中国区块链技术和应用发展研究报告

（2018）

编写单位：中国区块链技术和产业发展论坛

2018年12月18日发布

序

当前，国内外形势正在发生深刻复杂变化，我国发展仍处于重要战略机遇期。与此同时，新一轮科技革命和产业变革正在重构全球创新版图、重塑全球经济结构，以人工智能、量子信息、移动通信、物联网、区块链为代表的新一代信息技术加速突破应用，与制造、数字经济等产业深度融合，加快促进实体经济高质量发展。

区块链技术作为一种目前主流的分布式记账技术，利用巧妙的技术设计和数据治理方式，可以在多个领域为多方协作提供信任基础，有助于解决业务发展痛点，促进业务模式创新，推动供给侧改革和经济结构优化。近年来，联合国、国际货币基金组织加强对区块链技术的研究和探讨，ISO、IEEE-SA等国际标准组织通过标准化工作推动区块链技术的全球共识和规范化发展。全球主要国家加快布局区块链技术发展，产业界、学术界纷纷开展区块链技术创新和应用探索，取得了良好的发展成果。

为推动区块链技术和产业发展，在工业和信息化部信息化和软件服务业司的指导下，中国电子技术标准化研究院联合万向区块链、微众银行、平安保险等骨干企业，成立了中国区块链技术和产业发展论坛，并于2016年10月发布了《中国区块链技术和应用发展白皮书（2016）》，为行业技术、应用和标准化等工作提供了有益的方向指引。

2016版白皮书发布至今已经两年，在此期间，国内国际上的产业环境不断发展演变，出现很多进展和成果，表现出新的发展特点，也面临新的发展挑战。因此，从目前的行业发展阶段和发展需求来看，有必要对行业发展进行阶段性总结，并且针对现有行业发展的重点问题进一步探讨。为此，编写组在2016版白皮书的基础上，研究形成了《中国区块链技术和应用发展研究报告（2018）》，其中总结了2016年以来的区块链技术、应用和标准化发展情况，提出了应用场景选择、应用治理、应用评价等方法，并提供多个国内典

型应用案例。希望各界继续努力，积极把握区块链发展的历史性机遇，共同营造和维护良好的产业发展环境，持续推动我国区块链技术和产业发展。

内 容 摘 要

近两年来，在全球产业持续演进的背景下，我国区块链技术和应用继续保持良好的发展势头。各级政府加大对区块链的关注和支持力度，更多企业机构加快投入到区块链技术研发和应用推广中。区块链技术和应用成果涌现，产业未来发展空间广阔。与此同时，区块链技术和应用发展仍然面临一系列风险和挑战。为了进一步推动区块链技术创新和应用落地，引导行业良性发展，我们在《中国区块链技术和应用发展白皮书（2016）》的基础上，编写形成了本报告。其主要内容包括：

一、区块链技术和应用面临的机遇和挑战分析。分别从政策、产业和技术层面研究分析了当前发展面临的机遇，在此基础上重点总结了认识水平、概念炒作、技术和应用等方面的挑战。

二、区块链技术发展情况研究。提出了从区块链到分布式记账技术的演进路径以及相关概念的内涵和关系。结合国内国际标准化成果，总结了区块链系统架构的发展演进特征。根据技术发展的最新进展和发展趋势，研究了跨链和分片技术进展，并总结了安全与隐私保护等其他区块链核心关键技术的发展现状。此外还分析了国内主要区块链开源社区的发展演进情况。

三、区块链应用发展情况研究。首先，从技术、数据、业务和社会治理四个层面归纳形成了描述区块链核心应用价值的TD模型。其次，总结了金融服务和供应链管理等应用领域的最新应用进展，并分析了智慧城市和公共服务等新兴应用领域的典型应用场景。在此基础上，研究提出了从应用痛点出发分析选择应用场景的ASMI四步法以及区块链应用治理框架。最后，针对区块链应用评价，提出在技术、业务、社会效益3个维度下的14个评价指标体系。

四、区块链标准化最新进展研究。结合两级标准化体系，总结了区块

链的标准化演进路径。分析了国内参考架构、数据格式等方面的重点标准研制情况，以及国家标准、行业标准、团体标准的总体进展。此外，盘点了ISO、IEEE-SA、W3C、ITU-T等国际标准化组织的区块链标准化工作情况。

最后，作为本报告提供的区块链应用相关方法论的诠释和补充，提供了3个应用场景分析案例和6个具体应用案例。

编写单位（排名不分先后）

上海万向区块链股份公司
深圳前海微众银行股份有限公司
中国平安保险（集团）股份有限公司
北京蚂蚁云金融信息服务有限公司
众安信息技术服务有限公司
海航科技集团有限公司
三一集团有限公司
用友网络科技股份有限公司
北京瑞卓喜投科技发展有限公司
上海金丘信息科技股份有限公司
上海复星高科技（集团）有限公司
厦门安妮股份有限公司
北京京东尚科信息技术有限公司
三六零科技有限公司
普华永道中天会计师事务所（特殊普通合伙）
永辉超市股份有限公司
福建省海峡区块链研究院
易见供应链管理股份有限公司
江苏通付盾科技有限公司

特邀编写单位

中汇信息技术（上海）有限公司
中国移动通信集团有限公司
中证机构间报价系统股份有限公司
金拱门（中国）有限公司
中华联合保险集团股份有限公司

主要编写人员

周　平　唐晓丹　李　斌　谭智勇　廖娅伶　张开翔　李佳秾
陈家乐　韩　根　韩　梅　鞠　鹏　莫　楠　郝　汉　洪蜀宁
徐　磊　张　林　吴小川　陈　晓　夏　力　冯承勇　蔡　栋
王梦寒　孙海波　黄海泉　吕国新　刘天成　朱振博　季宙栋
尹雪蓉　郭燕飞　高林挥　李　鸣　殷　悦　王　珂　许　进
李　涛　杨　胜　陆一帆　王招军　郝玉琨　张卫中　赵达悦
卫冰飞　宋文鹏　王守超　黄　浩　赵　阳　李昊星　周海平
杜　宇　杨　波　郝振亚　刘　江　杨文涛　郭文婧　朱明礼
杨仁慧　邓伟平　朱天阳　张　擎　陈　锐　董　才　赵子龙
何　沉　柴庆朋　齐　源　赵博然　陈鲁鑫　颜爱军　周开宇
何永德　龚海刚　王晓颖　王　芳　陶　欣　杨　阔　孙　琳
张　屹　李永正　汪德嘉

目 录

目 录

目 录

一、概述

2016年10月，中国区块链技术和产业发展论坛成立以来，在工业和信息化部信息化和软件服务业司的指导下，先后发布了《中国区块链技术和应用发展白皮书（2016）》以及《区块链 参考架构》《区块链 数据格式规范》两项团体标准，建立了分布式应用账本（DAppLedger）开源社区，组织了两届开发大赛，并积极参与区块链国际标准研制。在技术研发、标准研制、应用培育方面取得了一系列成果，为我国区块链技术和应用发展做出了积极贡献。

在实际工作中，我们发现在区块链技术和应用快速发展的同时，业界对其认识还有待提高，底层技术平台架构和开放接口不统一，直接制约了不同应用之间的互联互通。另外，区块链应用面临场景选择和落地实施的困境，现有技术平台在可靠性和稳定性上依然面临很大的不确定性。与此同时，“首次代币发行（ICO）”及其变种，以及“空气币”、非法融资、传销等情况严重扰乱区块链行业健康发展。为了进一步推动我国区块链技术和应用发展，论坛理事会成员单位编写了本报告，目的是通过系统梳理现阶段区块链技术发展情况，明确分布式记账技术（DLT）概念，以及DLT技术与区块链、传统数据存储和处理技术之间的关系，提出区块链的应用路线图，并对未来的发展趋势做出研判。本报告的编写方法如下：

一是结合重点学术论文和技术专利情况，研究和总结了区块链技术的演进路径，介绍了核心关键技术及国外主流开源平台最新发展趋势。同时，分析了国内企业研发的区块链底层平台。

二是收集和整理了百余项区块链应用案例，重点研究分析了金融服务、供应链、智慧城市、公共服务等领域的典型应用案例，明确了区块链

的核心价值，并创新性地提出了区块链应用的场景和技术选择方法、应用治理和评价方式。

三是介绍了ISO、IEEE-SA、W3C、ITU-T等主要国际标准化组织区块链标准的研制情况，介绍了当前的成果及未来的工作计划。并结合国际进展介绍国内区块链标准化的现状。

除论坛理事会成员单位外，本报告还邀请了外汇交易中心、中国移动、中证报价等国内区块链重点应用单位参与编写。需要说明的是，研究报告中所采用的数据仅供参考，最新数据的截至日期为2018年12月。最后需要特别声明的是，本报告旨在服务国内区块链技术和应用发展，其内容不构成任何投资决策或建议，对如代币发行融资与交易以及“虚拟代币”相关的非法金融活动等不构成任何推荐或投资建议。

二、面临的机遇和挑战

当前，数字经济发展进入新时代，区块链对全球社会生产生活的影响逐渐扩大，我国区块链技术和应用在政策、产业和技术等方面面临良好的发展机遇。

1、各类政策相继出台，营造良好发展环境。2016年12月，国务院印发《“十三五”国家信息化规划》，将区块链纳入新技术范畴并作前沿布局，标志着党中央、国务院开始推动区块链技术和应用发展。2018年5月，习近平总书记在两院院士大会期间的讲话中明确提出区块链正在加速突破应用，这一重要论断标志着区块链技术和应用发展进入新阶段。各级地方政府积极推动区块链应用和产业发展。据不完全统计，2017年全国有9个省市出台了扶持区块链产业发展的相关政策措施；2018年以来，全国又有30余个省市两级政府颁布了40余项政策措施，重点扶持区块链应用，以带动地方区块链相关产业发展。党中央、国务院和各级政府的重视，为区块链技术和产业发展营造了良好的政策环境。

2、数字经济发展加快推进，创造广阔市场空间。2016年9月，G20杭州峰会发布《G20数字经济发展与合作倡议》，明确提出数字经济对加速经济发展、提高劳动生产率、培育新市场和产业新增长点、实现包容性增长和可持续增长具有重要作用。据相关研究估计，2017年我国数字经济规模已超过27.2万亿元，对国民经济的贡献显著增强，成为拉动经济增长的新引擎。2017年12月，习近平总书记在中央政治局集体学习会议上，再次强调加快形成以创新为主要引领和支撑的数字经济，推动实体经济和数字经济融合发展。总体来看，产业数字化和数字产业化两种数字经济发展的形态加速推进、融合发展，为区块链技术和应用创造了广阔的市

场发展空间。

3、相关技术创新加快，提供坚实发展基础。当前，各行业意识到区块链技术在创新业务模式、优化业务流程方面的巨大潜力，进一步加大区块链技术和应用研发。底层平台、共识算法、新型分布式存储机制、隐私保护机制、智能合约等技术和产品研究开发不断取得新突破，涌现出一批优秀的国内企业研发的底层平台（例如，微众银行、万向等联合推出的区块链开源平台BCOS/FISCO BCOS，众安科技推出的Annchain）及相关技术成果。

在不断取得重要进展的同时，区块链由于其自身发展阶段以及其他外部原因，技术和应用发展还面临以下五个方面的挑战：

1、对区块链的认识水平有待提升。首先，人们将区块链和以比特币、以太币为代表的形形色色的虚拟代币划等号，随着各类虚拟代币和ICO受到合法性质疑，区块链行业遭到连累和怀疑。其次，存在过度炒作和盲目夸大区块链功能的现象。区块链作为一种新兴的底层技术，普遍被认为能够适用于多种业务场景，从而创造丰富的价值，然而盲目夸大区块链功能的现象造成了一定的社会资源浪费，也不利于行业找到更优的发展方向。为规范区块链行业的健康发展，业界一方面要在技术研发和应用场景拓展上加大力度，另一方面也要面向社会各界加强知识普及宣传及相关政策引导，帮助人们正确认识区块链。

2、对区块链的应用存在误解和担心。当前，在全球范围内，区块链项目良莠不齐，虚假项目、夸大宣传和概念炒作等现象层出不穷，如何将区块链应用纳入有效监管已成为各国政府的共同关注点。基于区块链的ICO项目在近年来加速扩张，并以区块链具有的去中心化、防篡改、建立信任共识等特点作为项目卖点，大肆宣传吸引投资者，然而背后的技术风险以及监管缺失，常常使投资者承受难以弥补的损失。区块链作为新技术，在系统稳定性、应用安全性、业务模式等方面尚未成熟，现阶段其用

途和效果被夸大，有泡沫化的倾向。另一方面，参与项目门槛低，使得市场投机氛围严重。部分投资人不关心区块链项目方身份的真伪，也不在乎项目的虚实或项目前景，只关注能否通过区块链概念炒作创造升值空间，造成行业乱象。如果在做好风险控制的同时保护技术与业务创新，从外部监管和内部审计来看都具有很大的挑战性。区块链的商业应用与监管机制的有效结合，是未来需要重点考虑的问题。

3、区块链技术成熟度有待进一步提升，理论研究力量有待加强。区块链作为一种全新的计算机和网络技术的融合应用模式，在性能、安全、隐私保护、治理、跨链互操作等方面的技术仍不成熟，现有的应用多数仍处于研究和发展阶段。未来一段时期内，技术优化仍然是重要的课题。只有以共识机制、智能合约、跨链技术等为代表的核心技术不断创新演进和优化，区块链的适用范围才能得到不断拓展。此外，区块链是起源于实际应用的技术，长期以来以产业界的投入为主，高校、研究机构的参与程度总体不高，基础理论研究工作如何跟上产业发展的步伐，将是未来一段时期内的发展重点之一。

4、现有应用场景有待丰富，认可度有待提高。区块链虽然被达沃斯世界经济论坛列入“第四次工业革命”的技术范围，并被誉为能产生颠覆性革命的技术之一，但事实上目前其应用场景还不够丰富。目前，区块链主要应用于对账、清结算和存证等场景，应用范围有待进一步拓宽。同时，存在应用区块链改造传统中心化的基础设施的现象，这种应用往往成本高于收益，必要性不强。针对这些问题，业界需要在不断提升当前技术性能的同时，挖掘区块链的其他潜在优势，以持续拓展其应用场景。

5、区块链行业迅速发展，对标准化的需求日益迫切。当前区块链和分布式记账技术处于技术膨胀期，各行业缺乏核心的理念和基本技术共识，使得行业发展碎片化严重。同时，区块链应用的开发和部署缺乏标准化引导，更缺少安全性、可靠性和互操作性等评估方法，不利于区块链产

品和服务质量的提升。应对这些挑战，需要通过开展标准化工作来帮助各国家、各行业间达成共识，为产业共有的挑战提供解决方案，并能够进一步实现技术和经验的共享，为区块链大规模应用奠定基础。

三、区块链技术发展情况

3.1 技术发展路径

20世纪80年代，随着会计信息化的推进，账本实现了计算机化，极大地提高了记账效率，账本本身演变为新型的事务记录方式，例如交易信息、财务往来、征信数据等，同时数据的一致性、防篡改面临新的挑战。2008年区块链出现以来，由于其分布式对等、防伪造、防篡改、可追溯等优势，引发了业界对传统记账技术的新思考，衍生出新型的记账方式即分布式记账，以及分布式记账技术的概念。通过对账本、分布式账本、区块链、分布式记账技术的研究，本报告提出了图3–1所示的关系图。

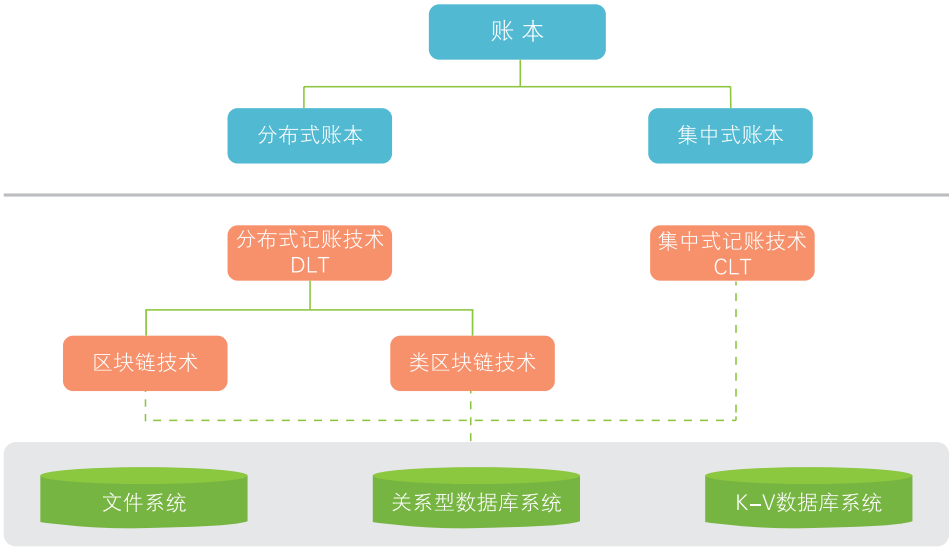


图3–1 账本、分布式账本、区块链、分布式记账技术的关系

其中，分布式账本是指以分布式的方式进行分享和同步的账本，分布

式记账技术是指赋能分布式账本运营和使用的技术。分布式记账技术所依赖的基础技术是文件系统和数据库系统，这与传统的集中式记账技术是相同的。但在账本的构建和应用方面更注重共识机制、智能合约、密码学等技术的应用，同时可按照去中心化或多中心化的技术架构实现账本的分享和同步。

分布式记账技术可以有多种不同的技术路径。结合ISO 23257《区块链和分布式记账技术 参考架构》最新成果来看，区块链是一种分布式账本，其典型技术特征是通过块链式的数据结构实现分布式账本。具体而言，区块链技术将账本数据打包为区块，并采用密码学技术组织成链状数据结构、在全网进行确认和验证。通过这种手段，实现防伪造、防篡改和可追溯等特性。

近几年来，区块链技术正处于不断的发展演变中，各种共识机制、隐私保护、跨链等新技术层出不穷，成熟度逐步提升。同时，受区块链应用的启发，陆续出现新的分布式记账技术，现阶段我们将之统称为类区块链技术。类区块链技术与区块链技术的主要区别是：不依赖块链式数据结构，事务数据可以不打包为区块而直接记录在账本中，或采用新型的拓扑结构。类区块链技术在提升性能和吞吐量方面做了大量探索，但安全和应用成熟度等方面仍然面临较大挑战。

3.2 区块链系统架构

《中国区块链技术和应用发展白皮书（2016）》中将区块链的技术实现分为以数字代币为典型特征的区块链1.0和以智能合约为典型特征的区块链2.0。两年多以来，区块链技术和应用不断演进变化，但目前尚未产生能被广泛认可的区块链3.0形态。

2017年5月，中国区块链技术和产业发展论坛发布《区块链 参考架构》团体标准，对统一区块链系统架构的认识发挥了重要作用。2017年

11月，ISO/TC 307正式启动了国际标准ISO 23257《区块链和分布式记账技术 参考架构》项目，在《区块链 参考架构》团体标准的核心内容基础上构建了国际标准的区块链系统架构，目前已初步达成共识。随着对区块链系统及技术理解的逐渐深入，国内和国际上逐渐达成了以功能组件为基础的分层框架形式的系统架构，如图3–2所示。

