

从资产上链的角度去理解 STO，从 70 万亿美元的股票资产，到 100 万亿美元的债权资产，再到兆级的金融衍生品资产，区块链作为一个显著更优的资产承载方式，将会迁移越来越多的合适资产，这将是一个波澜壮阔的资产数字化过程。

第九章 数据要素化时代的隐私计算

9.1 数据要素化时代来临

9.1.1 通用数据保护条例 GDPR

欧盟议会于 2016 年 4 月 14 日通过的《通用数据保护条例(General Data Protection Regulations)》(简称 GDPR)[14], 于 2018 年 5 月 25 日在欧盟成员国内正式生效实施。该条例被称为史上最严格的数据法规，它不仅对个人数据权力保护做出了详细说明，还对违规行为制定了严格的处罚措施。这些处罚是以行政罚款的形式出现的，可以对任何类型的违反 GDPR 行为进行处罚，包括纯粹程序性的违规行为。其罚款范围是 1000 万到 2000 万欧元,或企业全球年营业额的 2%到 4%。

GDPR 的设立缘由：

- 1）为欧盟公民提供更多使用自己的个人资料的权力；
- 2）加强数字服务提供者与他们所服务的人之间的信任；
- 3）为企业提供明确的法律框架，通过在欧盟单一市场上制定统一的法律来消除任何区域差异。

事实上，GDPR 的适用范围极为广泛，任何收集、传输、保留或处理涉及到欧盟所有成员国内的个人信息的机构组织均受该条例的约束。比如，即使一个主体不属于欧盟成员国的公司，只要满足下列两个条件之一就会受到 GDPR 的管辖：

- 1）为了向欧盟境内可识别的自然人提供商品和服务（包括免费服务）而收集、处理他们的信息。

[14] The European Unions, General Data Protection Regulations, www.gdpr.international.

➡ 2）为了监控欧盟境内可识别的自然人的活动而收集、处理他们的信息。

因此，GDPR 的影响是全球性的。GDPR 开启了全世界对数据隐私保护问题的关注。在 GDPR 的示范作用下，美国加州同年推出《加州消费者隐私法案》（简称 CCPA）。

9.1.2 数据安全管理办法

2019 年 5 月 28 日，国家互联网信息办公室发布《数据安全管理办法（征求意见稿）》（以下简称“管理办法”）。《管理办法》声明国家坚持保障数据安全与发展并重，鼓励研发数据安全保护技术，积极推进数据资源开发利用，保障数据依法有序自由流动。

《管理办法》重点内容如下：

1）明确监管主体，施行备案制管理

根据《管理办法》，在中华人民共和国境内利用网络开展数据收集、存储、传输、处理、使用等活动，以及数据安全的保护和监督管理均在此办法的监管范围。

《管理办法》又进一步明确了统一监管主体，即国家网信部门统筹协调、指导监督个人信息和重要数据安全保护工作，地（市）及以上网信部门依据职责指导监督本行政区内个人信息和重要数据安全保护工作。

在监管方式上，《管理办法》指出，网络运营者以经营为目的收集重要数据或个人敏感信息的，应向所在地网信部门备案。备案内容包括收集使用规则，收集使用的目的、规模、方式、范围、类型、期限

等。

2）建立个人信息收集使用规则，提出安全责任人制度

根据《管理办法》，网络运营者只要收集使用个人信息，应分别制定并公开收集使用规则，收集使用规则可以包含在隐私政策中，也可以其他形式提供给用户。并规定仅当用户知悉收集使用规则并明确同意后，网络运营者方可收集个人信息。

从收集使用规则的内容看，增加了对数据安全责任人的要求，并提到了应分别制定并公开收集使用规则。根据《管理办法》，网络运营者以经营为目的收集重要数据或个人敏感信息的，应当明确数据安全责任人，并规定了安全责任人的具体要求和职责。

3）约束默认授权、功能捆绑相关行为，要求停止“定推”后删除用户数据

《管理办法》规定网络运营者不得以改善服务质量、提升用户体验、定向推送信息、研发新产品等为由，以默认授权、功能捆绑等形式强迫、误导个人信息主体同意其收集个人信息。

同时还对“定向推送”做出了明确规定，要求网络运营者利用用户数据和算法推送新闻信息、商业广告等，应当以明显方式标明“定推”字样，为用户提供停止接收定向推送信息的功能；用户选择停止接收定向推送信息时，应当停止推送，并删除已经收集的设备识别码等用户数据和个人信息。

4）提出数据爬取要求，规定“合成”内容要求

《管理办法》对数据爬取和“合成”信息进行了首次规定。根据《管

理办法》，网络运营者采取自动化手段访问收集网站数据，不得妨碍网站正常运行；此类行为严重影响网站运行，如自动化访问收集流量超过网站日均流量三分之一，网站要求停止自动化访问收集时，应当停止。

对于“合成”信息，则要求网络运营者利用大数据、人工智能等技术自动合成新闻、博文、帖子、评论等信息，应以明显方式标明“合成”字样；不得以谋取利益或损害他人利益为目的自动合成信息。

《管理办法》的出台，第一，可以有效遏制目前市场上多数从事数据活动的机构盗用、滥用数据现象；第二，可以有效促成数据活动机构加强数据采集规范的研究，并为最终形成社会统一的数据采集标准提供基础；第三，为一些从事存储、传输的技术研究机构提供了一定的市场空间；第四，为市场上从事数据活动的机构提供了一个相对公平、公开的竞争环境。

2020 年 2 月 13 日中国人民银行发布的《个人金融信息保护技术规范》中明确规定了个人金融信息在收集、传输、存储、使用、删除、销毁等生命周期各环节的安全防护要求。并且明确了使用个人金融信息时“应向个人金融信息主体告知共享、转让个人金融信息的目的、数据接收方的类型，并事先征得个人金融信息主体明示同意，共享、转让经去标识化处理（不应仅使用加密技术）的个人金融信息，且确保数据接收方无法重新识别个人金融信息主体的除外。”

同时，中国人民银行发布的《个人金融信息保护技术规范》对于因金融产品或服务的需要，将收集的个人金融信息委托给第三方机构

(包含外包服务机构与外部合作机构)处理的情况，对第三方机构等受委托者要求：对委托处理的信息应采用去标识化（不应仅使用加密技术）等方式进行脱敏处理；应对委托行为进行个人金融信息安全影响评估，并确保受委托者具备足够的数据安全能力，且提供了足够的安全保护措施。

9.1.3 数据成为生产要素

GDPR 和《管理办法》的出台和实施标志着数据的收集与使用，经过最初的野蛮发展之后，开始进入规范发展阶段。

党的十九届四中全会通过了《中共中央关于坚持和完善中国特色社会主义制度、推进国家治理体系和治理能力现代化若干重大问题的决定》，其中第六部分第（二）条提出“健全劳动、资本、土地、知识、技术、管理、**数据**等生产要素由市场评价贡献、按贡献决定报酬的机制。” 这是七大生产要素概念的首次提出。

9.1.3.1 数据生产要素化的意义与影响

“按要素贡献分配”是我国改革开放进程中的重大分配制度理论进展，其理论的演化过程如下：（如图 9-1 ）

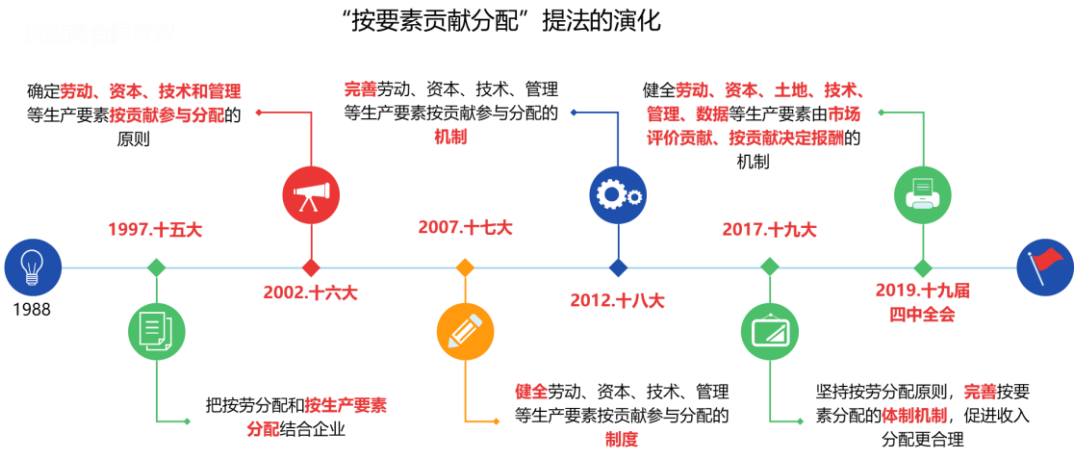

图 9-1 按要素贡献分配理论的进展

1997 年，党的十五大提出了“把按劳分配和按生产要素分配结合起来”，“允许和鼓励资本、技术等生产要素参与收益分配”——“按生产要素分配”这一概念被首次提出，并明确了“技术”是生产要素之一。

2002 年，党的十六大提出了“确立劳动、资本、技术和管理等生产要素按贡献参与分配的原则”——“按要素贡献分配”这一概念被首次提出，强调了是按“贡献”分配而非按“投入”分配，并在生产要素中增加了“管理”。

2007 年，党的十七大进一步提出了“健全劳动、资本、技术、管理等生产要素按贡献参与分配的制度”——完成了从“确立原则”到“健全制度”的变化。

2012 年，党的十八大提出“完善劳动、资本、技术、管理等要素按贡献参与分配的初次分配机制”——完成了从“健全制度”到“完善制度”的进阶。

2017 年，党的十九大提出“坚持按劳分配原则，完善按要素分配的体制机制，促进收入分配更合理、更有序”——再度强调了“按要素分配”和“完善体制机制”。

2019 年 11 月，党的十九届四中全会提出“健全劳动、资本、土地、知识、技术、管理、数据等生产要素由市场评价贡献、按贡献决定报酬的机制”——生产要素由之前的劳动、资本、技术、管理等“四项”变为“七项”，增加了土地、知识和数据，且对“按贡献分配”

做了进一步的阐释：“由市场评价贡献、按贡献决定报酬”，即对“贡献”的测度是“市场法”而非“成本法”，是看“产出”而非看“投入”，是看“功劳”而非看“苦劳”，凸显了“让市场在资源配置中发挥决定性作用”。

关于按要素贡献分配，其理论探讨虽然已经有数十年时间，但目前仍处在实践探索的初期，远未形成一种成熟的分配机制，原因就在于各要素的贡献难以真正做到精准量化，只能粗略估算。理论探讨迟迟不能落地，急需新的革命性的突破。

数据成为生产要素对于“要素分配理论”具有重要意义。

一方面，在新的数字经济和数字社会时代，数据本身就是生产资料。谁占有数据，就能够基于数据提供衍生服务，创造价值，提高生产力。没有数据，即便空有算力和算法，也“巧妇难为无米之炊”。

另一方面，数据要素是对上述劳动、土地、资本、管理、技术、知识六大要素的数字化，能够随时记录任一要素发生的变化，应用大数据技术和相关算法做出决策，通过改变六大要素的优化组合就能创造出更多的生产力。同时，有了实时的数据，就完全可以对任一要素的贡献进行精准计算，这样才能使“要素贡献理论”真正落地。

9.1.3.2 数据确权是要素市场化的要求

市场经济要求生产要素商品化，以商品形式在市场上通过市场交易实现流动和配置，从而形成各种生产要素市场。市场在资源配置中起决定性作用，前提是要形成统一、开放、竞争、有序的市场体系。

数据作为时代与科技发展带来的最新的生产要素，在市场化方面

具有先天的优势。但是，在数据进入市场之前，需要形成清晰界定所有、占有、支配、使用、收益、处置等产权权能的完整技术和制度安排。

数据确权是数据要素市场化的前提条件。数据确权是保障市场秩序的基础。各种类型的数据产权得到清晰界定、顺畅流转和严格保护，这是规范市场主体生产经营行为、优化资源配置、降低市场交易成本、形成良好市场秩序的重要保障。建立健全数据产权制度可以有效激发市场主体活力和创造力，稳定社会预期，增强经济发展的持久动力。

9.2 当前的隐私计算领域研究方向

隐私计算技术主要分为联邦学习、多方安全计算、全同态加密、差分隐私等几个主要方向。不管哪个技术路线，本质上都要满足数据隐私性的基本要求：“可用不拥”、“不可还原”、以及“不可重标识”的要求。

9.2.1 联邦学习

联邦机器学习(Federated machine learning/Federated Learning)，又名联邦学习，联合学习，联盟学习。联邦机器学习是谷歌（Google）2016 年提出的一个机器学习框架[15]，能有效帮助多个机构在满足用户隐私保护、数据安全和政府法规的要求下，进行数据使用和机器学习建模。联邦学习作为分布式的机器学习范式，可以有效解决数据孤岛问题，让参与方在不共享数据的基础上联合建模，能从

[15] Federated Learning: Collaborative Machine Learning without Centralized Training Data. https://ai.googleblog.com/2017/04/federated-learning-collaborative.html.

技术上打破数据孤岛,实现 AI 协作。

微众银行 AI 团队则从金融行业实践出发,关注跨机构跨组织的大数据合作场景，首次提出“联邦迁移学习”的解决方案，将迁移学习和联邦学习结合起来。据杨强教授在“联邦学习研讨会”上介绍,联邦迁移学习让联邦学习更加通用化,可以在不同数据结构、不同机构间发挥作用，没有领域和算法限制,同时具有模型质量无损、保护隐私、确保数据安全的优势。

联邦学习定义了机器学习框架，在此框架下通过设计虚拟模型解决不同数据拥有方在不交换数据的情况下进行协作的问题。虚拟模型是各方将数据聚合在一起的最优模型,各自区域依据模型为本地目标服务。联邦学习要求此建模结果应当无限接近传统模式，即将多个数据拥有方的数据汇聚到一处进行建模的结果。在联邦机制下，各参与者的身份和地位相同，可建立共享数据策略。由于数据不发生转移，因此不会泄露用户隐私或影响数据规范。为了保护数据隐私、满足合法合规的要求。

联邦学习有三大构成要素：数据源、联邦学习系统、用户。在联邦学习系统下，各个数据源方进行数据预处理，共同建立及其学习模型，并将输出结果反馈给用户。如图 9-2。

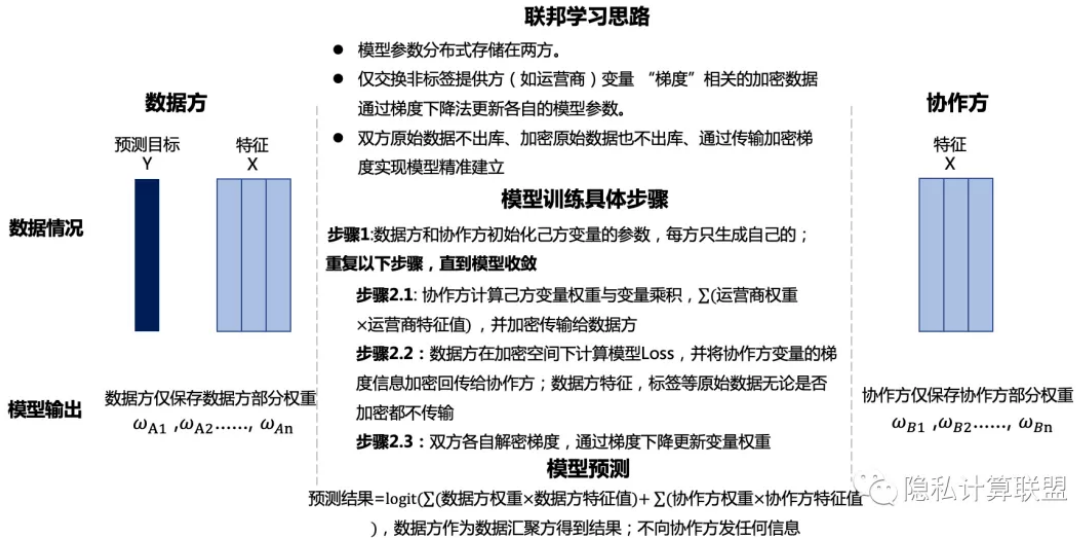

图 9-2 联邦学习流程示意图

通过上述的处理，联邦学习可以保障在不暴露明文数据及不暴露潜在数据信息的情况下，完成模型训练任务。联邦学习是机器学习技术和多种隐私保护技术的有机结合，包括多方安全计算，差分隐私等。按照参与方之间的数据特点，联邦学习可以分为横向联邦学习、纵向联邦学习和联邦迁移学习。

横向联邦学习

在两个数据集的用户特征重叠较多而用户重叠较少的情况下，我们把数据集按照横向(即用户维度)切分，并取出双方用户特征相同而用户不完全相同的那部分数据进行训练。这种方法叫做横向联邦学习。如图 9-3。

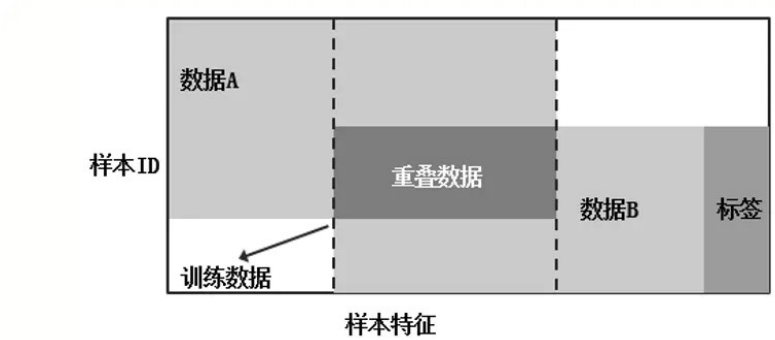

图 9-3 横向联邦学习示意图

比如业务相同但是分布在不同地区的两家企业，它们的用户群体分别来自各自所在的地区，相互的交集很小。但是，它们的业务很相似，因此，记录的用户特征是相同的。此时，就可以使用横向联邦学习来构建联合模型。

横向联邦学习中多方联合训练的方式与分布式机器学习（Distributed Machine Learning）有部分相似的地方。分布式机器学习涵盖了多个方面，包括把机器学习中的训练数据分布式存储、计算任务分布式运行、模型结果分布式发布等，参数服务器是分布式机器学习中一个典型的例子。参数服务器作为加速机器学习模型训练过程的一种工具，它将数据存储在分布式的工作节点上，通过一个中心式的调度节点调配数据分布和分配计算资源，以便更高效的获得最终的训练模型。而对于联邦学习而言，首先在于横向联邦学习中的工作节点代表的是模型训练的数据拥有方，其对本地的数据具有完全的自治权限，可以自主决定何时加入联邦学习进行建模，相对地在参数服务器中，中心节点始终占据着主导地位，因此联邦学习面对的是一个更复杂的学习环境；其次，联邦学习则强调模型训练过程中对数据拥有方的数据隐私保护，是一种应对数据隐私保护的有效措施，能够更好地应对未来愈加严格的数据隐私和数据安全监管环境。

纵向联邦学习

在两个数据集的用户重叠较多而用户特征重叠较少的情况下，我们把数据集按照纵向（即特征维度）切分，并取出双方用户相同而用

户特征不完全相同的那部分数据进行训练。这种方法叫做纵向联邦学习。如图 9-4。

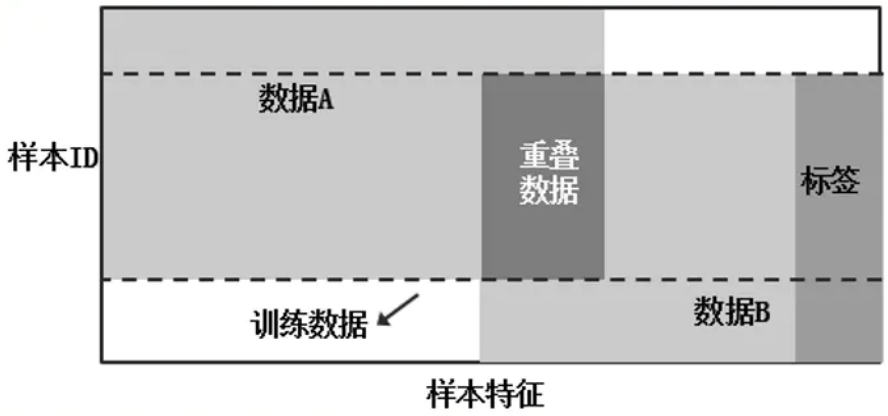

图 9-4 纵向联邦学习示意图

比如有两个不同机构，一家是某地的银行，另一家是同一个地方的电商。它们的用户群体很有可能包含该地的大部分居民，因此用户的交集较大。但是，由于银行记录的都是用户的收支行为与信用评级，而电商则保有用户的浏览与购买历史，因此它们的用户特征交集较小。纵向联邦学习就是将这些不同特征在加密的状态下加以聚合，以增强模型能力的联邦学习。目前机器学习模型如逻辑回归、决策树等均是建立在纵向联邦学习系统框架之下的。

联邦迁移学习

在两个数据集的用户与用户特征重叠都较少的情况下，我们不对数据进行切分，而可以利用迁移学习来克服数据或标签不足的情况。这种方法叫做联邦迁移学习。如图 9-5。

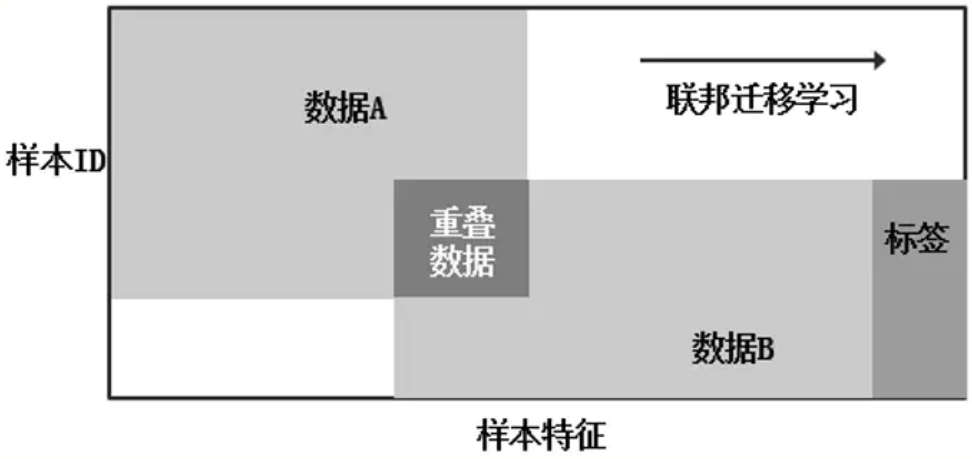

图 9-5 联邦迁移学习示意图

比如有两个不同机构，一家是位于中国的银行，另一家是位于美国的电商。由于受到地域限制，这两家机构的用户群体交集很小。同时，由于机构类型的不同，二者的数据特征也只有小部分重合。在这种情况下，要想进行有效的联邦学习，就必须引入迁移学习，来解决单边数据规模小和标签样本少的问题，从而提升模型的效果。

此外，在模型预测过程中，如果对模型预测任务不进行适当的限制，可能会导致模型参数或样本数据的泄露。所以，在模型实际应用过程中，需要对整体预测任务对模型的用法，对待预测样本的用量进行控制，以避免在模型预测过程中泄露模型参数及样本数据。

综上，通过传递参数、对参数进行保护以及在预测过程中的控制，联邦学习可以保证数据的“可用不拥”、“不可还原”、“不可重标识”，满足各项法律法规对合规性的要求。

9.2.2 安全多方计算

安全多方计算是密码学的重要分支，它通过一系列经过严格证明

的密码学协议（如秘密共享、不经意传输等），实现了互不信任的多个参与方在不泄露自身原始数据的前提下，得到准确的计算结果。

安全多方计算，(Secure Muti-party Computation，简称 MPC，亦可简称 SMC 或 SMPC）问题首先由清华大学姚期智教授于 1982 年提出了两方安全计算，之后 Oded Goldreich 等人在 1987 年发展到多方安全计算。简单来说，安全多方计算的原理是允许多个数据所有者在互不信任的情况下进行协同计算，输出计算结果。并保证参与计算的任何一方均无法得到除了应得的计算结果之外的其他任何信息。换句话说，MPC 技术可以获取数据使用价值，却不泄露原始数据内容。在最近几年多方安全计算已经广泛在区块链的各个数据应用领域里被采用。 如图 9-6。

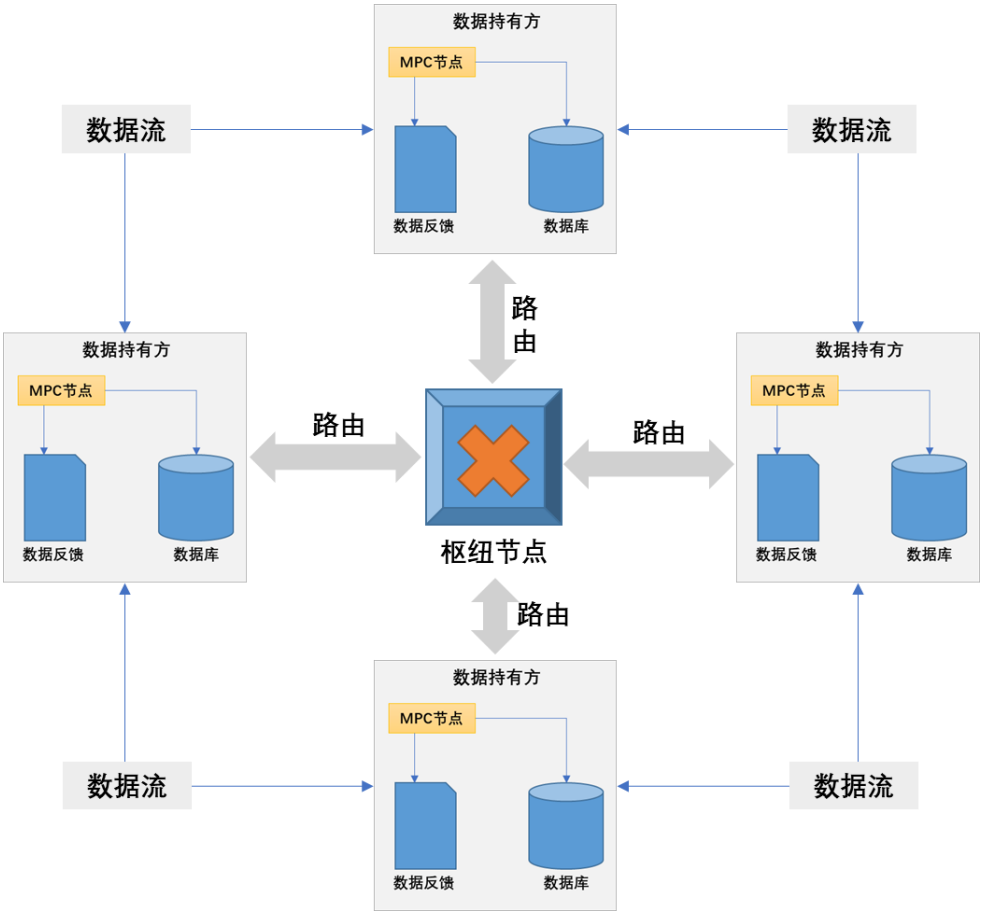

图 9-6 MPC 技术框架图

多方安全计算技术数据处理过程中各处理者所能获取的信息都被限定在了尽可能小的范围，同时通过对这些信息进行加密，就能从技术上限定这些信息仅能被用于当前的处理目的。所以，安全多方计算技术天然的满足“可用不拥”、“不可还原”、“不可重标识”的合规性要求。

9.2.3 同态加密

同态加密是基于数学难题的计算复杂性理论的密码学技术。对经过同态加密的数据进行处理得到一个输出，将这一输出进行解密，其结果与用同一方法处理未加密的原始数据得到的输出结果是一样的，从而实现数据的“可算不可见”，如图 9-7 所示。

