中国区块链技术和应用发展白皮书

（2016）

指导单位：工业和信息化部信息化和软件服务业司
编写单位：中国区块链技术和产业发展论坛

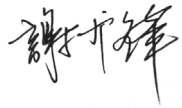
2016年10月18日发布

序

当前，全球新一轮科技革命和产业变革持续深入，国际产业格局加速重塑，创新成为引领发展的第一动力。在这一轮变革中，信息技术是全球研发投入最集中、创新最活跃、应用最广泛、辐射带动作用最大的领域，是全球技术创新的竞争高地，是引领新一轮变革的主导力量。

区块链作为分布式数据存储、点对点传输、共识机制、加密算法等技术的集成应用，近年来已成为联合国、国际货币基金组织等国际组织以及许多国家政府研究讨论的热点，产业界也纷纷加大投入力度。目前，区块链的应用已延伸到物联网、智能制造、供应链管理、数字资产交易等多个领域，将为云计算、大数据、移动互联网等新一代信息技术的发展带来新的机遇，有能力引发新一轮的技术创新和产业变革。

为推动区块链技术和产业发展，信息化和软件服务业司指导中国电子技术标准化研究院，联合蚂蚁金融云、万向控股、微众银行、乐视、万达网络、平安科技等骨干企业，开展区块链技术和应用发展趋势专题研究，编撰形成了《中国区块链技术和应用发展白皮书（2016）》。白皮书总结了区块链发展现状和趋势，分析了核心关键技术及典型应用场景，提出了我国区块链技术发展路线图和标准化路线图等相关建议。白皮书内容详实、分析透彻，具有较好的参考价值。希望各界共同努力，积极把握区块链发展趋势和规律，营造良好的发展环境，加速推动我国区块链技术和产业发展。



工业和信息化部

信息化和软件服务业司 司长

2016年10月

内 容 摘 要

近两年来，联合国、国际货币基金组织和多个发达国家政府先后发布了有关区块链的系列报告，探索区块链技术及其应用。在国内，金融企业、互联网企业、IT企业和制造企业积极投入区块链技术研发和应用推广，发展势头迅猛。为了积极引导我国区块链技术和应用发展，我们编写了本白皮书。其主要内容包括：

一、国内外区块链发展现状的研究分析。首先研究了区块链技术和应用发展的演进路径，提出了区块链的发展生态结构，盘点了7类典型参与者：开源社区、产业联盟、骨干企业、初创公司、投资机构、金融机构和监管机构的区块链实践进程。梳理了英国、美国、俄罗斯等国家的相关机构对区块链的态度，分析了区块链与云计算、大数据、物联网、下一代网络、加密技术和人工智能等6大类新一代信息技术的关系。

二、区块链典型应用场景及典型应用分析。通过分析全球200多个应用案例，提出了区块链的典型应用场景。列举了6个应用相对成熟、应用前景广阔或具有潜在应用价值的应用场景，并对区块链的应用价值进行了展望。

三、提出我国区块链技术发展路线图的建议。分析提出了由7个主要技术特征构成的区块链通用技术需求，结合国内外发展现状和应用场景，提出典型的区块链技术架构，并分析了共识机制、数据存储、网络协议、加密算法、隐私保护和智能合约等6类核心关键技术，以及区块链治理和安全。最后，结合国内外发展趋势，提出了我国区块链技术发展路线图建议。

四、首次提出我国区块链标准化路线图。结合区块链应用场景和技术架构，提出了区块链标准体系框架建议。通过分析国际标准化发展趋势，以及区块链技术和应用发展需求，提出了基础、业务和应用、过程和方

法、可信和互操作、信息安全等5类标准，并初步明确了21个标准化重点方向和未来一段时间内的标准化实施方案。

最后，基于对全球区块链发展趋势的研判，以及我国区块链技术和应用发展现状和趋势，围绕扶持政策、技术攻关和平台建设、应用示范等方面提出了相关建议。

指导单位

工业和信息化部信息化和软件服务业司

编写单位（排名不分先后）

中国电子技术标准化研究院
北京蚂蚁云金融信息服务有限公司
中国万向控股有限公司
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
乐视联服信息技术有限公司
万达网络科技有限公司