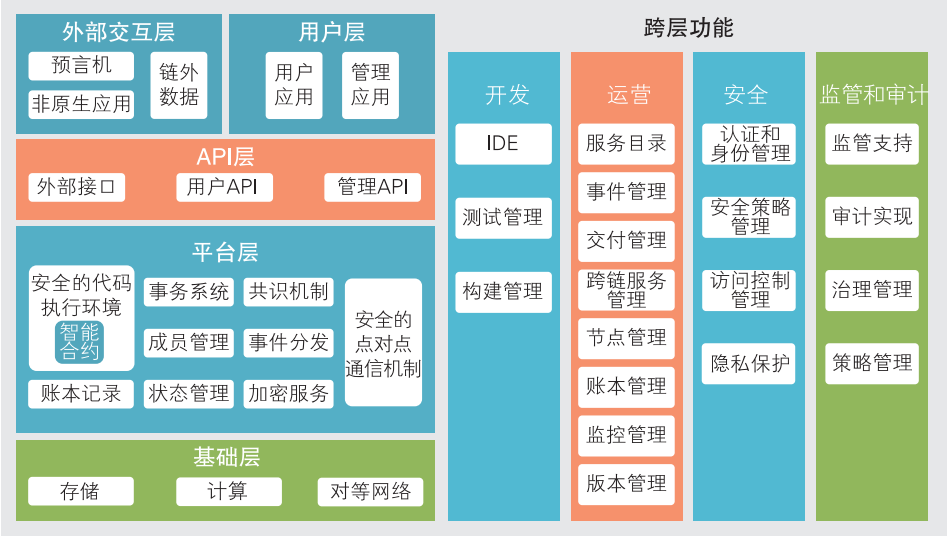


图3–2 区块链系统功能架构

分层框架的五层分别是：基础层、平台层、API层、用户层和外部交互层。跨越各层的功能称为跨层功能，包括开发、运营、安全，以及监管和审计。该系统架构在原区块链基础技术的架构上补充了区块链系统与外部程序、用户和数据等的交互和接口管理，并注重区块链系统全生命周期开发和运营的管理，进而强调了区块链系统各实现层级的安全、监管和审计管理，从架构层面提供了对区块链系统的理解以及实现上的框架指导。

基础层包含计算资源、存储资源和网络资源。该层提供了区块链系统

所需要的运行环境，可以用云计算的形式提供，也可以用本地服务器设备等形式来提供。

平台层支持的具体功能有：安全的代码执行环境与智能合约、账本记录、事务系统、成员管理服务、状态管理、共识机制、事件分发、加密服务、安全的点对点通信机制等，该层通过基于基础设施层提供的硬件或网络基础设施连接到API层实现相应功能。

API层通过调用平台层的功能组件为应用程序、用户和外部系统提供可靠、高效访问区块链的能力，同时提供统一的访问和节点管理功能。

用户层包含用户应用和管理应用。该层是面向用户的入口。通过该入口，使用服务的用户可以与区块链功能、区块链系统运营者进行交互。用户层也可与其他层通信，提供对跨层区块链系统的支持。

外部交互层包含三类服务：预言机、非原生应用和链外数据（源）。该层是为了实现业务目标，需要与区块链系统进行通信的外部系统。

3.3 核心关键技术发展情况

《中国区块链技术和应用发展白皮书（2016）》中总结了共识机制、数据存储、网络协议、加密算法、隐私保护和智能合约等六类核心关键技术。2016年以来，产业界、学术界持续加大对区块链相关技术的研究力度，六类核心关键技术不断取得新的进展，尤其是数据存储结构、共识机制、智能合约，以及安全与隐私保护等技术发展活跃，同时跨链、分片等技术进展较快，已成为新的核心关键技术方向。

3.3.1 安全与隐私保护技术

3.3.1.1 安全技术

安全技术在区块链中起着基础性作用，能保证区块链的数据一致性，并确保参与者身份的安全性。区块链涉及的安全技术主要包括数字摘要算

法、数字签名和加密算法。

数字摘要（又称哈希、散列或杂凑）算法能将任意长度的二进制明文映射为较短的固定长度的二进制值，即生成摘要（又称哈希值）。数字摘要算法具有输入敏感、输出快速轻量、逆向困难的特性，在区块链中，可用于实现数据防篡改、链接区块、快速比对验证等功能。此外，数字摘要算法还应用在消息认证、数字签名及验签等场景中。目前主流的数字摘要算法包括SHA256、SM3等。

数字签名算法主要包括数字签名和签名验签两个具体操作，数字签名操作指签名者用私钥对信息原文进行处理生成数字签名值；签名验签操作指验证者利用签名者公开的公钥针对数字签名值和信息原文验证签名。在区块链中，数字签名算法用以确认数据单元的完整性、不可伪造性和不可否认性。常用的数字签名算法包括RSA、ECDSA、SM2等。

根据加密密钥和解密密钥是否相同，加密算法可以分为对称加密算法和非对称加密算法。对称加密算法中两个密钥相同，并且加解密操作速度相对较快，一般用于普通数据的加密保护，主流的对称加密算法包括AES、SM4等。非对称加密算法的解密密钥是由解密者持有，而加密密钥是公开可见的，几乎无法从加密密钥推导出解密密钥，能够节约系统中密钥存储，一般用于对称密钥的封装保护和短数据加密，主流的非对称加密算法包括RSA、SM2等。在区块链中，非对称密钥算法可用于数字签名、地址生成、交易回溯和交易验证等。此外，在区块链网络系统中，密钥的有效保护和受限使用对整个系统的安全亦有重要影响。在公有链场景，用户密钥通常通过区块链客户端程序来进行保存、管理和操作等。在联盟链或专有链场景，通常会有更复杂多层级的用户管理和密钥托管的需求，包括身份鉴别和权限管理等。

此外，还应充分重视量子计算的技术演进对现有的密码学安全机制的影响。根据Shor算法，经典非对称算法（基于大数分解、离散对数等算

法，如RSA、ECDSA和SM2等）可以被稳定、可用的量子计算机攻破。虽然量子计算设备距离实际可用的通用计算机还有一定距离，但密码学术界和产业界对此广泛关注。例如，密码学家正积极探索能够抵抗量子计算机攻击的密码机制，如基于格的密码机制、基于纠错码的密码机制、多变量密码机制等；ISO、NIST等标准化组织也在进行抗量子密码的研讨和标准化工作。

3.3.1.2 隐私保护技术

区块链的数据组织采用了更为公开的分布式存储方式，在具体应用场景中隐私保护显得尤为重要。区块链系统中隐私保护的目标包含“身份的隐私性”和“数据的机密性”两个方面，前者主要是对区块链参与者身份的保护，后者主要是对记录内容、合约逻辑等数据的保护。隐私保护涉及的技术有环签名、同态加密、零知识证明和安全多方计算等。

环签名允许一个成员代表一个群组进行签名而不泄漏签名者信息，可以实现签名者完全匿名。环签名在匿名电子选举、电子政务、电子现金系统、密钥管理中的密钥分配、匿名身份认证以及多方安全计算等领域都有广泛的应用。利用环签名技术，可以在一定范围内隐藏区块链交易发起者的签名公钥，来实现身份的隐私性保护。

同态加密除了具有一般的加密操作之外，还能够实现直接对密文的计算操作，对密文的计算操作后获得的密文结果，解密后与对明文的计算操作获得的明文结果一致。同态加密在云计算和外包计算等场景中具有重要意义。在区块链智能合约中，可以借助同态加密，对密文直接进行处理，无需泄露真实明文，从而保证数据的机密性。同态加密算法通常分为加法同态、乘法同态、全同态等类型，其中加法同态已在一些区块链项目中落地实践，乘法同态、全同态在区块链中的应用还在研究中。

零知识证明是指一方（证明者）向另一方（验证者）证明某个事实的论断，同时不透露该事实的其他信息的方法。在区块链中，零知识证明用

来保证交易发起者计算的密文等信息具有正确的数据结构，从而在提供密文中私密信息机密性保障的前提下，使验证者确定发起者确实拥有该私密信息。

安全多方计算能够在保证输入数据隐私的前提下，为缺乏信任的参与方提供协同计算功能。在计算过程当中，操作逻辑是公开的，参与方无须泄露输入数据，通过正确执行操作逻辑即可得到最终结果。在计算正确性和去中心化方面，安全多方计算与区块链天然契合，安全多方计算具备的输入隐私性能为区块链中交易各方带来数据的机密性保护。

3.3.2 跨链技术

跨链泛指两个或多个不同区块链上资产和状态通过特定的可信机制互相转移、传递和交换的技术。随着区块链底层平台的多样化发展，区块链项目数量的快速增长，多链并行、多链互通逐渐成为未来发展趋势。跨链通信和数据交互日益重要，尤其是区块链网络间的数据传递以及智能合约的可移植性等方面技术亟待发展。如何提升可扩展性和执行效率，保证跨区块链网络间的数据一致性以及数据不一致时的共识成为跨链技术的发展重点。

跨链分为同构链的跨链和异构链的跨链。相比较而言，同构链的跨链交互在实现上相对容易，异构链的跨链技术实现难度较大，目前还较不成熟。目前主流的跨链技术有：公证人机制、侧链/中继、哈希锁定、分布式私钥控制等。

总的来说，当前跨链技术成熟度还较低，现有的跨链技术主要致力于解决可用性问题，对于跨链易用性、可扩展性以及安全性的研究还有待发展。基于技术发展现状分析，未来跨链技术的重点发展方向包括：加快交易速度，减轻主链负担，发展多链并行处理计算，支持海量交易，提升安全性和加强隐私保护等。

3.3.3 分片技术

分片技术本身是一种传统数据库技术，此前主要用于将大型数据库分成更小、更快、更容易管理的数据碎片。在区块链中，可将区块链网络分成很多更小的部分，即进行“分片”处理，每一个小网络只需要运行一个更小范围的共识协议，对交易或事务进行单独处理和验证，这样冗余计算量可大大减少，效率得到提升。

目前正在探索中的分片技术主要有网络分片、交易分片和状态分片三类。网络分片是利用随机函数随机抽取节点形成分片，从而支持更海量的共识节点。交易分片分为同账本分片和跨账本分片，主要思想是确保双花交易在相同的分片中或在跨分片通信后得到验证。状态分片的技术关键是将整个存储区分开，让不同的碎片存储不同的部分，每个节点只负责托管自身的分片数据，而不是存储完整的区块链状态。

3.3.4 其他核心关键技术改进情况

除了安全与隐私保护技术、跨链技术、分片技术，本报告还梳理了数据存储、共识机制、智能合约等其他核心关键技术的改进情况，如表3-1所示。

表3-1 核心关键技术改进情况

技术类型	技术发展	改进的内容
数据存储	分布式文件系统	链外数据的存储，除了传统集中的数据中心存储、云存储以外，产生了新的互联网点对点文件系统。其中代表性的有融合 Git、自证明文件系统（SFS）、BitTorrent 和 DHT 等技术的星际文件系统（IPFS），其提供全球统一的可寻址空间，可以用作区块链的底层协议，支持与区块链系统进行数据交互。

技术类型	技术发展	改进的内容
	新型网络拓扑结构	随着区块链技术的发展，性能方面的需求不断演进，出现了以有向无环图（DAG）为数据存储结构的技术方案。在DAG模式下，每一个新增的数据单元发布时，需要引用多个（通常为2个）已存在的较新的父辈数据单元，随着时间的推移，所有包含交易的数据单元相互连接，形成有向无环图的图状结构。DAG区块链在并行性、可扩展性上有较大改善，但此种结构对维持数据全局一致性提出一定挑战。
共识机制	新型共识算法	可验证随机函数算法（VRF）由Silvio Micali等在1999年提出，被用于在部分共识机制中提供抽签功能。该算法可以与BFT等共识算法集成，使用基于密码学技术的加密抽签方法随机选择参与者来创建和验证区块（这种抽签方法基于前一个区块的签名，选择过程是自动且随机的）。该算法采用验证人集合、验证人排序和打分的方式处理分叉，确保链的一致性，可以提供快速的区块最终一致性确认。此外，该算法能够提供较好的可扩展的能力、安全性和处理速度，并且由于对计算的要求不高，还具有非常好的经济性。
智能合约	形式化验证框架与通用型语言	安全性是智能合约的关键性问题，目前业内已开始探索利用形式化验证框架和方法解决智能合约安全和审计性问题。同时，智能合约编程语言逐渐从脚本型语言向通用型语言演变，大大丰富了智能合约的应用场景。此外，智能合约的执行逐渐从显式调用执行向由链上触发器(如预言机机制)自动触发执行的方向发展。

3.3.5 技术成熟度

从区块链核心关键技术现阶段的发展和应用情况来看，其重点方向是共识机制、智能合约等新兴技术，而P2P对等网络、密码学算法等基础组件技术已较为成熟。随着区块链应用的不断深入，未来对核心关键技术也将不断提出新的要求，包括抗量子、高性能共识算法等也将逐步走向成熟。

针对区块链核心关键技术中的具体技术点，本报告采用专家评价法，从技术成熟度和技术适用度两个维度，以定量评价的方式，形成了针对具体技术点的具有数理统计特性的评价性结论，具体结果如图3–3所示。

需要注意的是，相关技术仍然处于发展演化中，同时技术成熟度对于不同的应用场景或应用实施主体也有所区别，本部分内容旨在提供一种描述区块链技术成熟度的方法，图3–3所示的具体分值仅供参考。

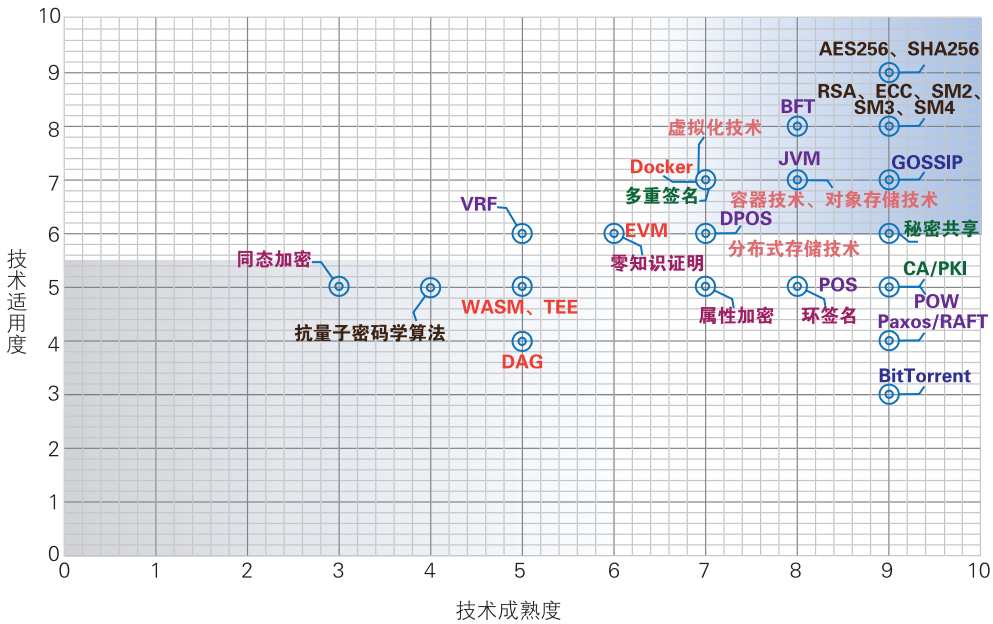


图3–3 区块链技术评价二维示意图

3.4 底层技术平台发展情况

3.4.1 国内外主要区块链平台

目前国外市场上受关注和应用较多的区块链底层平台有：以太坊、Hyperledger Fabric等。其中，以太坊项目由以太坊基金会于2013年启动，支持图灵完备特性智能合约，已有多种DAPP在以太坊网络上运行。Hyperledger（超级账本）由Linux基金会发起，目前孵化了包括Fabric、Iroha、Sawtooth在内的多个开源项目。

国内具代表性的开源社区是由中国区块链技术和产业发展论坛于2017年12月发起的分布式应用账本（DAppLedger）开源社区（如图3–4所示）。该社区以中国区块链技术和产业发展论坛成员自主开发的底层平台为基础，逐步建立多平台运营模式，在应用集成过程中探索最优架构，为国内区块链应用发展提供支持。其中重点孵化的开源项目有BCOS和Annchain等。其中，BCOS由微众银行、万向区块链、矩阵元联合开发建设，金融区块链合作联盟（简称：金链盟）开源工作组在此基础上，聚焦金融行业需求，进一步深度定制发展为FISCO BCOS，BCOS和FISCO BCOS皆已开源并互通有无。Annchain是众安科技自主研发的企业级区块链平台，该平台具有较强扩展性，同时采用交易即共识的方法，能有效提高效率并使交易可并发，可提供快速链部署、中间件、审计浏览、系统监控等支撑工具或产品。

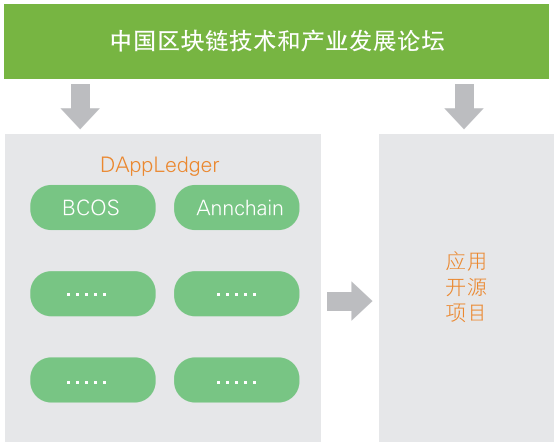


图3–4 DAppLedger的结构

典型的区块链开源底层平台的对比如表3–2所示。

表3–2 典型开源底层平台对比

维度	以太坊	Hyperledger Fabric	DAppLedger	
			BCOS/ FISCO BCOS	Annchain
平台类型	公有链	联盟链	联盟链	联盟链
治理	基金会	基金会	微众银行、万向区块链、金链盟开源工作组等	众安科技
权限管理	非授权	授权	授权	授权
共识算法	工作量证明（账本级）	0.6版本支持实用拜占庭容错算法（交易级），1.0版本后支持Solo（单节点共识）、kafka（分布式队列）和SBFT（简单拜占庭容错）	PBFT/RAFT	PBFT
智能合约	Solidity语言	Go、Java语言	Solidity	Java、Go
可扩展性	正在开发分片模型	支持通道设计，区分不同的业务	多链平行扩展设计，支持跨链调用	扩展DAG账本，可验证分布式计算模型升级
隐私保护	暂无	用通道隔离不同的业务，1.0版本后引入了私有状态和零知识证明	数据脱敏，分级隔离，并实现了零知识证明、群签名、环签名，同态加密等	链上、链下、加密通道结合安全多方计算、同态加密多维一体方式

注：非开源平台由于缺乏技术评估手段，在本报告中不做介绍。

3.4.2 开源社区发展情况

3.4.2.1 生态建设情况

2016年以来，区块链开源社区参与者数量快速增长。公开数据显示，截至2018年8月，Hyperledger开源社区成员由初创时的30多名增长到超过250名，共有27个组织、159名开发者参与了代码贡献。以太坊社区由全球开发者合作贡献代码，据资料介绍核心开发组织包含400多名开发者、密码学者等。随着企业级市场对区块链技术的需求提升，2017年以太坊企业联盟（EEA）成立，初创成员为30家，目前已有超过500家机构加入。与此同时，国内开源项目成长显著。BCOS/FISCO BCOS开源生态圈已逐渐成型，应用加速涌现。截至2018年四季度，BCOS/FISCO BCOS社区开发者成员已达数千，已有数百家机构使用BCOS/FISCO BCOS开源平台，数百个场景应用落地，覆盖范围包括以支付、对账、交易清结算、供应链金融、数据存证、征信、场外市场等为代表的金融应用，以及司法仲裁、文化版权、娱乐游戏、社会管理、政务服务等其他行业应用。Annchain已在数十家企业的商业场景中进行工程化应用，覆盖农业防伪溯源、共享广告、公益资金溯源、智能理财等众多领域。

在参与数量大幅增长的同时，参与者的角色也在丰富，除开发者外，各开源社区中出现了基于平台产品进行各种商业应用场景落地的参与者，包括投资人、集成商、应用开发者和第三方安全审计公司等，推动围绕DAPP的应用生态逐步繁荣。

3.4.2.2 产品特点

从各开源软件平台的版本发布特性分析，主要开源社区重点投入的方向包括易用性、隐私保护、可扩展性、安全防护以及整体架构优化等。

在易用性方面，随着开发者和社区用户的增加，对开源软件的部署、配置、应用开发和运营运维等方面都提出了更多要求，主流开源平台在开发工具、部署工具、数据查询和统计分析以及系统运维工具等方面做了大

量的工作，以降低使用者的门槛，加速开发效率。

在隐私保护方面，由于商业场景对商业数据、机构和人员等信息的隐私保护有很高的要求，主流开源平台普遍通过架构优化或密码学等方式实现不同力度的隐私保护。例如，Hyperledger Fabric在1.0版本加入了私有数据特性，在1.3版本实现了使用零知识证明来保证客户身份匿名和不可追踪等。BCOS/FISCO BCOS提供了可监管的零知识证明、环签名、群签名和同态加密等算法，帮助实现用户隐私保护。