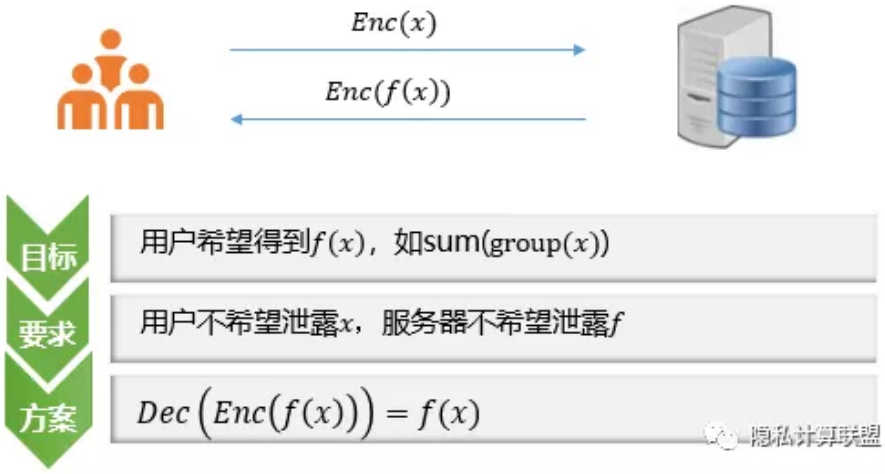

图 9-7　同态加密示意图

同态加密技术可以避免数据处理者接触明文数据，和“可用不拥”、“不可还原”、“不可重标识”的合规性要求是相通的，同样能够减少数据泄露的现实风险。

9.2.4 差分隐私

差分隐私（Differential Privacy）是一种数学技术，被《麻省理工科技评论》评为 2020 年全球十大突破性技术之一。差分隐私（Differential privacy）通过对原始数据加入噪声，在损失部分数据精度的前提下保护数据隐私。最早由 Dwork 在 2006 年提出，是针对统计数据库的隐私泄露问题的一种隐私保护技术。在这个场景下，差分隐私技术能最大限度减少个体被识别的机会，同时有效控制对计算结果的影响。差分隐私不仅仅被应用到统计数据库安全领域，也被广泛应用于数据隐私发布与数据隐私挖掘中。

差分隐私有两个重要的优点：

- 差分隐私假设攻击者能够获得除目标记录以外的所有其他记录信息，这些信息的总和可以理解为攻击者能够掌握的最大背景知识，在这个强大的假设下，差分隐私保护无需考虑攻击者所拥有的任何可能的背景知识。
- 差分隐私建立在严格的数学定义上，提供了可量化评估的方法。因此差分隐私保护技术是一种公认的较为严格和健壮的隐私保护机制。

差分隐私可以通过在数据中加适量的干扰噪声来实现，目前常用的添加噪音的机制有拉普拉斯机制和指数机制。其中拉普拉斯机制用于保护数值型的结果，指数机制用于保护离散型的结果。

与其他技术相比，差分隐私技术在“可用不拥”、“不可还原”、“不可重标识”的合规性要求中扮演的角色更特殊一些，具体可以分为两

类：

一方面，我们可以使用差分隐私技术，达到比“不可还原”、“不可重标识”更高的要求；例如我们可以给一个本身已经满足了“可用不拥”、“不可还原”、“不可重标识”的方案加入差分隐私，进一步降低其数据泄露风险；

另一方面，如果一个方案由于成本等种种原因，不得不传输或采集超出目标之外的信息，可以使用差分隐私技术对这些信息增加干扰，这样对于数据下游的接受方来说，其能够获得的额外信息量更少，更符合“可用不拥”、“不可还原”、“不可重标识”的合规性要求。

9.2.5 属性基加密机制 ABE

属性基加密机制 （ABE — Attribute-Based Encryption）这种加密算法最早是在 2005 年提出的，第一篇文章提出的时候也只有单一授权的概念，之后在 2011 年开始有团队把 ABE 用在区块链上。技术原理简单地说，就是把密钥（或密文）的属性加上一定的策略嵌入（加密）到密钥（或密文）上。所谓属性是指信息文件的特征，策略指的是这些特征直接的“与”“或”关系。举个例子，假设策略嵌入密文中，这就意味着数据拥有者可以通过设定策略去决定拥有哪些属性的人能够访问这份密文，也就相当于对这份数据做了一个粒度可以细化到属性级别的加密访问控制。

ABE 属于公钥加密机制，其面向的解密对象是一个群体，而不是单个用户。实现这个特点的关键是引入了属性概念。属性是描述用户的信息要素，例如：校园网中的学生具有院系、学生类别、年级、专业

等属性；教师具有院系、职称、教龄等属性。ABE 使用群体的属性组合作为群体的公钥,所有用户向群体发送数据使用相同公钥。上例中,{计算机学院,本科生}作为向计算机学院本科生发送密文的公钥，而私钥由属性授权机构根据用户属性计算并分配给个体。

算法的正确性和安全性、密钥管理、可扩展性是安全协议研究的核心问题。ABE 机制采用访问结构表示访问策略，而策略的灵活性会导致访问结构的复杂。　　在 ABE 系统中，属性的动态性增加了密钥撤销的复杂性；且属性密钥与用户标识无关，导致无法预防和追踪非法用户持有合法用户的私钥（盗版密钥）。而大规模的分布式应用需要 ABE 机制支持多机构协作以满足可扩展性、容错性的需求，这些因素给 ABE 的研究带来了挑战。

9.2.6 可信执行环境

可信执行环境（Trust Execution Environment — TEE）是可以保证不被常规操作系统干扰的计算环境，因此称为“可信”。也就是说，TEE 是一个与操作系统并行运行的独立执行环境，并且独立于操作系统和其上的应用，为整个软件环境提供安全服务。例如，在 ARM 计算机架构里的 TrustZone 即是支持 TEE 技术的产品。TrustZone 在概念上将 SoC 的硬件和软件资源划分为安全（Secure World）和非安全（Normal World）两个世界，所有需要保密的操作在安全世界执行（如指纹识别、密码处理、数据加解密、安全认证等），其余操作在非安全世界执行（如用户操作系统、各种应用程序等）。如图 9-8 。

在区块链网络中,有实务性研究正在将可信执行环境的范围扩大,

将原本限制在单点计算环境上的 TEE 通过 VPN 连接起来，在公共网络上构建以 VPN 连接的**可信执行网络（Trust Execution Network—TEN）**，进而保障计算和通信的隐私性。

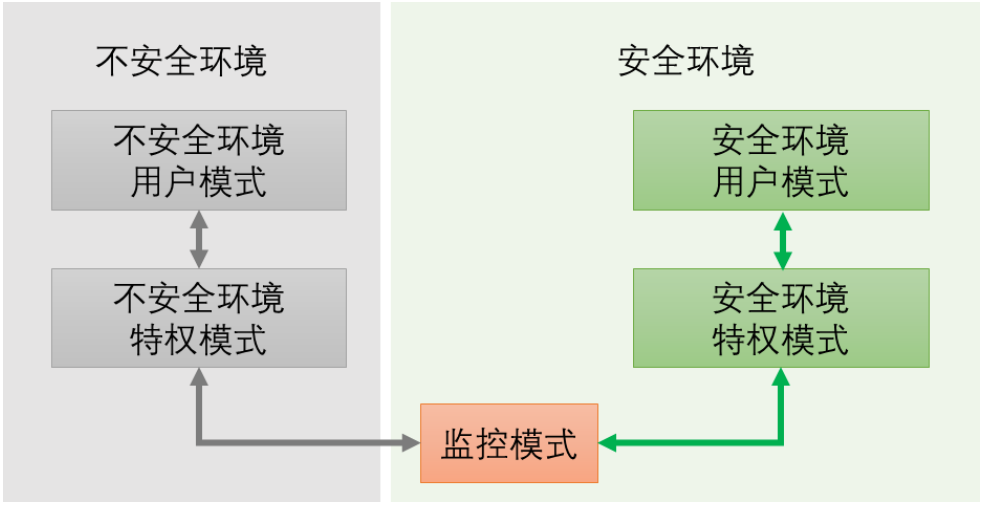

图 9-8 可信执行环境 TEE 及可信执行网络 TEN

9.3 基于区块链的隐私计算解决方案

区块链技术具有不可伪造抵赖、不可篡改、智能合约和分布式记账等技术特性，在实现数据确权与自主权管理方面具有优势。数据确权及自主权化管理是数据资产化时代，或者说数据要素化时代的基础问题，因此应用场景极为广泛。本节以政务大数据场景和个人医疗健康数据场景为例，说明区块链自主权数据管理的应用。

区块链自主权数据管理模型的基本内容如下：

- 基于数字身份对数据进行确权，并将数字身份延伸到智能合约、物联网 IOT 等非实体“用户”，让一切都可以用数字身份来表达，并成为一种基础治理能力；
- 数字身份不是简单的身份标识，而是用户账户数据（属性）与交易（行为）数据的集合。

- 自主权数据管理模型功能包括：数据确权（多方主权）、数据安全定义、数据共享与流转、数据有条件授权、数据隐私保护、数据防篡改、数据审计监督等。

自主权数据管理帮助用户掌控自己的数据，并在自己同意的情况下在可信实体之间分享数据。同时，企业需要进行用户身份的识别和验证，在遵守用户隐私规定的条件下，建立起完整的用户数据库。

数据加密的环节是自主权数据管理的基础。只有有了加密的手段，使得所有人需要保护隐私的时候、需要保护商业机密的时候、需要保护竞争利益的时候、以及需要满足政府监管要求的时候，有所有人共同认可的加密手段，使得数据交易不是把裸数据卖掉，而是数据使用权的分享和交易，是在加密状态下进行的数据交易，只有这样才能使得数据隐私及产权利益得以保护。

9.3.1 云计算时代的政府业务数据确权

国发〔2015〕5 号文《国务院关于促进云计算创新发展培育信息产业新业态的意见》指出，充分发挥云计算对数据资源的集聚作用，实现数据资源的融合共享，推动大数据挖掘、分析、应用和服务。政务云建设进入一个新的阶段，称之为“政务云 2.0 阶段”。政务云 2.0 阶段，在 IaaS 基础设施资源整合与共享的基础上，将会实现 IaaS/PaaS 深度融合，借助云计算技术推动政府大数据的开发与利用，实现跨系统的信息共享与业务协同，推进应用创新。政务云 2.0 的特征是以数据为核心、以 IaaS/PaaS 深度融合为支撑，以新架构的云应用创新为代表。在政务云 2.0 阶段，应用对业务连续性和数据安全可

靠性保障提出了更高要求。

政务大数据已经成为提升政府治理能力、重构公共服务体系的新动力、新途径。2015 年发布的《促进大数据发展行动纲要》提出建立“用数据说话、用数据决策、用数据管理、用数据创新”的管理机制；2016 年发布的《“十三五”国家信息化规划》指出“加快推进跨部门、跨层级数据资源共享共用”；2017 年发布的《新一代人工智能发展规划》进一步要求加强政务数据资源的整合、开发适于政府服务与决策的人工智能平台。相关行业部门、地方政府也出台了一系列推进政务大数据发展和应用的政策文件，鼓励相应的实践探索。

云计算和大数据推动政务云的协调发展。云计算为政务云提供了技术实现手段。政务云可以推动政府大数据的数据资源整合，为大数据分析提供数据基础。大数据可以为政务云的建设以及政务决策提供预测和数据支持。政务云和大数据分析都可看作是云平台上的应用。云计算其实就是资源的整合和虚拟，整合可以大致分为计算能力、存储能力和网络的整合。

国家政务大数据应用还处于起步阶段，尤其是在政务数据的采集、开放共享和跨领域应用方面仍有许多问题亟待解决。在非云计算时代，各个政府部门自建 IT 信息化系统，政府部门业务数据权属与 IT 系统的物理权属管理的安全责任是统一的。每个政府部门为自己的 IT 系统物理安全与业务数据安全负责；在云计算时代，IT 系统的物理权属和安全责任归属统一的云计算中心或者大数据中心，但是各部门的业务数据权属及安全责任仍归部门管理，IT 系统的物理权属和业务系

统的数据权属的安全责任是分离的。权属分离导致责任不清，这是目前政务数据上云和大数据中心数据收集的最大障碍。（如图 9-9 ）

图 9-9 业务数据权属分离是政务云的新问题

如何确保云计算时代，业务数据权属的安全责任是云计算时代带来的新问题。区块链对数据的确权，以及基于确权的共享能力将是云计算时代数据权属安全责任的重要解决方案。

基于区块链自主权数据管理，为每个业务部门建立数字身份，基于数字身份为业务部门的数据签名及加密，通过软件和算法确保业务部门数据不可抵赖和不可篡改，解决了云计算时代业务部门的数据权属问题。

区块链自主权管理在政务数据领域的实施将会极大推动政务数据上云及政务大数据中心的建设。

9.3.2 医疗健康数据的自主权管理

2018 年 7 月 12 日，为加强健康医疗大数据服务管理，促进“互联网+医疗健康”发展，充分发挥健康医疗大数据作为国家重要基础性战略资源的作用，根据相关法律法规，国家卫生健康委员会发布了《国家健康医疗大数据标准、安全和服务管理办法（试行）》。

从区块链技术的特征可以看出，医疗行业会成为受益最大的行业之一，因为该技术能够解决困扰医疗领域多年的痛点：医疗健康数据的隐私性与安全性。

首先，病人的医疗记录和个人隐私信息在任何时候都是需要被保密的。这需要医疗机构具有安全到足以令人信任的保密机制，尤其涉及到特殊敏感的治疗记录，如艾滋病、乙型肝炎、癌症，或是整容、心理疾病等等。而所有的这些医疗记录和信息如果只是被单纯放进机构运营的信息数据库里，已不再是稳妥可行的选择。因为在互联网时代往往由于网络安全等问题，“泄密”与“爆料”变得简单到不需要花费任何代价。例如：

- 2015 年 2 月，美国第二大医疗保险服务商遭到入侵，超过 8000 万患者和雇员的个人信息被盗，被誉为史上最大医疗信息泄露事件；
- 2016 年 7 月，加州大学洛杉矶分校健康服务系统由于用户数据没有加密，450 万份档案资料被泄漏。

其次，健康人群的身体数据也是现代社会的重要隐私情报。特别是像指纹或虹膜这种“身体密码”，它们不同于身高体重、血糖血压之类的传统数据，是绝对不能泄露的，如果这些涉及到唯一性的资料出现大规模泄露，将会引发金融灾难。此外，随着基因检测的发展，现在只要几百元和一点唾液，检测机构就能生成一份检测报告，包括个人基因数据、健康风险、遗传性疾病、药物指南等等，所有的个人隐私信息均被保存在该检测机构的数据库中。这种毫无保障的中心化数

据库里存储的用户健康信息，一旦出现泄露，很难想象会带来多少不可控事件的发生。

区块链技术为可以医疗行业提供了一个可行的“数据隐私”解决方案，这是一个能做到完全透明却又能尊重用户隐私的方案。

1）电子病历（Eletronic Medical Records，EMR）

区块链在医疗领域最主要的应用是：**个人医疗数据的自主权管理**。

EMR 的广泛使用给医疗领域带来非常大的便利，使得数据的存储复制非常简单。但存在如下缺陷：

- 首先，在现有的体系下，患者的个人健康数据是由不同的医院或企业来进行管理的，患者的个人数据是分散的，数据难以交互，互操作性差，难以协调管理。
- 其次，患者个人健康数据是有价值的，本质上归患者所有，但是管理数据的企业往往因为经济利益将这些数据占为己有，患者无法掌控和管理自己的个人医疗数据，无法对自己的数据进行访问控制、权限设定。
- 最后，医疗数据的安全性和有效性完全依赖于企业，一旦企业的数据库遭受破坏，医疗数据就会损失，难以恢复，且企业很可能会为自身利益，泄露医疗数据，对患者隐私造成危害。

基于区块链自主权管理医疗病历，就有了个人医疗的完整历史数据，看病也好，健康规划也好，就有历史数据可供使用，会对精准治疗和疾病预防有宝贵价值。而且这个**数据真正的掌握者是患者自己**，并不是某个医院或第三方机构，这对于消除医疗信息摩擦，包括信息

不完善、信息风险和信息无法访问等，以及保护数据的隐私性和安全性有重要意义。

2）健康管理

基于区块链技术搭建的健康管理平台，可在智能家居/办公环境中运作，让用户能够安全地跟踪并收集个人健康数据。这些数据多来自联网的可穿戴设备和其他家庭监控设备。在该应用场景下，智能合约将被用于医疗健康识别中，如遇紧急情况，还能触发潜在紧急健康状况的警报，并将适当的信息传递给临床医生和家庭成员。

3）DNA 钱包

基因和医疗数据基于区块链自主权管理，将形成一个 DNA 钱包。这使得医疗健康服务商能够安全地分享和统计病人数据，帮助药企更有效率地研发药物。服务商在使用个人数据时，要征得个人同意授权，并为个人提供相应补偿或回报。

4）医疗支付与理赔

全球每年的医疗总支出超过 7 万亿美元。其中，个人消费者每年直接自费支付近 18%或 1 万亿美元。尽管经济支出巨大，但医疗服务生态系统还不够完善，不能让消费者享有经济主体的主动权。消费者可能并不知道一些医疗服务的成本是多少，或者他们应该花费多少。基于区块链的自主权数据管理，在数据智能分析的帮助下，可以帮助患者在接受治疗前，提前确定自付费用金额，也能提供预付款等服务，避免造成患者意料之外的成本，医疗机构也能减少未收款项坏账。

医疗健康数据的区块链自主权管理可以显著地促进医疗信息的共

享，创造安全、可信和便捷的医疗记录，具有高度的完整性和可信性。区块链保证了数据的有效性和安全性，使得医院、保险公司和实验室能够实现连接并且及时无缝分享信息，而无需担心信息被泄露或者被篡改。通过在区块链上编写智能合约，可以对患者数据进行访问控制，保证患者对自己数据的所有权，在一定程度上保护患者隐私。区块链可为医疗行业带来的另一大变革是促进医疗服务向以患者为中心转变，在物联网及认知分析等技术的协同作用下，全新的远程医疗护理、按需服务和精准医疗将成为可能。

5）人民健康系统工程

习近平总书记在 2016 年 8 月 19 日至 20 日在全国卫生与健康大会上指出：“把以治病为中心转变为以人民健康为中心。” 把“人民健康系统工程”服务于以人民健康为中心的战略任务将成为我国医疗健康工作者和相关政府管理部门的重要工作目标。

人是具有高级意识活动的开放复杂巨系统。人健康的主要决定因素是开放的性质，即中医所述的“后天之气”。有序开放，使人健康，并能使人系统代表“先天之气”的多层次自组织功能更进一步发展。相反，如果开放的有序性不足，则会影响先天之气，使人系统稳态水平下降，甚至转化为病理性稳态，即表现为各类慢性病。因此，从系统论观点看，导致各类慢性病的主要原因就是代表开放的心、表、里、场四大通道输入的有序性不足所致。俞梦孙院士及其科学家团队积极响应和践行习近平总书记“把以治病为中心转变为以人民健康为中心”的指示，结合钱学森的人系统的整体功能态思想和中华传统医学“天

人合一心身协同整体观点”，提出遵循“规模化有序开放”原则，即系统地、有针对性地认识和把控人个体的先天遗传和后天“四大通道”输入，使气血畅通、阴阳平衡，始终处于健康状态。团队经过 30 年的研究探索，证实了从宇航员、飞行员、健将级运动员、一般工作人员，特别是一些慢性病患者，都多多少少存在某种程度上的“有序开放”不足而引起的健康“隐患或问题”。新型人民健康系统工程服务生态应运而生，涉及个人、家庭、企业、健康服务、监测、保险服务机构，以及政府监管等单位间的多种数据和多层次的数据交互。

基于医疗健康数据自主权管理的精准医疗和按需服务场景与流程举例如下：（如图 9-10 ）

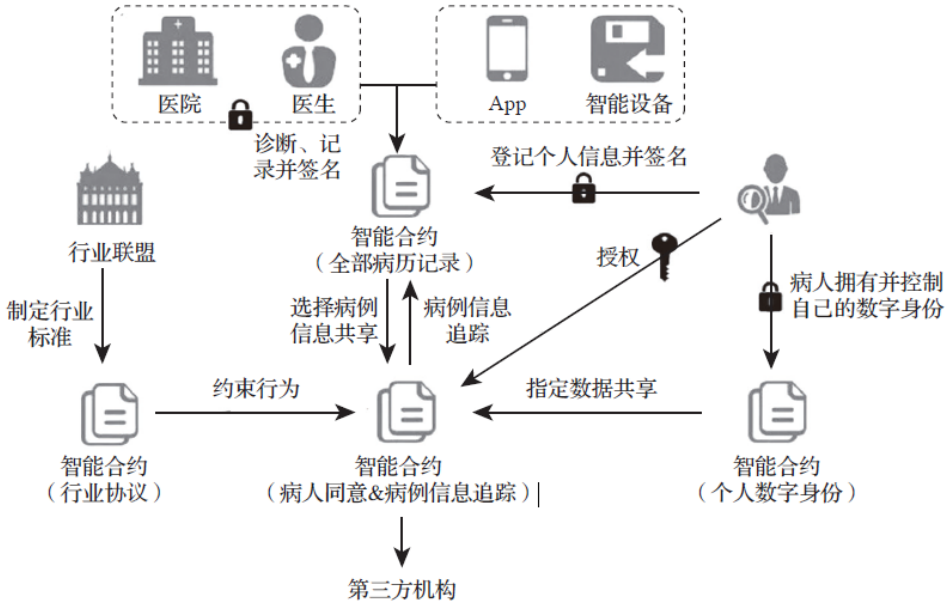

图 9-10 基于医疗健康数据自主权管理的精准医疗服务

场景一：药物适配

药企在后台管理系统提交自身要售卖的药品、服务、向系统发出分析请求。系统收到后抽取其相应受众可能具备的病理特征，再据此

向目标客户群（系统初步判断）发出授权请求，用户同意并授权药企后，系统将目标用户病理特征与授权群体中的病理特征（已脱敏）进行比对，并将对比结果及相似度反馈至药企。药企查阅后可选择相似度达60%以上的筛选条件作为门槛，向目标客户推送定制化服务。

场景二：保险定制

保险商在后台管理系统提交自身要售卖的服务，并向用户群体发出授权请求。

用户同意且保险商支付费用后，系统评估授权群体中患有某种疾病风险的概率，并将相关结果反馈至保险商，其查阅后可根据用户群体患有某种疾病的概率进行智能定价，并将不同的定制化服务推送至用户。

场景三：人民健康定制服务

人民健康定点服务单位向人民健康服务中心在后台提交人民健康监测服务分享请求，后台管理系统根据相应受众可能存在的健康隐患，向可能的用户群体发出授权请求。用户同意并授权中心或向中心支付费用后，系统评估授权群体中存在某种健康隐患风险的概率，并将相关结果反馈至定点服务单位，其查阅后可根据用户群体存在某种健康隐患的概率进行智能定价，并将不同的定制化服务推送至用户。所有层次的数据交互均经过相应不同层级的脱敏处理和合规分析。

第十章 数字政务

10.1 区块链数字身份管理

10.1.1 行政相对人数字身份及其应用

行政相对人是指行政管理法律关系中与行政主体相对应的另一方当事人，即行政主体的行政行为影响其权益的个人或组织。在制定法上“行政相对人”一般称“公民、法人和其他组织”。因此行政相对人的数字身份包括两类：

- 自然人数字身份系统，为政府及公民提供可信身份数据和公共服务认证接口;基于公民身份信息的 eID 服务平台如图 10-1 。
- 法人及社会组织数字身份系统，与企业和事业法人行为相关的工商（民政）登记信息、信用信息、经营信息、以及司法信息等。

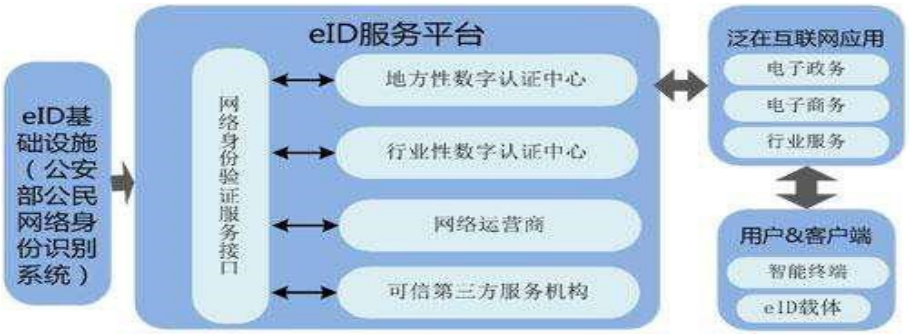

图 10-1 基于公民身份信息的 eID 服务平台

基于区块链技术实现行政相对人的数字身份管理以及基于数字身份的自主权数据管理，在数字政务领域将有非常多的具体应用落地场景。下面就几项典型场景进行详细说明。

1）实现身份信息共享

数字身份系统通过和政务、便民、公共服务、养老助残、医疗、人

社、教育、民政、住建等业务系统进行数据共享和联动，实现高效协作的政务联动协同管理，建立各个政务部门的工作衔接机制。平台实现互联互通，办公数据化，监管全覆盖，真实数据不可篡改，促进政务工作公开、透明、规范运行，并以高效协作的方式推进各部门政务服务迈上一个新的台阶。

2）实现跨部门无纸化审批

跨部门的事务审批通常是通过纸质出函方式，基于人工审批加复函的方式完成各种事务的审批工作。通过系统审批资料电子化和区块链分布式存储化，加入工作人员和审批人员的区块链电子签名技术，完成电子档案的区块链存储和数据共享，实现跨部门的无纸化审批流程，大大提高工作效率，也便于增强各部门的联动能力。

3）“零跑腿”便民服务升级

将数字身份控制权从中心服务器移交给个人，让个人拥有对数字身份的控制权，以个人主体为对象，围绕数据、业务、安全三个维度，构建个人主体相关数据及其关系的数据集合，打造“个人数据空间”。在此基础上，各个政务系统可以访问区块链中可信的个人数字空间，结合人脸识别、电话实名制认证、电子身份证等，实现政务服务的“零跑腿”，转变政府服务模式，变条件审批为信任审批，变被动服务为主动服务。

以协同理论为指导，建立以区块链为核心的数据共享平台，以数字身份这一应用场景为例，目前经过梳理已经可以在 20 多项政务业务场景中实现公民办理事务的“零跑腿”。（如图 10-2 ）

序号	事项名称	所属部门	序号	事项名称	所属部门
1	出具参保证明	社保	11	基本医疗保险个人账户查询	社保
2	出具领取基本养老金证明	社保	12	社保关系转成登记（养老缴费凭证打印）	社保
3	申请高龄老人津贴	民政	13	社保关系转成登记（医疗转移缴费凭证打印）	社保
4	老年人优待申请	民政	14	社保关系转成登记（失业转移缴费凭证打印）	社保
5	残疾人职业技能培训报名	残联	15	白内障复明证明	残联
6	残疾人生活津贴	残联	16	国家《流动人口婚育证明》办理	卫计
7	志愿者招募	团委	17	《独生子女父母光荣证》核发	卫计
8	开具个人所得税纳税证明	地税	18	计划生育情况审核	卫计
9	职工基本养老保险待遇领取资格认证	社保	19	生育保险参保职工计生情况确认	卫计
10	领取工伤保险长期待遇人员资格认证	社保	20	下岗失业人员免费技能培训报名登记	人社

图 10-2 基于区块链数据共享系统的“零跑腿”事项清单

4）公民和机构的诚信管理

在区块链系统登记个人信息的同时，也把个人的征信情况记录下来，这些信息在网络里对所有端口开放，在办理涉及个人的商业往来、借贷等事项时，通过区块链系统可以随时查询到个人和机构的全部诚信记录，可以避免许多纠纷事件，促进和谐社会发展。

10.1.2 不动产数字身份管理及其应用

2019 年 3 月 11 日，国务院发文《国务院办公厅关于压缩不动产登记办理时间的通知》，强调以推进国家治理体系和治理能力现代化为目标，以为企业和群众“办好一件事”为标准，大力促进部门信息共享，打破“信息孤岛”。基于数据共享交换平台，让信息多跑路、群众少跑腿，建立部门间信息共享集成机制，加强部门协作和信息互联互通，进行全流程优化，压缩办理时间，切实解决不动产登记耗时长、办理难问题。构建便捷高效、便民利民的“互联网+不动产登记”工作体系。

区块链技术在不动产数字身份管理及其应用领域的作用如下：

- 简化产权登记与交易流程：传统产权登记与交易受制于中介机

构、登记机构的审查以及资金交易环节的影响，流程较为繁琐；区块链帮助资金与交易过程直接对接，减少登记机构的审查、确认过程，从而简化产权登记与交易流程；

- 防止产权交易欺诈，提升交易透明度：传统产权登记机构缺乏登记机构间的数据共享，产权交易过程中透明度低，伪造、篡改产权难以避免；区块链可以提高产权交易透明度，加强对产权交易环节的有效保护，防止交易欺诈的产生。

“区块链+不动产”全生命周期服务解决方案是以区块链为技术支撑，基于不动产登记信息数据创建不动产数字身份，打通不动产交易中心、房地产管理局、税务局等多个部门数据互通，跨部门实现数据共享与安全；记录不动产业务过程中与外部进行数据交换的过程，包括预售、网签、登薄、挂牌、评估、交易、抵押、变更、公证等全生命周期运营数据；为涉及到不动产信息的政府部门、金融机构、社会组织提供信息查询、验证、业务办理等存证与验证服务，最终形成一套按时间为轴的全融合账本。实现不动产登记业务管理部门数据打通、数据实时准确、数据共享、安全确权、不可篡改、可追溯、优化流程、提高效率、业务融合的成长性不动产全生命周期服务平台。（如图 10-3 ）