编写人员

周　平	杜　宇	李　斌	李　奕	李升林	季宙栋
苏小康	余文波	陈家乐	唐晓丹	李仓良	华正皓
卢道和	黄宇翔	高林挥	蔡　栋	赵尊奎	范瑞彬
陈家乐	单　旭	段　玺	任重远	喻学才	梁　然
冯庆磊	姚辉亚	张开翔	陆一帆	汪东艳	金　巍
宋文鹏	胡　玮	韩　梅	李佳秾	李　璐	

目 录

一、概述 …… 1
1.1 背景 …… 1
1.2 编写方法 …… 2
1.3 术语和缩略语 …… 3

二、国内外区块链发展现状 …… 5
2.1 区块链发展演进路径 …… 5
2.1.1 技术来源 …… 6
2.1.2 区块链1.0——数字货币 …… 8
2.1.3 区块链2.0——智能合约 …… 10
2.1.4 区块链类型 …… 11
2.2 区块链发展生态 …… 12
2.2.1 开源社区 …… 12
2.2.2 产业联盟 …… 13
2.2.3 骨干企业 …… 13
2.2.4 初创公司 …… 14
2.2.5 投资机构 …… 14
2.2.6 金融机构 …… 15
2.2.7 监管机构 …… 16
2.3 部分国家和地区对区块链的态度 …… 16
2.3.1 英国政府：区块链及分布式账本技术有着颠覆性潜力 …… 16
2.3.2 美国特拉华州：区块链技术简化企业注册成本 …… 17
2.3.3 俄罗斯央行：研究区块链在金融领域的潜在应用 …… 17
2.3.4 欧洲证券及市场管理局：区块链技术可改进交易后流程 …… 18
2.3.5 新加坡政府：银行应持续关注技术变革 …… 18

目 录

2.3.6 香港特区政府：希望推动金融科技在香港金融服务业的发展 …… 19
2.4 区块链与新一代信息技术 …… 20
2.4.1 区块链与云计算 …… 21
2.4.2 区块链与大数据 …… 21
2.4.3 区块链与物联网 …… 22
2.4.4 区块链与下一代移动通讯网络 …… 22
2.4.5 区块链与加密技术 …… 23
2.4.6 区块链与人工智能 …… 23

三、区块链典型应用场景 …… 25
3.1 区块链应用场景概览 …… 25
3.2 区块链与金融服务 …… 26
3.2.1 行业痛点 …… 26
3.2.2 基于区块链的解决思路 …… 26
3.2.3 应用场景 …… 27
3.3 区块链与供应链管理 …… 28
3.3.1 行业痛点 …… 28
3.3.2 基于区块链的解决思路 …… 29
3.3.3 应用场景 …… 29
3.4 区块链与文化娱乐 …… 30
3.4.1 行业痛点 …… 30
3.4.2 基于区块链的解决思路 …… 30
3.4.3 应用场景 …… 31
3.5 区块链与智能制造 …… 32
3.5.1 行业痛点 …… 32
3.5.2 基于区块链的解决思路 …… 32

目 录

3.5.3 应用场景 …… 33
3.6 区块链与社会公益 …… 34
3.6.1 行业痛点 …… 34
3.6.2 基于区块链的解决思路 …… 34
3.6.3 应用场景 …… 35
3.7 区块链与教育就业 …… 35
3.7.1 行业痛点 …… 36
3.7.2 基于区块链的解决思路 …… 36
3.7.3 应用场景 …… 36
3.8 区块链应用展望 …… 37

四、我国区块链技术发展路线图 …… 39
4.1 区块链通用技术需求 …… 39
4.2 区块链技术架构 …… 39
4.2.1 核心技术组件 …… 40
4.2.2 核心应用组件 …… 41
4.2.3 配套设施 …… 41
4.3 区块链核心关键技术 …… 41
4.3.1 共识机制 …… 41
4.3.2 数据存储 …… 42
4.3.3 网络协议 …… 43
4.3.4 加密算法 …… 44
4.3.5 隐私保护 …… 45
4.3.6 智能合约 …… 45
4.4 区块链治理 …… 46
4.4.1 区块链治理规则 …… 46
4.4.2 区块链治理模式 …… 46