在可扩展性方面，主流开源平台分别根据自身架构，提出不同的可扩展性方案。Hyperledger Fabric基于通道的设计，允许机构根据业务类型接入不同节点，使不同的业务分布在不同的通道上。BCOS/FISCO BCOS采用平行多链架构支持更多的业务量并发，实现了同构链之间的跨链通信。以太坊目前正在开发类DPoS的共识算法以及推动侧链等可扩展方案。随着应用场景数量、链的使用者以及使用频度的增加，各平台需要在可扩展性方面持续演进，包括跨链、侧链、分片等技术都在社区中逐渐引入和实现，以应对更大的规模的网络以及满足更加丰富的互联互通场景。

在安全防护方面，许可链社区通常比较认可基于PKI体系的身份认证、权限控制等措施，持续丰富和细化证书的运用，以及在身份、网络、数据和交易规则等不同层面加入严密的保护。非许可链的安全问题主要体现在网络攻击、智能合约漏洞以及恶意分叉等，也促使以太坊社区持续对合约引擎、代码漏洞进行多方查验和修复，以及通过社区治理的方式，决定如何应对安全漏洞等问题导致的资产损失。

在整体的架构上，主流开源社区均推崇插件化的可扩展设计，通过插件化体系，使得平台产品可以灵活地支持不同的共识算法、密码算法、存储引擎，兼容多个版本的网络协议等，使得产品的演进具备更高的速度和更好的灵活性。例如，Hyperledger Fabric支持Solo（单节点共识）、kafka（分布式队列）和SBFT（简单拜占庭容错），BCOS/FISCO

BCOS支持PBFT和Raft共识算法；Hyperledger Fabric状态数据库可采用LevelDB、CouchDB或其他Key–Value数据库，BCOS/FISCO BCOS可支持LevelDB以及分布式的关系型数据库；国内多个开源社区通过插件化支持国密算法，以更好地适应国内商业场景需求。

四、区块链应用发展情况

4.1 区块链核心应用价值

区块链是建立信任的工具，通过分布式IT架构带来数据的流动、维护和使用的改进和提升，并能进一步带来在业务和社会治理方面的价值。总结分布式IT架构、数据、业务和社会治理四个层次的区块链应用特点和价值，我们提出区块链应用价值框架，又称为TD模型[1]（如图4–1所示）。

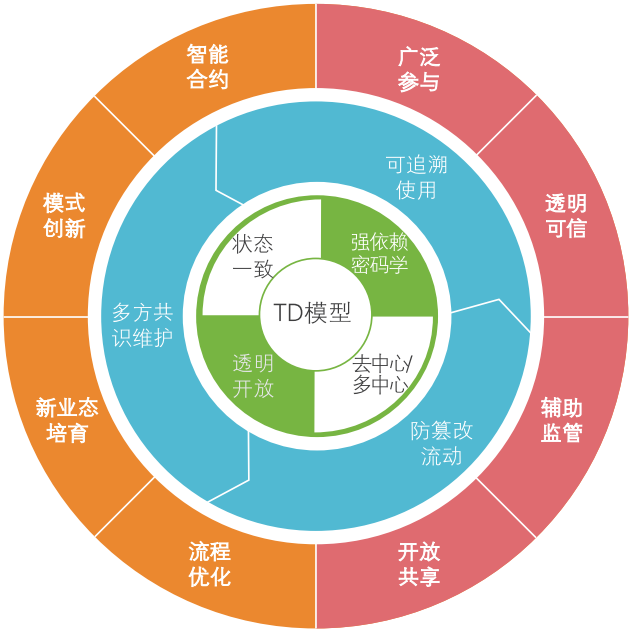


图4–1 区块链的特征与核心应用价值

技术层面上，区块链的分布式IT架构具有去中心、透明开放、状态一致、强依赖密码学的特征；在这些特征基础上，数据层面上，区块链能实

[1]TD：T（Technology，技术），D（Data，数据）。

现在多方共识的基础上保持数据一致，防止数据被篡改，并可对基于数据的应用全过程进行溯源；业务层面上，区块链能实现自动化执行的智能合约，并能在多个行业领域带来业务流程优化、模式创新和新业态培育等价值；在此基础上为社会治理的广泛参与、透明可信、开放共享和辅助监管等提供新方法。

4.2 区块链应用进展情况

《中国区块链技术和应用发展白皮书（2016）》中总结了金融服务、供应链管理、智能制造、社会公益、文化娱乐、教育就业等六大区块链应用领域。2016年以来，这些应用领域已有不同程度的进展，推动了区块链行业应用发展水平的提升，特别是金融服务、供应链管理等领域的应用发展尤为活跃。同时，区块链的应用领域仍在不断扩展，在智慧城市和公共服务等领域也逐步出现了新的应用。为此，我们选取了金融服务和供应链管理两个领域总结主要进展情况，并以智慧城市和公共服务两个新兴领域为例分析新的应用场景。

4.2.1 金融服务应用进展

金融服务是区块链最早的应用领域之一，也是区块链应用数量最多、普及程度最高的领域之一。区块链已成为众多金融机构竞相布局金融新科技的重要技术之一。国内主要银行包括中国工商银行、中国银行、交通银行、邮储银行、招商银行、中信银行、微众银行、平安银行、民生银行、兴业银行等纷纷开展区块链技术和应用的探索，在防金融欺诈、资产托管交易、金融审计、跨境支付、对账与清结算、供应链金融以及保险理赔等方面已取得实质性应用成果，一定程度上推动解决了此前金融服务中存在的信用校验复杂、成本高、流程长、数据传输误差等难题。目前，金融服务领域已有一些典型案例，例如，基于区块链的机构间对账平台、差异账

检查系统，以及通过区块链技术改造的跨境直联清算业务系统等。

在发展特点上，一方面由于金融服务行业注重多方对等合作，并具有强监管和高级别的安全要求，需要对节点准入、权限管理等作出要求，因此更倾向于选择联盟链的技术方向；另一方面该领域的应用更加强调可监管性，从金融监管机构的角度看，区块链为监管机构提供了一致且易于审计的数据，使得金融业务的监管审计更快更精确。例如，在反洗钱场景中，区块链可以实现每个账号的余额和交易记录都是可追踪的，任意一笔交易的任何一个环节都不会脱离监管的视线，将大大增强反洗钱的力度。

4.2.2 供应链管理应用进展

2016年以来，区块链的数据处理效率不断提高，可以更大程度上满足数据量和请求数量巨大的供应链基础设施的需求，供应链核心企业、商业银行、电商平台等相关力量不断加强区块链在供应链管理领域的应用探索，相关应用成果大量涌现。例如，在防伪溯源方面，国内的京东、蚂蚁金服、众安科技等科技企业纷纷投入基于区块链的食品、药品的防伪溯源应用，区块链正在成为食品、药品安全的有效保障手段；在供应链金融方面，央行数字货币研究所、央行深圳市中心支行推动“粤港澳大湾区贸易金融区块链平台”，万向区块链、平安壹账通、京东、腾讯等众多企业开展了覆盖多个行业的供应链金融区块链应用实践。

在发展特点上，一方面，供应链管理领域具有参与方种类多样，业务模式复杂的特点，因此协同多方参与是应用实施效果的重要保障；另一方面，在防伪溯源和物流等领域，与实体产品的深度耦合是实现区块链价值的保障，因此更注重与物联网、人工智能等技术的融合发展。

4.2.3 区块链与智慧城市

随着社会经济发展、技术进步和城市化进程加快，我国自2012年启动了智慧城市建设，在政策支持和技术发展的驱动下，近年来智慧城市建设蓬勃发展。2017年，十九大报告明确提出建设“智慧社会”，进一步加快了新型智慧城市的建设进程。区块链在建设智慧城市中的应用涵盖智慧园区、智慧物联网、智慧资产、智慧交通、能源电力、电子政务、法律应用等广阔领域。

4.2.3.1 区块链解决的问题

为提高城市的智能化感知，提升城市管理的效率，智慧城市建设需要使用大量物联网设备。传统方式是将设备接入互联网，通过云服务器等中心化基础设施验证连接。随着物联网生态体系发展和数据规模的不断增长，中心化基础设施的运算能力、存储能力、信息安全、稳定性都面临很大挑战。同时，智慧城市建设需要在政府及相关机构之间开展数据资源共享及协作，但往往由于数据孤岛现象，跨部门协同、精准快速服务难以实现。此外，医疗健康、公共服务等民生领域数据存量大，若能有效利用，对提升个人健康管理、公共安全等大有裨益，但目前这些数据的权属关系尚未明确。

引入区块链技术，采用分布式点对点的网络结构，可以使设备之间保持共识，实现点对点传输数据，可以减少甚至无需与中心服务器的数据库进行验证，避免对中心化设施的依赖，解决单点故障、批量信息泄露等数据安全问题。利用区块链数据防篡改、可追溯的特性，可以帮助打通政府各部门数据孤岛，为公众提供更加可信和有价值的服务。此外，可以利用区块链技术解决医疗等公众数据安全存储等难题，结合非对称加密技术实现个人数据权属与授权共享，有助于公众数据的安全有效利用。

4.2.3.2 应用场景

应用场景1：智慧物联

智能设备已广泛用于追踪桥梁、道路、电网、交通灯等设施设备状况，利用区块链分布式点对点的网络结构，能将各类设施设备更高效地连结连通，增强物联网络的健壮性和通讯的有效性。例如，可以通过区块链技术追踪联网汽车设备的各项参数，通过智能合约实现车辆保险条款自动追踪、车辆年检以及车辆自动理赔等，从而在汽车保险、车辆管理等领域实现模式创新。

应用场景2：智慧民生

应用区块链技术创建分布式公民登记平台，搭建开放共享、透明可信的公民数据账本，确保公民记录防篡改、可追溯，实现政府跨部门、跨区域共同维护和利用公民数据。在房屋租赁与二手房交易方面，将房源、房东、房客、房屋租赁合同等信息上链，通过多方验证防篡改，有望解决房源真实性问题，打造透明可信的房屋租赁生态。在电力供应生态中，利用家庭太阳能设备发电补充传统电力供应，可将每个用户的发电记录保存在区块链中，实现新型资产的智能登记，并可支持基于智能合约的相互兑换和交易剩余电力，促进全民共建节能环保城市。

应用场景3：智慧医疗

在医疗方面，利用区块链技术创建药物、血液、器官、器材等医疗用品的溯源记录，有助于医疗健康监管，使公共健康生态更加透明可信。通过区块链存储医疗健康数据，创建安全、灵活、可追溯、防篡改的电子健康记录，可以对用户身份确认和健康信息进行确权，并将权属信息等存证在区块链上，确保个人健康信息使用的安全合法。此外，利用智能合约自动识别交易参与方，结合用户对健康信息的使用授权，不仅可以优化医疗保险的快速赔付，还可以方便第三方健康管理机构基于全面的医疗数据提供精准的个人健康管理服务。

4.2.4 区块链与公共服务

随着经济社会的发展，公共服务的规模和范围不断扩张，影响力日益壮大，社会舆论对公共服务的信息共享、权限控制和隐私保护等提出更高的要求。以公众需求为导向的高质量的政务服务，将是未来公共服务发展的重要方向。目前，部分地方政府大力推进“区块链+政务”服务，已取得积极成效。

4.2.4.1 区块链解决的问题

从本质上讲，区块链是利用加密算法、共识机制等技术构造的信任机制，其存储的数据安全可靠且防篡改，可以提供公开透明的管理机制，提升公共服务的公信力。

在鉴证确权方面，利用区块链技术能将公民财产、数字版权相关的所有权证明存储在区块链账本中，可以大大优化权益登记和转让流程，减少产权交易过程中的欺诈行为。在身份验证方面，可以将身份证、护照、驾照、出生证明等存储在区块链账本中，实现不需要任何物理签名即可在线处理繁琐的流程，并能实时控制文件的使用权限。在信息共享方面，区块链技术用于机构内部以及机构之间的信息共享和实时同步，能有效解决各行政部门间协同工作中流程繁琐、信息孤立等问题。

4.2.4.2 应用场景

应用场景1：政务数据开放共享

信息系统整合、数据格式统一、数据实时共享是解决政务部门信息孤岛问题的关键。利用区块链技术可以实现各级政府之间、各部门之间的数据共享，有利于提升工作效率、降低行政成本，为公众带来更好的政务服务体验。目前，一些地方政府正在探索建设基于区块链的居民身份共识数据库，采集居民的身份、缴税、工作经历等相关信息作为身份与权利验证凭证，实现居民在办理不同事项时无需重复提交身份材料，从而有效提升政务服务质量。

应用场景2：知识产权保护

当前，信息经济、知识经济时代产生海量数字作品，数字作品复制盗版极为容易，而证明版权权属的成本相对较高，海量数字作品的版权保护面临巨大挑战。将区块链技术嵌入创作平台和工具中，利用其防伪造、防篡改特性，客观记录作品的创作信息，低成本和高效率地为海量作品提供版权存证，在此基础上，还可支持版权资产化与快速交易，以帮助解决数量巨大、流转频率高的数字作品的确权、授权和维权等难题。

4.3 区块链应用场景选择方法论

当前，理性识别区块链的真正应用需求，或摒弃不合理的应用需求对于区块链应用发展是十分关键的问题。区块链应用场景选择需要在区块链技术特征和发展阶段的准确把握基础上，结合市场需求和用户信息化水平等因素，着重分析应用区块链能够解决的业务痛点，以判断是否采用区块链以及选择哪些应用场景。

基于区块链核心应用价值研究和应用案例综合分析，本报告提供一个应用场景选择的方法——ASMI四步法[1]，其中以业务痛点为出发点，分四步逐步判断应用区块链解决具体业务需求的可行性和必要性，具体包括：分析识别（业务痛点识别和原因分析）、综合归类（痛点原因的综合归类），匹配映射（痛点原因与区块链价值的匹配映射）以及归纳总结（区块链适用度归纳总结）（如图4–2所示）。

[1]ASMI：A（Analysis & identification，分析识别），S（Synthesization & categorization，综合归类），M（Match & mapping，匹配映射），I（Inference & conclusion，归纳总结）。

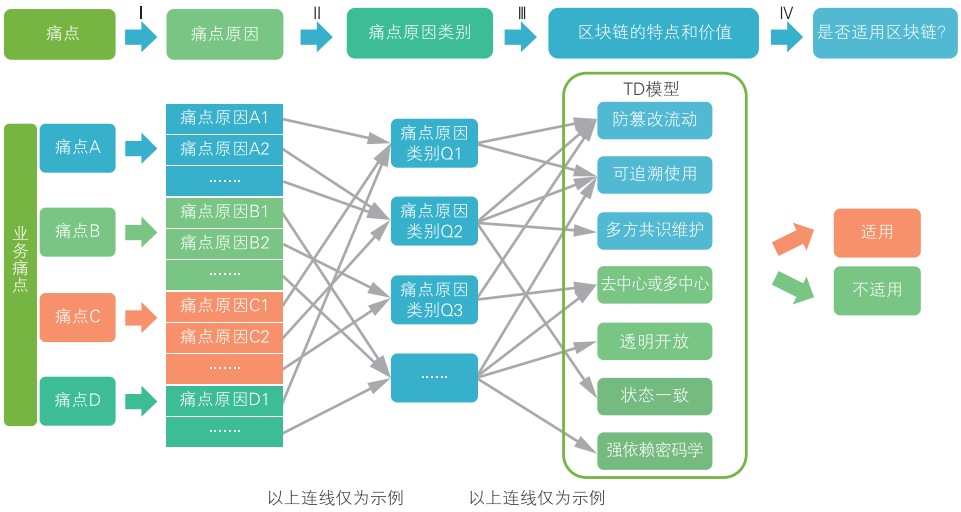


图4–2 ASMI四步法示意图

第Ⅰ步：分析识别——业务痛点识别和原因分析

应用场景分析需要对应用的诉求（例如解决业务痛点或应用创新需要）有清晰的认识，在此基础上清楚地分析和判断区块链技术可以带来哪些价值，以及这些价值是如何实现的。具体可逐个梳理和分析该应用场景下的业务痛点及相应原因，并将业务痛点与原因对应。

第Ⅱ步：综合归类——痛点原因的综合归类

实际业务中，不同的业务痛点可能会由共同的原因导致，因此第Ⅱ步需要对第Ⅰ步输出的业务痛点原因进行归类汇总，得到若干痛点原因类别。

第Ⅲ步：匹配映射——痛点原因类别与区块链价值的匹配分析

匹配映射是将业务痛点原因类别与区块链应用价值对应，以分析该场景与区块链技术的匹配程度。可重点考察业务痛点原因类别与区块链IT架构、数据两个层次的应用价值的匹配程度，将区块链技术可以解决或部分

解决的业务痛点原因类别与IT架构和数据层次的应用特征映射，最终体现业务和社会治理层面的应用价值。

第Ⅳ步：归纳总结——区块链适用度归纳总结

在第Ⅲ步区块链应用价值与业务痛点原因类别符合程度的基础上，对应用区块链的适用度进行归纳总结，最终得出是否采用区块链技术的结论。

4.4 区块链应用治理

4.4.1 区块链应用治理概述

区块链应用治理是指管理和控制区块链系统在当前和未来运行的一系列流程和规则。区块链应用治理原则通常是“链上设定规则，链下管理实施”，既包括设计具体的规则并写到区块链协议中，如：共识机制；也包括链下系统生态的管理和协调，如：通过用户投票决定区块链是否升级、通过对区块链的监控和分析配合监管和审计的需求等。

从区块链应用治理的目标和内容来看，完善的区块链应用治理架构应具备以下内容：

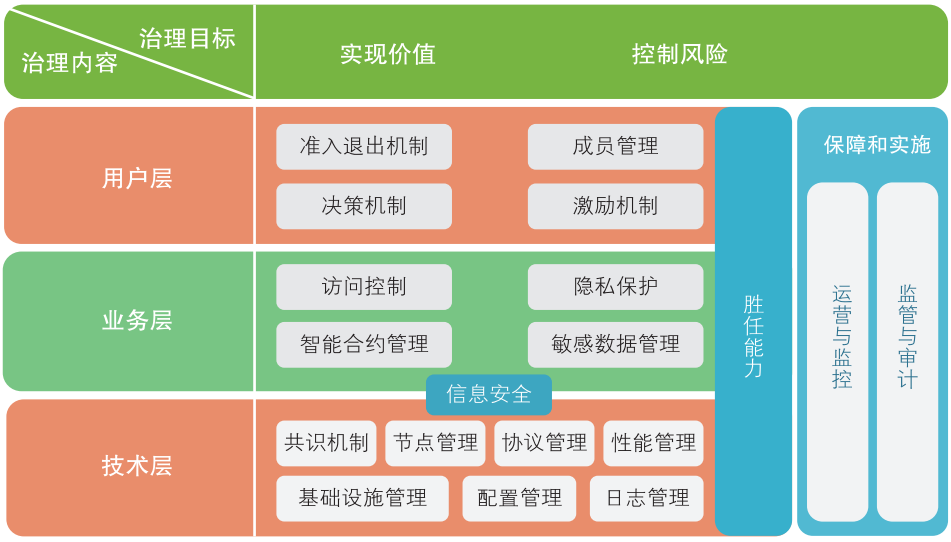


图4–3 区块链应用治理架构

根据非许可链和许可链的不同性质和目的，区块链应用治理呈现出不同的侧重点：

• 对于非许可链来说，治理的关键是采用多种机制来激励和协调，以支撑相关生态系统的运转和发展。

• 对于许可链来说，治理内容包括平台搭建、权限管理、节点管理、监管审计和监控等。

4.4.2 非许可链治理模式

对于非许可链来说，虽然链上的共识机制会有所区别，但链下目前大多采用社区成员投票的方式来决定影响项目发展的重大决策。以下以具代表性的案例为例，说明当前主流的几种非许可链治理模式。

• 比特币：主要依靠比特币核心开发团队对代码开发迭代，而代码更新是否被接受则需要得到大多数矿工（哈希算力）的支持。因此，比特币的治理体系可以抽象为核心开发者提供代码改进建议，全网算力决定是否

采纳。

• 以太坊：虽然以太坊的代码更新规则与比特币相似，但目前其实际治理过程更多受到社区领袖意见的影响，治理模式更接近于领袖型治理模式。

• EOS：EOS采用DPoS的共识机制，EOS用户通过投票选出21个超级节点，并由超级节点负责EOS的共识过程和系统升级提案决策等。如果用户对某个超级节点不满意，可以选择投票给其他节点候选人来替换之前的超级节点。因此，EOS的治理模式偏向于民主代理型治理模式。