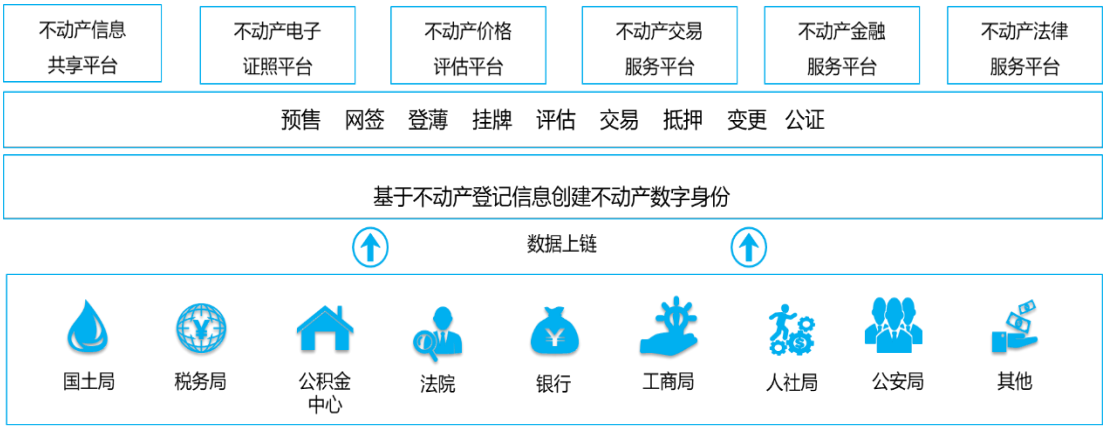

图 10-3 “区块链+不动产”全生命周期服务平台

基于区块链技术实现不动产数字身份管理以及基于数字身份的自主权数据管理，典型场景说明如下：

1）不动产产权登记与交易

不动产登记存在问题包括：信息共享与更新机制缺乏，基础数据一致性、准确性、权威性欠缺，房屋登记纳税监管存在漏洞，居民办事跑路多，以及房屋交易过程“阴阳合同”无法彻底解决。房地产交易市场在交易期间和交易后的流程中，存在缺乏透明度、手续繁琐、欺诈风险、公共记录出错等问题。

房产欺诈对全球房产所有者都已经造成风险。根据美国土地产权协会数据，所有交易过程中房产的产权有 25%存在瑕疵。任何瑕疵在其被修正之前，都会导致将财产所有权转让是非法的。这意味着业主通常要缴纳高额法律费用，以确保其财产的真实性和准确性。据报道，2015 年美国与房产欺诈相关的损失平均为约 103,000 美元。

基于区块链的不动产数字身份管理可实现对土地所有权、房契、留置权等信息的记录和追踪，并确保相关文件的准确性和可核查性。从具体的操作上看，区块链技术在房屋产权保护上的应用，可以减少

产权搜索时间，实现产权信息共享，避免房产交易过程中的欺诈行为，提高房地产行业的运行效率。

中国银行香港（BOCHK）在 2018 年中期表示，已经使用区块链平台处理 85%的房地产评估。过去，银行和房地产评估师必须交换传真和电子邮件，以生成和交付实物证书。现在，这个过程可以在几秒钟内在区块链上完成。

2）不动产租赁与物业管理

物业管理非常复杂，涉及许多利益相关者，包括房东，物业经理，租户和供应商。大多数房产租赁目前要么通过线下人工书面文件进行管理，要么通过多个互不兼容的软件程序进行管理。基于区块链数字身份可以实现从房屋历史信息追溯，到签署租赁协议，到管理现金流量，到提交维护请求的整个物业管理流程，以安全透明的方式进行。

10.1.3 知识产权及物权数字身份应用

1）知识产权数字身份应用

2019 年 11 月 24 日，中共中央办公厅、国务院办公厅联合发布《关于强化知识产权保护的意见》（以下简称“意见”）。

《意见》是第一个以中共中央办公厅、国务院办公厅名义出台的知识产权保护工作纲领性文件，将以前所未有的力度推动我国知识产权保护能力和保护水平全面提升。《意见》明确，地方各级党委和政府要落实知识产权保护属地责任，各地区各部门要加大对知识产权保护资金投入力度，并将知识产权保护绩效纳入地方党委和政府绩效考核和营商环境评价体系。《意见》提出要不断改革完善知识产权保护

体系，综合运用法律、行政、经济、技术、社会治理手段强化保护，促进保护能力和水平整体提升。

基于区块链技术为知识产权创建数字身份，将延伸知识产权整体保护的形式，明确知识产权的绝对归属。传统知识产权登记从成品环节开始，对成品之前的诸多环节缺少保护。区块链技术可以帮助知识产权实现成品之前环节上链，记录知识产权的形成过程，进而为知识产权鉴权提供更加丰富的依据。

基于区块链的知识产权数字身份管理将贯穿知识产权的形成、鉴权、验证、转让、仲裁、司法执行的全过程。（如图 10-4 ）

图 10-4 知识产权的数字身份管理

传统的版权登记流程至少需要一个半月时间，与数字内容创作和流通短平快的特性不相匹配。利用数字身份管理，将文化产业链条中的各环节加以整合，加速流通，能够有效缩短价值创造周期。通过区块链技术，对作品进行鉴权，证明文字、视频、音频等作品的存在，保证权属的真实、唯一性。作品在区块链上被确权，后续交易进行实时记录，实现文娱产业全生命周期管理，也可作为司法取证中的技术

性保障。

2）物权数字身份应用

物理资产，比如车辆等实物资产，基于资产上链的理念为资产创建数字身份，并实现资产的生产、采购、维修、转让、报销等全生命周期管理，实现完整信息的真实追溯。例如，雄安“千年秀林”项目，通过雄安森林大数据系统，为每颗树基于二维码创建专属“身份证”，实现从苗圃到种植、管护、成长的可追溯的全生命周期管理。

10.2 公民信用积分体系建设

10.2.1 个人公民诚信体系建设

为了加快社会信用体系建设，国家颁发了《社会信用体系建设规划纲要（2014-2020 年）》（以下简称《纲要》），在《纲要》中提出了进一步加快个人诚信记录建设，健全跨地区跨部门跨领域的守信联合激励和失信联合惩戒机制，使守信者受益、失信者受限，营造“守信光荣、失信可耻”的良好社会氛围。

作为社会主义核心价值观的重要内容，诚信是公民基本道德规范，是社会主义市场经济的重要基础。社会诚信是指在整个社会生活中逐渐形成的诚实守信的社会风气。社会诚信的形成不仅包括个人诚信，还包括在社会生活中被广泛认可的道德及规则。社会信用体系建设需要设计出一种能反映人们在诚信道德领域的数据模型，依据标准化数据、数字化各种诚信荣誉、使用矩阵化模式对海量信用信息进行收集、转化和大数据分析并重构为“个人的数字画像”。

调动各界力量对信用状况良好的市民实施守信激励，全面提升群众对社会信用体系建设获得感，营造诚实守信的社会氛围，是推出信用分激励场景的初衷所在。信用积分体系在常规的法律和行政手段之外，创建了道德规范层面的奖惩措施，是社会信用治理领域的创新。

2020 年 1 月 1 日正式实施的《大连市文明行为促进条例》（以下简称《条例》）及其提出的“文明行为信用积分”，是把道德要求贯彻到法治建设中，以法治承载道德理念的重要实践。

把社会主义道德要求体现到立法、执法、司法、守法之中，以法治的力量引导人们向上向善，是制定《条例》的应有之意，也是常态化长效化推进文明城市建设的重要保障。《条例》对见义勇为、志愿服务、慈善捐赠、捐献救人以及紧急救助等行为，细化了鼓励与支持措施;《条例》将养犬扰民、车窗抛物、机动车不礼让行人、驾驶中使用电话、行人闯红灯等群众反映突出的重点不文明行为纳入条例中，以形成文明行为规范。《条例》还将践行绿色、低碳、环保、健康的生活理念，从源头减少生活垃圾的产生量，主动做好垃圾分类等文明生活行为规范写入法规。

与行政相对人的数字身份相结合，基于区块链实现信用积分的获取、使用、修复、共享、披露的全周期管理。其中信用汇总积分作为公共数据，在政府信用门户网站可公共查询；信用详细数据属于个人隐私，需要建立安全保护机制以及授权查看机制。

信用积分将与行政相对人的公、检、法、司等相关部门的遵纪守法数据，政府各部门的行政管理信息的大数据，以及在日常生活或商

务场景中的履约情况，进行智能分析，形成综合信用评价。

在数字政务或者社会信用体系建设领域，个人信用评价有更丰富的内涵。传统金融领域的个人信用评分模型，选用了与个人信用相关的四十多个变量，概括起来可分为个人基本信息、银行信用信息、个人缴费信息、个人资本状况四类变量。金融领域的信用评估体系目标是为了通过历史信息预测未来风险，用于未来开展金融业务，特别是信贷业务，提供决策参考。金融领域的个人信用评分重在风险防范，其评分依据的事实性、精确性、和公平性要求不高。

数字政务与社会信用体系建设领域的公民个人信用评价，使用矩阵化模式对海量信用信息进行收集、转化和大数据分析并重构为“个人的数字画像”，目的在于加大对诚实守信主体激励和对严重失信主体惩戒力度，形成褒扬诚信、惩戒失信的制度机制和社会风尚。政务领域的公民个人信用评价应用于信用联合奖惩，对评价依据的事实性、公正性、和可解释性要求很高。任何信用评价的事实性差异都有可能导致行政复议，甚至行政诉讼。

数字政务与社会信用体系建设领域的公民个人信用评价模型的相关变量可能会达到数千个，归结起来可以分成如下六个方面：个人司法信用、个人行政信用、个人金融信用、个人职业信用、个人日常信用、公民信用积分。公民个人信用评价结果将应用于社会信用分级分类监管与应用。（如图 10-5 ）

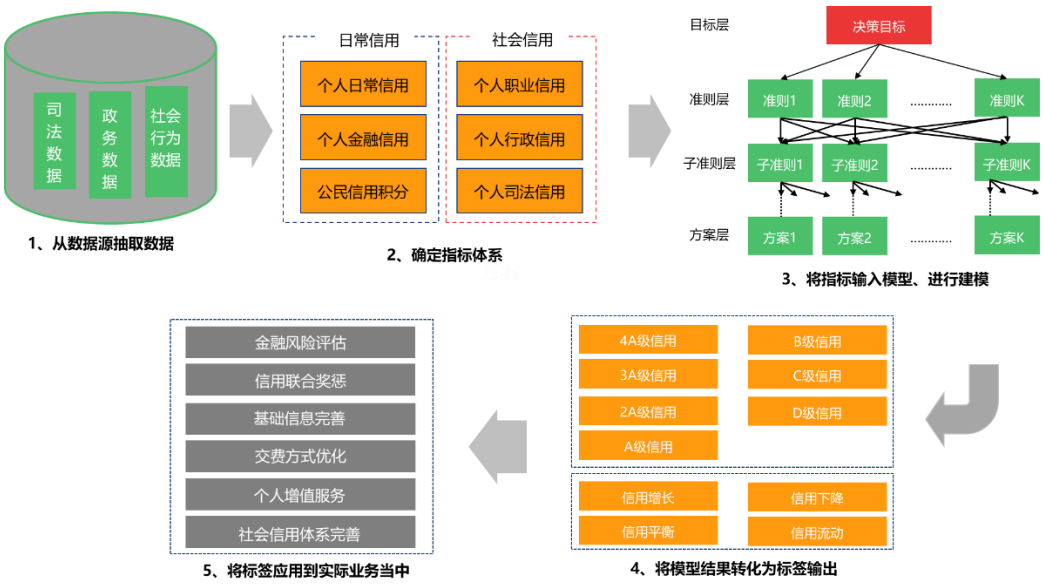

图 10-5 公民个人信用评价模型

10.2.2 中小企业信用分析与“信易贷”

2019 年 9 月 12 日，为认真贯彻落实习近平总书记在民营企业座谈会上的重要讲话精神，按照党中央、国务院关于解决中小微企业融资难融资贵问题的一系列具体部署，国家发展改革委、银保监会联合印发《关于深入开展“信易贷”支持中小微企业融资的通知》（发改财金〔2019〕1491 号，以下简称《通知》）。

《通知》从信息归集共享、信用评价体系、“信易贷”产品创新、风险处置机制、地方支持政策、管理考核激励等方面提出具体措施，破解银企信息不对称难题，督促和引导金融机构加大对中小微企业信用贷款的支持力度，缓解中小微企业融资难融资贵问题，提高金融服务实体经济质效。《通知》强调要建立“信易贷”工作专项评价机制，并从金融机构和地方政府两个维度开展评价。金融机构评价结果纳入小微企业金融服务监管考核评价指标体系，地方政府评价结果纳入城市信用状况监测。

区块链技术为“信易贷”提供了支撑技术手段。基于企业法人的区块链数字身份，整合税务、市场监管、海关、司法以及水、电、气费，社保、住房公积金缴纳等领域的企业信用信息，“自上而下”打通部门间的“信息孤岛”，降低银行信息收集成本。构建符合中小微企业特点的公共信用综合评价体系，将评价结果定期推送给金融机构，提高金融机构风险管理能力，减少对抵质押担保的过度依赖，逐步提高中小微企业贷款中信用贷款的占比。

将“信易贷”违约风险处置机制与社会信用联合奖惩结合起来，对失信债务人开展联合惩戒，严厉打击恶意逃废债务行为，维护金融机构合法权益。充分发挥信用手段在缓解中小微企业融资难融资贵问题中的重要作用。

图 10-6 给出了基于区块链数字身份实现中小企业综合信用评价，以及通过自主权数据管理与金融机构共享数据的“信易贷”平台模型。

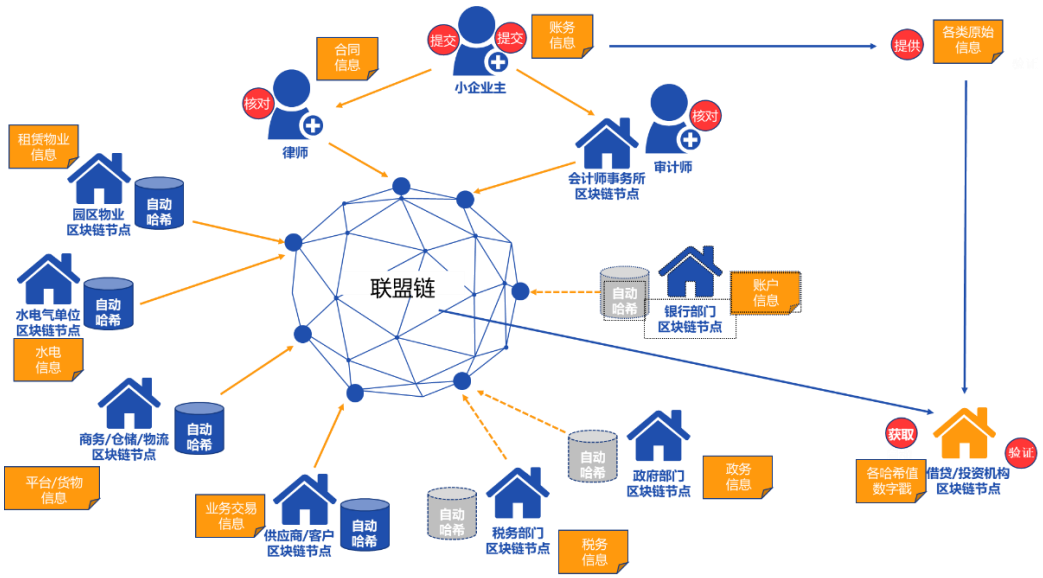

图 10-6 “信易贷”区块链平台模型

10.3 区块链业务过程管理

区块链的不可篡改、全历史记录的特质显著增加了造假的成本，为审计、审查、业务过程管理工作提供了便利。传统审计工作会消耗大量资源在收集信息、分析数据、判断问题严重性以及形成客观公正的结论上，而时间滞后性和覆盖范围的局限性容易影响审计结果的准确性。区块链以时间戳的形式在特定时间点固化凭证，在确保信息真实、完整方面能节省大量的工作资源。结合上数据智能和物联网技术，区块链在业务过程管理上具有丰富的应用场景。

10.3.1 数字发票解决方案

统计数据显示，2017 年我国电子发票开具量达 13.1 亿张，预计到 2022 年将可能高达 545.5 亿张，保持超过 100%的年均增长速度。相对纸质发票而言，电子发票在发票开立、申报、留存和成本等多方面有着诸如优点，比如实时性、交互性、低成本和易存储等。然而，电子发票行业共享难、流转难、归集难、查验难等现象成为行业发展“绊脚石”。其中比较典型的例子就是重复报销问题。因为电子发票是以电子文件的形式存在的，具有数据复制的完全无差异性，所以电子发票很难确权，常常导致电子发票重复报销的问题。当前，这一问题主要通过管理手段辅助解决，但并不能完全杜绝此类问题的发生。

区块链技术应用于数字发票系统，可以具备以下几个方面优势：

- 确权：确保电子发票信息在产生和存储过程中的唯一性，实现确权认证；
- 真实：企业或个人电子发票上的数据信息在产生和存储过程中

无法伪造、不可篡改，确保数据真实；

- 信任：基于区块链的加密算法、共识算法等机制从技术层面上建立起不同企业、机构和个人各方之间的信任。

税务机关、第三方技术服务机构和企业共同搭建数字发票区块链平台，对数字发票的开具、流转、报销和存档全流程进行管理，实现了平台之间的数据共享和互联互通，解决了传统电子发票系统的监管困难和重复报销等问题。（如图 10-7 ）

- 税务机关、财政部门、审计部门等作为监管部门加入区块链，统一制定区块链的运行标准和合约条件，负责对系统的运行和制度进行监督；
- 第三方技术服务商在税务机关授权 CA 证书的情况下，加人区块链作为电子发票产生节点。作为区块链发票生产者，第三方服务商负责将开票企业接入到区块链系统。在电子发票产生的过程中，第三方服务商需要使用自己的私钥对数字发票数据进行加密和签名，以保证数字发票的唯一性；
- 企业作为发票报销入账的发起者，通过第三方服务商系统向区块链发起报销入账请求操作。第三方服务商在区块链中查询相关电子发票信息，实现入账报销操作；
- 第三方服务商可向社会公众提供查验接口，以获取区块链上的发票数据。

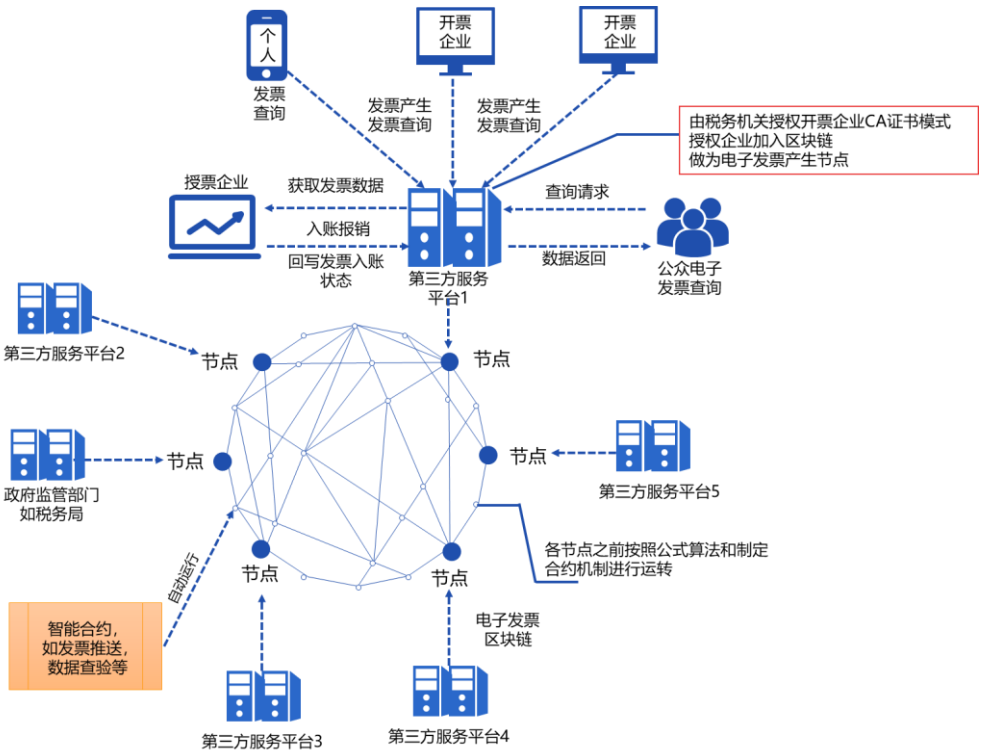

图 10-7 区块链数字发票平台

10.3.2 政府采购解决方案

2018 年，我国政府采购规模高达 35861.4 亿元，但当前政府采购行业出现高速发展与信息化程度不匹配的问题值得关注。政府采购目前存在的痛点和问题如下。

首先，政府采购信息零散化和碎片化现象仍然突出。一是平台分散化，未实现财政部平台、各中央集采机构平台、各地公共资源交易平台、各专业网站平台的信息共享；二是信息碎片化，2015 年实施的《政府采购法实施条例》对信息公开内容进行了约束和规范，但是，实际落实并不统一，目前对于信息公开的不规范尚属“民不举官不究”的状态；三是数据利用不充分，行业相关数据目前仍主要用于基本信息统计，针对产业、产品和交易数据的数据整合和挖掘做得不够。

其次，标准化建设不健全。当前，我国政府采购行业标准化还处

于内容层面，2017 年发布的《政府采购货物和服务招标投标管理办法》（财政部令第 87 号）中对公开招标和邀请招标的招标公告、资格预审公告、结果公告的内容进行了规范。《政府采购非招标采购方式管理办法》（财政部令第 74 号）规范了非招标采购方式的相应内容。以《政府采购法实施条例》规定的合同公告为例，目前合同公告仍存在上传不及时甚至漏传、不传现象，上传的数据格式也未统一，有的是影印件，有的是电子件（其中也分 doc 和 pdf 格式）。供给侧的产品数据信息同样在各厂商间未形成共识，整合难度较大。

再次，安全性存在隐患。中国将加快加入《政府采购协定》(GPA)进程。因此，政府采购将来面向外国开放后，数据信息必将面对安全挑战。此外，法律明确保密的采购评审环节的泄密时有发生，甚至有厂商依据窃密取得信息进行投诉质疑，泄密源头无从追溯。

最后，在各类政府采购程序中，公开招标占了全国政府采购规模的 70.5%（2018 年数据）。公开招标程序中，招标周期长，浪费大量资源;招标代理机构操控招标结果,导致国家财务损失;招标人串标、围标现象时有发生;投标文件约 1/3 的内容是进行投标企业的资质认证，且需要盖大量公章进行信息确认，招标单位资质和业绩造假问题无法甄别;评判专家人为影响招标结果,招标监管缺乏直接有效手段。招投标领域违规惩处措施不强，腐败现象和违规手段层出。

区块链+政府采购服务平台充分利用区块链、人工智能、大数据技术，严格按照政府采购管理规定、流程及相关制度和实施办法，将政府采购的全生命周期数据添加进基于区块链技术的信息共享平台中

存证。这样既可以实现多部门多级别间的数据共享，又可实现降低信任成本和数据可追溯，大大提高了政府采购行业信息的范围和效率。从根本上杜绝人为参与影响，最大限度保障政府采购的公开、公正，公平、透明。（如图 10-8 ）

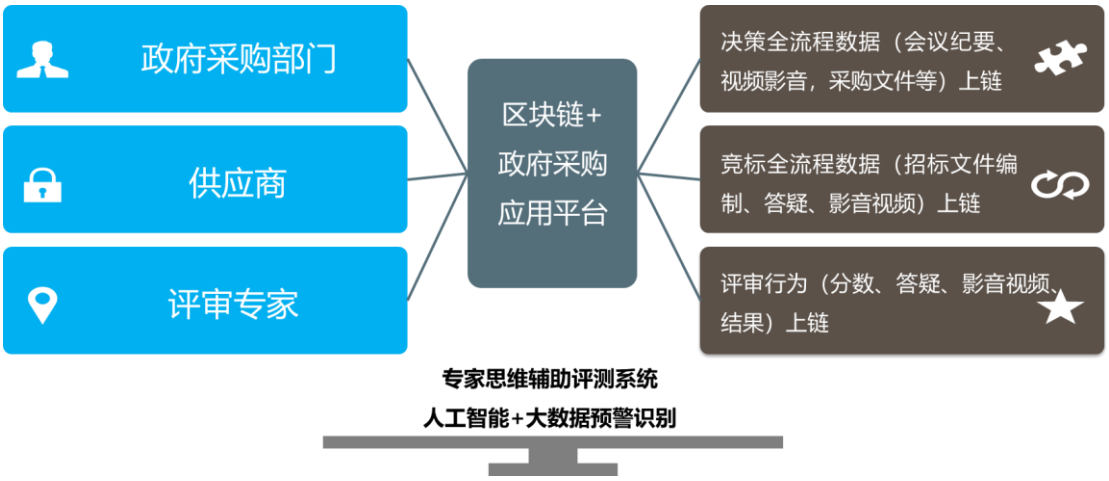

图 10-8 区块链+政府采购服务平台

针对传统招标和电子化招标存在问题，在电子化招标平台基础上充分利用区块链、人工智能、大数据技术，严格按照招投标法规、制度和实施办法、融入形成计算机“算法规则”，打造创新型基于区块链技术的招投标应用平台，实现如下功能：

- 招标行为及招标文件上链：招标决策全流程（会议纪要视频影像资料等）上链，监管部门随时可查；对招标文件关键条款的设置自动进行合理分析；同时增加异地专家辅助论证功能，并将论证意见上链；根据项目注册信息，匹配对应招标文件模板，并对招标文件上链。
- 招标代理机构行为上链：将代理机构行为（包括招投标文件编制过程、答疑、开标过程代理机构工作人员视频影像资料等）

数据上链，监管部门、社会监督委、投标人可以随时查阅并监督，督促招标代理依法依规操作，杜绝违规操作行为。

- 评标专家行为数据上链：评标专家行为（包括评标室的视频音频，专家个人视频，音频，专家个人电脑操作等）上链；评标结果上链；增加专家思维辅助评测系统，对评标专家评分的合理性进行分析。可实现评标专家公开、公平、公正开展评标工作，有效防止评委操控评标结果。
- 人工智能+大数据识别围标串标：对投标文件编制源头进行识别，分析同一项目投标文件关联度和相识度；利用大数据分析投标人与投标人之间关系，加强对围标，串标的识别和预警提示，便于监管部门严厉打击和查处。
- 开放金融服务接口：可接入金融机构与企业合作，可实现一次业务授信，循环额度使用，持续为投标企业业务拓展补充资本金，壮大投标企业核心竞争力。

基于区块链技术实现政府采购全流程监管到位，最大限度减少人为干扰和影响，杜绝串标、围标等违法、违纪情形发生，预计每年可以为国家节约 8—10%的财政支出。区块链技术能够实现招投标全程信息无盲点，清晰透明可追溯。同时能够帮助主管和监管机构对招标主体进行信用评级，真正意义上实现择优选择，引导良性竞争机制，形成健康有序的市场。

雄安新区已经在政府管理中引入大数据、区块链技术，对工程建设投标过程中的每一项决策，进行全过程信息留档，作为证据随时可以

调取查看，出现问题依法问责。

10.3.3 “区块链+物联网”政务应用

政府利用物联网，对公共资产实现统一管理，或对需要进行安全管理的有形商品（如危化品等）进行跟踪溯源。区块链技术应用在资产管理、防伪溯源领域的逻辑在于过程数据不可篡改和加盖时间戳，需要与物联网技术紧密结合。

公共资产管理系统结合区块链、物联网技术，可实现公共资产的采购、使用、升级的自动化及在线监管，提高公共资产管理的透明度，控制行政管理成本。例如公车的使用情况可在线实时查询监控，增加违规使用成本。

防伪溯源系统利用物联网技术建立起链上数字证明和链下实物商品的严格对应关系，利用区块链技术将物品流通全链条的信息输入权分散到多个机构或设备手中，大大提高造假成本、降低造假风险，实现透明公开的全流程信息管理管控。

10.3.4 人事档案及其他应用

1）干部人事档案管理

干部人事档案是干部管理的重要基础信息，各政府单位都有档案室，建有档案管理系统，能够方便查到干部的出生、籍贯、工作履历等综合信息。违法更改个人人事档案的事件屡有发生，如修改个人出生日期、修改工作经历、修改民族、修改学历等问题。现有人事档案管理方式不能完全杜绝人事档案修改作假。

应用区块链技术，通过区块链记录每个干部的出生日期、任职履

历等基础信息，形成无法篡改的个人电子档案，从技术上彻底解决传统干部档案管理中存在的问题和积弊。一旦干部档案信息经过验证并添加至区块链后，就会永久的存储起来，为干部人事档案的准确、完整提供了技术保障。

2）民政部门：扶贫与公益慈善项目监督

利用区块链技术全程记录、顺序时间戳、不可篡改、可追溯等特性，将扶贫的场景中的贫困人口识别、资金、管理、监督、政策等各个环节纳入区块链管理系统。通过将传统的人员管理方式与区块链技术应用有机结合，让扶贫基金沿着规定的用途、使用条件、时间限制等使用规范安全、透明、精准地投放使用。将传统的扶贫资金层层摊派改为针对项目、个人定向投放。

区块链上存储的数据，高可靠且不可篡改，天然适合用在社会公益场景。公益流程中的相关信息，如捐赠项目、募集明细、资金流向、受助人反馈等，均可以存放于区块链上。在满足项目参与者隐私保护及其他相关法律法规要求的前提下，有条件地进行公开公示，方便公众和社会监督，助力社会公益的健康发展。

3）教育部门：学历信息、学术成果存证

利用区块链技术，解决现有的学生信用体系不完整、数据维度局限、缺乏验证手段等问题，简化流程和提高运营效率，并能及时规避信息不透明和容易被篡改的问题。在区块链中记录跨地域、跨院校的学生信息，追踪学生在校园时期的行为记录，构建良性的信用生态体系。此外，通过区块链为学术成果提供不可篡改的数字化证明，可为

学术纠纷提供举证依据，降低纠纷事件消耗的人力与时间成本。

第十一章 数字金融

11.1 区块链在银行领域的应用

11.1.1 区块链在支付清算中的应用

在实践中，跨境支付的结算时间可长达五天，费用和结算时间的明确性不足。而跨境支付中的成本一般会转嫁给终端用户。区块链技术能够在收付款人之间直接连接，降低跨行、跨境交易复杂性和成本，确保交易记录透明、不可篡改，降低运营风险，优化现有代理行模式下的资金转移和信息传递方式，大大提高支付效率，降低业务成本。[16]

案例 11-1：JP Morgan 基于区块链的创新——IIN

银行间信息网络（IIN）是金融服务业中最大的区块链项目。截至 2019 年 9 月，德意志银行加入 INN 为止，已有超过 65 家银行在该系统上投入使用，另有 255 家银行签署了意向书。IIN 的目标是通过向支付链中的每家银行即时提供有关转账的信息，以减少支付的延迟和成本。

IIN 于 2017 年 10 月份开始试运行。在此之前，跨境结算代理银行只进行单向银行间的沟通。区块链改变了这种互动方式。当付款明细被标记为需要确认时，不同的参与方可以同时进行交互，请求和共享付款信息。

IIN 将会提高客户体验，降低支付所需的时间量和成本——从数周减少到数小时。区块链分布式账本允许被许可的银行交换有关合规检

[16] 中国工商银行城市金融研究所研究报告，分布式账本技术在支付清算领域的应用前景研究，2018.03.