目 录

4.5 区块链安全 …… 47
4.5.1 区块链技术特有的安全特性 …… 48
4.5.2 区块链技术面临的安全挑战与应对策略 …… 48
4.5.3 区块链的安全体系构建 …… 49
4.6 区块链技术发展路线 …… 50
4.6.1 区块链技术发展趋势 …… 50
4.6.2 区块链技术发展路线图 …… 52

五、我国区块链标准化路线图 …… 53
5.1 区块链标准化需求分析 …… 53
5.2 区块链标准体系建议 …… 54
5.3 区块链标准化重点方向 …… 56
5.3.1 基础标准 …… 56
5.3.2 业务和应用标准 …… 57
5.3.3 过程和方法标准 …… 57
5.3.4 可信和互操作标准 …… 59
5.3.5 信息安全标准 …… 60
5.4 区块链标准化实施方案 …… 61
5.5 区块链国际标准化 …… 63
5.5.1 国际标准化进程 …… 63
5.5.2 国际标准化策略 …… 65

六、推动区块链发展的相关建议 …… 67

参考文献 …… 70

一、概述

1.1 背景

区块链是分布式数据存储、点对点传输、共识机制、加密算法等计算机技术在互联网时代的创新应用模式。区块链技术被认为是继大型机、个人电脑、互联网之后计算模式的颠覆式创新，很可能在全球范围引起一场新的技术革新和产业变革。联合国、国际货币基金组织，以及美国、英国、日本等国家对区块链的发展给予高度关注，积极探索推动区块链的应用。目前，区块链的应用已延伸到物联网、智能制造、供应链管理、数字资产交易等多个领域。

近年来，区块链技术和应用在我国引起了多个行业的广泛关注，北京、上海、深圳等城市先后成立了不同形式的联盟，区块链的应用开发实践在以金融科技为代表的领域逐渐展开，同时在媒体的推动下不断掀起讨论热潮。总的来看，在多重力量和因素的催化下，区块链或许已经开启一个快速发展的时期。另外，我们也要清醒地看到，区块链技术是从比特币这一应用中衍生出来的技术，是否成熟可用，需要投入新的技术研发和应用实践来进行证明。因此，区块链的大发展并非万事俱备，而是机遇与风险并存，动力与障碍共同作用，特别是缺乏金融领域以外的成熟应用 ，至今仍是区块链的一个现实不足。更重要的是，近期发生的一系列安全事件，透露出区块链技术仍然面临安全风险和挑战。

为系统研究分析区块链技术和应用的发展趋势，梳理我国推动区块链技术和应用发展的路径，提出区块链技术和应用发展的相关建议，2016年7月，工业和信息化部信息化和软件服务业司印发了《关于组织开展区块链技术和应用发展趋势研究的函》（工信软函[2016]840号），委托中

国电子技术标准化研究院联合蚂蚁金服、万向控股、微众银行、平安科技、乐视金融、万达网络科技等单位开展区块链技术和应用发展趋势研究。为有效贯彻落实工信软函[2016]840号文的要求，推动我国区块链技术和产业发展，我们联合编写了本白皮书，目的是为各级产业主管部门、从业机构提供指导和参考。

1.2 编写方法

一是收集和分析国外最新文献资料。收集了联合国、国际货币基金组织，以及美国、英国、日本等国际政府间组织和主要国家政府发布的区块链相关报告，比特币、以太坊、超级账本等区块链开源技术平台的白皮书。例如联合国的《数字货币和区块链技术在构建社会团结金融中如何扮演角色》（How Can Cryptocurrency and Blockchain Technology Play a Role in Building Social and Solidarity Finance?）、英国政府首席科学顾问报告《分布式账本技术：超越区块链》（Distributed Ledger Technology: Beyond Blockchain）、日本产业经济省的《区块链技术及相关服务的调查报告（2015）》（Survey on Blockchain Technologies and Related Services FY2015 Report）等，累计研究分析了20多项最新的文献资料，系统掌握了国外区块链技术和应用发展最新动向。