4.4.3 许可链治理模式

许可链的治理过程与非许可链全网决策的形式完全不同，其治理内容也特有联盟构建、参与成员管理、权限管理、共识节点管理、监管和审计等。

4.4.3.1 联盟构建

联盟的构建形式直接决定了许可链的治理和运行模式，较为常见的联盟构建形式有：

• 联合治理形式：由联盟成员推举专人组建联合治理委员会，联合治理委员会负责管理许可链；

• 领导型成员治理形式：由联盟中占领导地位的一个或几个成员对许可链进行管理，其他联盟成员作为参与方加入到该许可链中；

• 法定机构治理形式：由法定机构或其他监管机构创建组织来管理和维护许可链的运行。

4.4.3.2 参与成员管理

与非许可链的自由加入不同，许可链成员的加入具有审核和准入机制，需要经过一定流程审核。

加入许可的流程通常包括：

• 身份核查：根据所在行业的监管要求及行业特性，对新加入成员的真实身份进行一定程度的核查；

• 成员协议：新成员加入许可链之前，需要签署正式的、具有法律效力的成员协议。

许可链的退出通常有成员自愿退出和联盟成员投票剔除两种机制。

4.4.3.3 权限管理

许可链可以采用面向角色的权限控制，每个参与成员可以拥有多个链上账户，分别对应不同的操作权限。从许可链上的操作权限管控粒度来看，权限类型可包括：

• 业务操作权限：使用许可链进行业务活动的权限，例如：业务数据的读取和更新权限、应用智能合约的执行权限等；

• 平台运营权限：许可链日常运营相关的权限，例如：链上用户账号及权限分配等；

• 运维开发权限：许可链技术层面的维护权限，例如：软件发布、参数配置权限等；

• 监管权限：独立于日常业务活动以外的监管或审计权限，包括检查链上的业务数据、监控许可链的运行状态等权限。

4.4.3.4 共识节点管理

一般来说，许可链中仅有部分节点是共识节点，这些共识节点参与共识过程，是许可链的记账者。对共识节点的治理内容包括：

• 共识节点加入：开展节点拥有者身份审查、节点安全性评估，并写入全局白名单配置；

• 共识节点监控：监控共识节点的运行状态，包括在线率、块高度、软件版本等，及时发现处于异常状态的共识节点；

• 共识节点替换：当某个共识节点自愿退出联盟，或者处于异常状态（例如节点故障、被黑客劫持、不满足联盟定义的节点规范等），选择一

个候选节点进行替换。

4.4.3.5 监管与审计

许可链需要在治理层面实现可监管和可审计，以达到合规的目的。根据许可链所处行业的监管环境和审计要求，可以通过设置独立观察节点、调用API数据接口、部署特定智能合约等方式，对链上活动进行即时监督，对异常活动进行干预，并保存完整的数据和日志等资料。

4.5 区块链应用评价

区块链应用评价是采购、开发和使用区块链系统和服务的重要依据，同时也是评价、考察行业发展水平的方式之一。对区块链应用的评价可以以质量评价为核心，同时考虑其业务改进能力和社会经济效益等。因此，本报告建议从业务、技术、社会效益等三个维度综合进行评价，并提供三个维度下的14个具体评价指标。需要注意的是，在实际操作中，需要根据不同的应用场景或应用案例，选择全部或部分的评价指标，并且根据不同指标的重要程度选取合适的权重，最终达到综合评价区块链应用的目标。

4.5.1 业务评价维度

业务评价维度的评价指标包括业务适当性、可治理性和经济可行性等。

1、业务适当性。区块链应用需要符合业务需求，应评估目标业务场景中是否存在区块链可解决的需求点，评估中心化系统在该业务场景中的痛点和不足，以及使用区块链技术后可为该业务带来的价值，例如，能否提升业务运行效率或促进业务的转型升级。

2、可治理性。鉴于区块链的业务系统与传统中心化系统在运营和管理上的差异，需要对业务的持续治理进行规划与调整，采用可行性、可持续性的治理结构，确保业务可控。

3、经济可行性。区块链的应用通常面临成本与收益的权衡取舍，优秀的区块链应用应能有效解决当前行业发展和业务流程中的痛点，带来经济价值的最大化和效率的提升。

4.5.2 技术评价维度

技术评价维度中的评价指标可结合《区块链 参考架构》团体标准和GB/T 25000.10《系统与软件工程 系统与软件质量要求和评价（SQuaRE）第10部分：系统与软件质量模型》规定的产品质量模型，针对具体的应用需求，从技术可行性、功能、性能、可靠性、安全性、可维护性、可移植性、互操作性、易开发性等方面综合评估。

1、技术可行性。区块链作为一种新兴技术，目前应用门槛还较高，应用时应选择较为成熟的细分技术组合，同时综合考虑自身的技术和人才储备情况。

2、功能。包括完备性、正确性、适应性和恰当性等评估指标，具体可包括：系统覆盖区块链主要核心功能，提供准确数据或相符结果的能力，满足使用目标和特定业务目标的功能要求，以及提供稳定和适用的功能。

3、性能。包括资源利用性、时间特性、容量等评估指标，可结合具体业务量、潜在业务增长规模、并发业务量等进行评估，具体包括：区块链应用运行时消耗资源的类型和数量，处理时间、响应时间、共识时间以及出块时间等时间特性，以及数据存量、存储的容量、区块的大小以及缓冲池的极限负荷等容量参数。

4、可靠性。包括成熟性、可用性、容错性以及易恢复性等指标，具体包括：运行规定的业务时区块链系统的可靠程度和运行、可访问程度；在出现故障、违反规定接口、节点失效或作恶情况下维持规定性能或正常执行业务的能力；系统在某些功能点发生中断或失效的情况下，恢复受损

数据并重建正常状态的能力。

5、安全性。可结合具体业务场景，从数据敏感性、数据安全性、数据可靠性等角度进行评估，同时考虑保密性、完整性、抗抵赖性、可追溯性和真实性，具体包括：确保数据只能被授权用户访问及防止私钥泄露；具有防止篡改程序或数据的能力；活动或事件发生后可以被证实且不可被否认；每个活动可被追溯的能力；对目标或资源的身份标识切实能够证实该目标或资源的能力；在遭受攻击（如DDoS、P2P攻击、共识攻击等）时确保数据及服务正确且可用的能力。

6、可维护性。包括平台搭建、配置管理、部署架构、权限控制、审计管理、监控体系、数据检索等评价内容。具体包括：系统搭建过程中各功能模块搭建的易用程度，系统中的各个模块配置的灵活程度，系统对不同机房、网络和云架构的支持程度，系统对访问权限的控制粒度，对审计的透明度，系统监控指标的完整程度，以及链上数据的可视化程度等。

7、可移植性。包括适应性、易安装性和易替换性等指标。其中，适应性指在不同约束条件下区块链系统能够稳定运行的程度；易安装性是指区块链系统软件安装包在特定环境中能够有效地进行安装部署调试以达到快速可用的程度；易替换性是指区块链系统各个组件模块在架构设计、组件升级、业务迁移等过程中对该组件模块进行替换的容易程度。

8、互操作性。包括数据一致性和可协同性等评价指标。其中，数据一致性指区块链系统实现降低数据同步延迟、保证数据的一致性、避免数据混乱和失准的能力；可协同性指区块链系统实现与其他区块链系统间互操作的能力。

9、易开发性。该评价指标是系统针对DAPP开发人员的友好程度。区块链底层系统需要能够提供足够便捷的环境、接口与文档使得技术社区能够便捷地基于底层平台开发应用，可着重考察区块链接口与SDK完善程度、智能合约体系易用性等维度。区块链的接口应封装完善，区块链的

SDK应支持多种语言（如Java、Python、Go等）并有完善的开发文档，智能合约体系易用性要求其开发环境稳定、开发语言完整并且图灵完备等。

4.5.3 社会效益评价维度

社会效益评价维度的评价指标包括政策合规性以及生态效益与产业融合等。

1、政策合规性。主要评估区块链应用的各个环节与流程是否遵循国家现有的监管要求、规章制度与法律框架。同时，基于区块链技术的不同行业的应用应符合各行业法律法规的要求，在全球范围内提供服务时还需要兼顾不同国家对区块链系统的监管要求。

2、生态效益与产业融合。主要评估区块链应用是否与现有商业生态有效结合，是否有效打通产业上下游，构建新的面向结构性特征的协同生态系统，形成新的价值共享应用生态，是否推动整个产业、经济体系实现技术变革、组织变革和效率变革，为构建现代化经济体系做出贡献。

五、区块链标准化发展情况

5.1 标准演进路径

2015年12月国务院发布的《国家标准化体系建设发展规划（2016–2020年）》提出“深化标准化工作改革，把政府单一供给的现行标准体系，转变为由政府主导制定的标准和市场自主制定的标准共同构成的新型标准体系”，并提出“在技术发展快、市场创新活跃的领域培育和发展一批具有国际影响力的团体标准”。2016年3月原国家质量监督检验检疫总局、国家标准化管理委员会发布的《关于培育和发展团体标准的指导意见》强调符合条件的团体标准向国家标准、行业标准或地方标准转化，提出“对于通过良好行为评价、实施效果良好，且符合国家标准、行业标准或地方标准制定范围的团体标准，鼓励转化为国家标准、行业标准或地方标准”。经过几年的发展，新型标准体系建设已实现快速推广，在新兴技术领域发挥市场自主作用，以培育团体标准为切入点，逐步带动国家标准或行业标准研制的整体路径已初显成效，并与政府主导型的标准化路径共同形成了新型的两级标准化体系（如图5–1所示）。

图5–1 两级标准化体系

一是自顶向下的政府主导型标准化制定路线。该路线适合国际国内标准化工作基础较好、技术发展较为成熟的领域，标准制定工作大多由政府主导，标准制定后通过试点示范等方式进一步推广应用。例如，为推动智能制造领域的标准化工作，工业和信息化部、国家标准化管理委员会发布《国家智能制造标准体系建设指南（2015年版）》，国家标准化管理委员会设立智能制造国家标准制修订专项计划，目前已批准发布70余项智能制造国家标准。

二是自底向上的以市场为导向分散自治式的标准化制定路线。该路线强调以企业为主体，以协会、联盟等为核心，采用高度开放、自愿的模式开展团体标准制定，经验证实施成熟的团体标准可向行业标准、国家标准转化，通过这种方式逐步建立起本领域的标准体系。该路线充分发挥市场和企业的作用，有助于保证标准符合产业发展实际、及时准确地反映并满足新技术实施需求，充分发挥标准在市场资源配置中的作用，特别适合区

块链等技术发展快、市场创新活跃的新兴技术领域。

5.2 国内标准化

国内的区块链标准化工作早在2016年就开始布局，《中国区块链技术和应用发展白皮书（2016中）》提出了我国区块链标准体系框架，将区块链标准分为基础、业务和应用、过程和方法、可信和互操作、信息安全5类，并初步明确了21个标准化重点方向。2017年，该标准体系框架写入了《软件和信息技术服务业“十三五”技术标准体系建设方案》，有效指导了国内区块链标准化工作。2016年以来，国内相关机构、标准化组织加快开展区块链领域的重点标准研制，按照“急用先行、成熟先上”的原则，采用团体标准先行，带动国家标准、行业标准研制的总体思路，目前已在参考架构、数据、安全与隐私保护等方面取得了一系列进展。

5.2.1 团体标准

在工业和信息化部信息化和软件服务业司指导下，中国区块链技术和产业发展论坛积极开展区块链领域的标准化工作，先后发布了《区块链 参考架构》《区块链 数据格式规范》2项团体标准，其中《区块链 参考架构》团体标准经验证实施成熟已转化为国家标准。此外，中国区块链技术和产业发展论坛还启动了智能合约、隐私保护、存证、信息服务等方面团体标准的研制。

5.2.1.1 《区块链 参考架构》

《区块链 参考架构》作为区块链领域的重要基础标准，给出了区块链和分布式记账技术相关的术语和定义，规定了区块链系统的参考架构，以及典型特征和部署模式，系统描述了区块链生态系统中涉及的角色、子角色、活动，以及主要功能组件。用户视图从用户视角考察区块链系统的组成，结合区块链的服务特点，提出了区块链服务客户、区块链服务提供方、区块链服务合作方3类角色及相应的15类子角色，以及每个子角色的

活动。功能视图主要从区块链功能角度考察区块链系统的组成，提出了基础层、核心层、服务层、用户层组成的分层架构，每层由不同的功能组件组成，同时包含开发、运营、安全以及监管和审计等跨层功能。此外，在《区块链 参考架构》中还加入了对用户视图与功能视图关系的描述，以帮助理解区块链系统的运营复杂性以及不同功能模块与角色的映射关系。

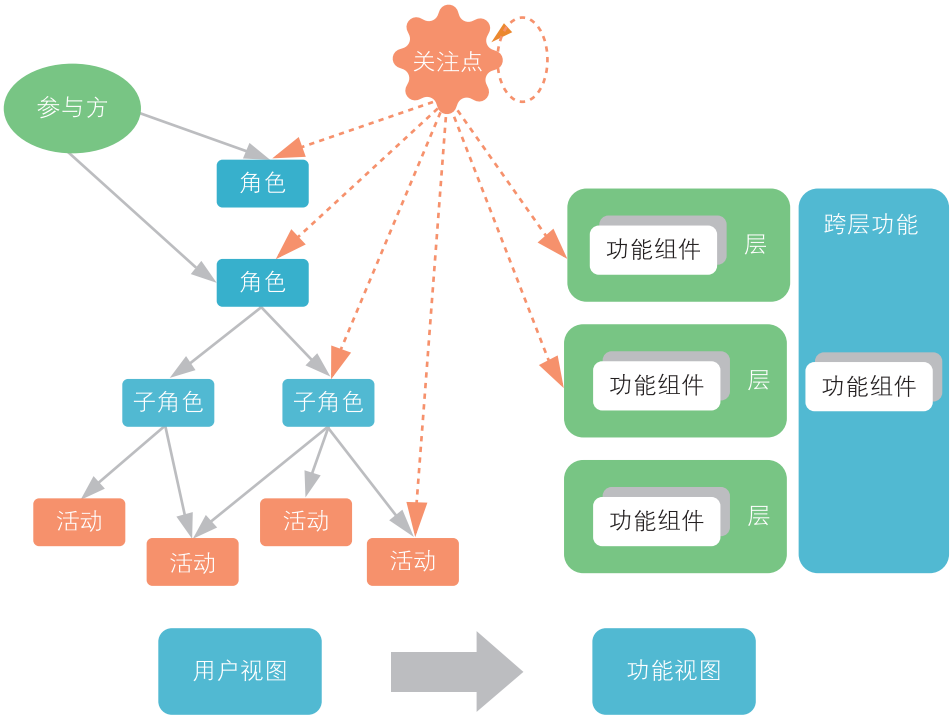


图5–2 《区块链 参考架构》用户视图和功能视图之间的关系

《区块链 参考架构》标准的目的是为计划使用区块链和分布式记账技术的组织选择和使用区块链服务或建设区块链系统提供支撑，指导区块链服务提供组织提供区块链服务，有利于统一业界对区块链的认识，对各行业开展区块链技术和应用活动具有重要的指导意义。

5.2.1.2 《区块链 数据格式规范》

《区块链 数据格式规范》团体标准从数据对象的类别出发，将区块链系统的数据分为账户数据、区块数据、事务数据、实体数据、合约数据和配置数据，并规定了各类数据的格式规范。标准内容包括：区块链系统相关的数据结构、区块链系统相关的数据分类及其相互关系、区块链系统相关的数据元的格式要求。

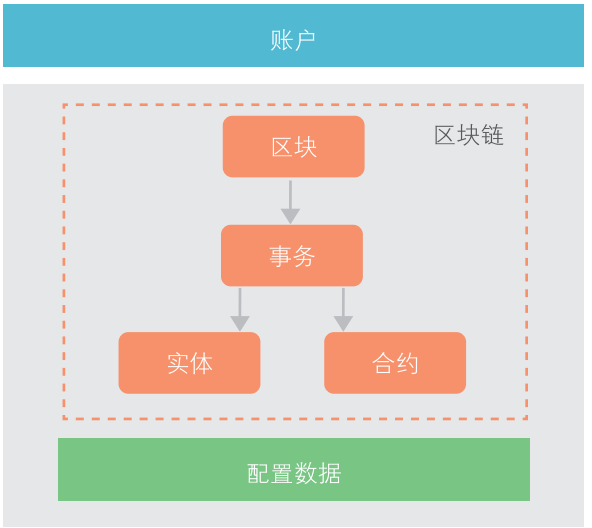


图5–3 《区块链 数据格式规范》中规定的数据结构

《区块链 数据格式规范》标准的目的是为计划使用区块链的组织建设区块链系统提供数据格式参考，指导区块链服务提供组织建立区块链系统数据结构，以及为区块链系统建设过程的中间件服务组织提供数据格式参考。

5.2.1.3《区块链 隐私保护规范》

《区块链 隐私保护规范》团体标准规定了区块链隐私保护的原则、关注点、管理要求、监管和审计要求等。标准提出区块链隐私保护应遵循最小授权原则和明示同意原则，规定了隐私相关的数据收集、数据存储、数据迁移、数据备份与恢复、数据应用、数据披露和数据处置等步骤应关注的保护要点，给出了隐私保护的日常管理和应急管理规范，并从结构设置、监管内容、审计过程三个方面提出要求。最后，标准还给出了参考性的隐私保护策略和技术，其中包括数据存储、传输过程中的技术和身份保护技术等。

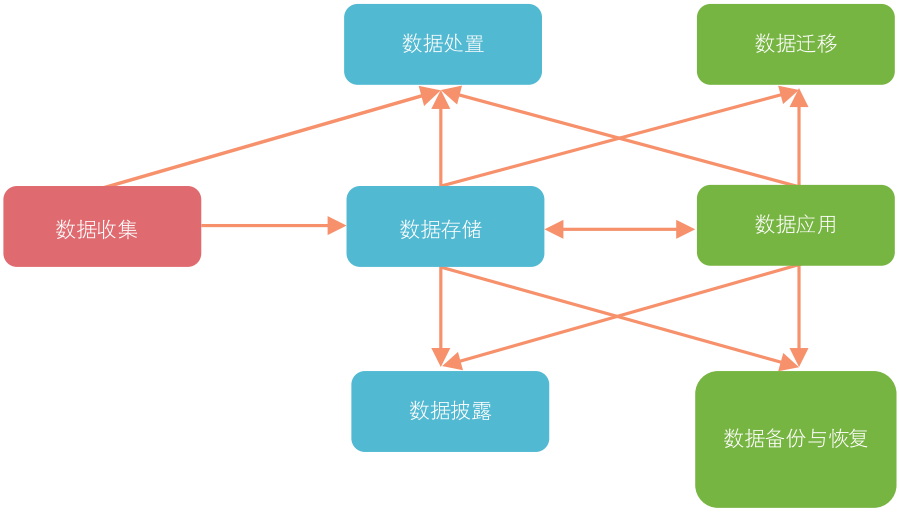


图5–4 区块链隐私保护关注点及其关系

《区块链 隐私保护规范》标准的目的是为区块链应用的信息安全与隐私安全提供依据，为计划使用区块链系统的组织和机构选择和使用区块链服务提供隐私保护的参考，以及指导区块链系统提供方在区块链系统中建立区块链隐私保护机制，并为第三方评价区块链系统服务提供方的隐私

保护能力提供参考。

5.2.1.4《区块链 智能合约实施规范》

《区块链 智能合约实施规范》团体标准规定了区块链智能合约实施的原则和主要关注点。标准规范了区块链智能合约全生命周期中的合约构建、合约触发、合约运行和合约评估等关键环节及实施要点，提出了合约创建和合约升级的要求，明确了合约触发的三种方式和合约事件规约，规范了合约部署、合约实例化、合约执行和合约废止等方面的实施规则要点，最后给出了在合约安全审计和合约形式化验证等方面的最佳实践。