查和其他妨碍完成付款的例外情况的信息。IIN 也尝试用作银行分享客户识别（KYC）信息的平台。

案例 11-2：JP Morgan 基于区块链的创新——JPM Coin

2019 年 2 月 14 日 JPMorgan 宣布推出 JPM Coin。[17] JPM Coin 本质上是一个锚定美元的数字货币。当摩根大通的客户将存款存入一个指定账户时，可以获得等量的 JPM Coin；获得 JPM Coin 的客户可以通过区块链网络与摩根大通的其他客户进行点对点的交易；JPM Coin 的持有者可以在在摩根大通随时兑换美元。

根据 JPM Coin 的白皮书，JPM Coin 有三个典型应用场景。

第一，针对大型企业客户的国际支付。目前这种支付通常在金融机构之间进行电汇。由于金融机构有交易截止时间，不同国家可能使用不同的交易系统，经常需要一天以上的时间进行结算。而通过 JPM Coin，付款将会实时结算，并且可以选择在一天中的任意时间进行结算。

第二，跨境证券交易。摩根大通在区块链平台上测试了一次债券发行，为一家加拿大银行创建了一个 1.5 亿美元存单的虚拟凭证。通过传统方式使用电汇购买债券，从支付到处理存在时间差。而通过 JPM Coin，这一切都可以瞬时完成。

第三，替代大型企业在全球分支机构所持有的美元现金。全球性公司，例如霍尼韦尔和 Facebook 等公司，基于美元转账支付全球员工薪资和供应商货款等。在大型企业的不同分支机构中，资金流动造成

[17] J.P. Morgan Creates Digital Coin for Payments[OL], https://www.jpmorgan.com/global/news/digital-coin-payments , 2019.02.

了很多不必要的效益损失。使用 JPM Coin 而非现金转账，将减少许多不必要跨境服务费用。

11.1.2 区块链在贸易金融中的应用

贸易金融是商业银行在贸易双方债权债务关系的基础上，为国内或跨国商品贸易和服务贸易提供的贯穿贸易活动整个价值链的全面金融服务，它是金融市场与实体经济相互促进的纽带。贸易金融体系的五个主要功能，即贸易结算、贸易融资、信用担保、避险保值、财务管理。贸易金融的核心是贸易融资，信用证、托收、汇款是贸易融资的三种基本结算方式。近年来，企业对贸易金融服务的需求已经超越简单的融资和结算，希望银行能基于企业经营交易特点，提供集流动性支持、营运资金调度、财资管理为一体的“交易银行”服务，提高资金使用效能。

区块链贸易金融是指银行基于区块链技术实现贸易金融业务在联行间的实时传输、自动触发和全流程监控，并能够确保传输信息的真实性和不可篡改性。

案例 11-3：民生银行基于区块链打造国内信用证

传统的国内信用证业务并没有较好的信息传输机制，当前主要采用信开和 SWIFT 加押电文的方式，没有直接信息交互通道；同时由于业务流程较为复杂，各金融机构的信息系统架构、安全标准、网络控制机制不一致，导致信用证流转效率低下，难校验，业务流程不透明。

2017 年 7 月，中国民生银行推出了基于区块链的国内信用证信息传输系统（BCLC），改变了银行传统信用证业务模式。该系统目前已

有民生银行、中信银行、苏宁银行等多家银行接入。

信用证的开立、通知、交单、承兑报文、付款报文各个环节均通过该系统实施，缩短了信用证及单据传输的时间，报文传输时间可达秒级，大幅提高了信用证业务处理效率，同时利用区块链的防篡改特性提高了信用证业务的安全性，使信用证流转过程更加透明可追踪，各个节点都能看到整个信用证业务的办理流程和主要信息，比传统信用证业务更透明和高效，避免错误和欺诈的发生。（如图 11-1 ）

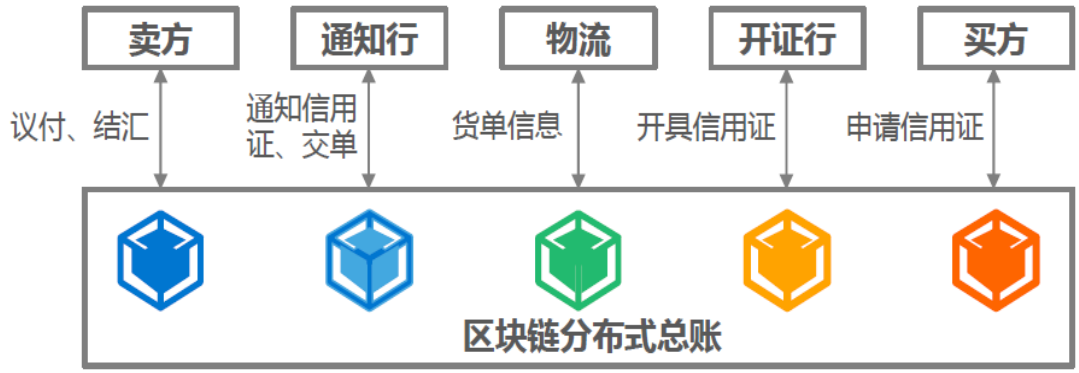

图 11-1 基于区块链的国内信用证信息传输系统

基于区块链实现国内信用证业务，可以满足客户对高效结算融资服务需求，进一步缩短全业务流程，全面提升客户的业务体验。客户只需上传标准化的开证申请书，引入影像切片集中录入，操作便捷，无需将纸质材料多个角色间流转，全线上电子化处理。

对银行而言，国内信用证业务经济资本仅占用 20%，优化后的信用证业务流程将使得客户相比银行承兑汇票等更愿意使用国内信用证，在提升业务风险控制能力的同时降低对银行的经济资本占用。

未来，可将同业银行、运输公司、保险机构、税收部门、监管机构等纳入区块链网络，完成全新信任机制，由点及面、快速拓展的链式

网络的搭建，自主扩展业务产品，及最终构建兼具跨行结算和融资功能的完整交易平台。

案例 11-4：邮储银行 U 链福费廷业务系统

福费廷业务是银行根据客户或其他金融机构的要求，在开证行、包买行或其他指定银行对信用证项下的款项做出付款承诺后，对应收款进行无追索权的融资。福费廷业务凭借其独特的优势得到银行青睐，迅速取代了传统出口押汇和国内信用证卖方押汇/议付的市场地位。

在福费廷业务中，卖方银行通常在信用证项下买断受益人对开证行的债权，自行持有或在二级市场进行转卖。因为有开证行的承兑或承付，所以对买入福费廷的银行来说属于低风险业务。但福费廷业务也存在一些风险隐患，特别是在涉及司法纠纷时，其法律适用的不确定性一定程度上影响到银行资产的安全，必须对其潜在风险予以充分关注。

近年来，企业伪造虚假贸易背景的手段越来越隐蔽，部分企业借贸易融资之名，骗取银行融资进行投机。近期我国经济呈现下行态势，部分大宗商品价格剧烈波动，贸易背景真实性屡受质疑，企业资金链紧绷甚至断裂。在此背景下，福费廷融资的风险转移功能难以完全发挥。 例如，企业资金链断裂势必影响银行风险防控工作质效。

邮储银行基于区块链技术开发了 U 链福费廷业务系统。实现信用证从开具到承兑全流程链上跟踪，并建立“福费廷区块链系统交易市场”，能够有效撮合金融机构间交易，建立一个基于区块链的让渡报文通知模式。邮储银行 U 链福费廷业务系统实现了信用证产生的项下

议付、福费廷等融资业务的区块链业务系统。该系统具有追溯精度优化、去中心化、强隐私安全、去信任中介等特点。U 链福费廷业务系统提高了一级市场的业务审单效率，减少人工判断失误；为业务提供增信，降低业务风险；打通信用证的一级市场与二级市场，完成从信用证至福费廷业务的信息共享，实现了福费廷业务处理流程的衔接及优化。

U 链福费廷业务系统已于 2018 年 6 月底上线，该系统实现了交易双方无需线下协调，可在线上交易市场发布收证意向及包买意向，有效撮合交易。该系统在处理福费廷业务时，受益人（企业、债权持有行）可以将债权直接转卖，与信用证开证行、包买银行达成三方共识，完成债权让渡。在债权让渡、单据凭证等智能合约的帮助下，该系统支持三方就数据一致性的理解以及历史业务资料进行共享。二级市场能够获取一级市场数据以及历史包买银行的业务审查背书，使得债权让渡能够快速衔接一级市场，有效提升业务效率。U 链福费廷业务系统进一步完善了银行服务模式，加快向现代化商业银行转型的步伐。

11.1.3 区块链在供应链金融中的创新

银行供应链金融业务包括票据业务以及基于供应链的信用融资业务，这两项业务因人为介入多，产生了许多违规事件及操作风险。

1）票据业务

2015 年中，国内开始爆发票据业务的信用风暴。票据业务在创造了大量流动性的同时，相关市场也滋生了大量违规操作或客户欺诈行为，陆续有多家商业银行的汇票业务事件集中爆发。

国内现行的汇票业务仍有约 70% 为纸质交易，操作环节处处需要人工，并且因为涉及较多中介，存在管控漏洞，违规交易的风险很高。票据的交易一直存在第三方的角色来确保有价凭证的传递是安全可靠的。在纸质票据交易中，交易双方的信任建立在票据的真实性基础上；即使在现有的电子票据交易中，也需要通过央行 ECDS 系统的信息进行交互认证。

但借助区块链的技术，可以直接实现点对点的价值传递，不需要特定的实物票据或是中心系统进行控制和验证；中介的角色将被消除，也减少人为操作因素的介入。在数字票据领域，可以通过区块链搭建票据交易系统，让每个参与交易的企业都登记注册为区块链的用户，可以提升票据运转效率和流通性，降低交易风险，有利于中小企业的信用积累。

2017 年，中国人民银行基于区块链技术建立的数字票据交易平台（上海票交所）已经成功完成测试。

2）供应链金融业务

供应链金融也因为高度依赖人工，在业务处理中有大量的审阅、验证各种交易单据及纸质文件的环节，不仅花费大量的时间及人力，而且各个环节都有人工操作失误的可能。

区块链技术可以帮助供应链金融业务大幅减少人工的介入，将目前通过纸质作业完成的程序数字化。所有参与方（包括供货商、进货商、银行）都能使用一个分布式共享账本分享文件，并通过智能合约在预定的时间和达到预期结果时自动进行支付。这将极大地提高效率

及减少人工交易可能造成的失误。

基于区块链的数字化解决方案能够完全取代现今的纸笔人工流程，实现端到端完全的透明化，提高处理的效率并减少风险。

案例 11-5：浙商银行“应收款链平台”

2017 年 8 月 16 日，浙商银行推出业内首款基于区块链技术的企业“应收款链平台”，在平台上应收账款可转化为电子支付结算和融资工具。浙商银行是业内首家将区块链技术应用于应收账款融资的商业银行。

企业可通过应收款链平台签发、承兑应收账款，将账面的应收账款转变为安全、高效的支付结算工具，盘活应收账款，减少对外负债；围绕核心企业，银行机构为应收账款流通提供信用支持；上游企业收到应收账款后，可在平台上直接支付用于商品采购，也可以转让或质押应收账款盘活资金，方便对外支付和融资。

浙商银行应收款链平台可以提供单一企业、产业联盟、区域联盟等多种合作模式，助力企业构建供应链“自金融”商圈。

- 单一企业商圈，由集团企业发起建立、成员企业和供应链上下游企业共同参与，在商圈内办理应收账款的签发、支付、融资等业务，并可以转让至圈外机构，增强流动性。
- 产业联盟商圈，由核心企业发起建立、产业链上下游企业和联盟成员共同参与，从下游客户签发应收账款开始，在物流中无缝嵌入资金流，减少联盟成员外部融资和资金沉淀。
- 区域联盟商圈，由区域内龙头企业发起、其他加盟企业参与，

延伸到各加盟企业的供应链上下游客户，根据真实交易和商业信用签发应收账款，在联盟内进行转让、融资等。

应收款链平台上线一年时间内，浙商银行已开通核心企业应收款链平台 1111 个，辐射客户 4672 户，累计签发区块链应收款 40373 笔，签发金额 902 亿元，服务的客户中民企的数量和融资金额均占绝大部分。

11.1.4 区块链助力客户识别与征信

银行的客户征信及法律合规的成本不断增加。过去几年，商业银行为了满足日趋严格的监管要求，不断投入资源加强信用审核及进行客户征信工作，以提升反欺诈、反洗钱能力，抵御复杂金融衍生品过度交易导致的系统性风险。因此，征信市场的空间巨大。但目前整个行业信息不能共享，无法挖掘更大的价值。究其原因，跨领域、跨行业、跨机构，用传统技术实现大量信息共享难度大成本高，同时还存在数据易被篡改、无法追溯、难以实时同步等问题。

针对目前我国传统征信行业的现状与痛点，区块链可以在征信数据共享交易领域着重发力，实现面向相关各行各业的数据共享交易，构建基于区块链的征信数据共享交易平台，使参与交易方风险和成本最小化，加速信用数据的存储、转让和交易。

记载于区块链中的客户信息与交易记录有助于银行识别异常交易并有效防止欺诈。区块链的技术特性可以改变现有的征信体系。在银行进行“客户识别”（KYC）时，将有不良记录客户的数据储存在区块链中。客户信息及交易记录可以随时更新，并同时在客户信息保护法

规的框架下，实现客户信息和交易记录的加密关联共享，帮助银行能省去许多 KYC 的重复工作。银行也可以通过分析和监测在分布式共享账本内客户交易行为的异常状态，及时发现并消除欺诈行为。

区块链能帮助用户确立自身的数据主权，生成自己的信用资产。在数据与信用确权的基础上，以用户数字身份作为数据聚合点，连接各个企业及公共部门，进而开展用户数据授权，不但可以解决数据孤岛的问题，而且能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，大大降低征信运营成本。

区块链征信平台有助于征信机构以低成本方式拓宽数据采集渠道，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。区块链可以使信用评估、定价、交易与合约执行的全过程实现自动化运行与管理，从而降低人工与柜台等实体运营成本，大幅提高银行信用业务处理规模。

案例 11-6：KYC 数据共享

苏宁金融于 2018 年 2 月上线金融行业区块链黑名单共享平台系统，将金融机构的黑名单数据加密存储在区块链上，实现了无运营机构的分布式黑名单共享模式，及解决了行业痛点，又保护了客户的隐私和金融机构的利益。（如图 11-2 ）

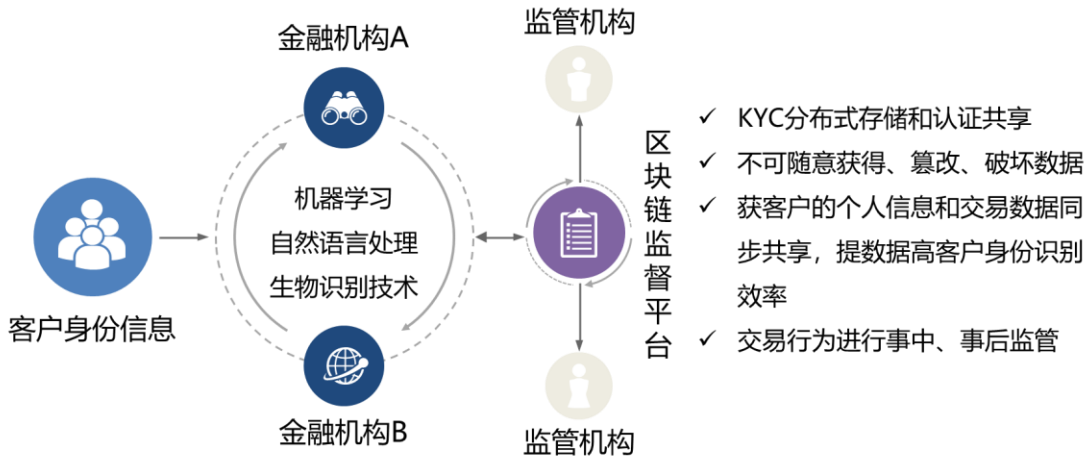

图 11-2 基于区块链的 KYC 数据共享平台

案例 11-7：农行在普惠金融领域的应用创新

长期以来，小微企业、“三农”客户融资难、融资贵的问题一直制约着企业的发展。其问题根源在于抵押品不足、信用数据匮乏，难以对这类客户建立有效的信用模型和风险防控措施。

农业银行通过积极推动传统信贷产品的线上化改造和基于区块链、大数据技术的新型网络融资产品创新，依托产业链上下游的经营、交易和财务等数据，探索建立多维度信用评价模型开展纯信用的网络融资业务。逐步实现小微企业、“三农”客户信贷业务的“标准化、模型化、规模化、自动化”作业，为农业银行在发展普惠金融领域打开新的局面。（如图 11-3 ）

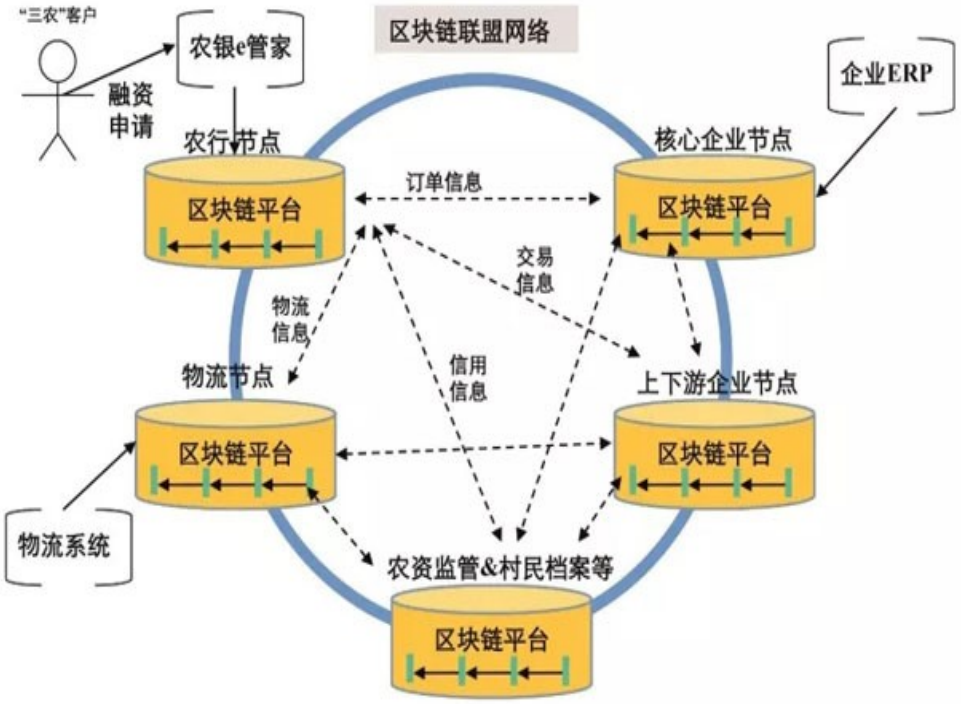

图 11-3 基于区块链和大数据的新型融资产品创新

“农银 e 管家”电商金融服务平台（以下简称电商平台）是农业银行为生产企业、分销商、县域批发商、农家店、农户打造的一款线上“ERP+金融”综合服务平台。以现有供销关系快速线上化为突破口，融入小微企业、“三农”客户的生产和生活场景，为工业品下乡、农产品进城搭建线上金融服务渠道。平台运行以来，客户活跃度较高，交易规模呈快速发展趋势，运行状况和市场评价良好，积淀了大量有价值的数据。通过应用区块链技术，将历史交易数据映射到区块链平台中，同时每天产生的数据也入链登记，不断积累以逐步形成企业和农户可信的、不可篡改的交易记录，反映了客户的真实信用状况。

除了充分挖掘和利用农业银行自有电商平台的交易和经营数据之外，通过与核心企业合作，有限度获得核心企业 ERP 订单数据；通过

与当地农村供销社、政府部门合作，经授权后获得农户信用数据，包括农资交易、档案信息、政府补贴等；通过与当地农资监管和物流追踪平台对接，获得物流数据。将这些数据的提供方作为参与节点加入区块链网络，不断向区块链网络推送有效数据，使整个业务场景视图更加丰富和完备。随着区块链联盟网络的不断扩大，加入用户的增多，信用的维度将更健全，从而彻底将区块链网络打造成一个信任网络。同时以智能合约形式约定统一数据共享标准，并尝试将授信模型内嵌进智能合约代码中，实现银行授信、审批和用信等环节的智能化、自动化处理。通过借助智能合约实现的新型信用模式，将融资产品嵌入到支付框架中，实现在支付订单时即完成放款的功能。

为了防范风险，采用受托支付的方式完成订单，资金不经过客户账户，并且后台通过自动审批的方式完成每笔订单的贷款审批工作，尽量让客户感知不到贷款的流程，实现便捷快速的支付体验。通过这种方式，客户的信用数据进一步丰富，基于这些信用数据的融资产品不仅解决了客户融资难的问题，还通过区块链技术实现为客户增信，同时在采用全新的科技手段后极大降低融资的成本，给客户最大实惠。

11.1.5 区块链助力多方资金监管

银行资金监管是指交易资金通过银行进行监管，专款专用，买卖双方一旦达成成交意向，并完成交易，监管银行接到双方成交指令，放款给卖方，规避了部分交易商的信用风险，真正解决了买卖双方在交易过程中互相担心，不敢先付款或不敢先付货的问题。银行资金监管的介入，可以提高交易双方的诚信度，构建安全交易平台。资金监

管的场景很多：主要用于房地产交易、工程建设、扶贫资金使用等场景。

案例 11-8：工行资金监管“区块链+基建+金融”

在建筑行业里，经常采用多层分包制，从一级分包商，到二级甚至到三级承包商，导致工资支付链条长，整个支付链条缺乏监管手段。整个劳务工薪市场已经达到了万亿的规模，涉及劳务工人数众多。政府非常关注建筑劳务工的工资拖欠问题，2020 年 1 月国务院常务会议通过《保障农民工工资支付条例》，将于 2020 年 5 月 1 日正式实施。因此，建筑行业存在极大的资金监管需求。

工行基于区块链创新建筑行业的资金监管与金融服务模式。首先，将建筑工程相关的所有商务及劳务合同信息上链，实现从地产商、到建筑承建商、以及逐级分包合同，一直到劳务公司的工人劳务合同。

基于区块链实现“三透明”，即合同信息、履约信息、支付信息上链，确保整个项目全流程数据透明。并基于链上数据实现“三勾稽”，把劳务权益与合同信息勾稽、劳务权益与支付信息勾稽、合同与支付信息勾稽。基于此，实现劳务权益的真实记录，基于履约信息，形成合法的劳务权益，并基于权益的多方确认实现权益的精准兑付。

案例 11-9：工商银行创新扶贫金融服务

为做好扶贫工作，全社会投入了巨大的社会资源，仅贵州就已成立规模超过 3000 亿的脱贫攻坚基金。但是，面对规模如此巨大的扶贫资金，如何确保“募得了、投得好，管得住，收得回，不出事”已成为摆在各级政府面前的重要课题，而能否找准“穷根”、明确靶向、

量身定制、对症下药也成为各级政府扶贫攻坚的成败所在。

为破解困扰政府扶贫管理的难题，在贵州省政府的支持下，工商银行通过银行金融服务链和政府扶贫资金行政审批链的跨链整合与信息互信，以区块链技术的“交易溯源、不可篡改”实现了扶贫资金的“透明使用”、“精准投放”和“高效管理”。

2017 年 10 月，工商银行正式启动与贵州省贵民集团联合打造的脱贫攻坚基金区块链管理平台，这是业界首个服务于精准扶贫的区块链平台。

平台具有如下特点：

- “透明使用”，即每一笔扶贫资金的审批流程全部上链，每一个环节都责任到人，让审批信息和实际支付信息紧密勾稽在一起，区块链“多方共识、信息共享”的特点，让扶贫相关的各级政府管理部门和银行机构都自动加入到监管之中，使整个审批过程真正透明，消除腐败滋生的可能。
- “精准投放”，即通过区块链技术对扶贫资金投放进行精准管理，资金使用方式由原来先层层拨付再确定扶贫项目的“推动”方式，变成了先确定用款项目和款项用途再根据实际资金需求配套资金的“拉动”方式，彻底将“大水漫灌”变成了“精准滴灌”。
- “高效管理”，即金融服务链与扶贫资金行政审批链的跨链整合使“区块链”和“大数据”有机结合在一起。宏观层面上，各级政府能够自顶向下地实时掌握辖内扶贫资金的需求、配套、

拨付、实际使用情况；微观层面上，上级政府部门实现了对每一个扶贫项目、每一笔扶贫资金的穿透式管理。

贵州省政府将建档立卡扶贫户、社会诚信等信息导入这个由金融链和行政链共同支撑的体系之中，后续将实现对每笔扶贫资金使用效果的量化和精准评估，彻底解决扶贫项目资金使用中管理信息回馈不及时性、回馈信息失真等问题，大幅提高扶贫资金的管理和使用效率。

案例 11-10：电子审计函证业务

与银行资金监管相关的一项业务是企业资金审计过程中的函证业务。

审计函证是指注册会计师为了获取影响财务报表或相关披露认定的项目的信息，通过直接来自第三方对有关信息和现存状况的声明，获取和评价审计证据的过程，例如对应收账款余额或银行存款的函证。函证是注册会计师获取审计证据的重要审计程序，多用于执行审计和验资业务。通过函证获得的证据可靠性较高，因此，函证是受到高度重视并经常被使用的一种重要程序。

审计是构建社会信任的基础，函证/第三方验证是审计工作的基础。目前，注册会计师行业以近乎原始的手工信函方式，每年花费巨大的人力和物力开展函证工作。据统计，仅毕马威会计事务所一家，每年在函证上花费的人力物力成本约 10 亿元左右。

审计函证标准工作流程如下：

- 将被询证者的名称、地址与被审计单位有关记录核对；
- 将询证函中列示的账户余额或其他信息与被审计单位资料核

对；

- 在询证函中指明直接向接受审计业务委托的会计师事务所回函；
- 询证函经被审计单位盖章后，由注册会计师直接发出；
- 将发出询证函的情况形成审计工作记录；
- 将收到的回函形成审计工作记录，并汇总统计函证结果。