二是研究分析国外典型应用案例。累计研究分析了金融服务、供应链管理、文化娱乐等领域的200多个应用案例，包括所采用的底层基础设施、应用架构、服务内容和应用价值等方面。例如全球开发者共同开发和维护的比特币和以太坊、美国区块链创业公司Skuchain的区块链供应链解决方案、美国Blockai公司的数字作品知识产权保护方案，初步掌握了区块链技术在全球的总体应用情况以及存在的问题。

三是系统梳理国内区块链研发和应用实践。重点分析了蚂蚁金服、万向控股、微众银行、平安科技、乐视金融、万达网络科技、钜真金融等

数十家企业在区块链底层技术平台研发、区块链即服务（Blockchain as a Service，简称BaaS）实践和行业应用推广。例如，万向区块链实验室的BaaS平台、微众银行的银行间联合贷款清算项目、蚂蚁金服的社会公益项目、钜真金融的区块链底层架构平台等，全面掌握了区块链技术在国内的研发和应用最新进展以及未来的发展趋势。

四是联合开展研究。共同开展“十问区块链”专题研究，研究分析区块链的关键技术、区块链架构、应用全景等。例如，在“十问区块链”专题研究中涉及了区块链是技术还是模式、区块链安全等问题；在区块链架构方面，提出了3层结构的方案，分析了区块链与新一代信息技术的关系，并初步规划了我国区块链标准体系建设和标准化实施方案。

另外，需要特别说明的是，在编写白皮书的过程中，所采用的数据仅供参考，同时最新数据的截至日期为2016年9月中旬。

1.3 术语和缩略语

本白皮书中涉及的重点术语及其所表达的意义如表1–1所示。

表1–1 术语

术语	定义/解释
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应用模式。
分布式	相对于集中式而言。在白皮书中，分布式是区块链的典型特征之一，对应的英文是Decentralized，完整的表达形式是不依赖于中心服务器（集群）、利用分布的计算机资源进行计算的模式。
金融科技	通过科技让金融服务更高效，通常简称为FinTech。
普惠金融	立足机会平等要求和商业可持续原则，以可负担的成本为有金融服务需求的社会各阶层和群体提供适当、有效的金融服务。
数字货币	货币的数字化，通过数据交易并发挥交易媒介、记账单位及价值存储的功能，但它并不是任何国家和地区的法定货币。

术语	定义/解释
共识机制	区块链系统中实现不同节点之间建立信任、获取权益的数学算法。
智能合约	一种用计算机语言取代法律语言去记录条款的合约。
挖矿	比特币系统中争取记账权从而获得奖励的活动。
分布式账本	一个可以在多个站点、不同地理位置或者多个机构组成的网络中分享的资产数据库。其中，资产可以是货币以及法律定义的、实体的或是电子的资产。

本白皮书中涉及的缩略语如表1–2所示。

表1–2 缩略语

缩略语	原始术语
PoW	工作量证明（Proof of Work）
PoS	权益证明（Proof of Stake）
DPoS	股份授权证明（Delegate Proof of Stake）
PBFT	实用拜占庭容错（Practical Byzantine Fault Tolerance）
P2P	点对点（Peer to Peer）
DAPP	分布式应用（Decentralized Application）
KYC	客户识别（Know Your Customer）
RSA	RSA加密算法（RSA Algorithm）
ECC	椭圆加密算法（Elliptic Curve Cryptography）
BaaS	区块链即服务（Blockchain as a Service）

二、国内外区块链发展现状

2.1 区块链发展演进路径

区块链技术起源于化名为“中本聪”（Satoshi Nakamoto）的学者在2008年发表的奠基性论文《比特币：一种点对点电子现金系统》。狭义来讲，区块链是一种按照时间顺序将数据区块以顺序相连的方式组合成的一种链式数据结构，并以密码学方式保证的不可篡改和不可伪造的分布式账本。广义来讲，区块链技术是利用块链式数据结构来验证与存储数据、利用分布式节点共识算法来生成和更新数据、利用密码学的方式保证数据传输和访问的安全、利用由自动化脚本代码组成的智能合约来编程和操作数据的一种全新的分布式基础架构与计算范式。