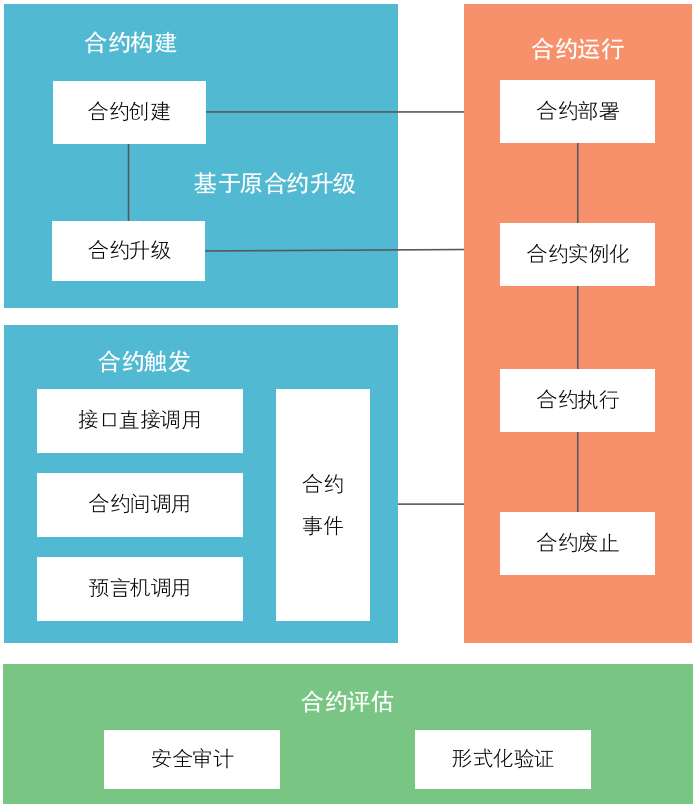


图5–5 智能合约实施框架

《区块链 智能合约实施规范》规定了图灵完备的智能合约实施规范，目的是为计划使用区块链的组织建设区块链系统提供智能合约实施参考，指导区块链服务提供组织区块链系统智能合约的实现，以及为区块链系统建设中智能合约运行环境的实现提供参考。

5.2.1.5《区块链 存证应用指南》

《区块链 存证应用指南》团体标准从存证应用的实际业务需求出发，规定了区块链存证有效性原则、区块链存证相关方以及区块链存证关键过程。标准给出了区块链有效性原则，在业务系统、电子数据存取的有效性、时间的有效性、存证证明机构的有效性以及存证核验的有效性等五个方面给出了要求；明确了区块链存证业务相关方与区块链存证系统支持相关方两类区块链存证相关方角色；最后，给出了区块链存证的七大关键步骤，包括定义区块链网络及共识机制、写入区块链数据预处理、电子数据签名、存证过程、存证公示和查询、提取存证和存证第三方验证等。

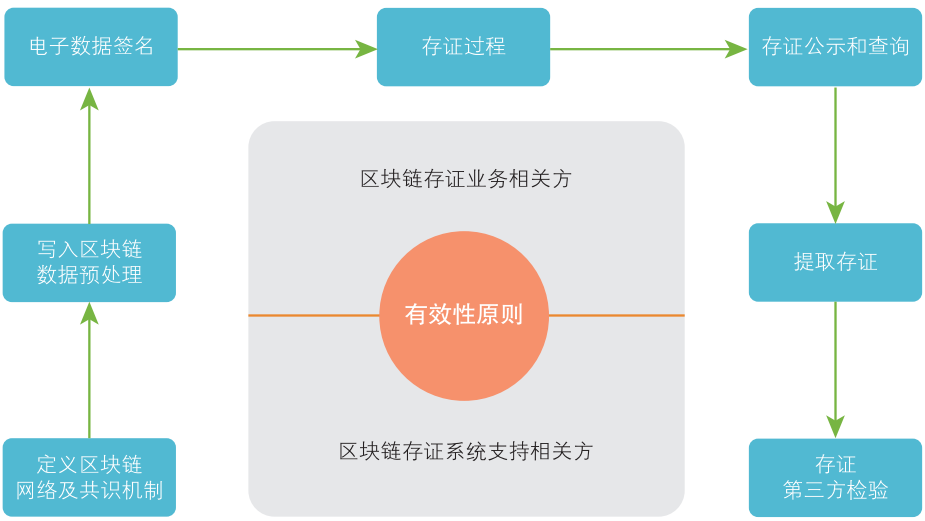


图5–6 区块链存证应用模型

《区块链 存证应用指南》标准的目的是为各行业基于区块链技术开展存证应用的活动提供基本指引，指导区块链存证应用的设计、开发、部署、测试、运行和维护等活动，帮助更准确、高效、便捷地搭建区块链存证应用系统。

5.2.2 国家标准/行业标准

目前，区块链领域的国家标准/行业标准还处于较早发展阶段，仅有少量基础性的标准立项并处于研制阶段。已立项国家标准信息如表5–1所示。

表5–1 区块链领域在研国家标准

序号	标准名称	计划编号	标准类型
1	信息技术 区块链和分布式账本技术参考架构	20173824–T–469	国家标准

5.3 区块链标准化现状

5.3.1 国际标准化组织（ISO）

2016年9月，国际标准化组织（ISO）成立了区块链和分布式记账技术技术委员会（ISO/TC 307），主要工作范围是制定区块链和分布式记账技术领域的国际标准，以及与其他国际性组织合作研究该领域的标准化问题。截至2018年12月，ISO/TC 307已成立了4个工作组（基础工作组，安全、隐私和身份工作组，智能合约及其应用工作组，治理工作组），2个研究组（用例研究组，互操作研究组），以及1个联合工作组（区块链和分布式记账技术与IT安全技术）。

图5–7 ISO/TC 307工作组/研究组

2017年下半年以来，ISO/TC 307加快推动基础、智能合约、安全、隐私保护、身份和互操作等方向重点标准项目的研制工作。截至2018年12月，术语、参考架构、分类和本体等11项国际标准项目已正式立项（如表5–2所示），进入制定阶段。11项国际标准项目的开展，将有助于打通不同国家、行业和系统之间的认知和技术屏障，防范应用风险，为全球区块链技术和应用发展提供重要的标准化依据。

在参与国际标准化工作过程中，中国将《区块链 参考架构》等团体标准成果作为贡献物提交至ISO/TC 307，推动了参考架构等国际标准的立项。目前中国专家担任参考架构国际标准的联合编辑、分类和本体技术规范的编辑，并牵头区块链数据流动和数据分类相关课题的研究工作。

表5–2 ISO/TC 307标准项目情况

序号	标准标号	英文名称	中文名称	项目类别
1	ISO/CD 22739	Blockchain and distributed ledger technologies——Terminology	区块链和分布式记账技术——术语	国际标准

序号	标准标号	英文名称	中文名称	项目类别
2	ISO/NP TR 23244	Blockchain and distributed ledger technologies——Overview of privacy and personally identifiable information (PII) protection	区块链和分布式记账技术——隐私和个人可识别信息（PII）保护概述	技术报告
3	ISO/NP TR 23245	Blockchain and distributed ledger technologies——Security risks and vulnerabilities	区块链和分布式记账技术——安全风险和漏洞	技术报告
4	ISO/NP TR 23246	Blockchain and distributed ledger technologies——Overview of identity management using blockchain and distributed ledger technologies	区块链和分布式记账技术——用区块链和分布式记账技术的身份管理概览	技术报告
5	ISO/AWI 23257	Blockchain and distributed ledger technologies——Reference architecture	区块链和分布式记账技术——参考架构	国际标准
6	ISO/AWI TS 23258	Blockchain and distributed ledger technologies——Taxonomy and Ontology	区块链和分布式记账技术——分类和本体	技术规范
7	ISO/AWI TS 23259	Blockchain and distributed ledger technologies——Legally binding smart contracts	区块链和分布式记账技术——有法律约束力的智能合约	技术规范
8	ISO/NP TR 23455	Blockchain and distributed ledger technologies——Overview of and interactions between smart contracts in blockchain and distributed ledger technology systems	区块链和分布式记账技术——区块链和分布式记账技术系统中智能合约的交互概述	技术报告
9	ISO/NP TR 23576	Blockchain and distributed ledger technologies——Security of digital asset custodians	区块链和分布式记账技术——数字资产托管的安全	技术报告
10	ISO/NP TR 23578	Blockchain and distributed ledger technologies——Discovery issues related to interoperability	区块链和分布式记账技术——发现与互操作相关的问题	技术报告
11	ISO/NP TS 23635	Blockchain and distributed ledger technologies——Guidelines for governance	区块链和分布式记账技术——治理导则	技术规范

5.3.2 其他标准组织

5.3.2.1 电气电子工程师学会标准协会（IEEE-SA）

电气电子工程师学会标准协会（IEEE-SA）自2017年启动了在区块链领域的标准和项目探索。目前，《区块链在物联网中的应用框架》《区块链系统的标准数据格式》《分布式记账技术在农业中的应用框架》《分布式记账技术在自动驾驶载具（CAVS）中的应用框架》《区块链在能源领域的应用》《分布式记账技术在医疗与生命及社会科学中的应用框架》六项标准已立项。其中，《区块链系统的标准数据格式》由中国专家牵头。此外，IEEE-SA还同步开展了区块链技术在数字惠普、数字身份、资产交易及互操作等方向的标准化研究。

5.3.2.2 万维网联盟（W3C）

W3C启动了3个区块链相关的社区组来开展区块链标准化活动，分别为：1）区块链社区组，主要研究和评价与区块链相关的新技术以及用例（例如，跨银行通信），基于ISO 20022创建区块链的消息格式，并孵化FlexLedger项目，重点关注区块链间的数据交互性；2）区块链数字资产社区组，主要讨论在区块链上创建数字资产的Web规范；3）账本间支付社区组，目标是连接世界范围的多个支付网络。

5.3.2.3 国际电信联盟标准化组织（ITU-T）

国际电信联盟标准化组织（ITU-T）于2017年初前后启动了区块链领域的标准化工作。SG16、SG17和SG20三个研究组分别启动了分布式账本的总体需求、安全，以及在物联网中的应用研究。此外，成立了三个区块链相关的焦点组（分别为：分布式账本焦点组、数据处理与管理焦点组和法定数字货币焦点组）。

六、未来发展展望

作为一种新兴技术产业，区块链已经历多年的蓬勃发展，形成一定的发展基础，拥有广阔的发展前景。同时也应看到，区块链尚处于概念验证和技术发展阶段，技术、市场和管理还有很多不确定性，尚需时间进行技术验证和经验积累。未来一段时期内，区块链将加速向更多领域延伸拓展，可能带来的产业变革值得密切跟踪，同时可能带来的风险和挑战也需要持续关注。

（一）全球主要国家政府对区块链的定位逐渐清晰，持续加快推动区块链发展

近年来，随着区块链技术在各行各业的创新探索和应用落地，全球主要国家越来越关注其发展潜力，通过政策、资金和应用试点等方式加以支持，抢占区块链技术和产业发展先机。与此同时，各国政府逐渐将对比特币等数字代币的审慎监管与对区块链技术发展的鼓励加以区分，在引导区块链技术健康发展的同时逐步拓展区块链的发展空间。另一方面，从整体上看，目前全球各国政府对区块链产业的支持还以点状的项目鼓励为主，未来随着产业的持续发展，各国政策有望进一步加强布局，全面推进区块链与实体经济的大范围结合，加快推动区块链产业规模发展壮大。

（二）区块链相关概念不断发展演进，技术发展逐渐走向体系化和多元化

区块链是从比特币的技术设计中抽离出来的一套技术体系，主要解决构建多方共享和同步的记录账本的问题，这种账本也可以通过不同于区块链的技术来实现，为此出现了分布式账本和分布式记账技术等概念。同时，区块链的核心关键技术逐步发展，在原有的共识机制、数据存储、隐

私保护和智能合约等技术不断改进的同时，分片、跨链等技术也加快发展。2015年以来，全球区块链专利数量快速增加，特别是国内专利申请数量已位居全球首位。2017年以来，区块链领域的学术论文大幅增多，反映出对区块链的基础技术的理论研究进一步加快。总体上看，区块链在安全、数据隐私保护、治理、跨链互操作等方面的技术还不成熟，未来一段时期内，技术的优化和发展仍是重要的课题。此外，由于适应场景类型、治理和运营模式的差异，许可链和非许可链正逐渐走向不同的技术发展路线。

（三）区块链应用积极性不断提高，未来有望成为数字经济基础设施之一

近年来，区块链在各行业的应用探索加快，应用领域逐渐拓展，应用项目数量和质量不断提升，并渐渐加强与实体经济的结合。基于区块链的信任机制有助于促进社会分工协作，降低社会分工和交易成本。区块链的应用有助于提升多个行业的数字化水平，促进新模式新业态培育，甚至实现行业革新。由于在社会经济发展以及社会治理水平提升等方面的作用日益突出，区块链正逐渐成为数字经济发展的关键支撑，尤其是未来随着区块链3.0时代的到来，区块链将广泛应用于人类活动的规模协调，有望逐步发展成为数字经济基础设施之一。不过，当前区块链应用整体还处于早期阶段，缺乏大规模成功案例，各领域发展程度不均衡，在一些国民经济发展的关键领域，例如工业区块链，由于场景复杂、置换成本高等原因，目前区块链应用案例还较少。从全球来看，未来区块链产业竞争的关键将是尽快实现规模化应用或实现国民经济关键性领域的成功应用。

（四）国内外区块链创新创业活跃，产业发展生态持续完善

当前，国内外主流金融机构、IT企业、初创科技企业等纷纷探索和推动区块链技术和应用发展，通过开发区块链基础平台、探索各领域的应

用、开展技术创新活动、投资区块链项目等方式积极布局，带动新一轮的区块链创新创业浪潮。区块链产业生态经过发展演化，较之两年前进一步打开。具体表现在：一是政府普遍强化了对区块链的监管和引导；二是更多区块链技术和服务提供商进入行业，提供区块链底层平台、BaaS平台、区块链解决方案等多种形式的产品和服务，其中包括IT企业、咨询公司等类型，例如IBM、微软、甲骨文、英特尔、微众银行、华为、德勤等；三是越来越多的用户关注、探索和推动将区块链应用在金融服务、智能制造、供应链管理、文化娱乐等多个行业，例如沃尔玛、京东推动区块链在商品防伪溯源方面的应用，马士基推动区块链在航运方面的应用；四是高校、研究院所等技术力量进一步加大投入，技术生态逐渐构建。未来产业发展生态的不断完善将有助于持续推动协同创新水平，降低技术和市场风险，加强产业布局的合理性，促进区块链应用的良性发展。

（五）国内国际标准化组织大力推动区块链标准化，产业服务水平不断提升

随着区块链技术和应用的持续发展，在基础术语和架构、安全与隐私保护、互操作以及治理等方面的规范化、标准化发展的需求日益突出。自2016年以来，国内和国际标准化组织大力推动区块链标准化工作，取得了一些初步的成果，已有一批基础性和关键性的标准项目立项。此外，在政府的引导下，相关机构陆续推出区块链测试、人才培训等产业服务，加快建设相关产业服务平台，为区块链从业机构提供必要的产业资源和条件保障。与此同时，还需认识到目前区块链标准体系仍不完善，区块链产业服务体系还处于发展的初期阶段。未来一段时期内，通过标准化和产业服务体系建设提供强有力的发展支撑，不断提升整体竞争力，将是推动区块链产业发展的重要路径。

附录A 术语和缩略语

表A–1 术语

中文术语	英文术语	定义 / 解释
区块链	Blockchain	一种在对等网络环境下，通过透明和可信规则，构建防伪造、防篡改和可追溯的块链式数据结构，实现和管理事务处理的模式。 注：事务处理包括但不限于可信数据的产生、存取和使用等。 【CBD—Forum—001—2017《区块链 参考架构》】
共识机制	Consensus Mechanism	区块链系统中各节点间为达成一致采用的计算方法。 【CBD—Forum—001—2017《区块链 参考架构》】
联盟链	Consortium Chain	仅由一组具有利益相关的特定区块链服务客户使用，仅有授权节点可接入，接入节点可按规则参与共识和读写数据的一类区块链部署模型。 【CBD—Forum—001—2017《区块链 参考架构》】
跨链协议	Cross—chain Protocol	一种协议或技术，使得区块链之间（同构或者异构区块链之间）能够协同操作，实现链之间的信息和链状态转移。
分布式账本	Distributed Ledger	以分布式的方式共享和同步的账本。 【ISO/CD 22739《区块链和分布式记账技术 术语》（技术委员会草案）】
分布式记账技术	Distributed Ledger Technology	实现分布式账本的运行和使用的技术。 【ISO/CD 22739《区块链和分布式记账技术 术语》（技术委员会草案）】
专有链	Private Chain	仅由单个区块链服务客户使用，仅有授权的客户节点可接入，接入节点可按规则参与共识和读写数据的一类区块链部署模型。 【CBD—Forum—001—2017《区块链 参考架构》】
公有链	Public Chain	任意区块链服务客户均可使用，任意节点均可接入，所有接入节点均可参与共识和读写数据的一类区块链部署模型。 【CBD—Forum—001—2017《区块链 参考架构》】
许可链（系统）	Permissioned Blockchain	节点需要被授权的区块链（系统）。 【ISO/CD 22739《区块链和分布式记账技术 术语》（技术委员会草案）】

中文术语	英文术语	定义 / 解释
非许可链（系统）	Permissionless Blockchain	节点无需被授权的区块链（系统）。 【ISO/CD 22739《区块链和分布式记账技术 术语》（技术委员会草案）】
智能合约	Smart Contract	以数字形式定义的能够自动执行条款的合约。 注：在区块链技术领域，智能合约是指基于预定事件触发、不可篡改、自动执行的计算机程序。 【CBD—Forum—001—2017《区块链 参考架构》】

表A-2 缩略语

缩略语	原始术语
API	应用编程接口 (Application Programming Interface)
BFT	拜占庭容错算法 (Byzantine Fault Tolerance)
CA	电子认证 (Certification Authority)
CLT	集中式记账技术 (Centralized Ledger Technology)
DAG	有向无环图 (Directed Acyclic Graph)
DAPP	分布式应用 (Distributed Application)
DDoS	分布式拒绝服务 (Distributed Denial of Service)
DLT	分布式记账技术 (Distributed Ledger Technology)
DHT	分布式哈希表 (Distributed Hash Table)

缩略语	原始术语
DPoS	股份授权证明 (Delegated Proof of Stake)
PBFT	实用拜占庭容错 (Practical Byzantine Fault Tolerance)
PKI	公钥基础设施 (Public Key Infrastructure)
SDK	软件开发工具包 (Software Development Kit)

附录B 应用案例及分析

本报告提供两种形式的应用案例，一种是较为抽象的场景分析，提供了版权、供应链金融和冷链物流三个场景（见B.1–B.3），应用本报告正文第四章的方法论分析如何推动该场景应用；另一种是具体的应用产品和服务的实例分析，提供涵盖存证、国际贸易融资、电子营业执照、供应链金融、再保险交易和钻石溯源等场景的六个实例分析（见B.4–B.9）。

B.1 数字版权场景

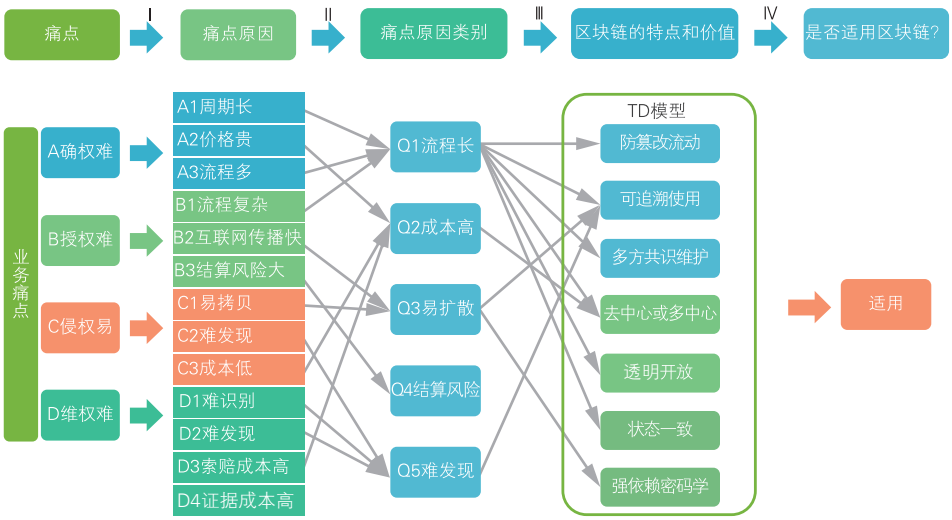
B.1.1 应用场景概述

数字内容涵盖八大领域数字游戏、计算机动画、数字学习、数字影音应用、移动应用服务、网络服务、内容软件、数字出版与典藏等领域。互联网时代，数字内容爆发式增长，越来越多的人参与到创作中来，创作内容变现的市场规模呈几何级增长。相关数据显示，国内数字内容用户付费规模增长迅速，2017年已超过两千亿元。