基于区块链技术实现企业、审计公司、银行、监管机构等多方电子函证过程，并将结果存证，不可篡改的函证数据将成为未来发生纠纷的司法证据。（如图 11-4 ）

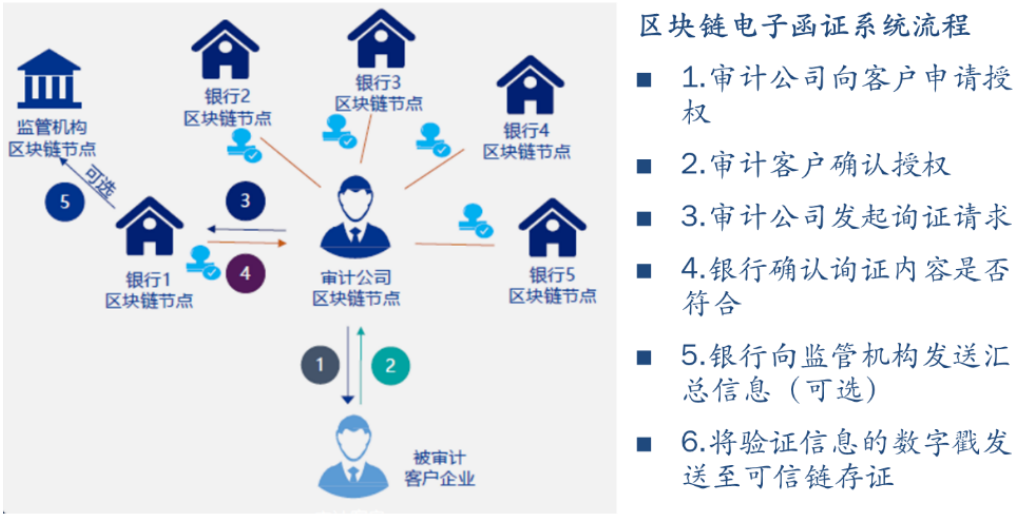

图 11-4 区块链电子函证流程

11.1.6 区块链实现多方异构系统协同

新金融时代，国有银行和股份制银行实力雄厚，纷纷成立金融科技子公司，推进金融科技战略。但是对于中小银行，科技壁垒越发成为银行业务拓展的痛点。

在资管新规以及银行业大零售转型的背景下，广大中小银行积极

开展同业合作，寻求业务综合化发展和财富管理能力的提升。但在现有的合作模式中，往往需要中小银行进行对应的科技开发、测试、运维工作，给中小银行拓展业务带来新的负担。区块链技术可以通过分布式共享账本实现多方协同，并基于数据自主权管理实现金融机构数据安全。

案例 11-11：交通银行“轻科技”系统对接方案

交通银行面向中小银行打造丰富的银银合作业务体系，为解决中小银行科技实力相对薄弱、系统开发运维负担较重的痛点，推出“轻科技”系统对接方案，通过区块链技术应用、一对多渠道对接、前置机代理开发服务等创新手段，有效减轻合作银行科技负担，加快系统对接效率，实现银银合作展业模式的创新，与中小银行合力打造综合化财富管理服务，为普惠金融和实体经济发展助力。

“轻科技”系统对接方案详细内容：（如图 11-5 ）

一是依托区块链技术，重塑平台逻辑。应用区块链技术，整合银银合作多套代理、代销业务应用系统，整合形成银银合作区块链云平台，以“分布式系统架构+前置设备输出”的组合化方案，便利合作银行快速对接交行银银平台。

系统首创以区块链方式开创性应用于账户认证、电子签约等应用领域，保障客户信息安全。并通过整合原有多套业务系统，形成统一业务平台，实现业务集成化处理，为业务发展奠定坚实基础。

在此模式下，通过将交行和合作银行之间客户校验信息上链，以及将交行和合作银行客户之间电子化协议上链，实现信息的不可篡改，

并实现信息的分布式维护和共享。在多节点、多场景的应用环境下，实现交行与合作银行更快速的对接合作。

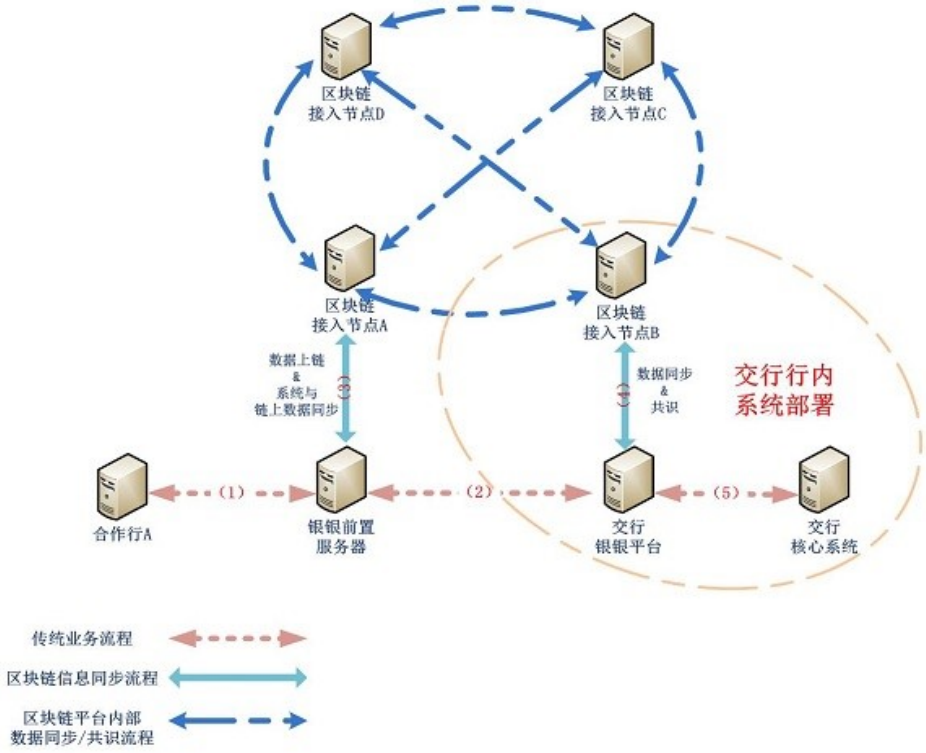

图 11-5 基于区块链的银行系统对接与协同

二是接入清算机构，打造一对多业务渠道。基于原有业务合作一对一对接基础上，加快与特许支付清算机构合作，实现一对多对接，快速实现与中小银行开展业务合作。

交行已与特许清算机构在多个业务领域探索开展“1+1+N”清算模式。一是试点开展“柜面通”业务，通过特许清算机构和中小银行网点对接的区位优势，实现共同面向客户提供存取款普惠服务。二是试点开展个人银行结算账户认证合作，通过账户认证合作，建立交行与合作银行间个人客户信息、账户信息的“直通通道”，便于合作银行客户对接使用交行的金融服务产品。

三是科技前置，提供代理开发服务。基于重塑后的集成化系统，

交行为中小银行提供前置机代理开发、调试，进一步减少对方开发工作，并以上门贴身服务的方式，大幅减少调试应用的周期，进一步加快银银合作系统对接速度。

基于区块链的“轻科技”系统对接方案，为银银同业合作开辟了一个新的思路，未来可以广泛的用于金融机构与金融科技服务机构之间的技术对接与合作。

11.2 区块链在证券领域的应用

11.2.1 国际证券业对区块链应用的分析与探索

美国证监会 SEC 以及金融监管局 FINRA 的研究[18]认为，区块链技术（在证券金融行业，更常用的区块链技术的另一个名字，即分布式账本技术 DLT）在证券业具有广阔的应用前景。应用范围大致按照交易前、交易中和交易后三个环节分类如下：

- 交易前环节，包括客户识别、反洗钱、信息披露等；
- 交易中环节，包括股票、债券、集合债务工具、衍生品的发行和转让；
- 交易后环节，包括登记、存管、清算、交收、数据共享、股份拆分、股东投票、分红付息、担保品管理等。

在实践中，证券业对区块链技术应用也开展了广泛的探索。目前在股权、债券和衍生品市场应用或者正在尝试的区块链技术应用如下。

- （1）股票市场：非上市公司股权方面，基于 DLT 的应用实现系统追踪非上市公司股权的交易和所有权情况；上市公司股票方

[18] FINRA , Distributed Ledger Technology: Implications of Blockchain for the Securities Industry [M/OL], https://www.finra.org , 2017.01.

面，在 DLT 平台探索发行与股票交易的清结算。

- （2）债券市场：回购协议领域，回购市场存在的问题包括交易对手风险和相对缺乏透明度，一些市场参与者正在探索使用 DLT 推动回购交易的清算和结算，以减少结算时间，降低结算失败的风险。公司债券领域，一些市场参与者正在探索在 DLT 系统中应用公司债的发行与交易，在债券的条款嵌入数字资产的代码，这将允许完全自动计算、订单的支付与赎回。
- （3）衍生品市场：信用违约掉期，在进行某些衍生品交易和清算时，这些工具涉及复杂的后交易事件，市场参与者和监管者可以从市场更为强化的透明度中获益。
- （4）行业设施：产品参考数据，一些市场参与者正合作创建和管理基于 DLT 的各种证券产品标准化参考数据中心库。这样可以不再需要每个市场参与者维护参考数据托管，并将有利于证券产品标准化参考数据的使用。

总体上看，区块链技术的应用研究探索实践呈现“全覆盖”的特点。需要特别说明的是，区块链技术作为一种分布式技术，相对中心的系统是天然存在性能劣势的。因此区块链技术不适合证券及期货交易所的基于订单驱动的集中撮合成交环节。从目前全世界证券行业正式宣布的区块链技术应用环节也可以看出，当前区块链证券领域的应用主要集中于私募股权等场外市场证券的发行与交易，以及交易所场内市场的交易前与交易后服务环节。

世界主要国家和地区区块链技术在证券领域的应用探索见图 11-

6 。

应用领域	国家和地区	相关实践
证券发行、非上市公司证券交易	法国	法国政府已批准利用区块链技术交易非上市证券
	美国	美国SEC已批准在线零售商Overstock.com在区块链上发行该公司新的上市股票
		纳斯达克宣布与Chain.com合作推出基于区块链技术的私募股权交易平台Nasdaq Linq
		特拉华州通过基于区块链的股票发行相关法律修正案
	香港	港交所计划2018年发起基于区块链的私募市场
证券交易及清算、结算	美国	花旗集团与芝商所推出用于证券交易后台管理的区块链平台
	德国	德国复兴信贷等多家银行利用区块链模拟证券交易
	韩国	韩国证券交易所尝试使用区块链技术开发柜面交易系统
	澳大利亚	澳大利亚证券交易所正式宣布使用区块链技术为基础的系统取代现有交易后结算系统CHESS
		悉尼证券交易所搭建区块链结算系统
	加拿大	多伦多交易所TSE已招募区块链初创公司，试图搭建基于分布式账本的结算系统。
		加拿大证券交易所CSE宣布计划对证券交易引入搭载区块链技术的清算和结算平台
	直布罗陀	直布罗陀股票交易所GSE表示与金融科技公司进行战略合作，计划将区块链技术应用于交易结算系统。
金融衍生品	美国	高盛、摩根大通等金融机构将DLT用于股权互换测试
监管合规	瑞士、英国	瑞银携手巴克莱、瑞信等大型银行机构推出智能合约驱动的监管合规平台
客户管理及其他	美国	纳斯达克为南非资本市场开发基于区块链技术的电子股东投票系统

图 11-6 区块链在证券行业的应用探索

11.2.2 区块链在证券发行与交易的应用

证券的发行与交易清结算的流程手续繁杂且效率低下。区块链技术使得金融业务流程更加公开、透明、有效率。通过共享的网络系统参与证券发行与交易清结算，原本高度依赖中介的传统模式变为分散的平面网络交易模式。

首先，能大幅减少证券发行与交易清结算成本，区块链技术的应用天生的基于云计算服务，可减少对功能重复的 IT 系统的依赖，提高市场运转的效率。

其次，区块链技术可实时地记录证券交易者的身份、交易量等关键信息，有利于证券发行者更快速和清晰地了解股权结构，提升商业决策效率，同时减少了暗箱操作、内幕交易的可能性，有利于证券发

行者和监管部门维护市场。

最后，区块链技术使得证券交易日和交割日时间间隔从1～3天缩短至“交易确认即结算”，减少了交易的交割（DVP）风险，提高了交易的效率和可控性。特别对于一些非标准化的证券来说，比如有着复杂命名、复杂交割条件又必须通过律师或者其他交易所的介入才能完成交易的期权，通过智能合约可以代替复杂的手续，自动地执行复杂的证券交割。

在监管合规方面，由于合规成本过高或监管不全面，金融机构不能及时发现道德风险，最终给投资者利益带来重大损失。区块链技术将交易透明化，所有接入的节点都能通过追溯交易历史核验金融机构运行是否合规，有利于简化业务流程，维护金融稳定及防范金融风险。

案例11-12：港交所私募股权交易市场

香港交易所2018年发起基于区块链技术的私募市场——香港交易所私募市场（HKEX Private Market）。该平台将使用区块链技术为早期创业公司及其投资者提供一个股票登记、转让和信息披露的共享服务平台。

在执行一笔完整的非上市公司股权交易过程中，由于存在股东名册繁琐，历史交易难追溯，信息不透明等问题，致使各参与主体间存在反复验证的行为，同时各主体内部也有繁杂的审批流程，难以实现交易信息的实时同步。这不仅使整个交易过程变得复杂，交易周期也变得不可预测。如果某笔交易存在跨地域，有时间先后顺序等特殊要求，交易流程和成交周期更将变得更加漫长，交易信息滞后会带来潜

在重复质押的隐患，导致投资人利益受到损害。因此提高各参与主体的信息同步和协同效率是股权交易的重中之重。

将区块链引入股权的登记和交易结算，结合现有法律法规，提供股权数字化唯一性凭证，可以实现一个围绕股权资产的多方参与的且共同维护的分布式共享账本。

整个系统采取“分层多链”的技术架构，将提供业务支撑的核心链和提供交易服务的业务链隔离。其中核心链成员共同审查用户认证身份，为业务链提供全局身份验证服务。（如图 11-7 ）

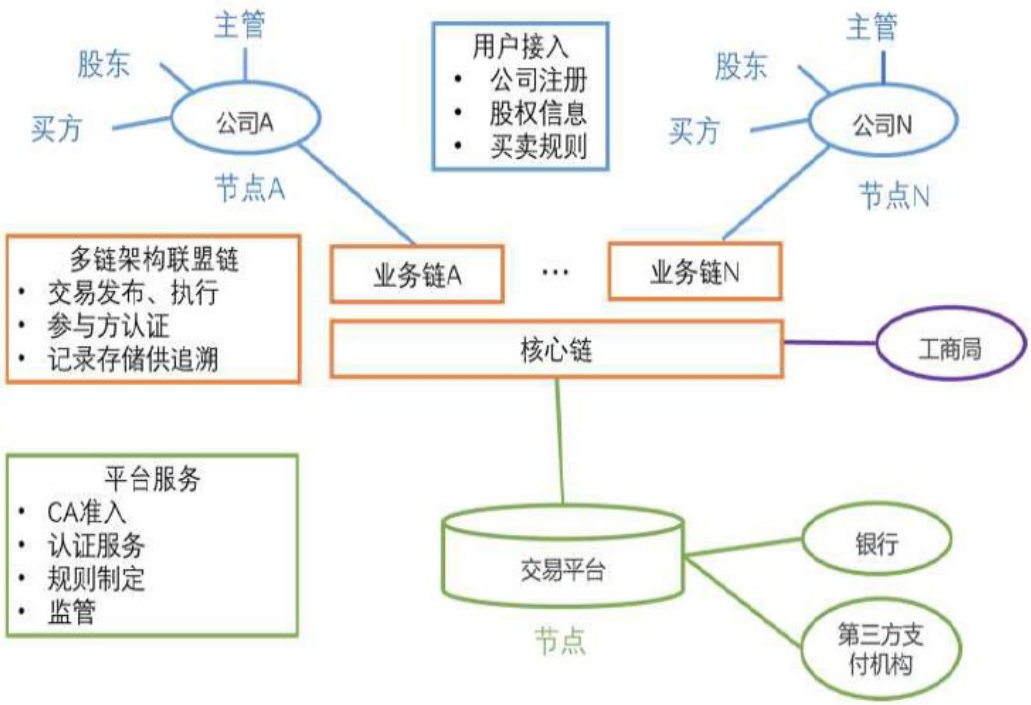

图 11-7 基于区块链的港交所私募市场

在权益证明方面，由于区块链上的每个参与维护节点都能获得一份完整的数据记录，利用区块链账本不可篡改和强一致性的特点，可对权益的所有者实行有效确权。股权所有者凭借私钥，可证明拥有该股权的所有权，股权转让时通过区块链系统转移给下家，流程清晰，

产权明确，记录完整，整个过程无需第三方的参与便可实现。

案例 11-13：浙江金融资产交易中心资产发行审核系统

金融产品在发行前都需经过严格的发行审核机制，参与审核的部门与机构包括交易中心各事业部、会计事务所、律师事务所、第三方评级机构等。由于产品审核过程严格，周期较长，参与部门众多，相关资料繁杂，且存在大量线下纸质凭证，因此在发审过程中，各部门在产品进度跟踪与资源协调管理上存在信息不一致、凭证需反复确认等问题，影响工作效率，提升风控难度。

浙江金融资产交易中心于 2018 年初开展区块链发审系统项目合作，为参与发审的各部门、机构搭建一套数据实时同步、防篡改、可溯源的发审系统。目前该系统已与浙金中心风控系统对接，并接入多家外部会计事务所，律师事务所，评级机构等发审参与方，为金融产品的发行审核提供有利依据与保障。（如图 11-8 ）

图 11-8 浙江金融资产交易中心区块链发审系统

通过构建金融产品发审链，接入包括产品发行方，交易中心各审核部门（事业部、风险管理部、法律合规部、审核委员办公室、交易运营部等），会计事务所，评级机构，律师事务所在内的各发审参与方，并将原有的线下流程通过智能合约的应用实行链上操作，简化操作流

程。基于区块链账本的强一致性与实时性，各参与方可获取实时的产品信息与操作记录，为产品挂牌发行以及后期管理提供审议和决策依据。

案例 11-14：纳斯达克私募股权市场 LINQ

2015 年 11 月，纳斯达克推出了基于区块链的企业级应用 LINQ，作为其私募股票交易平台的补充，用于扩张和增强纳斯达克私募股票交易市场平台股票管理能力。 LINQ 是首个基于区块链技术建立起来的金融服务平台，能够展示如何在区块链技术上实现资产交易。这同样也是一个私募股权管理工具，作为纳斯达克私募股权市场的一部分，为企业家和风险投资者提供完整解决方案。

11.2.3 区块链助力 ABS 产品发行与交易

资产证券化（Asset-backed Securities，简称 ABS），是指以基础资产未来所产生的现金流为偿付支持，发起人通过特殊目的机构（Special Purpose Vehicle，简称 SPV）发行可交易证券的一种融资形式。

传统融资（股权和一般债务）对企业资产的收益表现和信用条件的要求较高，融资难度较大。由于风险隔离和信用增级的使用，资产证券化在融资上可以摆脱企业资产本身的信用条件限制，从而可以降低融资门槛。只要企业有可预见的，能够产生稳定现金流的资产或者资产权益，就可以在资本市场中获得融资。

从 2013 年开始，资产证券化的浪潮开始席卷中国金融市场。从银行贷款、信用卡贷款、车贷、房贷到学费贷款、公司的应收账款等等，

都开始被当作资产证券化的标的资产。中国资产证券化的发展步伐越来越快。2019 年，资产证券化产品新增发行接近 2 万亿，产品市场存量接近 4 万亿。[19]

在 ABS 产品的设计与发行过程，ABS 资产包信息分布在多个参与机构中，投资者无数据对接渠道，投后管理没有数据来源，无法监控 ABS 底层资产现金流回收与风险；ABS 业务因存在多方参与、中间环节较长、关键数据易被篡改、信息不对称等问题，使得监管难以执行到位，制约了当前 ABS 业务发展。

基于区块链以及智能合约实现灵活的 ABS 业务场景。利用智能合约实现监管体系建设，对信息披露及时性，ABS 业务规模等关键指标进行监控;利用智能合约进行底层资产筛选,现金流预测、信用定价，杜绝中间环节造假可能。帮助资产方、计划管理人、律师事务所、评级机构、会计师事务所、托管行等 ABS 业务参与机构优化业务流程，提升 ABS 发行业务效率。

ABS 二级市场的客户群体与债券市场、同业市场、甚至 ABS 一级市场并不完全重叠，因此寻找交易对手费时费力。基于区块链实现产品底层资产追溯，为产品交易和定价提供数据支撑，并实现 ABS 分层证券的通证化（Tokenized），便于数字化资产在二级市场以点对点的方式进行场外交易转让。

案例 11-15：交通银行聚财链

2018 年 6 月，交通银行正式上线区块链资产证券化平台“聚财

[19] 中国资产证券化分析网，2019 年度中国资产证券化市场白皮书[M]，2020.01.

链”，迈出了区块链技术应用于资产证券化领域的重要一步。平台以区块链技术为纽带连接资金端与资产端，提供 ABS 产品从发行到存续期的全生命周期业务功能，利用区块链技术实现 ABS 业务体系的信用穿透。平台重新设计与定义资产登记、尽职调查、产品设计、销售发行等各个环节，将基础资产全生命周期信息上链，实现资产信息快速共享与流转，保证基础资产形成期的真实性和存续期的监控实时性，同时将项目运转全过程信息上链，使得整个业务过程更加规范化、透明化及标准化。（如图 11-9 ）

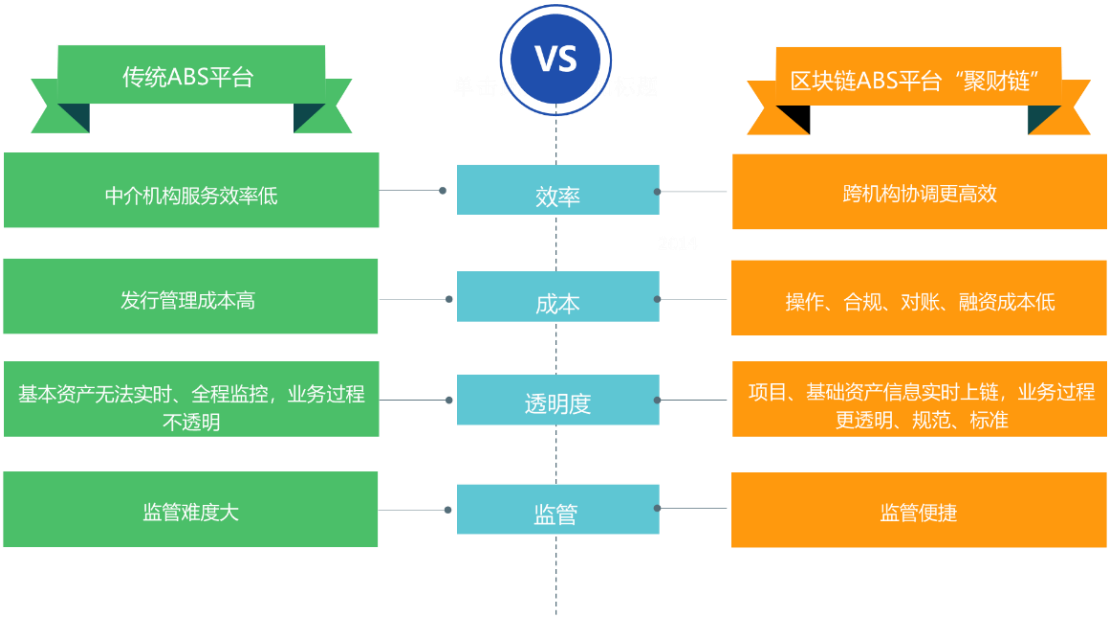

图 11-9 区块链 ABS 平台“聚财链“的优势

聚财链一期实现了项目信息与资产信息上链、跨机构尽职调查流程等业务功能以及区块链配置更新流程、智能合约升级流程等基础功能。后续，聚财链将实现 ABS 产品全生命周期的业务功能，贯穿资产筛选、尽职调查、产品设计、销售发行、存续期管理等各个环节，同时平台还提供风险定价、现金流分析、压力测试等智能分析工具。

聚财链将建立一套可配置的产品模板，能支持多种类型 ABS 产品

的快速发行，且具备灵活的升级机制，可快速适应市场变化与政策调整。信贷 ABS 产品，如信用卡分期、住房按揭、对公贷款、不良贷款；企业 ABS 产品，如小额贷款、应收账款、信托收益权、租赁租金。

聚财链平台的目标不仅是建立 ABS 业务的综合化平台，更希望借助这一平台连接 ABS 业务各参与方，实现业务流程和数据的高效对接，构建一个开放、共享、可信的联盟生态圈，打造全新 ABS 时代的命运共同体。

2018 年 9 月 26 日，交通银行作为发起机构的“交盈 2018 年第一期个人住房抵押贷款资产支持证券”成功发行，项目规模 93.14 亿元，该产品是市场首单基于区块链技术的信贷资产证券化项目。

案例 11-16：京东数科基于区块链的 ABS 全流程解决方案

京东数科基于区块链的 ABS 全流程解决方案包括资产池统计、切割、结构化设计、存续期管理、二级市场交易等系统功能，为中介机构提供全流程的分析、管理、运算体系。

基于区块链的 ABS 全流程解决方案首先建立由各参与方共同组成的 ABS 区块链联盟，在此基础上，在 ABS 全部流程的落地中运用区块链技术，使 ABS 实现更加精确的资产洞察、现金流管理、数据分析和投后管理。（如图 11-10 ）

- Pre-ABS 底层资产形成阶段，可以做到放款、还款现金流和信息流实时入链，实现底层资产的真实防篡改。同时，各类尽职调查报告，资产服务报告可以通过智能合约自动生成。
- 在产品设计和发行阶段，交易结构和评级结果由评级公司和券

商确认后共识入链；将投资人身份及认购份额登记入链；交易所从链上获取全部申报信息，将审批结果入链。

- 在存续期管理阶段，回款数据、循环购买数据、资产赎回、置换和回购数据均可入链，并生成资产服务报告。
- 在二级市场交易阶段，证券底层现金流信息可从链上获取，帮助交易双方进行实时估价；投资人可通过交易撮合智能合约，在链上完成证券所有权的转移。

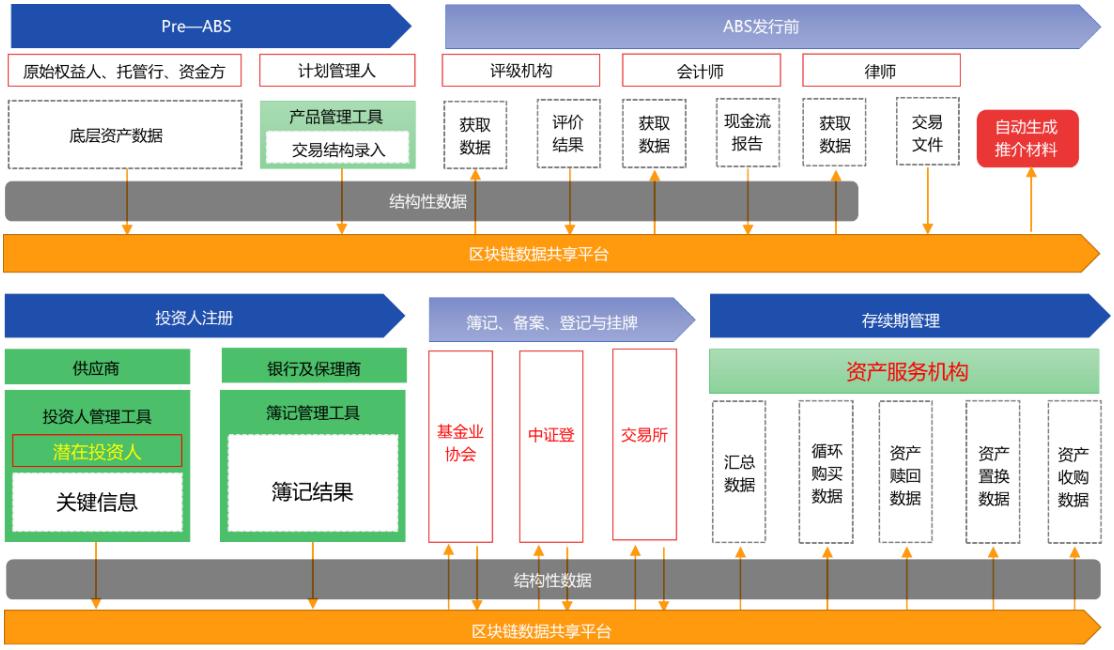

图 11-10 基于区块链的 ABS 全流程解决方案

2018 年 6 月 13 日，“京东金融-华泰资管 19 号京东白条应收账款债权资产支持专项计划”成功设立并在深交所挂牌转让。京东金融与华泰证券资管、兴业银行共同组建资产证券化联盟链，此项目通过区块链技术的分布式记账、防篡改以及实时安全传输等核心特性应用，其底层资产及现金流、产品、账务等数据信息流在原始权益人、管理人、托管人等多个参与方之间实时共享并确认交易，这有助于实