目前，区块链技术被很多大型机构称为是彻底改变业务乃至机构运作方式的重大突破性技术。同时，就像云计算、大数据、物联网等新一代信息技术一样，区块链技术并不是单一信息技术，而是依托于现有技术，加以独创性的组合及创新，从而实现以前未实现的功能。

至今为止，区块链技术大致经历了3个发展阶段，如图2–1所示。

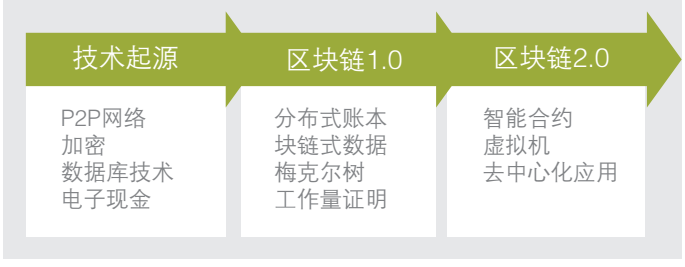


图2–1 区块链的演进路径

2.1.1 技术来源

1、P2P网络技术是区块链系统连接各对等节点的组网技术，学术界将其翻译为对等网络，在多数媒体上则被称为“点对点”或“端对端”网络，是建构在互联网上的一种连接网络。图2–2a) 所示为一种P2P网络模式，图2–2b) 为典型中心化网络模式。

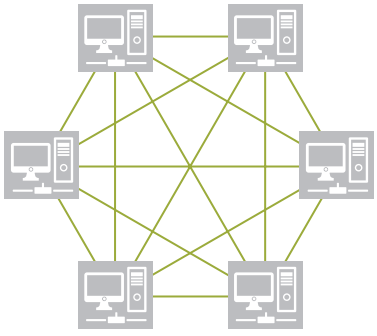


图2–2a) P2P网络模式

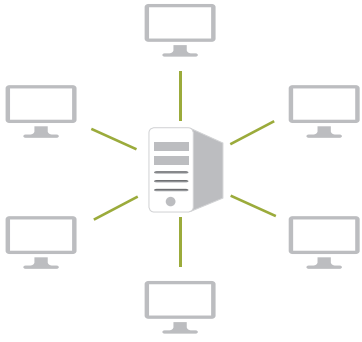


图2–2b) 中心化网络模式

不同于中心化网络模式，P2P网络中各节点的计算机地位平等，每个节点有相同的网络权力，不存在中心化的服务器。所有节点间通过特定的软件协议共享部分计算资源、软件或者信息内容。在比特币出现之前，P2P网络计算技术已被广泛用于开发各种应用，如即时通讯软件、文件共享和下载软件、网络视频播放软件、计算资源共享软件等。P2P网络技术是构成区块链技术架构的核心技术之一。

2、非对称加密算法是指使用公私钥对数据存储和传输进行加密和解密。公钥可公开发布，用于发送方加密要发送的信息，私钥用于接收方解密接收到的加密内容。公私钥对计算时间较长，主要用于加密较少的数据。常用的非对称加密算法有RSA和ECC。非对称加密算法的过程如图2–3所示。区块链正是使用非对称加密的公私钥对来构建节点间信任的。