与此同时，数字内容侵权现象层出不穷，侵权方式呈多样化。传统的版权保护手段和交易方式耗时耗力，沟通及各项成本都较高，使原创者无法快速有效地出售自己的版权，也难以及时获知自己的作品是否被侵权。如何低成本、高效地实现版权保护、版权交易授权和侵权检测维权，已成为数字版权保护行业的关键问题。随着新一代信息技术的快速发展，业内企业加强区块链、大数据、人工智能等技术在数字版权领域的应用探索，以提升数字版权保护水平。

B.1.2 应用场景选择分析

本部分结合数字版权业务的特点，围绕确权难、授权难、侵权易、维权难等业务痛点，使用ASMI四步法进行应用场景分析，以判断数字版权场景中应用区块链技术的可行性（如图B.1–1所示）。



图B.1–1 数字版权场景选择ASMI四步法分析示意图

经过分析可以看出，针对数字版权的业务特点，使用区块链技术能够非常精准地解决部分痛点，同时有些痛点例如易扩散、难发现等还需要引入其他技术辅助解决。

B.1.3 应用技术选择分析

考虑版权区块链系统方案时通常需要解决业务流程设计、合适的区块链平台和相关技术选择以及严密的存证内容结构设计等问题。

1、业务流程设计中涉及的技术选择。基于区块链的数字版权应用要解决确权、可信存证、维权以及可信取证等问题。在业务流程设计中，需

要重点考量的是业务流程在逻辑上的严密性、外部支持系统的切入时机以及衔接方式，例如：鉴别用户身份的CA认证中心的介入方式、国家授时服务中心的服务支持及核验方式、司法鉴定中心的介入方式等。

数字版权应用对数据安全要求较高，同时与大数据和人工智能的结合也有大量场景需求。例如，在数字版权维权过程中，利用大数据和人工智能结合进行全网侵权数据监测，发现问题后可实现一键固定证据到区块链上。在系统设计中对于这类支持类服务的接入时机和接入方式需要融入整体的业务流程设计。

此外，业务涉及到高并发量时，可考虑区块链分片技术的选择与验证；业务系统涉及多链交互时，可考虑跨链技术的选择与验证。

2、底层平台及相关技术选择。数字版权区块链存证平台选择前需要选定存证模式，大致可分三种：1）独立联盟链方式，即仅有一个自成系统的联盟链网络；2）“联盟链+公有链”方式，即在联盟链信息基础上提炼出更简要的信息存入公有链；3）“联盟链+联盟链”方式，即通过互相存储对方的全量或部分数据来增强透明度与可信力。

对于底层平台的选择，需要重点考虑稳定性、性能、平台的业内认可程度等因素，同时还可考虑平台运行安全体系的严密性、接口开发的便捷性等。

3、严密的存证内容结构设计。存证信息的构成设计是区块链数字版权存证的关键环节。目前来看，数字版权存证信息中需至少包含以下信息：存证主体信息及验证信息、国家授时信息、数字产品信息的哈希值。同时，存证信息需要解决存证信息的隐私性与机密性两个问题。隐私性可以用数字签名的方式解决，如有更高要求，也可考虑采用环签名或零知识证明等方式。机密性主要从两个方面考虑：1）在设计存证信息时，尽量采用哈希值关联，数字摘要技术的强度至少需要达到SHA256的水平；2）可在智能合约中应用同态加密技术，同时需要考虑性能与存储代价是否合

适；3）在通讯加密中需要考虑到密钥协商、传输加密等问题，涉及到的对称加密算法有AES、SM4等，非对称加密算法有RSA、ECC、SM2等。

4、其他考量。考虑到技术和需求的发展，对于变动性比较强的模块建议采用插件化、低耦合度的方式。例如，为应对量子计算的挑战，涉及到密码及加密的模块，可以设计得灵活一些，以便于替换。

B.1.4 应用治理分析

数字版权应用一般采用许可链的治理模式。联盟构建可采用联合治理或领导型成员治理形式。参与成员管理方面可按需要进行成员检查并签署成员协议。

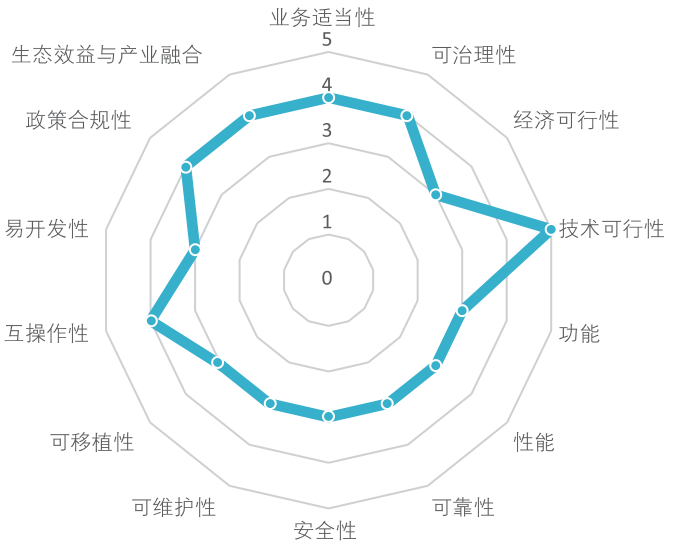
权限管理上一般利用CA认证授权实现联盟链准入以及业务操作、平台运营、运维开发、监管等权限控制。

节点管理方面，可以根据不同组织的角色赋予不同的权限范围。例如，对于CA认证节点，可以提供监察的权限，包括查询指定存证内容、在指定存证内容里核验是否采用了本机构颁发的证书等。具体的权限划分可以根据应用系统的需要进行功能的扩展。

监管和审计方面，可以考虑引入法院、仲裁机构等，通过设立监察或记账节点，结合智能合约及区块链框架平台进行权限划分，为不同机构提供不同类型和层级的监管和审计功能。

B.1.5 应用评价分析

对于数字版权场景下的应用，可从业务、技术、社会效益三大维度下的14个指标进行综合评价，其中可以特别注意业务适当性、安全与隐私、互操作性、可治理性以及生态效益与产业融合等指标。针对数字版权业务场景，各评价指标的权重建议如图B.1–2所示。



图B.1–2 数字版权场景区块链应用综合评价指标权重

B.1.6 小结

基于区块链技术的数字版权应用可将版权资产上链，有效地利用区块链技术的信任穿透机制，实现数字内容版权的确权、授权和维权，为版权的保护和流转提供更加快捷的通道，将原本高费用和长时间的版权确权变得低价和高效，从而加速版权的流通。

（本案例由厦门安妮股份有限公司提供）

B.2 供应链金融场景

B.2.1 应用场景概述

当前，在激烈的市场竞争下，企业面临各种风险和挑战，企业融资难、融资贵问题日益凸显。传统银行融资方式偏重企业还款现金流和抵质押物的考量，无法解决供应链中企业（特别是中小企业）的短期融资问

题。2018年世界银行发布的《中小微企业融资缺口：对新兴市场微型、小型和中型企业融资不足与机遇的评估》报告显示，中国40%的中小微企业存在信贷困难，或是完全无法从正规金融体系获得外部融资，以及从正规金融体系获得的外部融资不能满足融资需求的情况，融资缺口达1.9万亿美元。

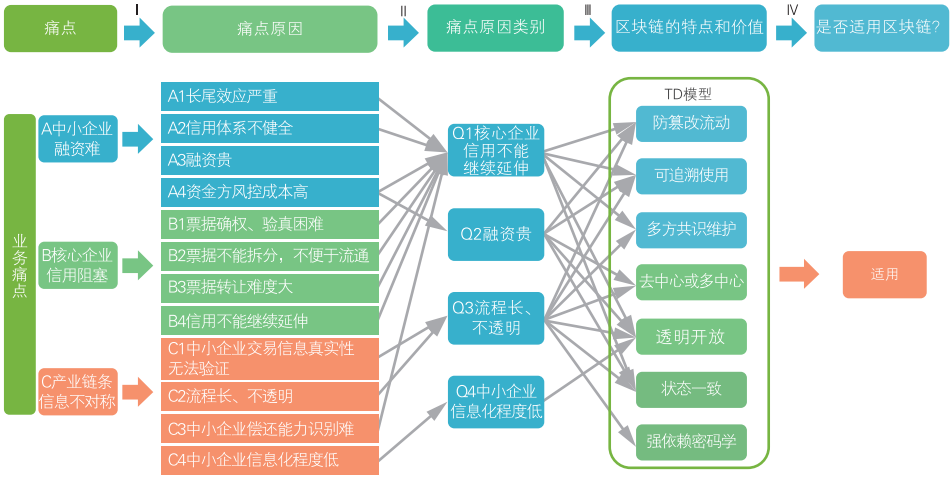
供应链金融是指将供应链上的核心企业以及与其相关的上下游企业看作一个整体，以核心企业为依托，以真实贸易为前提，运用自偿性贸易融资的方式，对供应链上下游企业提供综合性金融产品和服务。在新技术的驱动下，传统金融进一步升级，供应链金融市场呈现爆发式增长。根据有关数据统计，2017年，我国工业企业应收账款达13.5万亿，供应链金融市场规模达14.9万亿，预计到2020年，供应链金融市场规模将超过18万亿。

我国政府大力支持供应链金融发展。2017年10月，国务院办公厅发布的《关于积极推进供应链创新与应用的指导意见》提出要积极稳妥发展供应链金融；2018年4月，商务部、工业和信息化部等8个部门联合下发《关于开展供应链创新与应用试点的通知》，重点部署了供应链金融试点工作。

供应链金融是典型的多主体参与、信息不对称、信用机制不完善、信用标的非标准的场景，与区块链技术有天然的契合性。供应链金融围绕核心企业，覆盖其上下游中小微企业，需要商业银行、保理公司等资金端的支持，物流、仓储等企业的参与，以及企业信息技术服务、金融科技服务的支撑。多参与主体间信用的高效传递是供应链金融的关键要点，实体经济发展中所面临的中小企业融资难、融资贵的问题，关键突破点在于打通信用流转，以更好地盘活资产。

B.2.2 应用场景选择分析

本部分结合供应链金融业务的特点，围绕中小企业融资难、核心企业信用阻塞、产业链条信息不对称等业务痛点，使用ASMI四步法进行应用场景分析，以判断供应链金融场景中应用区块链技术的可行性（如图B.2–1所示）。



图B.2–1 供应链金融场景选择ASMI四步法分析示意图

经过分析可以看出，针对供应链金融的业务特点，使用区块链技术能够非常精准地解决部分痛点。在区块链上保存完整数据，使得不同参与者使用一致的数据来源，保证了供应链信息的可追溯性，实现了供应链透明化，并可支持可靠的审计跟踪，有助于建立透明可信的供应链金融系统。

B.2.3 应用技术选择分析

供应链金融场景在数据隐私和性能方面要求比较高，因此在应用区块链时需要特别注意通过合适的共识机制和隐私保护等技术提升性能和数据信任能力。根据场景特点，在共识机制方面可优先选择BFT类的共识机

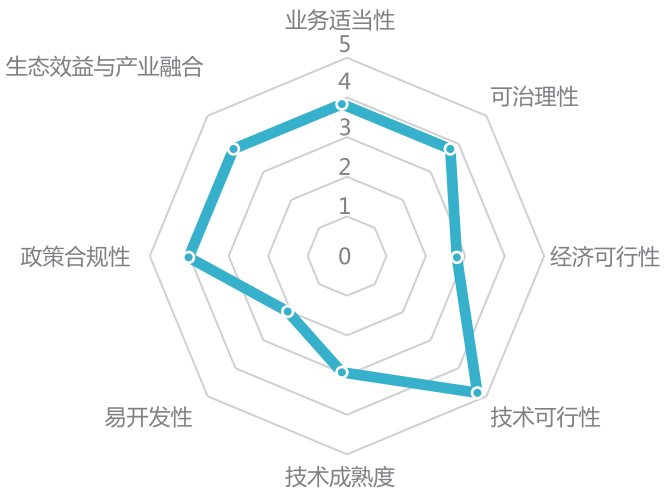
制，隐私保护方面可优先选择采用非对称加密技术和智能合约权限控制。

B.2.4 应用治理分析

供应链金融应用一般采用许可链治理。联盟构建可采用联合治理或领导型成员治理形式。参与成员管理可按需要进行成员检查并签署成员协议。新用户加入需提出申请并经过联盟管理成员同意，签署用户协议后方可加入，用户协议规定用户权限和义务。技术上，对于联盟成员可采用CA认证授权的许可链准入机制，通过CA授权的成员才被联盟中的其他节点承认。

B.2.5 应用评价分析

对于供应链金融场景下的应用，可从业务、技术、社会效益三大维度下的14个指标进行综合评价，其中可特别注意业务适当性、安全与隐私、经济可行性、可治理性以及生态效益与产业融合等指标。针对供应链金融业务场景，各评价指标的权重建议如图B.2–2所示。



图B.2–2 供应链金融场景区块链应用综合评价

B.2.6 小结

基于区块链技术的供应链金融应用通过将多方贸易关键数据上链和交叉验证，实现物流、商流、资金流、信息流“四流合一”，可提供企业融资所需的真实贸易背景信息；通过将核心企业到多级供应商的应收账款数字资产上链，将应收账款数字化并实现可拆分、可转让，构建核心企业信任穿透机制，可以有效地拓宽中小企业的融资渠道，有利于提升资产流动性，深度盘活金融资源，有力支撑供给侧改革。

（本案例由上海复星高科技（集团）有限公司提供）

B.3 冷链物流场景

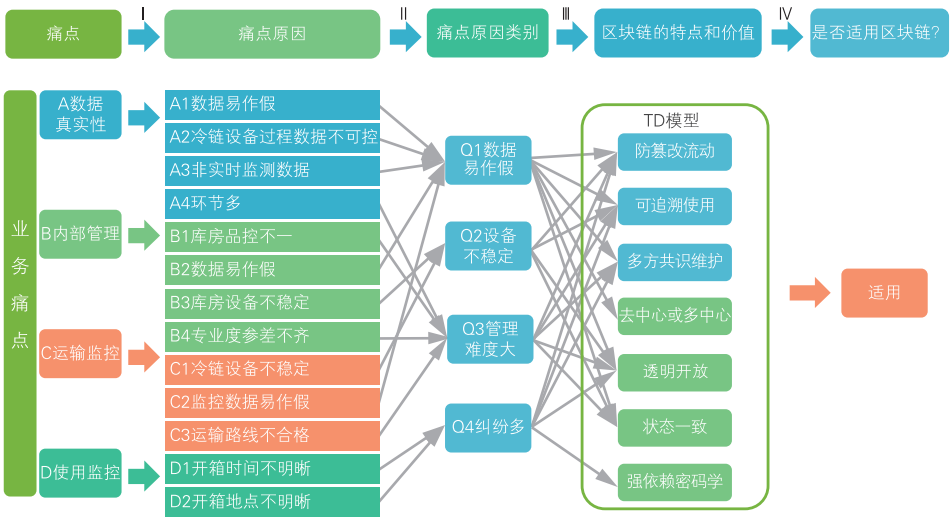
B.3.1 应用场景概述

冷链物流是指以冷冻工艺为基础、制冷技术为手段，使冷链物品从生产、流通、销售到消费者的各个环节中始终处于规定的温度环境下，以保证冷链物品质量，减少冷链物品损耗的物流活动。对于新鲜蔬菜瓜果、生鲜、疫苗药品等对温度要求较高的产品，冷链的作用在于对全链路中温度的严格控制，以确保产品在交付给消费者时，具有较高的安全性和良好的品质。近年来，生鲜电商的兴起以及O2O生鲜模式的发展，推动了生鲜市场的快速成长，加之疫苗有效性问题的暴露，冷链物流的市场规模迅速扩张。

随着连续测温等技术的发展，测温设备不断升级，冷链物流已经逐渐实现自动化测温。但由于库房管理与冷链运输能力的良莠不齐，市场竞争混乱，温度是否准确可靠成为冷链物流行业亟待解决的问题。加强冷链物流全链路的温度监控，并建立起安全可靠的数据追溯机制，可以说是冷链物流品控和安全保障的突破口。区块链技术防篡改和可追溯的特性，能够帮助在冷链物流过程中把控温度数据，保证冷链物流数据的可靠性。

B.3.2 应用场景选择分析

本部分结合冷链物流业务的特点，围绕数据真实性、内部管理、运输监控、使用监控等业务痛点，使用ASMI四步法进行应用场景分析，以判断冷链场景中应用区块链技术的可行性（如图B.3–1所示）。



图B.3–1 冷链物流场景选择ASMI四步法分析示意图

经过分析可以看出，针对冷链物流的业务特点，使用区块链技术能够非常精准地解决部分痛点。此外，还需要结合物联网等技术保证整个冷链物流生命周期中温度的实时监控。

B.3.3 应用技术选择分析

在冷链物流仓储和运输过程中，一般每隔5–30秒采集一次数据，每次采集的数据量比较小，仓储时数据可以定时批量上链，运输时监控数据需要实时上链。整体上看，冷链物流场景具有数据并发量大、对性能要求高，以及对于数据隐私性要求一般等特点。从业务痛点方面来看，上链数

据的防篡改和可追溯是关键点，所以特别需要共识机制和业务层应用治理方面的技术来提升数据的可靠性。针对冷链物流场景性能方面的需求，在共识机制方面可优先选择BFT类的共识机制，以提升效率和容错性。

B.3.4 应用治理分析

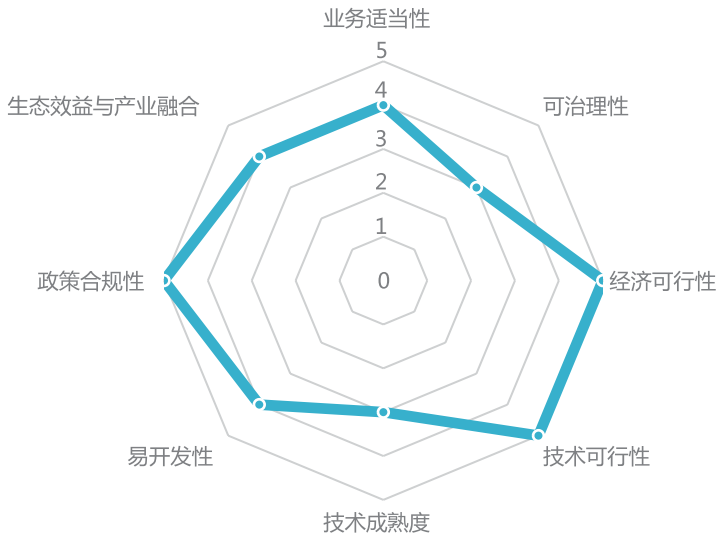
在用户层，冷链物流应用一般采用许可链治理，可采用成员准入机制：新用户加入需提出申请并经冷链物流联盟链同意，在签署用户协议后方可加入冷链物流联盟链，用户协议确定用户角色以及相应的权利和义务，以及可访问数据的范围，如用户违反协议将被强制退出。

在业务层，冷链物流区块链的区块中记录冷链服务管理过程中温度变化的完整信息。冷链物流数据是由物联网硬件自动产生并封装后上传区块链网络，在运输过程中产生的监测数据可以有效避免人为干预。

在技术层，区块链共识网络是整合冷链物流的底层基础；数据安全包括权限控制、链式存储和物联网硬件接入等方面；数据交换可以通过标准API、EDI/ebXML和物联网信息交换实现。

B.3.5 应用评价分析

对于冷链物流场景下的应用，可从业务、技术、社会效益三大维度下的14个指标进行综合评价，其中可以特别注意业务适当性、政策合规性、经济可行性、可治理性以及生态效益与产业融合等指标。针对冷链业务场景，各评价指标的权重建议如图B.3–2所示。