现信息透明化、提高操作效率，并降低信用风险。同时由于白条资产是小而分散的特性，单笔金额小、笔数多，通过该项目的实践，可以看出区块链技术在技术性能上逐渐成熟，能够成功支持每日大数据量的读写。该项目首次购买入链资产约为 150 万笔，在项目存续期每日约有 5 万笔资产数据持续更新。

案例 11-17：国泰君安区块链 ABS 系统方案

2015 年 8 月，国泰君安资金同业部发行了国内首单以券商两融债权为基础资产的 ABS—“国君华泰融出资金债权 1 号资产支持专项计划”。国泰君安根据两融债权 ABS 的业务流程（如图 11-11 ）设计了基于区块链技术的 ABS 业务系统。

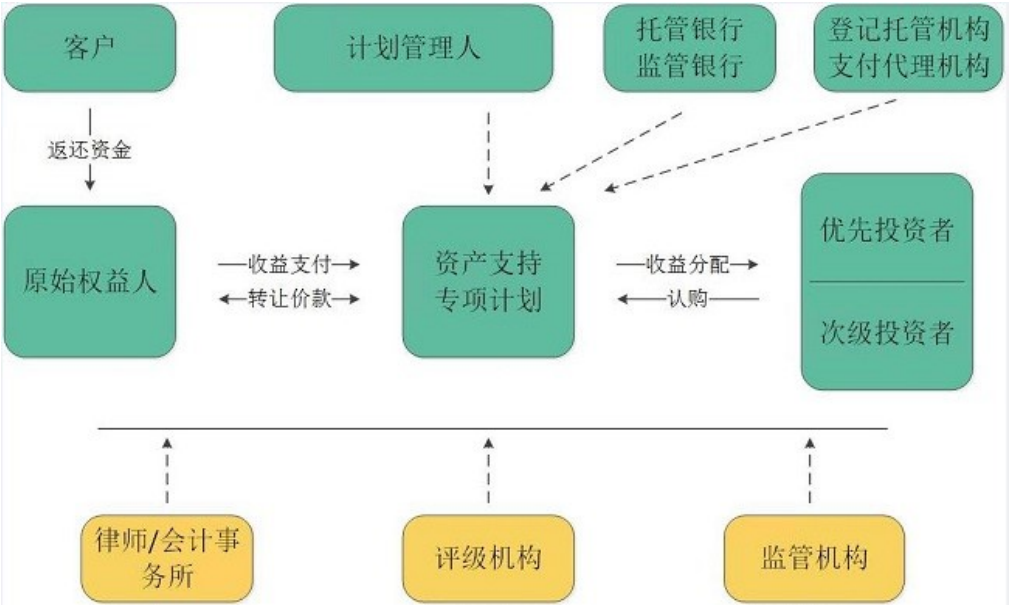

图 11-11 两融债权 ABS 业务流程

基于不同的基础资产的 ABS 产品有不同的融资特点。对于两融债权类资产，主要根据客户历史履约意愿、逾期情况、维持担保比率等指标进行现金流预测及信用定价，而对于股票质押资产则关注标的股票评级，客户信用评级，融资规模等指标。系统抽象出通用要素设计

为父合约，将个性化要素设计为子合约，通过父合约调用子合约可实现灵活的智能合约模板。

系统利用智能合约实现基础资产筛选、现金流预测、信用定价、重复转让检查等关键逻辑。在两融债权场景中，券商通过集中交易系统导出每日客户两融数据，需要按双方事前约定好的规则，筛选出最优的每日合约资产，故可利用智能合约进行筛选和最优性校验。由于智能合约一旦确定即会按规则执行，故可确保筛选出的是最优资产，将信任由“人”转移到“代码”，增强了公信力。

区块链及智能合约对于 ABS 业务流程设计优化如下：

- 利用智能合约，强制 ABS 各业务关联方及时完整的定期披露相关信息，例如资产管理报告，重大事项公告等，对于不按时披露的进行发函警示或业务禁止，严重的进行资金冻结。
- 对业务流程中涉及的关键数据，包括资金池情况、债权汇款情况、债权人信用变化情况等信息实时上链固化保存，对任何修改做到溯源可查。
- 利用智能合约设计一系列激励机制，鼓励各业务参与方诚信交易，按时履约。系统对能体现参与方诚信度的关键指标进行监控，例如历史违约记录，基础资产质量等。对于履约能力好，信用评级高的交易方给与一定积分激励，由智能合约自动发放。对于获得较高评级积分的交易方，享有一定优选权，如产品排名优先、交易费率抵扣等。后续可利用该积分开展跨机构合作，例如黑名单共享、数据价值流通、营销引流等。

将区块链技术应用在 ABS 场景中有很好的发展前景[20]，具体表现在：

- 区块链共享了 ABS 账本数据，并由不可篡改的技术进行信任背书，使得机构间信任得以增强，有助于更加高效透明的进行业务协作，提升业务效率；
- 利用智能合约实现 ABS 关键业务流程，使得 ABS 全生命周期业务流程得以有效管理，形成一个完整的跟踪链，杜绝了任何环节造假的可能，在一定程度上降低事中风险，同时也使得业务流程更加自动化；
- 区块链分布式、点对点的架构模式，使得参与系统的各方享有平等地位，有利于异构的金融机构加入，减小了因信息不对称造成利益损失的风险；
- 监管机构可作为节点加入，能够实时获得账本完整数据，有利于监管机构及时高效执行监管要求，缩减中间环节，提高智能化监管能力。

11.3 区块链在其他金融领域的应用

11.3.1 区块链在保险领域的应用

区块链对于保险行业的改造主要包括以下几个方面：

首先，基于区块链的可信存证系统以及自动执行智能合约，增强用户信任，现阶段对于互助保险性产品尤其重要。相互保险机构或者网络互助平台可以将涉及投保人利益的赔付信息等存储在区块链上，

[20] 姚前，资产证券化区块链平台的创新设计及其应用[J]，第一财经，2018.10.12.

同时引入具有监督效力的第三方来共同维护账本以提高信息的篡改难度。投保人可以根据自身需求随时查询了解，这能有效减少保险人与投保人之间的信息不对称现象。

其次，创建多方维护的共享透明账本，以加强保险数据整合分析，提高保险机构间协作效率，尤其针对直保公司与再保险公司之间。基于区块链的技术融合方案，一定程度上能实现在不共享隐私数据的情况下完成数据的运算和检验，为直保公司之间的数据共享提供新的思路和可能性。

最后，区块链还可以作为保险资产证券化产品的登记交易系统。并能够在农业险、自然灾害险等领域，对动植物的动态生长信息、气候地理等动态变化信息提供可信记录及追溯的能力。

案例 11-18：传统保险巨头区块链探索

2016 年 10 月，欧洲保险业五大巨头，安联保险、荷兰全球人寿保险、慕尼黑再保险、瑞士再保险和苏黎世保险就联合组建了区块链研究组织联盟 B3i，致力于探索区块链在保险行业内的应用。2018 年 4 月，B3i 宣布在瑞士苏黎世成立了 B3i 服务有限公司，简称 B3i 公司，这是一个重要的里程碑，标志着其作为拥有自有资本和知识产权的独立实体，将会开始进行区块链解决方案的开发，测试和商业化。

2016 年，阳光保险集团推出基于区块链技术的国内首个可互赠的航空意外险微信电子卡单，用户可以通过微信等社交软件将卡单互相赠送。

2017 年，众安科技发布了基于区块链技术和人工智能的安链云平

台，上线了电子保单存储系统，尝试通过区块链技术保证电子保单的安全性，实现保单信息的去中心化存储。

2017 年 1 月，蚂蚁金服支付宝宣布将会在公益保险产品中引入区块链技术。2018 年蚂蚁金服与信美人寿合作推出基于区块链的健康互助产品相互保。同年互联网科技企业水滴集团也宣布将会在旗下的健康互助产品水滴互助当中引入区块链技术。

案例 11-19：保交链为保险行业提供底层基础设施

保交链是上海保交所区块链团队打造的区块链技术平台。保交所是一个集中、公开、标准化的保险市场，保交链的研发正是为了进一步提高保险市场交易效率，成为保险行业标准化交易的底层基础设施。

根据保交链白皮书内容，其整体架构包含四大服务体系，身份认证服务体系，共识服务体系，智能合约服务体系，平台服务体系。

保交链的研发目标是提高保险市场交易的标准性和便利性，因此其应用场景的设计目前主要集中在两块：保单上链与保单质押。

保单上链。保交所区块链数字保单具有灵活性、安全性、敏捷对接、前瞻性等特性。保险机构可以在其内部搭建节点，也可以成为保交所云平台上的节点，搭配保交所的云存储服务，可以将保单的文件信息和指纹信息记录下来，从而实现保单数字化托管，为终端用户提供验真功能。区块链数字保单能够有效解决保单电子化以后的信任问题。减少了传统保单在整个托管和验真过程中的纠纷与摩擦，使下一步保单数字化、保单快速流转成为可能，这对未来保险资产证券化的进一步推进有非常重要的意义。

保单质押。保交链支持的保单质押平台，可以引入区块链对保单冻结，质押，解冻等状态进行登记，银行和保险公司等可以利用区块链上的数据，获取具体可信的保单状态信息，从而较少纠纷与摩擦。利用区块链技术构建的保单质押平台使得保单质押行为更为安全；质押流程更加高效。

目前保交所已经与太平洋资产管理有限公司完成了“另类投资债权计划互联互通”的区块链验证，以及与长江养老保险股份有限公司完成了“年金运营管理中应用”的区块链验证，未来随着合作的深入以及技术发展的成熟，保交链将会在效率、成本、安全性上给传统的保险业带来进一步的提升。

案例 11-20：再保链将分保业务上链运行

2018 年 6 月，中再集团联合众安科技、汉诺威再保险上海分公司、德国通用再保险上海分公司发布了《再保险区块链（RIC）白皮书》。再保险区块链重点专注于解决再保险行业日常业务中的问题。

第一，提升保单流转效率。传统再保险分保过程的合同签订多为邮件往来，交易常为手工统计，高度依赖人力在其中反复协调，容易造成再保险交易的纠纷频发，且效率低下，错误频出。基于区块链技术搭建再保险平台，提升数字保单流转效率，并可能实现再保险业务自动对账结算。

第二，提升直保分保之间的可信数据传输效率。再保险交易当中原始保单数据由直保公司掌握，逐单核对流程复杂，且周期较长。再保险公司往往需要一个季度才能收到分保业务的数据，导致再保险公

司并不能及时了解公司在交易过程当中的风险累积情况，信息传输的缓慢也导致了理赔过程的冗长繁琐。通过将保单的信息登记上链，再保险机构可以得到直保公司的授权下访问查询相关的保单数据。

目前，再保险区块链重点是为解决财产险合约再保险、财产险临分再保险、人身险合约再保险和人身险临分再保险以及转分保等业务场景。（如图 11-12 ）

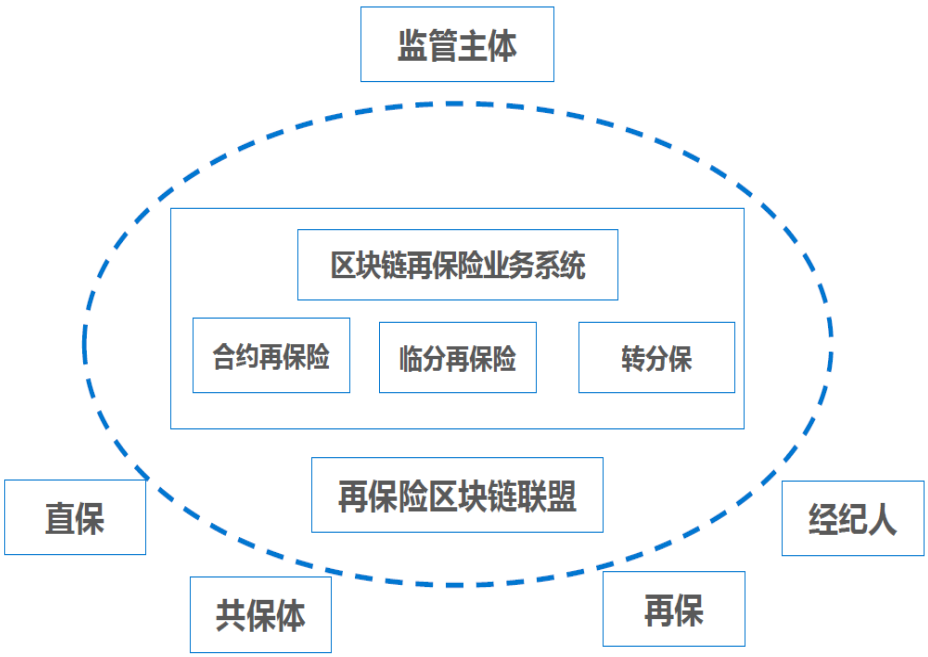

图 11-12 再保险区块链示例

11.3.2 区块链助力金融业务委外管理

各大银行针对不良资产主要采用内部清收和委外清收两种方式，而不论哪种形式，逾期用户与清收方的关系总伴随着很多不和谐。而另一方面，随着近些年零售业务的飞速发展，以银行业务系统为准的中心化信用卡清收业务管理模式逐渐体现出它的局限性，比如业务处理效率低、数据割裂、人力成本、存在监管盲区高等系列问题。

案例 11-21：广发银行信用卡委外催收应用

鉴于日均数百亿规模的委外资产处理压力，广发银行基于对区块链技术与不良资产委外清收业务场景相结合，实现外包运营全流程监控以及外包机构考核体系自动化功能等创新管理，在减少人力成本的同时，处理不良资产清收业务更加高效、安全、也增加了委外机构对银行的信任度。

广发银行信用卡中心“利用区块链技术的信用卡委外催收应用实践项目”，首创利用区块链技术实现银行不良资产委外清收的全流程处理。在行业内率先提出委外资产竞价业务模式，借助区块链智能合约功能部署公开、公正的竞价规则，实现不良资产包“一键发布”、机构竞价、智能合约自动撮合、佣金自动结算、机构身份管理等委外处理全生命过程。

针对当下的大数据安全与信息保护需求，广发银行借助于区块链技术自身数据不可篡改和可追溯的特性，通过区块链的加密算法与数据存储技术，最大程度保证信息安全。

广发银行基于区块链的委外管理实践为金融行业的第三方合作管理提供了指引与参考。基于区块链技术，在保证数据安全的情况下，实现与第三方系统与数据对接，对第三方的服务进行信用与质量评价，并保证历史记录完整可追溯。可以预期，未来基于区块链的业务委外管理将成为金融机构的业务标准。

11.3.3 更多区块链的金融应用场景

金融业是联结国民经济各方面的纽带。从国内看，金融连接着各部门、各行业、各单位的生产经营，联系每个社会成员和千家万户，

成为国家管理、监督和调控国民经济运行的重要杠杆和手段；从国际看，金融成为国际政治经济文化交往，实现国际贸易、引进外资、加强国际间经济技术合作的纽带。

金融天生需要面对两个问题：一是构建信任机制，二是实现多方协作。区块链的技术特性正好可以解决金融的问题，因此可以说区块链技术为金融服务而生。可以毫不夸张的说，只要有金融业务存在的地方，就有区块链技术的价值空间。本文所描述的区块链在金融场景的应用仅仅是区块链在金融领域应用的一部分，还有大量的应用场景等待去挖掘。**未来，新金融的主要生产方式将会是建设基于区块链技术的平台生态。**

案例 11-22：邮储银行资产托管区块链平台

2016 年 11 月，中国邮储银行基于区块链的资产托管业务场景上线。传统资产托管业务涉及资产委托方、资产管理方、资产托管方以及投资顾问等多方金融机构，各方都有自己的信息系统。传统的交易主要通过电话、传真、邮件等方式进行信用检验，而基于区块链技术的资产托管平台解决了相互信用校验的成本，将业务环节缩短了 60%-80%。

案例 11-23：基于区块链的数据确权及交易溯源

数据共享存在风险。从过往经验来看，金融服务行业在隐私保护与数据应用上的目标往往是矛盾的，需要在数据共享价值与潜在的隐私风险间进行权衡，这也直接导致许多原本似乎很有希望落地的数据共享项目被束之高阁。

贵阳大数据交易所对基于区块链技术的数据共享，起到了重要的示范作用。

贵阳大数据交易所在贵州省政府、贵阳市政府的支持下，于 2014 年 12 月成立，2015 年 4 月正式挂牌运营，成为全国重要的综合性大数据交易服务平台。截至 2018 年 3 月，贵阳大数据交易所会员数达 2000 家，已接入 225 家优质数据源，可交易数据产品 4000 余个，涵盖包括金融大数据、政府大数据、医疗大数据、社会大数据、社交大数据等在内的三十多个领域。

2017 年 5 月，贵阳大数据交易所编制了《大数据交易区块链技术应用标准》，在最新版的交易系统内加入了区块链技术，利用该技术推进数据确权、数据定价、数据指数、数据交易、结算、交付、安全保障、交易溯源、数据资产管理等综合配套服务，实现数据资产的可信交易。（如图 11-13 ）

图 11-13 基于区块链技术的数据共享与交易

第十二章 产业互联与社会治理

12.1 区块链在产业互联网的应用

商品溯源是指追踪记录商品从生产到零售的全部环节，它的实现需要产业链上下游各方共同参与。商品溯源属于一种多环节协同的综合性商业行为，集合了物联网技术、防伪技术、信息系统与溯源机制。

12.1.1 区块链商品溯源及其分类

传统的防伪溯源，是通过防伪码数据和商品实现了一一对应。但这种防伪码是由商家提前编辑好，容易被大规模仿制。造假者只需获得一个真品的防伪码，就可以复制出很多，导致消费者即便购买到了假冒伪劣产品，扫码显示的都是正品。

基于区块链的数字防伪技术，商品信息一经“上链”不可篡改，这就形成了商品上下游产业链的可追溯性，解决了信息不对称的问题。通过区块链技术，消费者等利益相关方能够看到商品从原材料开始，一路来到消费者手上，期间全部流程产生的电子数据信息，保障了产品质量可追溯，品质安全有保障。[21]（如图 12-1 ）

[21] 中国物流与采购联合会，中国物流与区块链创新融合创新应用蓝皮书[M]， 2019.01.

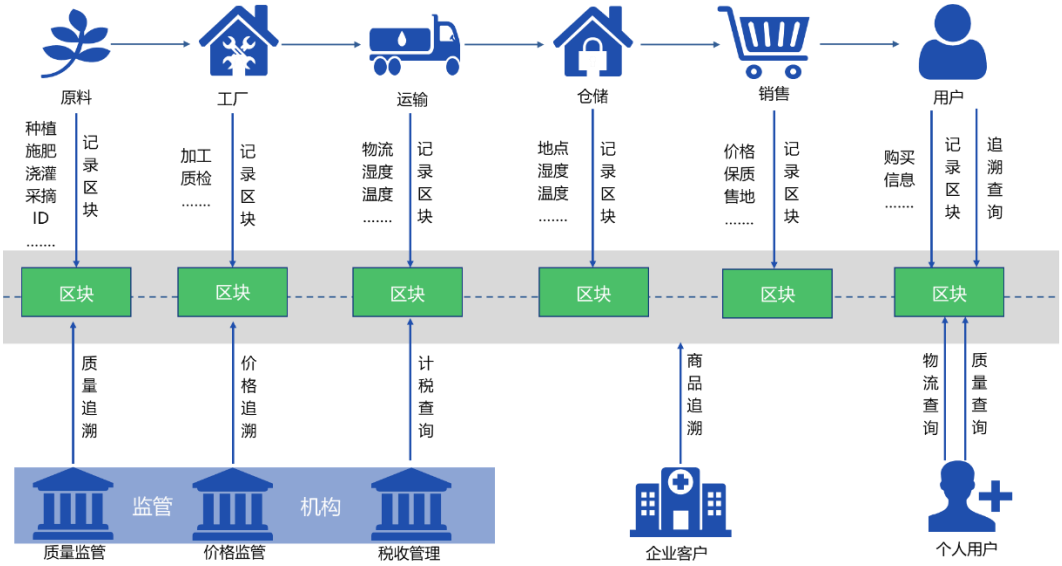

图 12-1 区块链商品追溯应用场景示意图

基于区块链技术的商品防伪，同时具备溯源、防恶性窜货、数据分析等多样化功能，由此实现的商品质量管理模式创新，能够强化商品生产信息互通与共享，提高企业管理效率，降低销售成本，甚至引导供给端生产企业优化产能。

- 防止假冒产品：跟踪最终产品每个部分的来源，因此所有相关方都可以看到审计跟踪，确保商品的真实性并减少了假冒商品；
- 库存和偷窃跟踪：从供应商到零售商的端到端可见性确保了涉及多个供应商的透明度和真实性；
- 退货跟踪：区块链系统可以帮助零售商确保将退回的货物追溯到供应商，以及更好的管理退货的合同；
- 商品再交易市场：对于可以再次或者多次使用的商品，基于区块链组织商品的再交易市场，链上数据提供商品的全生命周期溯源。

针对商品本身的特性，商品溯源可以分为强溯源和弱溯源。

强溯源，是指针对高价值且具有特异性的物品进行上链溯源。比如钻石、名画、定制奢侈品等。将高值特异性物品进行 360 度全息摄影，提取物品特征值，并哈希上链以实现防伪溯源功能。物品特征值的选择要求**“难以造假，易于验证”**。高价值特异性商品溯源防伪，可提高产品信用，降低交易成本，属于区块链商品溯源的强需求。

弱溯源，是指针对非特异性商品，在区块链上以端到端的方式记录供应链数据，从而跟踪库存或打击假货。为此，每个零售实体的每个环节都要参与进来，从工厂、分销商、发货商、仓库一直到店铺，这样每个环节都不存在数据缺口。非特异商品区块链溯源经济效用不强，具有经济外部性。在食品药品安全领域，政府监管将经济外部性内部化，将对区块链商品溯源的弱需求转换为强需求；在其他非政府监管领域，经济外部性较强，对区块链防伪溯源的需求较弱。

12.1.2 区块链商品溯源案例

1）强溯源案例

基于区块链的商品溯源对钻石这样的高值特异商品具有重要意义。据行业数据披露，钻石等产品终端售价的 80%被流通环节消耗，大多为房租等非增值性消耗。基于区块链的商品溯源体系将重建商业信用机制，压缩流通环节消耗，将节约出来的成本分配给消费者和剩余产业链环节。

戴比尔斯（De Beers，全球最大钻石开采公司）钻石溯源系统。2018 年 1 月起，戴比尔斯采用了 Tracer 系统，利用这一技术实现“从矿场到消费者”的全价值链对钻石商品进行防伪溯源。

IBM 在 2018 年春季公布了 TrustChain 钻石认证计划，与一系列黄金和钻石企业包括矿商和零售商，以及第三方检测实验室合作，目的是“为消费者提供信任链”。此前，整个流程中的每个阶段都有自己的跟踪和验证系统，大多数工作是在纸上或是早已过时的软件上面完成。通过 TrustChain，所有信息都可以在一个在线平台获得，包括钻石的重量和特征，黄金的提炼，珠宝的库存单位和价格，以及最终的零售商等等。

2）食品药品溯源

近十年来，从苏丹红鸭蛋、三聚氰胺奶粉、地沟油，到镉大米、毒胶囊、长生疫苗，中国食药品安全问题层出不穷，消费者对食药品安全的信任已然降至冰点。在这种形势下，食药品安全迫切需要引入科学有效的监管机制，而溯源正是最为重要的手段之一。实际上，早在二十年前，我国已经着手建立可追溯管理体系，但直至今日仍未能实现全面有效的食品追溯。这是因为现代食品的种养殖生产环节繁复，加工程序多、配料多，流通进销渠道复杂，出现食品安全问题的概率大大增加，相应的追溯和问责的难度也不断上升。

案例 12-1：沃尔玛与 IBM 合作可信食品计划

IBM 推出的一个新的食品供应链区块链工具，可以追踪食品的供应链路径。IBM Food Trust™使用区块链技术在食品供应链中创造前所未有的可见性和问责制。它通过食品系统数据的许可，永久和共享记录连接种植者，加工商，分销商和零售商每一个生产环节的信息。

沃尔玛基于 Food Trust 把绿叶蔬菜放在区块链上，以保证实时的，

端到端的，从农场到餐桌的产品跟踪并加速食品安全问题的识别、研究和反馈。沃尔玛中国区块链试点项目能够在 2.2 秒的时间内有效追踪所有绿叶蔬菜的源头。而此前，这一过程需要花费 6~7 天。

案例 12-2：家乐福 Auvergne 鸡

零售业巨头家乐福首次在法国使用区块链技术进行商品溯源，标志性的产品是家乐福 Auvergne 鸡。消费者通过扫码能够找出每只鸡的饲养地点和方式，农民的名字，使用的饲料，是否使用过抗生素治疗等信息。从农场到商店的鸡肉的整个过程都将被跟踪记录。目前为止，家乐福已经推出了八种应用区块链溯源技术的产品，如鸡蛋，奶酪，牛奶，橙子，西红柿，鲑鱼和碎牛肉。其创新的系统设计保证了消费者完整的产品可追溯性。

案例 12-3：疫苗电子追溯系统

2019 年 6 月 29 日，十三届全国人大常委会第十一次会议表决通过了《中华人民共和国疫苗管理法》（简称“疫苗法”），于 2019 年 12 月 1 日开始施行。

《疫苗法》第十条规定国家将实行疫苗全程电子追溯制度。国务院药品监督管理部门制定统一的疫苗追溯标准和规范，建立全国疫苗电子追溯协同平台，整合疫苗生产、流通和预防接种全过程追溯信息，实现疫苗可追溯。疫苗上市许可持有人应当建立疫苗电子追溯系统，与全国疫苗电子追溯协同平台相衔接，实现生产、流通和预防接种全过程最小包装单位疫苗可追溯、可核查。疾病预防控制机构、接种单位应当依法如实记录疫苗流通、预防接种等情况，并按照规定向全国

疫苗电子追溯协同平台提供追溯信息。

在《疫苗法》的要求下，疫苗将全程使用冷链运输，并对运输过程中的实时温度、湿度等信息全程追溯，以确保疫苗的合规、有效使用，并能在发生问题后迅速定位责任人与事故原因。区块链技术结合物联网技术将在疫苗全过程溯源发挥重要作用。（如图 12-2 ）

图 12-2 “区块链+物联网”实现疫苗全过程追踪

12.1.3 区块链溯源面临的问题

区块链技术为溯源、防伪场景提供了有力的工具。但是区块链追踪实体货物的一个巨大障碍在于如何从源头上确保数据的真实性。常见的解决方案有：

- 更多地利用 NFC、RFID 等物联网相关技术，以技术录入替代人工录入；
- 在有法律效力的供货合同里对数据上传行为进行明确的规范，让供应商对自己所上传信息的真实性承担相应的法律责任；
- 发动供应链上关键环节关键利益各方的能动性，建立适合的互证机制。

在防伪打击假货层面，区块链溯源只是一种手段、一种工具，如果没有政府监管部门、检测检验部门等相关部门的监管机制配合，一切都是空谈。这就需要强有力的监督机制与惩罚措施配合。一旦发现商家上传的数据存在造假，必将通过法律手段严惩不怠，同时利用区块链溯源配合相关部门及时进行问题商品的精准召回，这样才能实现有效的防伪溯源，提升整个产业链的执行效率。

并不是非要使用区块链技术才能实现这样的货物追踪方式，但通过将相关环境信息上传至区块链，可以根据运输过程中可能发生的环境变化自动执行智能合约，比如疫苗运输过程中的环境数据超标将导致疫苗失效。这意味基于区块链技术方案的自主权与问责制度将要比手动、劳动密集型流程更可靠也更具效率。

但是由于物联网设备会长期存在于生产、运输等外部环境且无人看管，因此其必然面临着数据遭到篡改，甚至物理结构遭到破坏等风险的威胁。因此，区块链商品溯源方案不仅需要保证所收集到的数据经过严格的安全加密，同时也要确保所使用的设备足以抵御恶劣的天气以及居心不良者的攻击。

12.2 区块链在社会治理的应用

党的十九大报告提出，加强社区治理体系建设，推动社会治理重心向基层下移，发挥社会组织作用，实现政府治理和社会调节、居民自治良性互动。党的十九届四中全会通过的《中共中央关于坚持和完善中国特色社会主义制度、推进国家治理体系和治理能力现代化若干

重大问题的决定》提出，坚持和完善共建共治共享的社会治理制度，建设人人有责、人人尽责、人人共享的社会治理共同体。

社区治理共同体既是当前我国社区管理创新的现实基础，也是完善国家治理能力现代化、创新社会建设与社会管理体制机制的重要举措。我国城市社区呈现出社区组织碎片化、社区公共性衰落、社区生活个体化三大新困境。社区治理共同体成为化解城市社区问题的有效理念。共同体以政府、社区、社会组织和居民为主体，以社会再组织化为手段，以实现社区多元主体共同治理为根本目标。社区治理共同体是国家与社会、政府与社会、国家参与社会的自治组织实现合作主义的具体实践。这不仅有利于激发社会活力，更有利于加强基层社会建设，创新社会治理体制。

早在春秋战国时期，商鞅变法做了有记录的最早的社会治理尝试。《商君书·禁使》中论述道：“人主之所以禁使者，赏罚也。赏随功，罚随罪。故论功察罪，不可不审也。夫赏高罚下，而上无必知其道也，与无道同也。故恃丞、监而治者，仅存之治也。通数者不然也。别其势，难其道，故曰：其势难匿者，虽跖不为非焉。且夫利异而害不同者。先王所以为保也。故至治，夫妻、交友不能相为弃恶盖非，而不害于亲，民人不能相为隐。利合而恶同者，父不能以问子，君不能以问臣。吏之与吏，利合而恶同也。夫事合而利异者，先王之所以为端也。” 基于上述理论，商鞅制订了赏罚严明的制度，并“五家为伍，十家为什”编订户口，实行连坐制。实行连坐法的目的，就是要使得人民互相保证，互相监视，互相揭发，一人有罪，五人连坐，即使是

盗跖也没有办法为非作恶。

商鞅通过连坐法及相关赏罚制度实现了群体利益与个人利益一致化，这与美国二十世纪七十年代进行的通证经济研究有异曲同工之妙。

通证经济是在斯金纳的操作条件反射理论和条件强化原理的基础上，形成并完善起来的一种行为疗法。通过某种奖励系统，使目标人群所表现的良好行为得以形成和巩固，同时使其不良行为得以消退。通证经济在污染治理、能源节约、工作绩效评价、现实社区自治、种族融合、军事训练、社区与社会制度设计等方面进行了广泛的社会实践。[22] 通证经济的研究成果在社会治理共同体的建设中将发挥重要的指导作用。

昆明金沙社区“小金豆构筑大平安”本质上就是通证经济在社区治理中的具体应用。（如图 12-3 ）

[22] Alan. Kazdin, The Token Economy A Review and Evaluation [M], PLENUM PRESS, 1977.