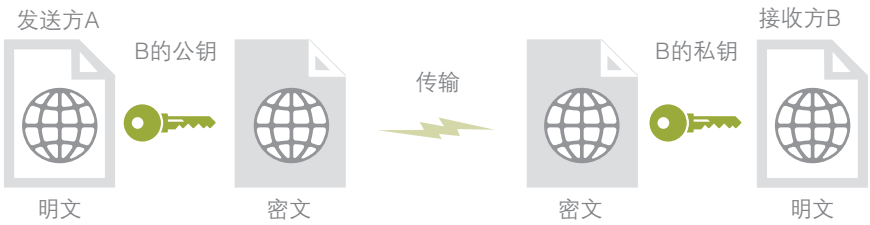


图2–3 非对称加密解密过程

3、数据库技术涉及计算机技术发展的大半历程，是基础性技术，也是软件业的基石。数据库技术脱胎于软件业，将数据储存独立于代码，改变了此前数据处理软件的架构。数据库技术从早期的网状结构、层次结构发展到基于严密关系代数基础的关系型。关系型数据库用简单的二维表格集存储真实世界的对象及其联系，有业界统一的SQL语言，被极为广泛地用于构建各种系统和应用软件。世界互联网产生的海量数据催生了以键值（简称：Key–Value）对为基础的分布式数据库系统。目前，世界上主要的互联网公司根据各自需要研发和构建了NoSQL数据库管理系统。在区块链系统建设方面，传统的关系型数据库和分布式键值数据均适用。

4、数字货币（Digital money） 又被称为电子现金（Ecash）或电子货币（Emoney），视为对现实货币的模拟，涉及用户、商家和处于中心化地位的银行或第三方支付机构。数字货币是电子商务和网上转账的基础。现实中数字货币也指一类免密支付的卡，如公交卡。第一个数字货币方案于1982年被Chaum创造性地提出，致力于解决重复花费问题，使用了盲签名技术，可以完全保护用户隐私。完全匿名的数字货币不能满足政府和金融机构的监管要求，于是匿名可控的概念被学者们提出。匿名可控即在适当条件下可以撤销匿名性且用户无法察觉,也可以是在审计时用户主动撤销匿名性。数字货币的使用过程如图2–4所示。

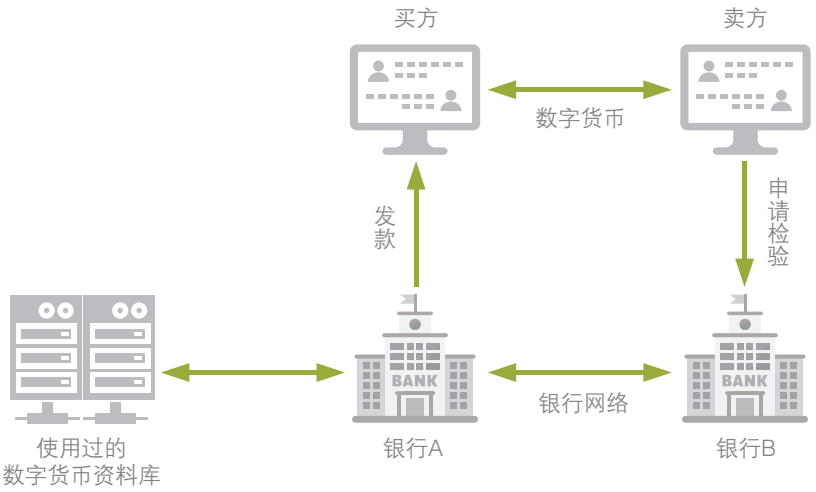


图2-4 数字货币的使用过程

2.1.2 区块链1.0——数字货币

2009年初，比特币网络正式上线运行。作为一种虚拟货币系统，比特币的总量是由网络共识协议限定的，没有任何个人及机构能够随意修改其中的供应量及交易记录。在比特币网络成功运行多年后，部分金融机构开始意识到，支撑比特币运行的底层技术——区块链实际上是一种极其巧妙的分布式共享账本及点对点价值传输技术，对金融乃至各行各业带来的潜在影响甚至可能不亚于复式记账法的发明。

若从其实质分析，区块链就是一种无须中介参与，亦能在互不信任或弱信任的参与者之间维系一套不可篡改的账本记录的技术。区块链1.0的典型特征如下：

1、以区块为单位的链状数据块结构：区块链系统各节点通过一定的共识机制选取具有打包交易权限的区块节点，该节点需要将新区块的前一个区块的哈希值、当前时间戳、一段时间内发生的有效交易及其梅克尔树根值等内容打包成一个区块，向全网广播。由于每一个区块都是与前续区块通过密码学证明的方式链接在一起的，当区块链达到一定的长度后，要