图B.3–2 冷链场景区块链应用综合评价

B.3.6 小结

基于区块链技术的冷链物流应用可以实现产品从生产端到消费终端流转过程中的温度等信息实时上链记录与追踪，有效解决了目前冷链物流行业中承运商责任不明、追溯困难、温度信息由于人工记录导致的可靠性低、实时性差等难题，极大地便利了生产企业端到端的质量控制和管理，在食品、药品安全问题日益受重视的社会环境下，区块链技术助力冷链物流发展，将带来很好的社会效应。

（本案例由上海复星高科技（集团）有限公司提供）

B.4 基于区块链的存证实践案例

B.4.1 应用/产品概况

证据的真实性、可追溯性是司法场景中最重要的要素之一。2017年10月，微众银行联合广州仲裁委（以下简称：仲裁机构）、杭州亦笔科

技（以下简称：存证机构）三方基于区块链技术搭建了面向司法仲裁行业的“仲裁链”。“仲裁链”发挥区块链技术的透明、防篡改、全流程追溯等优势，利用分布式数据存储、加密算法等技术对交易数据进行共识签名后上链，将实时保全的数据通过智能合约形成证据链，以满足证据的真实性、合法性、关联性要求，进而实现证据及审判的标准化。

业务发生时，用户的身份验证结果和业务操作证据产生的哈希值均通过区块链技术进行记录。需要仲裁时，后台人员只需点击一个按键，相应的证据便会传输至仲裁机构的系统平台上，仲裁机构收到数据后与区块链系统节点中存储的数据进行校验，确认证据真实、合法有效后，依据网络仲裁规则和国家相关法律规定进行裁决并出具裁决书。

通过使用“仲裁链”，仲裁机构可参与到存证业务过程中来，共同见证、实时共识验证，一旦发生纠纷，经核实签名的存证数据可视为直接证据，有助于仲裁机构快速完成证据核实，极大地缩短了仲裁流程。

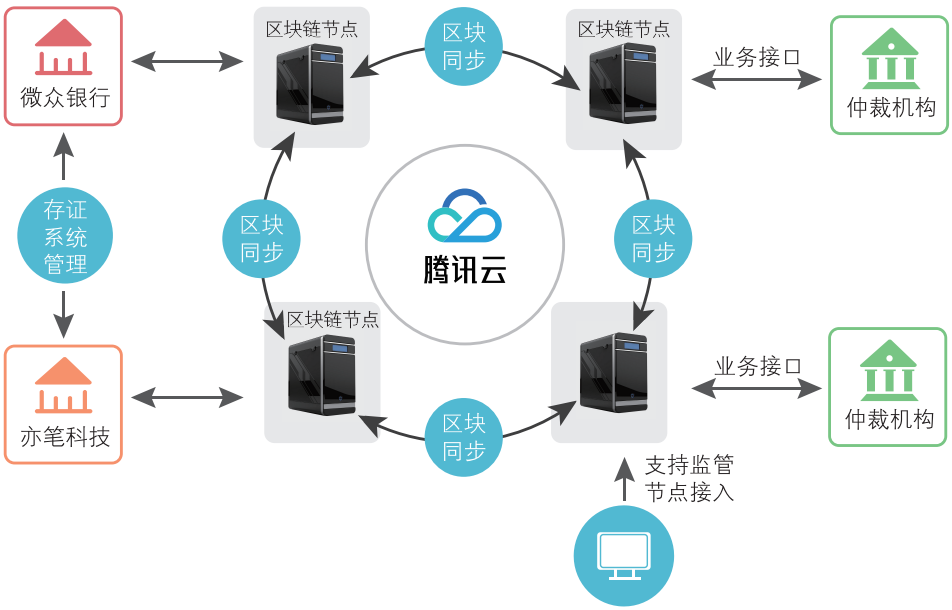
2018年2月，广州仲裁委基于“仲裁链”出具了业内首个裁决书。“仲裁链”发布以来，已有十余家存证机构和仲裁机构加入仲裁链生态，截至2018年四季度，已完成超过千万份合同的存证，涉及资金规模达千亿级。

B.4.2 应用技术选择情况

“仲裁链”基于FISCO BCOS区块链底层开源平台搭建，FISCO BCOS是以金融业务实践为参考样本、为金融行业量身定制的开源区块链底层平台，是BCOS开源平台的金融分支版本，由微众银行、深证通、腾讯云等金链盟开源工作组的多名成员牵头创建。FISCO BCOS提供了全面的监管和审计支持模块，包含准入控制、CA身份认证、账户管理体系和安全监控等功能，可支持海量数据容量存储和弹性扩容，具备密钥管理机制和隐私保护机制，可充分满足存证仲裁的技术要求。

B.4.3 应用治理情况

“仲裁链”采用联盟链的治理方式，图B.4–1展示了“仲裁链”的业务架构图。在该网络中，微众银行、存证机构、仲裁机构和其他业务相关方都可作为链上节点加入，形成一个可靠的联盟链网络。



图B.4–1 “仲裁链”业务架构图

“仲裁链”在业务设置上采用符合仲裁业务特点的治理方式保障良好的安全特性和隐私保护能力，并对如何清晰、便捷地监控联盟链运行状况、支持监管和审计诉求进行了深入研究，以确保满足金融行业对数据结构化、可视化、可监管和可审计等要求。具体包括：1）仅允许经过许可的成员加入，避免了无关成员加入到链上以及由此带来的数据泄露隐患；2）联盟链拥有良好的管理机制，可以通过联合治理、法定机构治理、领导成员治理等多种机制来实现，处理各种问题，优化管理过程；3）每个参与成员可以拥有不同的操作权限，清晰地定义职责分工，避免数据隐私

被泄露至不恰当的成员；4）可以通过设置独立观察节点、调用API数据接口、部署特定智能合约等方式，对链上活动进行实时监督，并对异常活动进行干预。

具体来讲，区块链浏览器、监控体系、监管节点以及反洗钱接口都是治理的实施环节。具体包括：1）“仲裁链”提供区块链浏览器，能将区块链上的数据可视化，并进行实时的展示，用户即使毫无技术背景，也可以通过web页面便捷地获取其部署的区块链节点、区块和交易信息；2）优化了监控统计日志，使开发者可以快速获取区块链系统运行过程中的重要参数，从多个维度对系统的运行状态进行评估；3）监管或审计部门可以作为特殊的监管节点接入，可以即时同步数据并对数据的完整性、有效性等进行监控或审计，同时也可以进行业务流程的合规检查、反洗钱等操作。

B.4.4 小结

“仲裁链”可将传统模式下长达1–3个月的仲裁流程缩短到7天左右，司法成本也降低至传统模式的10%。区块链技术及运作机制客观透明，其应用使得证据或合同的容灾能力、可靠性和容错性更强，从而可免去很多因摩擦纠纷产生的支出，并有效降低人工操作风险与道德风险，有效地解决了取证难、仲裁难的痛点，同时也有利于维护执法透明、司法公正与社会和谐。

（本案例由深圳前海微众银行股份有限公司提供）

B.5 香港国际贸易融资网络应用

B.5.1 应用/产品概况

香港国际贸易融资网络（简称：HKTFP）项目由香港金融管理局牵头，香港贸易融资平台有限公司主导实施。平安金融壹账通作为技术服务提供商，基于自主研发的底层BaaS平台FiMAX，助力香港的各大商业银行为贸易企业提供贸易融资服务，参与方包括汇丰银行、渣打银行、澳新银行、中国银行、东亚银行、星展银行和恒生银行等数十家国际和国内银行。

国际贸易融资业务是银行对公业务的重要一环，国际知名的大型商业银行通常会为此业务打造一套中心化的内部系统，以完成与客户间的交互及内部业务流程的管理。然而贸易融资业务实则是一个多主体参与、容易发生信息不对称进而导致风险的业务场景，中心化的内部系统并不能有效解决上述问题。

HKTFP通过区块链技术链接起各银行间的贸易融资系统，打造出一个弱中心化的业务协同网络，利用FiMAX的可授权加解密及零知识证明技术，打破信息壁垒，帮助银行大幅降低业务风险和操作成本，从而使企业实现更高的融资成功率和更低的融资成本，最终为实体经济的健康发展提供助力。

B.5.2 应用技术选择情况

根据贸易融资的业务特点，区块链应用在技术上需要做到：1）让各参与方上链的数据能够得到隐私保护，消除参与方数据上链的后顾之忧，从而将贸易信息及融资信息线上化、结构化；2）使数据可被多方“共享”使用（可以在明文及密文这两种条件下被使用），帮助银行验证贸易真实性，并防范重复融资的风险。

为此，HKTFP使用了平安金融壹账通FiMAX产品的以下三项技术：

• 可授权加解密技术：上链数据可加密，并且做到逐字段加密，帮助各类企业及银行保护自身的数据隐私。参与方可基于业务需求，向特定的其他参与方针对特定的数据字段进行解密授权。在被授权前，任何参与方均无法解密其他参与方上链的数据。

• 零知识证明技术：数据能够在加密状态下被使用，可用于进行不同参与方之间的数据交叉验证。其中，交叉验证可以是数据的直接比对，例如：判断卖方提供的订单总金额与买方所提供的订单总金额是否一致，或判断用于发起融资申请的基础资产（如订单或发票）是否已被用于在其他任何银行获取过融资（即验证是否出现了重复融资的风险）；也可以是经过运算后的结果比对，例如：判断卖方的发票中每项商品的总金额是否等于买方订单中商品的单价乘以物流公司送货单中的运送数量。

• 智能合约：利用智能合约自动匹配数据项完成交叉验证，并找出其中信息的不符点，能有效提高核验效率并降低贸易欺诈风险。同时，也将其他线下文件线上化，利用智能合约自动监测并触发下一环节，加速贸易流程。

B.5.3 应用治理情况

由于HKTFP项目涉及众多参与方，例如，大型海内外银行、核心企业、物流公司等，因此合理有效的应用治理结构就显得尤为重要。治理机制可重点考虑联盟构建机制、会员管理机制、会员权限控制等方面。

B.5.4 小结

贸易与贸易融资业务是非常典型的多参与方协同作业的场景，各参与方之间需要共享业务及流程信息以达成业务的合作和效率的提升，但由于各参与方均为独立的法人主体，不完全信任和信息隐私保护成为深化合作的障碍。平安金融壹账通搭建的HKTFP网络在区块链技术的基础上，运用

了可授权加解密、零知识证明以及智能合约等技术，帮助各参与方在保护自身数据隐私的同时，保证密文数据能够被其他参与方使用并产生价值，从而降低业务风险与成本，达成信任关系，促成业务落地，提升业务效率，并最终为网络中的各方带来经济效益。同时，HKTFP网络作为国际大型有真实生产贸易数据交易的区块链网络系统，对于区块链技术应用于实际生产领域具有重要意义。

（本案例由中国平安保险（集团）股份有限公司提供）

B.6 京东区块链电子营业执照

B.6.1 应用/产品概况

电子营业执照是无纸化的电子牌照，是根据有关登记注册法律、法规，由依法成立的具有认证资格的第三方机构以数字证书为基础制作的载有企业注册登记信息的信息证书。

当前，电子营业执照面临诸多痛点，例如，营业执照多次提交、经营者营业执照登记地与实际经营地点不一致、网络市场监管部门汇集的中心数据与电商平台之间数据相互孤立，以及数据篡改和造假较容易且审核成本高等问题。区块链技术具有分布式记账、自动广播、全流程可追溯、信息防篡改以及多方共识维护等特点，可助力营业执照业务实现跨主体信息的共享及协作。通过区块链的共识机制和自治性，还能帮助实现国家企业信息公示系统中可公开的工商行政管理监管执法信息互通共享。

京东电子营业执照区块链应用可以很好地满足各方对电子营业执照数据安全、便捷和保密的要求。该应用将政府电子营业执照数据上链，由京东平台自动审核并快速反馈审核结果，审核通过后将企业开店信息上链。营业执照信息一旦写入区块链，即自动同步到所有节点，某一节点只要获得授权，即可查询对应营业执照信息。同时对营业执照从开出到每一次信

息变更的全量信息及流程进行记录，市场监管部门通过查询页面，可以便捷地查询营业执照的全流程信息，包括开出时间、写入区块链时间、写入方、签名方、变更信息时间和变更信息内容等。对商家来说，该应用可以加快其入驻京东平台的速度；对于京东来说，可以大幅提升商家入驻的审核效率，降低平台管理及服务成本；对于监管部门来说，可以为开展在线监测、及时发现问题、打破数据共享壁垒等提供有力的支撑。

目前，宿迁工商局、京东益世商服、京东商城三方已成功在京东智臻链平台完成部署，已有数千家商家营业执照信息成功上链。未来，京东将致力于协同各监管机构，不断拓展联盟节点，整合各监管与服务部门数据，推动形成基于营业执照的企业生态链。

B.6.2 应用技术选择情况

区块链电子营业执照应用主要考虑区块链组网模式、访问控制机制、数据隐私保护等方面的技术选择。

1、区块链组网模式。区块链电子营业执照应用由相关行政职能部门牵头，相关方多方共治，当前组网模式主要考虑采用联盟链的模式。

2、访问控制机制。区块链电子营业执照应用涉及行政主管部门、周边服务从业企业、证照信息使用企业、技术服务提供企业等参与方，不同的参与方在应用治理体系中的职能和诉求不同。区块链电子营业执照应用需要区块链平台和相关产品提供严格的用户身份检查功能，并能支持灵活细粒度的权限控制，用户身份检查可采用CA方式，权限控制可采用RBAC（基于角色的访问控制）、ABAC（基于属性的访问控制）权限控制模型。

3、数据隐私保护。区块链电子营业执照应用中涉及私密敏感信息，需要提供健全的数据隐私保护机制。可以选择的隐私保护技术包括摘要上链、加密上链、加密传输、零知识证明、同态加密等。其中，摘要上链和加密上链用来避免私密信息直接暴露在账本中，加密传输主要用来防止通

信过程中的信息泄漏，零知识证明主要用来避免在验证环节公开私密信息，同态加密可用于确保数据私密下的信息处理。

B.6.3 应用治理情况

区块链电子营业执照应用联盟采用联合治理形式，由工商行政管理部门牵头组建联合治理委员会。在参与成员管理方面，通过基于CA的身份认证实现联盟链准入控制，并且新成员加入许可链之前，需要签署正式的具有法律效力的成员协议。

区块链电子营业执照应用采用面向角色的权限控制，不同参与成员根据职责定位拥有不同的权限，具体权限类型包括：

• 业务操作权限：工商行政管理部门（宿迁工商局）负责将电子营业执照登记、变更、审核等信息写入区块链，电商平台参与者（京东商城）拥有链上电子营业执照信息的读取权限；

• 平台运营权限：联合治理委员会负责平台运营，具体实施中，联合治理委员会可委托有资质的技术公司负责平台运营；

• 运维开发权限：联合治理委员会负责运维开发，具体实施中，联合治理委员可委托有资质的技术公司负责运维开发；

• 监管权限：当前由联合治理委员会代理监管和审计权限，包括检查链上业务数据、监控许可链的运行状态等。

区块链电子营业执照应用对于共识节点的管理包括：

• 共识节点加入：联合治理委员会进行节点拥有者身份审查、节点安全性评估，并将授权的共识节点写入区块链配置中；

• 共识节点监控：联合治理委员会监控共识节点的运行状态，包括在线率、块高度、软件版本等，及时发现处于节点故障、被黑客劫持、不满足联盟定义的节点规范等异常状态的共识节点；

• 共识节点退出：共识节点可自愿退出联盟，或是由联合治理委员会

将处于异常状态的节点强制退出；

• 共识节点替换：当有共识节点自愿或强制退出后，联合治理委员为可根据需要选择一个候选节点进行节点替换。

此外，区块链电子营业执照应用中通过设置独立观察节点和监管审计智能合约，对链上活动进行即时监督，对异常活动进行干预，并保存完整的链上数据和日志等资料。

B.6.4 小结

基于区块链的电子营业执照应用可将监管部门的营业执照及相关字段上链，确保上链的数据不被篡改，保证数据真实性，提高企业办事效率，加速政务电子化及效率提升，同时可实现各方数据互通匹配，大大缩短商户入驻所需资质材料的审核时间，减少人工审核的时间成本，协助监管部门实现数字化管理，助力企业全面实行数字化转型。

（本案例由北京京东尚科信息技术有限公司提供）

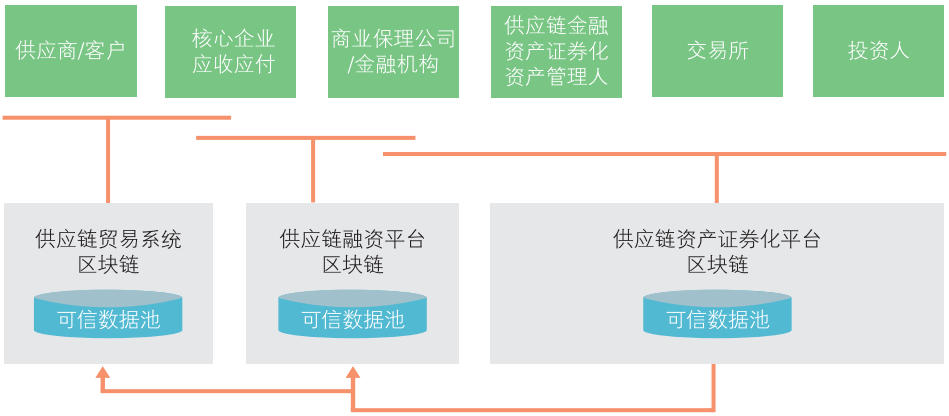
B.7 可溯源供应链金融解决方案

B.7.1 应用/产品概况

可溯源供应链金融解决方案（易见区块2.0）是由易见股份开发的基于区块链的供应链金融服务解决方案。自2016年起，易见股份就致力于“区块链+供应链金融”技术平台的研发，2017年4月，易见区块1.0系统正式上线，目前的易见区块2.0于2018年9月发布。易见区块2.0采用了具有自主知识产权的可信数据池和业内领先的多链数据可追溯技术，已帮助近200家企业及金融机构完成了超过40亿元的供应链金融业务，线上融资合同近500份，涉及医药、化工、制造、大宗、物流、航空和地产等多个行业。

易见区块2.0供应链金融系统解决方案的产品体系包括易见供应链贸

易系统、易见供应链融资平台和易见资产证券化平台。其中易见供应链贸易系统由供应商与核心企业参与，易见供应链融资平台由供应商、核心企业及金融机构共同参与；易见供应链资产证券化平台则满足资产证券化各参与方动态资产管理、资产质量趋势分析及透明监管等需求（如图B.7–1所示）。



图B.7–1 易见可溯源供应链解决方案

易见区块2.0采用基于区块链底层技术的可信数据池，确保企业对数据池中数据所有权的控制、各贸易方数据账本的独立分布式存储、智能合约的高效执行以及不同系统与数据池间的跨链交互，并通过独立的审计账本实现信息数据与读写操作的可溯备查。在系统应用方面，易见区块2.0在供应链贸易系统中以难以篡改的方式刻画交易双方真实贸易背景；提供可视化贸易信息，从购销信息发布、货流实时监控、单据传递跟踪至结算都准确快捷；在供应链融资平台上支持开放式的融资需求双向选择、融资随借随还等多样化流程设计；实现金融机构对贸易融资投放与回收的专户管理，解决供应链金融中信息闭环与资金闭环两个核心风控问题。

B.7.2 应用技术选择情况

在供应链金融中应用区块链技术，除了利用其可溯源、防篡改、多方验证等基本能力，还需关注企业级应用所关注的数据安全、隐私保护、访问授权等。对核心企业而言，供应链贸易数据中，供应商列表、采购数量和价格等都属于企业核心业务敏感信息，需要严格保护；另一方面，金融机构需要在融资过程中通过相关信息审核获得授权。也就是说，需要做到数据的可控交互。

易见区块2.0的可信数据池采用多链多账本架构，可供供应链贸易的参与方根据需要创建或加入贸易链，并且拥有不同主体的数据节点。贸易数据只记录在核心企业及其上下游企业参与的数据账本中，在源头防止贸易数据被存储在非贸易参与方而带来的数据泄露隐患。在贸易链中，由于参与方为核心企业及其上下游企业，为保证数据的公正性，可信数据池在贸易链中还加入独立的审计账本，并由第三方（平台运营方，如易见股份）加入，实现对贸易链数据的第三方见证；在审计账本中仅存储数据账本中的数据哈希及操作，实现了贸易数据对第三方的保密。