- 金沙社区“警务雷达、金豆兑换、卫星布防”警民联动模式，社区志愿者可上报各类信息和案件，经核实后，上报人可获取相应的金豆。若上报案件需要紧急处置，平台工作人员可立即将案件通过“警务雷达”系统派遣给当前辖区正在巡逻的治安队员和志愿者进行处置，参与案件处置的人员也可获取金豆。
- 建立起了志愿者群防群治防控网，近 800 名“金豆哥”散布在社区的各个角落，有效改善了社区治安状况。
- 志愿者们积攒的金豆，可以到社区内的 100 多家金豆兑换商家进行消费。志愿者的金豆除了消费，还可以捐赠给社区的特殊人群。
- 社区成立了“金豆基金”，将募资的所有款项直接汇入昆明市青少年发展基金会账户。每月根据系统记录金豆兑换明细，以现金形式将兑换金豆返还“金豆商家”， 并定期公开基金用途及明细。
- 社区警情同比下降 60%以上，案件同比下降 40%以上，金沙社区也从之前的“脏、乱、差、案件高发”社区变成了盘龙区治安良好的平安社区。

图 12-3 昆明金沙社区社会治理实践

区块链技术结合通证经济，将解决通证经济运行过程中的公平性问题和成本性问题，提高通证经济建设社区治理共同体的投入产出比，加速把通证经济的成功经验在全社会进行复制。

12.3 能源电力领域应用

12.3.1 可再生能源电力消纳

近年来，可再生能源发电量呈现明显快速上升趋势。2018 年，我国可再生能源发电量达到 1.87 万亿 kWh，占全部发电量比重从 2012 年的 20%提高到 2018 年的 26.7%，其中非水电可再生能源发电量占全部发电量比重提高了 5.8 个百分点。可再生能源的快速发展促进了能源结构优化，非化石能源占一次能源消费比重比 2012 年提高 4.6 个

百分点。在此进程中，水电、风电、光伏发电的送出和消纳问题开始显现。为解决可再生能源消纳问题，自 2017 年起，我国先后出台了《国家发展改革委、财政部、国家能源局关于试行可再生能源绿色电力证书核发及自愿认购交易制度的通知》(发改能源〔2017〕132 号)、《国家发展改革委 国家能源局关于印发<清洁能源消纳行动计划（2018—2020 年）>》（发改能源规〔2018〕1575 号)、《国家发展改革委 国家能源局关于建立健全可再生能源电力消纳保障机制的通知》（发改能源〔2019〕807 号）（简称《通知》）等一系列政策，要求落实消纳责任。

12.3.1.1 可再生能源电力消纳业务现状及特点

随着能源结构的不断优化，可再生能源发电占比不断提高，弃风弃光率也在不断下降，然而我国可再生能源电力消纳仍然存在一些问题。一方面我国可再生能源电力供需仍以省内平衡和就地消纳为主，可再生能源电力的间歇性特性，使得可再生能源发电的成本除了电场的建设成本和接网费用外，还包含新增备用容量和调峰等备用成本。我国可再生能源发电项目上网电价高于当地常规电价的部分以及接网费用，通过向电力用户征收电价附加的方式在全国范围内分摊，而备用等辅助服务相关的费用由省级电力调度交易机构在省内平衡，这导致各省对消纳省外的可再生能源电力缺乏积极性。另一方面在《通知》出台之前，我国出台了一系列政策逐步规范优化可再生能源电力消纳市场，但在消纳可再生能源电力方面缺乏激励且市场机制不够健全。欧美国家将配额制和其他补贴政策配合实施，激发部分企业认购

热情，取得了良好的效益。我国对可再生能源电力消纳采取的绿证自愿认购制度。绿证是绿色电力证书的简称，是国家对发电企业每兆瓦时非水可再生能源上网电量颁发的具有唯一代码标识的电子凭证。绿证由于政策激励不够，且中心化管理且只能交易一次，市场化不足导致并没有取得良好的效果，公众对绿证的认购意愿不高。

《通知》中的可再生能源电力消纳保障机制旨在通过设定可再生能源电力消纳责任权重指标，督促消纳困难地区积极采取措施，引导各类市场主体公平承担可再生能源电力消纳责任来解决上述问题，提升各省本地消纳能力，形成可再生能源电力消费引领的长效发展机制，解决可再生能源电力消纳问题，引导用户侧绿色用能。

12.3.1.2 基于区块链的可再生能源电力消纳解决思路

可再生能源电力消纳凭证是电力交易中心统一对可再生能源电力消纳量从源头进行绿色编码，生成可再生能源电力消纳凭证（以下简称“凭证”），每兆瓦时消纳量对应一个凭证，凭证分为水电凭证和非水电凭证，凭证具有唯一编码。基于区块链构建可再生能源电力消纳保障机制，利用区块链技术多方协作、数据可追溯性和不可篡改的特点，进一步提高凭证在签发、交易等全流程的透明性与可控性，为凭证增信。基于区块链的可再生能源电力消纳解决思路如图 12-4 所示，通过将消纳责任权重计算公式、消纳责任权重、凭证等信息上链等方式，可有效保证数据的真实性、不可篡改，使各市场主体积极主动承担自身的消纳责任。凭证的发行和交易通过智能合约自动执行，降低了交易中心的人工成本，可提升可再生能源消纳水平。利用区块链技

术的核心在于可以将可再生能源消纳凭证上链存证，可以在点对点网络中支撑交易的流程，增加凭证的权威性，实现全程溯源，解决凭证核发流程烦琐的问题，便于生成统计报表。同时可防止虚假交易和重复交易，促进可再生能源消纳。

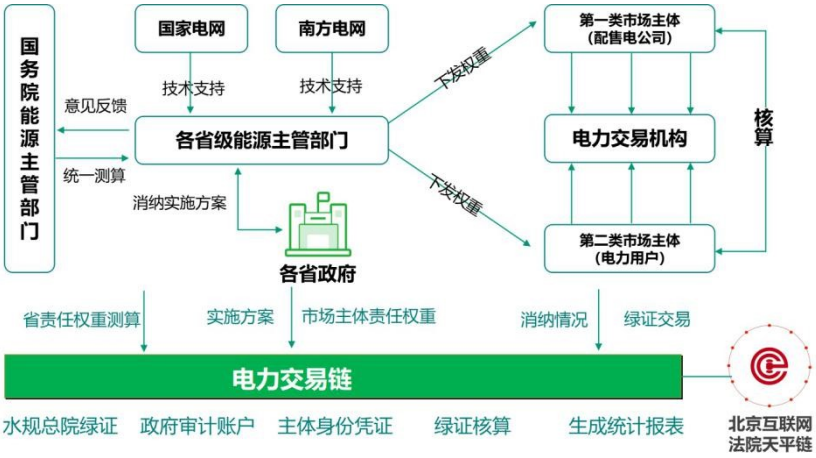

图 12-4 基于区块链的可再生能源电力消纳解决思路

1. 凭证签发

为有效保障消纳责任权重的客观公正，依据《通知》规定，国务院能源主管部门组织有关机构按年度对各省级行政区域可再生能源电力消纳责任权重进行统一测算，并结合各省级能源主管部门会同经济运行管理部门等各方面意见，综合论证后于每年 3 月底前，国务院能源主管部门会向各省级行政区域下达当年可再生能源电力消纳责任权重，各省级能源主管部门根据下发的当年权重制定的本省级行政区域可再生能源电力消纳实施方案，方案内包含年度消纳责任权重及消纳量分配。

可再生能源电力消纳凭证签发流程如图 12-5 所示，电力交易平台组织市场主体和发电厂交易，交易完成后，由交易平台向可再生能源超额消纳凭证交易系统同步发送可再生能源市场化交易的物理执行

结算结果，权重系统依据交易合同和交易信息，通过区块链智能合约对超额消纳量核发相应的凭证。

此凭证具有唯一编码，内嵌对应可再生能源电力的生产者、生产时间、生产地点、电力电量类别、有效期等信息，电力交易中心对以上内容电子签名（包含签名和电力交易中心身份信息）。凭证上链，返回存证地址；把存证地址再补到凭证上。最终生成的凭证下发写入各消纳责任主体的消纳账户。

凭证被核发时通过区块链标记，并设置凭证失效时间，避免凭证在次年被重复统计，同时通过链上共识，确保发电企业所发的每兆瓦时可再生能源电力只会被核发一次凭证，不会被重复核发。

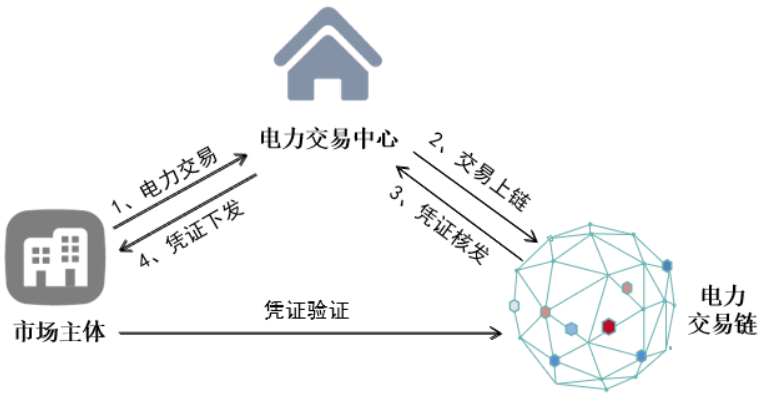

图 12-5 凭证签发流程

2. 凭证交易

按照《通知》要求，超额消纳量交易可作为各省完成责任权重的补充。因此市场主体可以在凭证交易系统上出售超额完成的凭证，或发起凭证购买信息，利用区块链共识机制满足交易双方价格协商，一旦双方对交易价格达成一致即可通过智能合约自动签署合约。交易执行过程，是用购买方的电子签名覆盖出售方凭证的电子签名。

凭证交易流程如图 12-6 所示，市场主体 A 由于未完成消纳量，通过区块链广播发起凭证/消纳量交易需求，市场主体 B 超额完成消纳量指标，也通过区块链发起凭证出售信息。双方通过区块链达成价格共识后，使用区块链电子合同签署凭证交易合同，并将交易合同关键信息上链。在需求方完成支付后，触发凭证转移合约，该合约执行 A 到 B 的凭证转移，增加一条 B 到 A 的“转移”记录，由 B 对 A 的公钥+凭证进行签名，然后上链，市场主体 A 获取到凭证以及凭证对应的链上地址。同时电力交易中心的可再生能源电力消纳系统中对应的消纳量统计信息也自动发生变化，市场主体 A 已完成消纳量增加，市场主体 B 账户消纳量减小。

为确保各省可再生能源电力消纳量指标完成，规范凭证交易，限制了若所在省消纳量没有达到最低消纳量标准，则该消纳责任主体只能在省内市场交易超额消纳凭证，不能跨省交易超额消纳凭证。

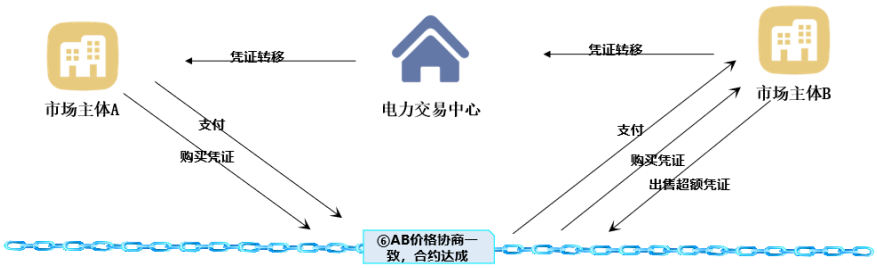

图 12-6 凭证交易流程

3. 凭证核算

凭证在交易过程中始终带有所属方的电子签名，通过电子签名对责任主体分别统计，就可以生成凭证统计报表，进而核算各消纳责任主体的消纳量。

根据《通知》，自愿认购的绿证也可作为各省完成责任权重的补充，

在核算消纳量完成情况时，需计入自愿认购的绿证对应的消纳量。在电力交易中心和可再生能源信息中心之间建立数据共享机制，通过区块链实现凭证交易系统和绿证认购平台的互联互通，当消纳责任主体将认购的绿证相关信息上传到消纳系统，能够快速准确地识别绿证的有效性，一旦判定符合消纳量核算要求，自动计入该消纳责任主体消纳量完成指标，实现消纳量统计报表的快速核算。

4. 凭证验证与追溯

凭证验证与追溯如图 12-7 所示。由于电力交易链全程记录了凭证核发、转移全过程，所以用户都可以对凭证真伪在电力交易链进行验证，追溯核发、转移过程，同时借助区块链上各个参与方共同对凭证签发、交易、核算等全流程形成有效监管。

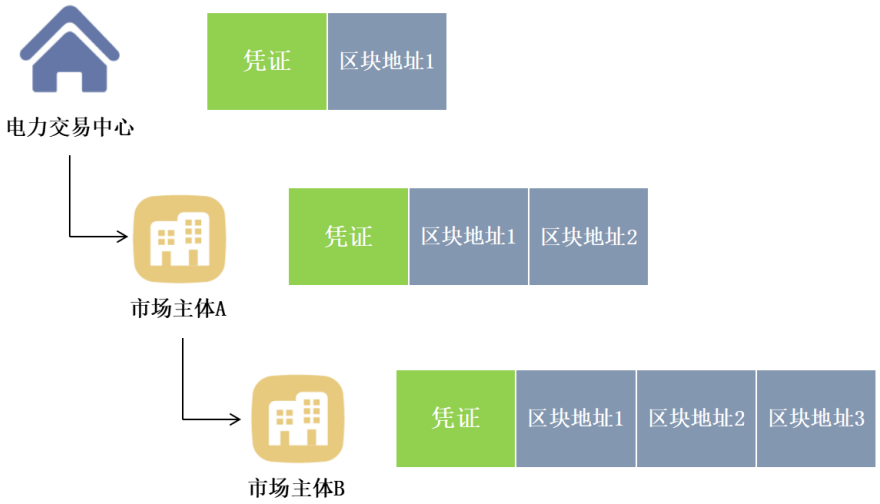

图 12-7 凭证验证与追溯流程

12.3.1.3 基于区块链的可再生能源电力消纳应用成效

凭证交易系统，不仅能够记录各市场主体的消纳量从下发、交易流转到核算完成的全程数据，同时还可以将发电厂、电力交易中心、购电企业以及电量、价格等各种信息附在凭证中，以便用于后续数据

分析。

北京电力交易中心已组织开展了凭证交易系统的研发，并于2020年7月上线试运行。该系统利用区块链可实现核心数据上链存证、智能合约和凭证管理服务，对内实现权重管理、超额消纳量交易、支付清算、消纳核算等应用，对外提供市场管理、数据申报、查询等服务。该系统利用区块链在接近零成本的前提下实现具备法律效力的身份认证，为百万级市场主体提供便捷可靠的身份认证服务，可节约大量第三方数字证书费用，同时确保消纳量核算交易过程公开透明，实现凭证的全过程管理，降低交易运营管理成本、优化管理流程、提高交易效率。该系统将全面支撑可再生能源电力消纳保障机制的实施，促进清洁能源消纳。

12.3.2 碳排放交易

碳排放权是对各行业二氧化碳排放的一种分配和计量方式。政府有关部门结合我国碳减排目标，根据各行业排放情况，对产生排放的各主体分配一定配额的碳排放权。排放超过配额的主体要被处以罚款。多产生的碳排放需要通过额外购买排放权的方式抵消，排放权有余额的参与主体可以将多余部分转移给排放超额的主体，从而获取利润。随着对可持续发展的重视和对节能减排要求的提升，联合国政府间气候变化专门委员会1997年通过《京都议定书》，确立了二氧化碳排放权的认证及其交易机制。

我国各省市碳市场仍以二级市场现货交易为主，主要交易产品包括各省市的碳排放权配额和经审定的项目减排量两大类。根据近十年

统计结果显示，能源行业是最主要的碳排放源。2017 年，发展改革委以电力行业为突破口，按照《全国碳排放权交易市场建设方案(发电行业)》率先启动了全国碳排放交易体系，努力培育市场主体，完善市场监管，扩大市场覆盖范围，逐步建立公开透明、监管完善、运行流畅、具有国际影响力的碳市场。因此，如何利用科技创新手段促进碳市场流畅运行、透明监管等，是我们当下工作重点。

12.3.2.1 碳排放交易业务现状及特点

我国统一碳市场目前尚处于发展初期，2011 年国家发展改革委率先批准北京市、天津市、上海市、重庆市、湖北省、广东省、深圳市开展碳排放权交易试点；2016 年，福建省启动了第 8 个交易试点。2017 年 12 月，国家发展改革委印发了《全国碳排放权交易市场建设方案(发电行业)》(发改气候规〔2017〕2191 号)，标志着全国碳排放交易体系正式启动。截至 2019 年 10 月底，我国碳交易试点地区的碳排放配额成交量达 3.47 亿吨二氧化碳当量，交易额约 76.8 亿元人民币。自 2011 年开展试点以来，我国的碳市场发展取得了一定的成效，但在数据采集、信用监管、信息流通等多个方面依然存在问题。

1.碳排放数据采集缺乏标准，数据真实性、实时性有待考证

数据的不同采集点之间、政府与企业之间、各个企业之间都有可能不同。现实数据的采集由于统计口径和渠道的不同导致整体和局部、经济和能源等数据不匹配。曾有试点专家指出当前存在明显的“自上而下算出来的数，和自下而上算出来的数，对不上。行业协会报上来的数和排放清单的数，也对不上”的情况。

2.碳指标发放、交易无法追踪溯源

碳指标的获得方式有政府配额、有偿竞拍两种，目前仍以政府配额为主。企业得到配额后，多余的部分进入二级交易市场。而整个过程中数据的追踪只有各个站点的数据汇报，无法形成一个交易闭环，数据不能追本溯源，导致对数据的信用存疑。

3.监管制度不完善，缺乏碳指标、碳排放的统一监管体系

国内碳排放交易市场尚未完全成熟，有关市场的交易机制、监管机制等方面不完善。此外，涉及碳排放交易第三方的核证机构，有待进一步培育，认证、认可和登记注册系统要进一步的建立，交易平台建设等技术标准，还需要进一步的协调统一。

12.3.2.2 基于区块链的碳排放交易解决思路

区块链技术可以将现实资产向虚拟资产进行真实映射，适用于涉及所有权的资产交易以及产业链整合。将区块链技术应用于碳交易解决方案中，可以实现对碳交易配额分配、交易、消耗等过程的全流程数据实时跟踪记录，同时可以将企业信息、交易价格等各种数据附加在配额数据中，便于后期对各项数据的综合分析。基于区块链的碳排放权交易解决方案如图 12-8 所示，各级碳排放企业的相关数据全部上链，通过基于区块链技术的数据中心实时跟踪记录各企业能耗数据，政府与碳排放企业间关于配额申请、分配的信息，不同企业间配额交易的信息等，整个交易过程数据安全透明、可追溯，有效解决了现有交易中存在的数据不真实、追溯难、监管难等问题。

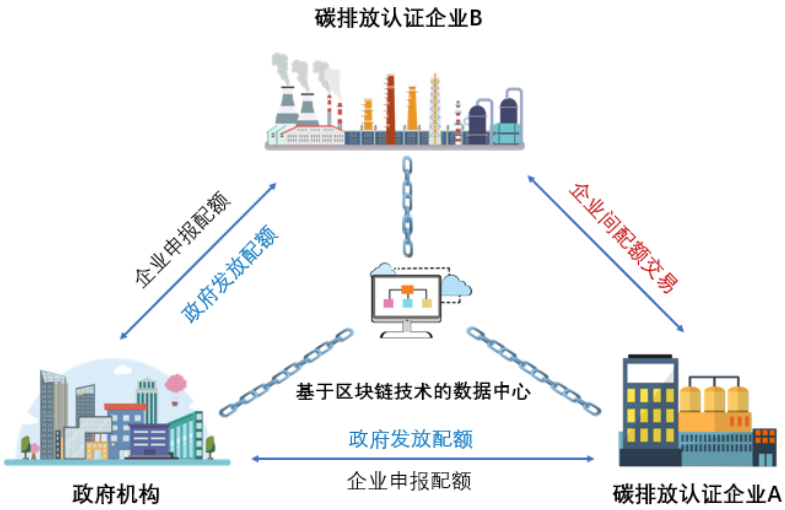

图 12-8 基于区块链的碳排放权交易解决方案

1. 碳排放权配额认证

政府对碳排放企业配额认证工作量巨大，且由于碳排放权的频繁交易，使得追溯过程极其复杂，数据可信度不高。区块链能够为碳排放权的认证和碳排放的计量提供一个智能化的系统平台，具体而言，采用区块链技术搭建碳排放权认证和交易平台，给予每一单位的碳排放权专有 ID，加盖时间戳，并记录在区块链中。每个企业的排放量实时向区块链进行更新；区块链系统将根据企业排放情况，采用智能合约方式自动确认碳排放权消耗量；碳交易时，每当碳排放权发生一次所有权转移，交易信息即记录在区块链中，并且不可篡改；区块链系统自动对超标排放的企业进行罚款。

2. 市场信用监管

结合区块链技术构建碳排放权认证交易平台，将监管政策等内容纳入平台的智能合约系统，具体如图 12-9 所示。当企业有碳排放权买入或卖出需求时，首先在交易平台提出买、卖申请，交易平台通过

智能合约系统自动审核、判断买卖双方是否符合信用条件，当双方均符合信用要求时，系统自动匹配交易双方并完成交易。企业的每一次交易行为均会被记录，当有企业发生不守信用的行为时，相关行为会被实时记录到区块链系统。在进行下次交易时，可以对企业征信进行查询。这样可以最大程度地对参与碳市场交易企业的信用进行监管、客观评价，从而得到真实有效的企业信用情况。

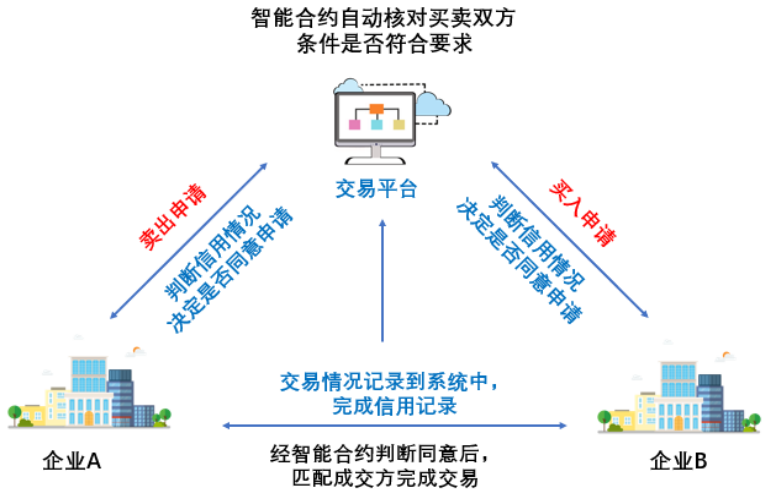

图 12-9 区块链技术在交易信用监管中应用

3. 基于碳指标的企业金融

近几年，我国碳金融市场发展势头强劲，但传统市场中常见的存在产品种类单一、信息不对称等问题在碳金融市场中同样明显，而区块链技术去中心化、开放透明、可信度高等特点，与新兴碳金融市场发展的需求相契合。

在基于区块链技术的碳排放权认证交易平台中，各企业交易数据实时上链，利用区块链上的数据具有不可篡改、可追溯性等特性，为碳排放企业建立征信系统，征信数据将为银行贷款、碳金融产品发放

提供有效依据，同时可以吸引国内外资本进入，促进碳金融体系的建立。如图 12-10 所示，区块链交易平台通过记录碳排放企业交易信用数据，并将数据提供给各类金融、非金融机构，当碳排放企业向金融、非金融机构申购已发行的金融产品、贷款时，金融、非金融机构可以对企业快速做出评估，市场交易更加快速、有序。同时，政府机构对整个市场交易行为、参与主体等进行监督，保证碳指标的有序流动与“碳行为”追踪。

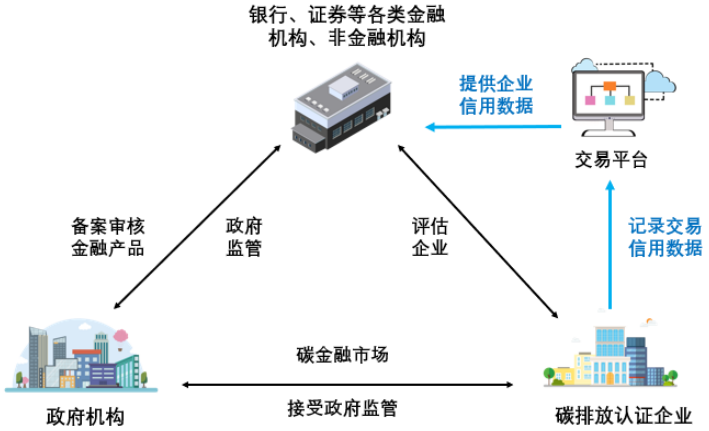

图 12-10 碳金融市场体系

12.2.3 基于区块链的碳排放交易预期成效

应用区块链技术能够为碳排放权的认证和碳排放的计量提供智能化的系统平台，实现智能化碳排放权配额认证，保证每一单位碳排放权的来源以及交易路径能被追根溯源。此外，根据碳排放交易的路径，还能够计算碳排放在电网中的流动情况，为碳排放流的计算提供基础数据。区块链上智能合约可记录自动实现碳排放的计量认证以及确认配额是否被使用，让碳排放的计量过程更加智能化，整个流程变得透

明、可视、公开。同时，智能合约的自动执行，可减少业务执行过程中的人为干预，保证政策执行力，提升业务管理效率，降低管理成本，保证碳排放市场高效、快速地流通。

第四篇 区块链的重新诠释与未来展望

第十三章 区块链的重新诠释

13.1 区块链技术哲学的重新诠释

2008 年 9 月，以美国四大投行中的雷曼兄弟的倒闭为开端，金融危机在美国爆发并向全世界蔓延。这次金融危机是美国自大萧条以来最严重的一次金融危机，被称为金融市场的“911”。为了应对危机，美国政府采取量化宽松等政策，不断增发美元刺激经济。这些政策引起了民众对美国经济政策是否合理的广泛质疑。

在这样的时代背景下，中本聪在 2008 年 10 月 31 日发布了比特币白皮书。仔细探究比特币网络社区，以及之后的区块链虚拟货币项目，它们基本上都基于这样一些基本的哲学理念：

- 技术至上，代码即法律；
- 去中心化，政府不可信；
- 社群自治，绝对民主化；
- 私人财产，隐私要保障。

总结而言，比特币技术哲学本质上是利用技术构建无政府主义乌托邦！比特币秉持的哲学理念在很长一段时间内都主导了区块链行业的发展。无政府、反监管、自金融成为过去一段时间内区块链项目的主导思想和重要特征。因此，在法律制度不完善的地区，非法集资和诈骗成为区块链项目的主要表现形式，而比特币也主要用于洗钱和地下非法交易。

无政府主义的理想与现实的反差在以比特币为代表的区块链原生

态中表现的淋漓尽致。比特币与区块链的“原教旨主义”信仰者们，宣称要基于区块链打破信息不对称，消除垄断与不平等，实现个体自由与权力的回归。但现实是，在 ICO、IEO、IMO、Defi 等无数新名词的掩盖下，肆意的进行传销、非法集资、和金融诈骗。无监管的虚拟货币交易所发布虚假交易信息，自雇团队“坐庄”，堂而皇之“割韭菜”。区块链虚拟货币领域的无政府主义者，不是不要政府，是要他们自己的小圈子、小政府说了算，制造混乱并从中牟利，金钱是他们的唯一信仰。

因此，有必要将区块链技术与比特币的无政府主义哲学剥离，重新基于区块链的技术特征，诠释区块链技术的经济特征和哲学特征。

区块链技术，作为密码学、分布式计算、分布式网络技术的综合运用，具有不可伪造抵赖、数据不可篡改、分布式共享账本、智能合约等技术特性，可以实现从信息互联网到信任互联网的跨越，从个体信息化的数据孤岛到全链条信息化的数据协同，将数字经济发展深入推进到数字社会建设，迈向共建共治共享的社会命运共同体。（如图 13-1 ）

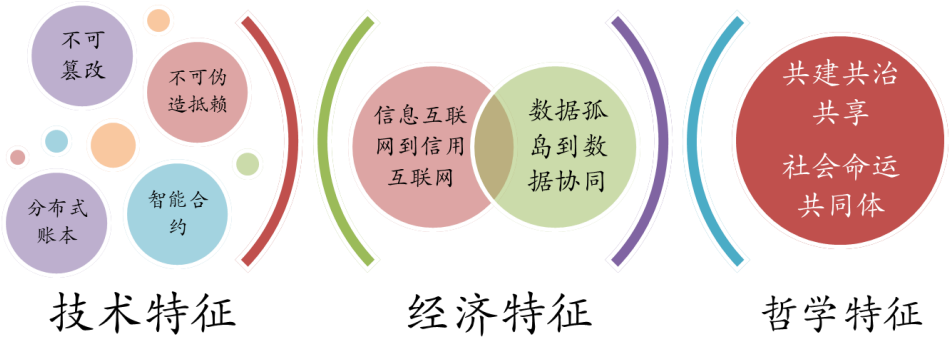

图 13-1 区块链技术、经济、哲学特征的重新诠释

13.2 选择区块链应用的标准

区块链解决了分布式场景下的信任互联与数据协同问题，因此理论上任何一个多方参与过程，并需要共享信息、数据与价值交换，智能合约降本增效都是区块链可以发挥作用的地方。（如图 13-2 ）

图 13-2 区块链技术的适用场景

据普华永道 PWC 2018 年报告[23]显示，节约成本、提高可追溯性和透明性是区块链项目的三大驱动力。

在具体判断某个场景是否适合区块链应用时，有“强、弱、伪、非”四个标准可以参考：

- 强需求：通过数据主权化管理和智能合约解决用户在原有中心化系统难以解决的痛点，解决方案中存在最大利益主体，且付费意愿强；
- 弱需求：原有中心化系统可以解决，但也适合区块链应用场景，区块链作为一项成熟技术集成，同等效果下实施周期短，效果

[23] PwC, Blockchain: The next innovation to make our cities smarter [M], PwC India, 2018.