修改某个历史区块中的交易内容就必须将该区块之前的所有区块的交易记录及密码学证明进行重构，有效实现了防篡改。

2、全网共享账本：在典型的区块链网络中，每一个节点都能够存储全网发生的历史交易记录的完整、一致账本，即对个别节点的账本数据的篡改、攻击不会影响全网总账的安全性。此外，由于全网的节点是通过点对点的方式连接起来的，没有单一的中心化服务器，因此不存在单一的攻击入口。同时，全网共享账本这个特性也使得防止双重支付成为现实。

3、非对称加密：典型的区块链网络中，账户体系由非对称加密算法下的公钥和私钥组成，若没有私钥则无法使用对应公钥中的资产。

4、源代码开源：区块链网络中设定的共识机制、规则等都可以通过一致的、开源的源代码进行验证。

以上技术的组合，就是区块链1.0的典型实现，其完整的技术架构如图2–5所示。

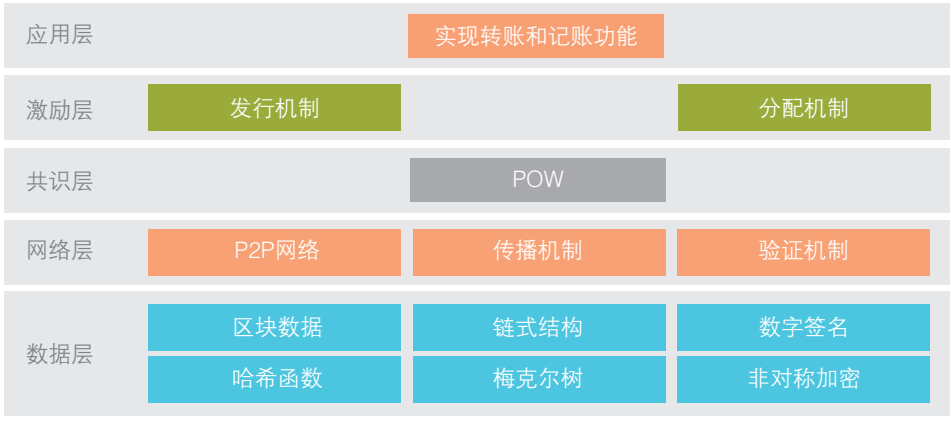


图2–5 区块链1.0技术架构

2.1.3 区块链2.0——智能合约

2014年前后，业界开始认识到区块链技术的重要价值，并将其用于数字货币外的领域，如分布式身份认证、分布式域名系统、分布式自治组织等。这些应用称为分布式应用（DAPP）。用区块链技术架构从零开始构建DAPP非常困难，但不同的DAPP共享了很多相同的组件。区块链2.0试图创建可共用的技术平台并向开发者提供BaaS服务，极大提高了交易速度，大大降低资源消耗，并支持PoW、PoS和DPoS等多种共识算法，使DAPP的开发变得更容易。