除贸易链之外，易见区块2.0中还包括融资链及资产证券化链。这两种链的参与方除了核心企业及其有融资需求的上下游企业之外，还包含金融机构、交易所等金融业务参与方。当有融资需求时，数据由贸易链推送至融资链或资产证券化链，并授权给相应机构。这种多链构造一方面可以实现各个链上的数据完全隔离，需要授权才能进行数据访问；另一方面数据在多链网络中可被跨链访问，从而实现供应链金融资产可溯源。

B.7.3 应用治理情况

由于供应链业务本身具有准入特性，因此易见区块2.0选择许可链的模式。由于易见区块设计上是多链结构，不同链的治理模式各有差异。

- 贸易链：贸易链围绕供应链贸易本身，而供应链贸易是围绕核心企

业开展的。因此，贸易链的联盟构建采用领导型成员治理形式，即由核心企业主导管理。

• 融资链：融资链主要支持融资业务，在融资业务中占主导地位的是金融机构，同时融资平台运营方需要协调金融机构的参与。因此，融资链采用联合治理形式，由平台运营方与选定金融机构共同管理联盟。

• 资产证券化链：在资产证券化中，重要的参与方包括券商、交易所等，因此也采用联合治理形式。需要指出的是，交易所事实上行使监管权力，因此交易所在资产证券化链中具有监管权限。

以上三种链中，成员认证（KYC）统一由平台运营方完成，但被认证成员能否加入某一特定的链中由该链的联盟治理者决定。联盟治理者同时负责成员的权限分配。

此外，由于三种链均基于可信数据池产品，该产品有独立的审计账本记录所有操作，因此实现了基于区块链的全量审计日志记录。同时，基于审计账本的记录可以实现异常行为监测等功能。

B.7.4 小结

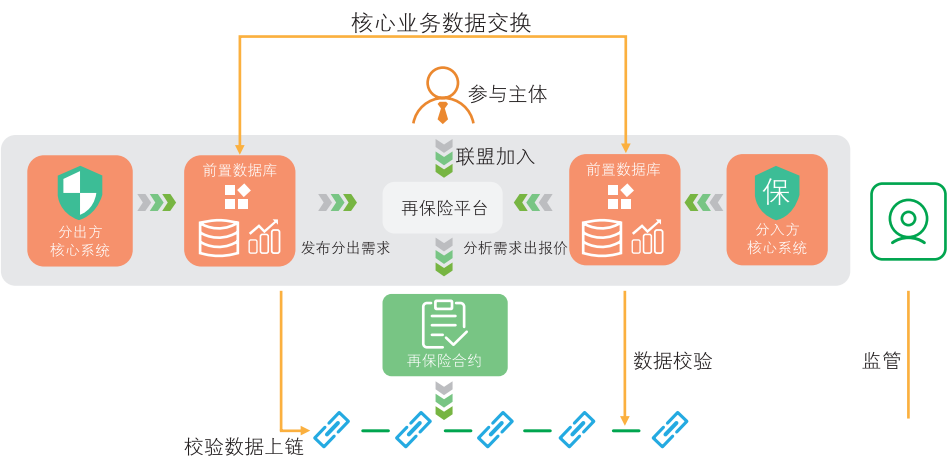
可溯源供应链金融解决方案关注供应链金融的中小企业融资难、成本高，贸易数据验证成本高以及供应链金融体系效率偏低等业务痛点，从“信息闭环”与“资金闭环”两个核心风控逻辑出发，将区块链作为底层技术，使用难以篡改的方式刻画交易双方真实贸易背景，解决贸易真实性难以保证、数据缺乏透明性以及数据交叉验证工作量大等问题，从而帮助提升整个供应链链条的运行效率，降低融资成本。

（本案例由易见供应链管理股份有限公司提供）

B.8 基于区块链的再保险交易系统（RIC）

B.8.1 应用/产品概况

基于区块链的再保险交易系统（RIC）由上海保监局牵头，众安保险、中再、汉再、通用再等多家再保机构共同参加，系统由众安科技与英特尔联合研发，利用区块链技术整合再保险产业链上中下游多家机构，搭建以再保险信息数据共享以及安全监管为核心的再保险生态联盟（如图B.8-1所示）。通过区块链技术把直保公司的保单信息进行有效安全传输并存储，实现与再保险公司间的信息共享；利用区块链智能合约不可篡改的特性，实现直保公司与再保公司之间的分出业务、多个再保公司之间转分保业务的记录和记账，保障了业务安全性；基于可溯源、防篡改的特征，确保数据交易的真实性，解决消费误导、骗保骗赔等问题；利用智能合约技术，实现自动理赔，提高理赔效率。区块链技术的引入很好地解决了再保险业务中所面临的“共享、信任、监管”等问题，有效实现了安全数据交易共享，提升了再保险业务效率。

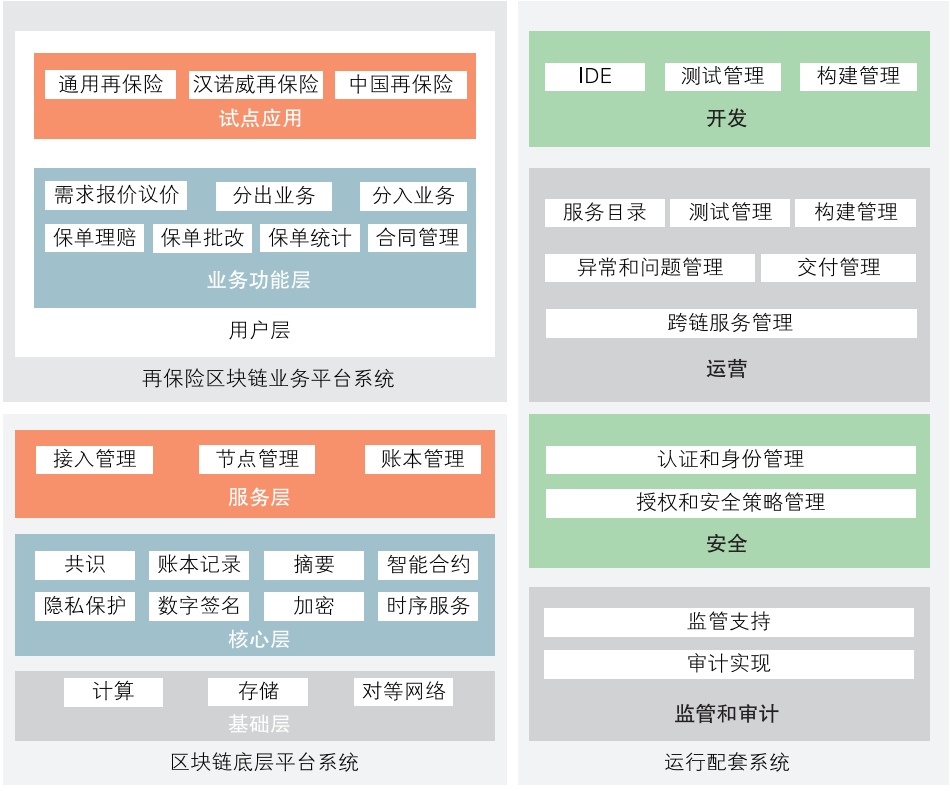


图B.8-1 基于区块链的再保险交易应用场景图

B.8.2 应用技术选择情况

结合再保险场景性能和系统稳定性方面的需求，在共识机制方面可优先选择PBFT类的共识机制，隐私保护方面可优先选择采用非对称加密技术和智能合约权限控制。同时，为保障其对于数据以及访问的高安全需求，可以结合软硬一体化安全登录技术与多方隐私数据共享传输机制。

基于区块链的再保险交易系统架构如图B.8–2所示。



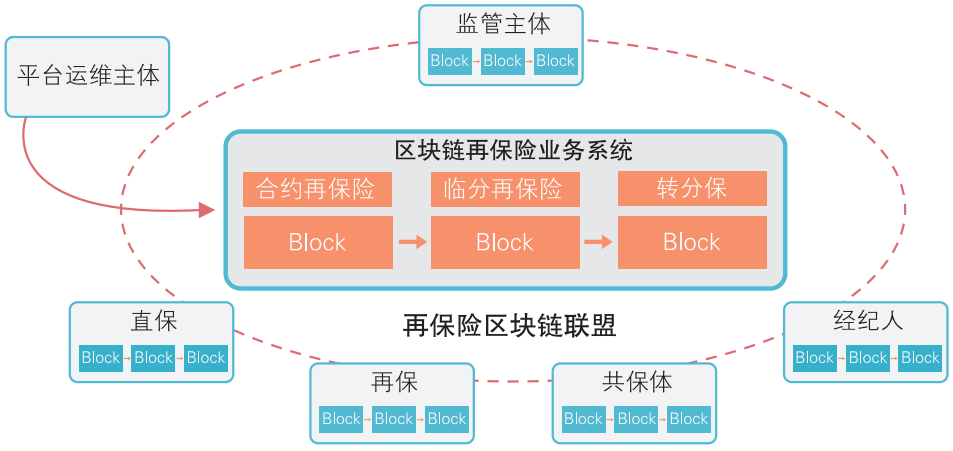
图B.8–2 基于区块链的再保险交易系统逻辑架构视图

该系统主要分为三大系统域：区块链底层平台系统、再保险区块链业务平台系统和再保险区块链运行配套系统，支持报价议价、分出业务、分

入业务、保单理赔、保单统计、合同管理、对账等功能，在合约、临分等再保险业务场景下具有广泛的应用前景。其中，区块链底层平台系统包含支撑区块链运行所需要的核心功能和服务，主要包含有共识、智能合约等功能；再保险区块链业务平台系统构建在区块链系统的业务应用模块上，主要是面向具体的业务场景，包括根据再保险行业在合同约定、自动控制、泛在交互以及分布式结算等业务场景的报价议价、分出业务、分入业务、保单理赔、保单统计、合同管理等通用需求提炼的业务应用模块，对上层应用提供通用服务；运行配套系统主要是针对再保险区块链系统运行中的迭代开发、日常运营、安全管理以及监管审计方面的支撑，保障整个系统的持续与稳定运行。

B.8.3 应用治理情况

基于区块链的再保险交易系统中参与方由交易主体、平台运营主体和监管主体等类型主体构成，其业务架构如图B.8–3所示。



图B.8–3 基于区块链的再保险交易系统业务架构视图

系统的治理需要满足许可链的相关治理要求，包括平台搭建、权限管理、节点管理、监管审计和监控等治理内容。

用户层采用成员准入机制，基于区块链技术构建联盟。新用户加入需提出申请并经过所有联盟成员同意，在签署用户协议后方可加入，用户协议确定用户角色、相应的权利和义务，以及可访问数据的范围，如用户违反协议将被强制退出。

业务层主要的治理内容有：区块信息中记录再保险服务管理过程中承保、变更、理赔、缴费的完整信息，数据由各相关机构的核心系统通过前置数据库封装后上传区块链网络。

技术层主要的治理内容有：共识网络是整合RIC的底层基础结构，包括共识机制、智能合约、分布式账本和成员管理；数据安全包括权限控制、链式存储和前置数据库数据接入；数据交换层实现再保险业务过程中的数据交换，数据交换可以通过标准API实现。

B.8.4 小结

基于区块链的再保险交易系统充分利用了区块链技术公开透明、数据防篡改、自动执行等特点，保障了交易安全，有助于提升各个保险机构的服务水平，促进再保险交易的高效达成，并且可以优化交易监管，推进再保险业务的健康发展。

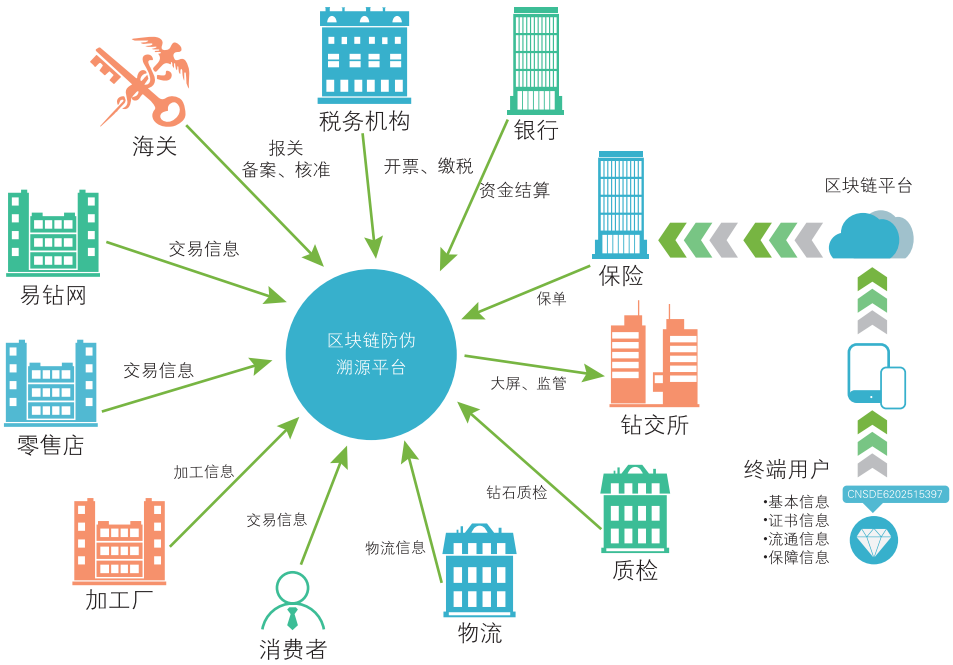
（本案例由众安信息技术服务有限公司提供）

B.9 基于区块链的钻石溯源系统

B.9.1 应用/产品概况

基于区块链的钻石溯源系统由鼎钻科技与众安科技联合开发，利用区块链技术整合钻石产业链的各个参与方，组建钻石溯源联盟，将区块链技术应用到钻石从开采、切割、鉴定、报关到交易的整个生产、流通过程

（如图B.9–1所示）。利用区块链记录钻石的整个生产及流通过程，实现全流程可追溯，解决钻石流通交易中信息不透明的问题；通过智能合约在可信交易方面的安全性及不可逆转性，实现钻石产业链上下游机构基于区块链的钻石交易确权，降低交易成本和交易风险；基于区块链防篡改的特性，钻石交易监管机构也可以对钻石交易更方便地实施监控，从而加强对钻石走私的打击力度。



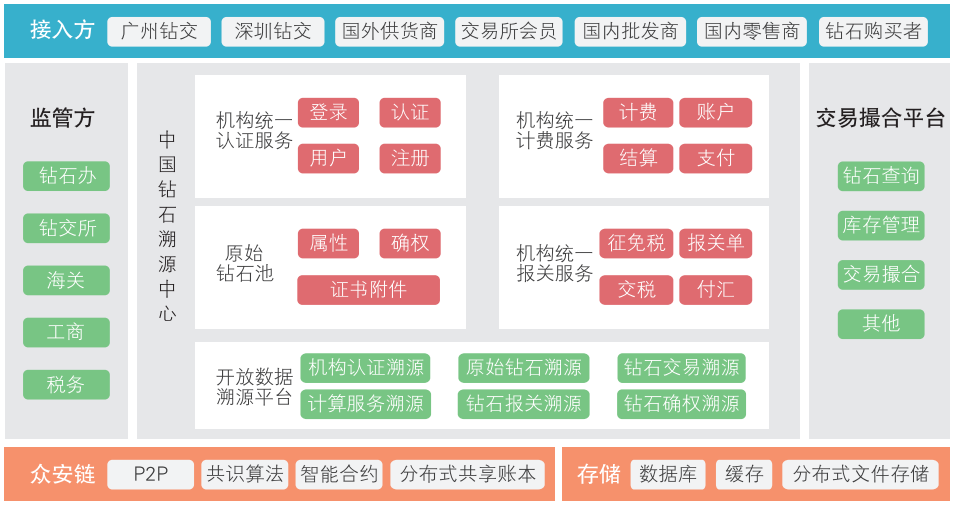
图B.9–1 基于区块链的钻石溯源应用场景图

B.9.2 应用技术选择情况

由于钻石溯源场景性能和系统稳定性方面的需求，在共识机制方面可优先选择PBFT类的共识机制；隐私保护方面可优先选择采用非对称加密

技术和智能合约权限控制。

基于区块链的钻石溯源系统逻辑架构如图B.9–2所示。



图B.9–2 基于区块链的钻石溯源系统逻辑架构视图

该系统分为底层区块链层、业务应用层以及网关层，支持机构登记、钻石报关、钻石交易、钻石质检及其溯源、电子合同签署和钻石线上验证等功能，在钻石进口、报关和交易等业务场景下均有广泛的应用场景。底层核心功能模块主要包括数据层、网络层、共识层、合约层。其中数据层选用LevelDB数据库做数据存储，对数据进行密码算法的非对称加密存储。网络层支持P2P网络的通信协议，保障节点之间的交互通信。共识层采用PBFT共识机制，保障2/3节点正常工作的情况下可以快速达成共识。合约层支持基于EVM（以太坊虚拟机）和JVM（Java虚拟机）的智能合约部署和运行。业务应用层在底层区块链的基础上，对外提供机构统一认证、计费服务，机构报关服务，钻石原始信息溯源及钻石的报关、交易、确权溯源和钻石查询验证、交易服务等服务。网关层对外提供统一入口，

供外部机构接入，并对接入数据进行身份和安全验证，防范外部流量的攻击，保障底层系统的安全性。

B.9.3 应用治理情况

基于区块链的钻石溯源系统的参与方由钻石产业链的相关企业构成，包括国外供货商、钻石交易所会员机构、国内批发商、国内零售商、报关公司、质检机构和物流公司等。在平台中，钻石的每一次流通行为，都必须由相关的双方基于在线电子合同进行签约，确保钻石流通信息的真实可靠，并通过Ukey对签约信息进行签约上链，确保流通信息不被篡改。

基于区块链的钻石溯源系统的治理需要满足许可链相关治理要求，包括平台搭建、权限管理、节点管理、监管审计和监控等治理内容。

采用成员准入机制，基于区块链技术构建联盟。新用户加入需提出申请并经过所有联盟成员同意，在签署用户协议后方可加入，用户协议确定用户角色、相应的权利和义务，以及可访问数据的范围，如用户违反协议将被强制退出。

区块信息中记录钻石从开采、切割、进口、报关、批发到零售的完整信息，数据由各相关机构的核心系统通过前置数据库封装后上传区块链网络。

B.9.4 小结

基于区块链的钻石溯源系统借助区块链防伪溯源技术，进入该平台的钻石在传统GIA、NGTC等证书的基础上，可以再额外获得一张区块链“电子身份证”——钻石溯源证书，该证书可以真实记录钻石从开采到交易的所有信息，实现“传统证书+电子身份证”的“双保险”。

（本案例由众安信息技术服务有限公司提供）

参考文献

[1] 中国区块链技术和应用发展白皮书，中国区块链技术和产业发展论坛，2016年10月

[2] 区块链 参考架构，中国区块链技术和产业发展论坛，CBD—Forum—001—2017

[3] 区块链 数据格式规范，中国区块链技术和产业发展论坛，CBD—Forum—002—2017

[4] 系统与软件工程系统与软件质量要求和评价(SQuaRE)第10部分：系统与软件质量模型，GB/T 25000.10—2016

[5] GentryC. A fully homomorphic encryption scheme, Stanford University, Doctoral Dissertation 2009

[6] 冯登国，陈成，属性密码学研究，密码学报，2014，1(1)

[7] Bellare M, and Phillip R. Random oracles are practical: A paradigm for designing efficient protocols. Proceedings of the 1st ACM conference on Computer and communications security, 1993

[8] Rivest R, Adi S, and Yael T. How to leak a secret. Advances in Cryptology—ASIACRYPT, 2001

[9] MicaliSilvio, RabinMichael O., VadhanSalil P, Verifiable random functions, Proceedings of the 40th IEEE Symposium on Foundations of Computer Science.1999

[10] 区块链平台调研与分析，安永，金链盟，2017

[11] 郝汉，基于区块链技术的微版权确权模式构想，信息技术与标准化，2017年第12期

[12] Vitalik Buterin, Chain interoperability. 2016

[13] 冷链物流分类与基本要求，GB/T 28577—2012