好，原有用户不愿付费改变，但新增用户愿意付费；

- 伪需求：需求存在经济外部性，多方受益，但找不到项目最大利益主体，无人愿意付费承担成本；
- 非需求：区块链对比中心化系统无任何优势，为区块链而区块链。

分布式商业场景中的外部性又称为溢出效应，指一个人或一群人的行动和决策使另一个人或一群人受损或受益的情况。外部经济（正外部性）就是一些人的生产或消费使另一些人受益而又无法向后者收费的现象；外部不经济（负外部性）就是一些人的生产或消费使另一些人受损而前者无法补偿后者的现象。

当外部效应出现时，一般无法通过市场机制的自发作用来调节以达到社会资源有效配置的目的。让外部性内部化，即通过制度安排经济主体经济活动所产生的社会收益或社会成本，转为私人收益或私人成本，一般通过政府干预来实现。

13.3 区块链技术与应用的挑战

区块链技术的发展速度较快，国内外的不少组织机构、学者以及企业都在对它进行研究和开发利用，这也从客观上说明了其价值已经得到了各行各业的广泛认可。但是不可否认的是，此项技术的发展并不成熟，仍然有很多问题有待解决，特别是在与不同领域的应用相结合的过程中。针对不同行业的特点，区块链技术仍然面临着许多问题，在实现其技术运用的过程中还存在不少挑战。

1）安全保密

区块链技术的安全性是完全建立在非对称密钥技术上的。它利用了现代计算机技术难以在有效时间内破译私钥的特点保障区块链体系中加密系统的安全。然而，量子计算却对非对称密钥技术有直接的威胁。2019 年 10 月谷歌的 Sycamore 量子处理器在 200 秒内，完成了世界上最强大的超级计算机需要 10000 年才能完成的计算，实现了名为“量子霸权”的里程碑。虽然这尚不足以说明谷歌的量子计算机能立刻威胁区块链系统的加密算法，但这意味着量子计算机的研发取得了惊人的进步，区块链加密体系可能面临的威胁已经看到了苗头。如果不尽早研究抗量子算法在区块链加密体系中的应用，则有可能导致区块链体系在不久的未来受到直接的威胁。

世界顶级安全专家、世界级黑客 Benjamin Kunz Mejri 在 2017 中国互联网安全大会上曾经说过“没有攻不破的系统”。任何技术的安全性都是相对的。区块链技术应用的场景多为核心、涉密程度较高的环境，一旦出现安全漏洞，将造成重要信息和数据资料的泄露，后果不堪设想。

因此，安全问题是区块链应用方面需要解决的首要问题。这里的安全问题既包括区块链技术可以应用的对象，也包括此项技术本身。区块链技术包含共识机制、加密算法、智能合约和分布式系统等多个模块的内容，系统的正常运转需要对各个模块进行合理、高效的组合运用。因此，区块链的安全问题既有可能来自外在的主动攻击（如量子计算），也有可能来自系统内部设计所存在的缺陷。例如，不完善的加密算法可能带来安全漏洞，不恰当的共识机制可能会造成关键时

刻出现系统崩溃的现象。

另外，对区块链技术在被正式应用之前的保密性评估与认证，目前还没有专门的机构负责，在应用的性能测试方面还缺乏明确的标准和依据。[24]

2）通用型应用与特殊性应用相结合

在金融、供应链等领域，目前已经开发出了不少区块链技术的商用产品，数字政务在开发具有行业特色的特殊性应用时，也应该关注技术相对成熟、通用性较强的产品。

国际上较大的区块链开源社区包括以太坊和超级账本项目等，不少区块链应用都是由它们衍生出来的，并且已经有了不少成功的案例。如果能够将这些发展较为成熟的应用与场景特点相结合，将会在应用的开发过程中有效节约成本和时间，并且能够在应用的稳定性方面得到一定的保障。目前，还缺少适当的机制和评价体系对基于区块链技术的产品进行全方面的评估，那些运行同样稳定且性能可能更加优良的应用产品很难被发现。

3）大文件数据的存储

目前，区块链作为账本数据库，存储的数据类型多为文本，单个文件的数据量都不是很大。随着技术的不断发展，应用中使用的文件资料格式也在发生改变，不仅仅局限于文本数据，未来更多的可能是以视频材料为代表的多媒体资源，但这些文件通常所占存储空间较大，在目前的区块链系统结构下很难完成存储。以太坊虽然在理论上可以

[24] 国家互联网金融安全技术专家委员会，区块链技术安全概述[M]，2018.08.

进行视频文件的存储，但因为要涉及将文件分段并分别计算哈希值，随之产生的数据量也相对较大，费用成本高昂，所以目前其只能作为技术手段的验证．并不适合大规模应用。

4）“价值孤岛”问题

自 2009 年比特币主网上线到现在，区块链诞生了各种不同形态的链，但是目前这些链自成体系，逐渐形成了“价值孤岛”，链与链之间进行资产交换十分困难。所以如何通过技术创新来实现区块链之间的互联互通，实现区块链“孤岛”间价值流动的畅通无阻，成为当前区块链发展的重要挑战。

另外，不只是区块链链上资产交换存在挑战，链下资产与链上资产的联动也同样面临很大的挑战。目前成功的区块链案例里的资产是虚拟的，全部是在线上的闭环里进行流通，没有跟真实世界相对应，线下资产也存在上链难的问题。与区块链之外的世界进行对接，需要考虑实现方式以及实现成本，这部分的可行性与普及性要很大程度上取决于物联网的发展，取决于各种传感设备和具有计算能力的微小设备的演化。

5）人才缺乏的挑战

区块链技术本身就是一个非常复杂的技术，它涉及密码学、计算数学、人工智能等诸多跨学科、跨领域的一些前沿学科，一些普通的工程师是很难在短期内去完全掌握它的。目前区块链技术人才的匮乏亦是成为制约区块链行业发展的主要瓶颈之一，人才欠缺无疑是区块链产业发展的一大挑战。

13.4 区块链发展建议

区块链在发展初期从技术层面上来说，在得到大规模应用和推广之前，技术的可落地性、有效性、可扩展性、兼容性等方面均有达不到人们预期的可能，大规模推广商用的局限性还依然存在。

从监管和法律风险上来说，由于其数字货币的存在，区块链技术的应用和发展也可能存在相应的风险。所以针对目前区块链的发展现状，国内区块链的发展建议应从技术和政策两个层面出发，推动和拉动区块链的发展。

在技术层面，通过技术创新来推动区块链的发展。首先，组建专门攻关小组；以专攻小组的形式积极参与区块链核心技术开发，密切观察和参与区块链最新进展，并努力进行技术创新。其次，加强核心技术攻关；国内重点企业、科研、高校和用户单位联合加快技术攻关，加大研发投入力度，建设区块链通用开发平台，降低应用成本。再者，要密切跟踪量子计算技术的发展，尤其关注抗量子算法在区块链技术中的应用以及如何解决区块链底层架构的安全所面临的威胁。最后，建设人才培训基地；鼓励和支持重点高校设置区块链专业课程，加快建立人才培养体系。

在政策层面，通过政策鼓励拉动区块链发展。首先，设立区块链应用创新试点区域，在试点地区简政放权、放管结合，放宽区块链准入限制，加强事中事后监管，营造有利于区块链发展的环境。其次，资金扶持；鼓励和支持有条件的重点企业联合，设立投资基金，加快投融资和并购，推动关键技术攻关。最后，弥补政策空白，紧密跟踪

并加大力度研究国际政策走向，并结合本国区块链技术和应用发展情况制定相关政策、建议。

第十四章 数字社会的未来畅想

14.1 数字孪生，镜像世界

2019 年中国国际大数据产业博览会上，《连线》杂志创始主编、《失控》作者凯文·凯利发表了以“数字孪生，镜像世界”为主题的演讲。这是凯文·凯利对未来 20 年数字世界的描绘，就像世界上所有信息的连接（互联网），以及人与人之间的连接（社交媒体）一样，数字孪生和镜像世界将物理世界与虚拟的数字信息链接起来，在人与计算机之间创造出一种无缝的交互体验。

14.1.1 数字孪生（Digital Twin）

数字孪生：是充分利用物理模型、传感器更新、运行历史等数据，集成多学科、多物理量、多尺度、多概率的仿真过程，在虚拟空间中完成映射，从而反映相对应的实体装备的全生命周期过程。

NASA 最早将数字孪生的理念应用在阿波罗计划中，开发了两种相同的太空飞行器，以反映地球上太空的状况，进行训练和飞行准备。通过传感器实现与飞机真实状态完全同步，这样每次飞行后，根据结构现有情况和过往载荷，及时分析评估是否需要维修，能否承受下次的任务载荷等。[25] 在产业界，数字孪生的概念最早由密西根大学教授迈克尔·格里弗斯于 2003 年提出，并应用于产品生命周期管理。2014 年，迈克尔·格里弗斯在其撰写的《Digital Twin: Manufacturing Excellence through Virtual Factory Replication》白皮书中对数字孪生的理论和技术体系进行了系统的阐述。在此之后，数字孪生逐

[25] E. Glaessgen and D. Stargel, The Digital Twin Paradigm for Future NASA and U.S. Air Force Vehicles, 53rd Structures, Structural Dynamics and Materials Conference, 2012.

渐被产业界广泛接受。数字孪生被 Gartner 评为未来最为重要的十大关键技术之一。Gartner 认为，到 2021 年，一半的大型工业公司将使用数字孪生，从而使这些组织的效率提升 10%。数字孪生的发展历程如图 14-1。

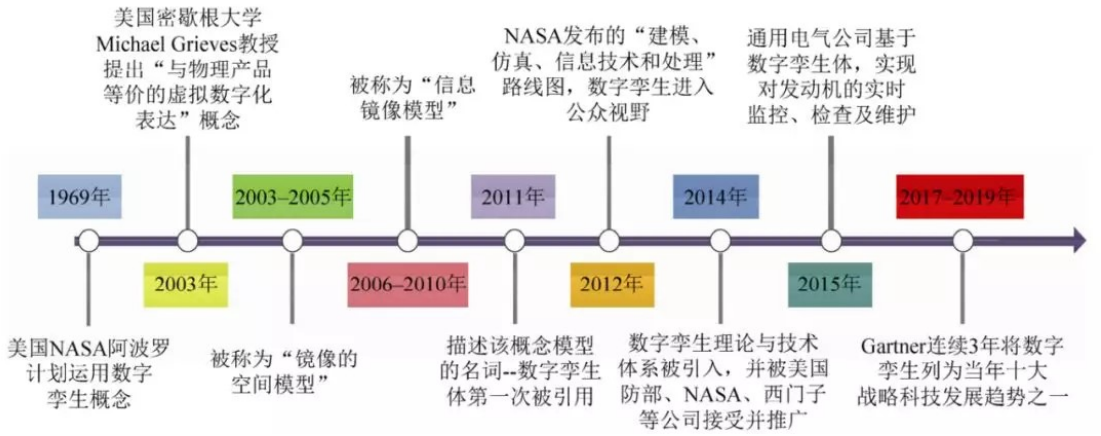

图 14-1 数字孪生的发展历程

从概念上来看，数字孪生有几个核心点：[26]

- 一是物理世界与数字世界之间的映射；
- 二是动态的映射；
- 三是不仅仅是物理的映射，还是逻辑、行为、流程的映射；比如生产流程、业务流程等。
- 四是不单纯是物理世界向数字世界的映射，而是双向的关系，也就是说，数字世界通过计算、处理，也能下达指令、进行计算和控制。
- 五是全生命周期，数字孪生体与实物孪生体是与生共有、同生同长，任何一个实物孪生体发生的事件都应该上传到数字孪生

[26] M. Grieves, Digital Twin: Manufacturing Excellence through Virtual Factory Replication, Michael W. Grieves, LLC, 2014.

体作为计算和记录，实物孪生体在这个运行过程中的劳损，比如故障，都能够在数字孪生体的数据里有所反映。

数字孪生诞生于工业生产制造领域，但是目前数字孪生目前的应用远远超越工业制造领域。数字孪生催生智慧城市 2.0。随着 ICT（信息、通信、技术）成为智慧城市发展的主要动能，移动通信、互联网、云计算、物联网、人工智能、大数据在智慧城市都得到了广泛应用。全域感知、数字模拟、深度学习等各领域的技术发展也即将迎来拐点，这使得城市的数字孪生应运而生。

智慧城市是把新一代信息技术充分运用在城市中各行各业，是基于知识社会下一代创新的城市信息化高级形态。智慧城市实现信息化、工业化与城镇化深度融合，有助于缓解“大城市病”，提高城镇化质量，实现精细化和动态管理，并提升城市管理成效和改善市民生活质量。

数字孪生在智慧城市发展与建设中的核心价值在于，它能够在物理世界和数字世界之间全面建立实时联系，进而对操作对象全生命周期的变化进行记录、分析和预测。智慧城市中的数字孪生可以分为四个阶段（如图 14-2），分别是：

- 对城市现状进行精准、全面、动态映射的现状孪生；
- 从历史数据中学习、分析、识别、总结并发现城市运行规律的学习孪生；
- 人工监督下模拟不同环境背景下的发展情景的模拟孪生；
- 最终通过实时数据接入与人工智能自动决策的自主孪生。

图 14-2 数字孪生的四个层次

智慧城市数字孪生的发展还有很长一段路要走。数字孪生高度依赖物联网所采集的数据和信息，而就目前的技术水平来看，精细化尺度下城市数据的全域感知和历史多维数据的获取，依旧有难度。智慧城市物理实体空间的数据还不够详尽，仅处于现状孪生的初级建设阶段。

14.1.2 镜像世界（Mirror World）

镜像世界，是耶鲁大学计算机科学家 David Gelernter 在 1991 年提出的概念。镜像世界是将一些巨大的结构性的运动的真实生活，像镜像图景一样嵌入到电脑中，通过它你能看到和理解这个世界的全貌。

如今人类已进入大数据文明当中，承载大数据的数字平台既是用户的应用中枢，更是重要的基础设施，其根据发展路径可以分为三个阶段：

- 第一个数字平台是基于互联网，人类可以把所有信息进行数字化并进行互联，使知识受制于算法的力量，这个时代的代表者是谷歌、百度等公司；

- 第二个数字平台是人类关系网络，人类的行为和关系置于算法的力量之下，可以进行数字读取，代表者是 Facebook 和微信；
- 第三个数字文明平台就是镜像世界，它将整个现实世界都 1:1 映射变成数字社会，这其中大数据、人工智能、区块链都将作为基础技术加以应用。

现实中的人和虚拟的人也可以成为一个镜像，当真实和虚拟进行叠加，整个世界都变成机器可读的世界。

人们可以去搜索世界的任何东西，只要有信息就可以做任何事情，也可以把这个世界进行归类，把它变为一本目录，所有与互联网连接的东西都将连接到这样的镜像世界。

镜像世界融合了当下多种技术，比如人工智能、VR/AR 等，但想真正实现镜像世界还需要大量的基础设施，同时需要计算机科学的突破，大量需要实时操作的数据也需要新算法、新的计算机科学突破来处理。

镜像世界里，像 Siri 这样的人工智能助理将有一个具象化形像，可以与人类产生互动。它们将来不仅能够听见人类的声音，还能看到人类的虚拟化身，捕捉到脸部、手臂之类的动作变化、细微表情和情绪波动。

未来的数字世界将被数据所包围，不管是建筑还是虚拟的人物都会由数据组成，所有这些数据都要进行抓取，然后进行处理、存储，这将是一个规模庞大的数据量。

在大数据的世界，镜像世界的另一大优势在于你可以随时随地组

织数据，可以将有关建筑物的数据放在建筑物本身所处的地方，一切都是三维的。这样组织数据就好像电脑桌面上的文件夹，帮助人类建立对三维世界的感知。

14.1.3 数字科技驱动未来

数字孪生的出现源于感知、网络、大数据、人工智能、控制、建模等技术在最近十年的集中爆发。尤其是传感器和低功耗广域网技术的发展，将物理世界的动态，通过传感器精准、实时地反馈到数字世界。数字化、网络化实现由实入虚，网络化、智能化实现由虚入实，通过虚实互动，持续迭代，实现物理世界的最佳有序运行。

根据德勤研究报告[27]的观点，数字孪生由六大部分组成：

- 一是传感器：物理世界中的传感器负责搜集数据、传递信号；
- 二是数据：传感器提供的实际运营和环境数据和企业的生产经营数据合并形成数字孪生的数据来源；
- 三是集成：传感器通过集成技术（包括边缘计算、通信接口等）实现物理世界和数字世界之间的数据传输；
- 四是分析：利用分析技术开展算法模拟和可视化程序，进行大数据分析；
- 五是模型：基于上述数据与信息，建立物理实体和流程的数字化模型，通过模型计算物理实体和流程是否出现错误偏差，从而得出解决错误偏差的方式和行动；
- 六是控制器：基于模型计算的结果，通过控制器开展行动，调

[27] 德勤咨询，2019 技术趋势报告：超越数字化[M]， 2019.03.

整和纠正错误。

以数据为核心的城市生态链构架了智慧城市的顶层设计，形成以共享信息为中心、各行业协同实现的“感知—应用—共享信息”的智慧城市模式。在区块链、大数据、人工智能、云计算、物联网等新兴数字科技的推动下，多维的海量城市数据也逐步以不同方式被挖掘并应用在智慧城市的研究和实践中。

数字孪生的核心原则是，对于一个物理实体或资产来说，数字等价物存在于虚拟世界中。复制一个实体——无论是机器、基础设施还是生物——数据都是极其重要的。所需数据的性质将超越目前收集的数据。由物理属性、对象间交互和未来状态组成的新数据流将在数字世界和物理世界之间无缝交换。

数据的真实、准确、完整、安全是数字孪生的基础。就公共基础设施而言，错误的数据会导致城市治理的混乱；就企业而言，篡改基础数据可能导致预测出现偏差，使竞争走上错误的轨道；当涉及到个人，任何人都不愿意看到的是自己的健康状况隐私泄露，并围绕它推销产品。

区块链技术使数字孪生走上正轨。以区块链技术的核心特性——不可抵赖伪造、不可篡改、智能合约、分布式共享账本——为骨干，数字孪生能够更好地创新，并保持数据的可信与安全。

物联网设备从物理世界收集数据并传输到数字世界，可以使用区块链技术进行保护，保证数字孪生程序的数据不变性。物理世界的历史可以准确地存储和回放。通过使用区块链智能合约，多方利益有关

者、合作者和竞争各方可以被置于一个公平开放的数字孪生交互场景。利益攸关方成为把关人，在不损害敏感信息和集体利益的前提下，加强透明度和问责制。区块链技术实现了物理世界和数字世界的连接。（如图 14-3）

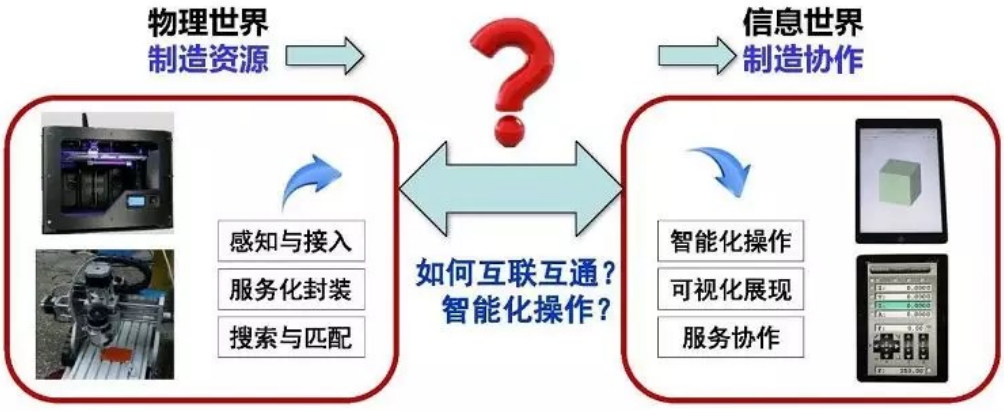

图 14-3 区块链实现物理世界与虚拟世界的可信连接

值得注意的是，在所有关于数字孪生的描述与讨论中，都局限在物理世界实体与数字世界的映射与交互上，没有涉及物理世界经济活动与信息的映射。要实现真正的镜像世界，必须将与物理世界有关的经济活动与信息同步映射到数字世界。典型的如城市基础设施工程建设领域，必须要将建设过程中的工程造价信息同步镜像。区块链为资产属性的完整数字镜像以及未来的经济活动数字化提供解决方案。

在数字孪生、镜像世界的理念引领下，在数字科技的驱动下，人类社会数字化迁移的大潮即将到来。

14.2 数字货币战争

基辛格有句名言：“谁控制了石油，谁就控制了所有国家；谁控制了粮食，谁就控制了人类；谁掌握了货币发行权，谁就掌握了世界。”大国之间的金融和货币战从来没有停止过，争夺货币主导权的斗争也

一直在持续。任何一个国家，走向繁荣的战略选择，都不可能避开的这样一个挑战性问题。自从二战之后，英镑拥有的储备货币地位被美元夺走，美元就一直处在世界经济和结算的中心。

起源于区块链技术的数字货币形态和理念，其深入发展将成为中美货币金融博弈的重大变数。数字货币不但带来技术革新和支付革命，而且将是未来中美货币战和铸币权博弈的主战场。

数字货币不同于电子货币。金融体系经过数百年的发展，在信息技术的推动下，已经形成了基于账户和现金的相对完整的治理体系。账户是实名制的，基于账户可以执行反洗钱、反恐怖融资、防止用于网络赌博和任何网络犯罪活动的功能。现金是匿名的，用于满足小额支付场景以及大众金融的需求。电子货币，本质上是一类法定的，与银行账户关联的，由实物或者非实物作为载体的互联网支付技术。数字货币则更多保持了现金的属性和主要特征，满足了便携和匿名的需求。数字货币脱离了原有的银行账户体系，与现金类似，具有支付即清算的特征，因此也脱离了现有国际支付清算体系的束缚。

2016 年，中国人民银行提出发行“主权数字货币”这一设想。主权数字货币是由主权中央银行发行的、加密的、有国家信用支撑的法定货币。以国家信用为保证，可以最大范围实现线上与线下同步应用，最大限度实现交易的便利性和安全性。主权数字货币本质上仍属于纯信用货币，但主权数字货币可以进一步降低成本，应用于更为广泛的领域。2019 年，中国人民银行宣称其主导设计的主权数字货币 DC/EP 已经完成了所有的技术准备。

2019年10月24日,Facebook创始人扎克伯格在美国国会的Libra听证会暗示:即将崛起的中国数字货币可能损害美元在全球贸易和金融中的主导地位。

2019年11月11日，曾获得2011年德意志银行金融经济学奖，并于2001年至2003年担任国际货币基金组织首席经济学家,现任哈佛大学经济学和公共政策教授Kenneth Rogoff发表文章《即将降临的高风险数字货币战争》[28]。文章表示，对美国而言，真正的挑战不是Facebook提出的天秤币，而是像中国计划的那样由政府支持的数字货币。一个广泛使用的、由国家支持的中国数字货币肯定会对美国利益产生影响，尤其是在那些中国的利益与西方利益不一致的地区。

2019年11月19日，哈佛大学肯尼迪学院旗下的贝尔弗科学与国际事务研究中心举办一次针对数字货币的危机模拟——“数字货币战争：一次国家安全危机模拟”，多位来自哈佛大学和MIT的专家学者以及前美国政府高官参加讨论。

此次模拟的危机发生时间定于2021年11月19日。在假设的情境中，朝鲜利用中国的央行数字货币（DC/EP）躲避了美国对其实施的经济制裁并成功向日本关岛附近的菲律宾海域发射一枚导弹。由于朝鲜和中国的经济往来都在中国自主的基础设施上进行,所以美国无法获取朝鲜的经济活动的信息。也就是说，在该情境中，中国央行发行的数字货币极大地破坏了美元在全球经济体系中的霸权地位。

讨论中，麻省理工学院管理学院全球经济与管理实践教授、美国

[28] Kenneth Rogoff, The High Stack of Coming Digital Currency Wars [OL], http://jordantimes.com/opinion/kenneth-rogoff/high-stakes-coming-digital-currency-war , 2019.11.11.

商品期货交易委员会前主席Gary Gensler认为，中国将资金从长期使用的SWIFT系统中转移出来，这是一个严峻的挑战。哈佛大学校长，美国前财政部长Summers表示同意，并指出华盛顿一直依赖SWIFT系统作为在面对国家安全威胁时施展影响的重要工具。随着中国数字货币的崛起，美国有失去这一影响的危险。如果美国拥有数字货币，反而可能会增加冲突，使世界走上“完全破碎”的道路。

中国央行数字货币DC/EP呼之欲出，而美国政府在数字货币的探索上已经落于人后。此次多位美国前政府官员组织数字货币战争演习，显然已经意识到数字人民币对于美元主导地位的动摇。模拟演习最后给出了两个选择：加强SWIFT系统和探索美国的数字货币。

总之，数字货币将颠覆现有的国际支付清算体系，进而带来国际贸易与金融体系的解构与重建。这个过程一定不会是风平浪静、一帆风顺的。数字货币战争不仅仅是文学家笔下的阴谋论，而是在可见的未来一定会出现的过程。经历数字货币战争后建立的数字世界新秩序，才是全世界数字社会发展的牢固基石。

中国通信学会

地址：北京市海淀区万寿路 27 号院 8 号楼

邮政编码：100840

联系电话：010-68203021

传真：010-68203004

网址：https://www.china-cic.cn/