区块链2.0的典型特征如下：

1、智能合约：区块链系统中的应用，是已编码的、可自动运行的业务逻辑，通常有自己的代币和专用开发语言。

2、DAPP：包含用户界面的应用，包括但不限于各种加密货币，如以太坊钱包。

3、虚拟机：用于执行智能合约编译后的代码。虚拟机是图灵完备的。

区块链2.0的技术架构如图2–6所示。

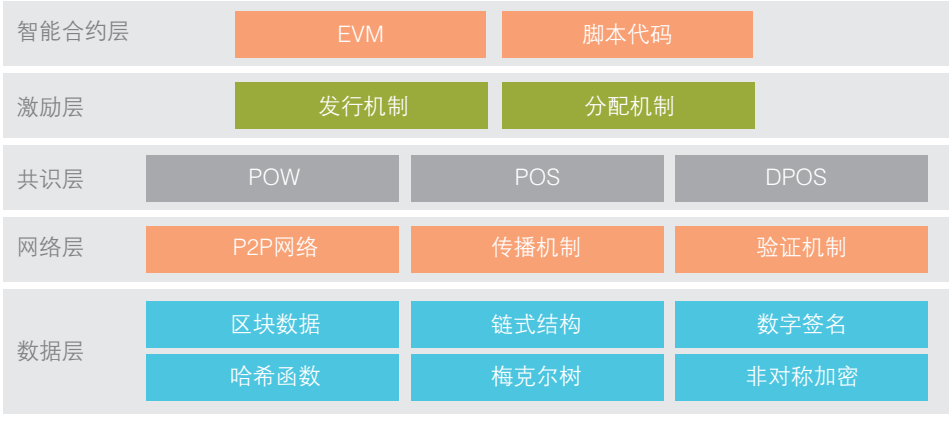


图2–6 区块链2.0技术架构

随着区块链技术和应用的不断深入，以智能合约、DAPP为代表的区块链2.0，将不仅仅只是支撑各种典型行业应用的架构体系。在组织、公司、社会等多种形态的运转背后，可能都能看到区块链的这种分布式协作模式的影子。可以说，区块链必将广泛而深刻地改变人们的生活方式。区块链技术可能应用于人类活动的规模协调，甚至有人大胆预测人类社会可能进入到区块链时代，即区块链3.0。

2.1.4 区块链类型

区块链系统根据应用场景和设计体系的不同，一般分为公有链、联盟链和专有链。其中：

公有链的各个节点可以自由加入和退出网络，并参加链上数据的读写，运行时以扁平的拓扑结构互联互通，网络中不存在任何中心化的服务端节点。

联盟链的各个节点通常有与之对应的实体机构组织，通过授权后才能加入与退出网络。各机构组织组成利益相关的联盟，共同维护区块链的健康运转。

专有链的各个节点的写入权限收归内部控制，而读取权限可视需求有选择性地对外开放。专有链仍然具备区块链多节点运行的通用结构，适用于特定机构的内部数据管理与审计。

上述3种类型的区块链特性如图2–7所示：

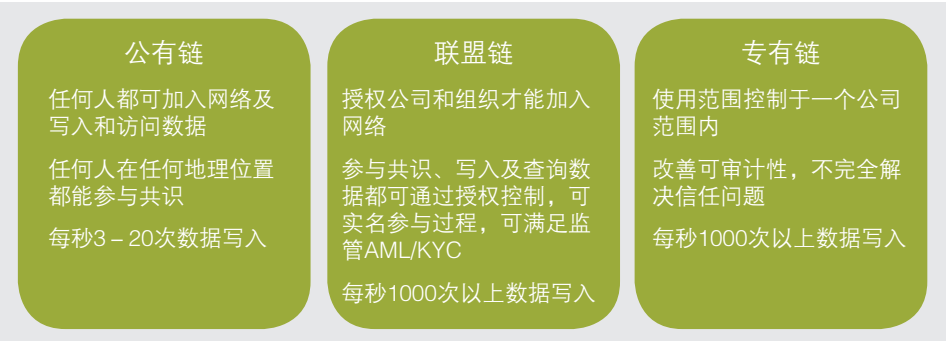


图2–7 区块链的类型及特性

2.2 区块链发展生态

随着区块链技术的演进，越来越多的机构开始重视并参与到区块链技术的探索中来。从最初的以比特币、以太坊等公有链项目开源社区，到各种类型的区块链创业公司、风险投资基金、金融机构、IT企业及监管机构，区块链的发展生态也在逐渐得到发展与丰富。总的来看，区块链完整的发展生态如图2–8所示。

2.2.1 开源社区

不同于很多其他技术，区块链技术并非发源于科研院所，也不是来自于企业，而是发源于开源社区，并在社区中发展壮大，此后逐渐受到金融机构、IT巨头等机构的关注。目前，具有代表性的区块链开源项目有两类：一类是以比特币、以太坊为代表的源自于技术社区的开源项目。这一类项目主要以公有链为主，大部分项目采用PoW作为共识机制。相应的社区组成包括了开发者、矿工、代币持有者及代币交易平台等。另一类则是由传统企业发起的区块链开源项目，最具代表性的便是Linux基金会于

2015年发起的超级账本项目（Hyperledger Project）。

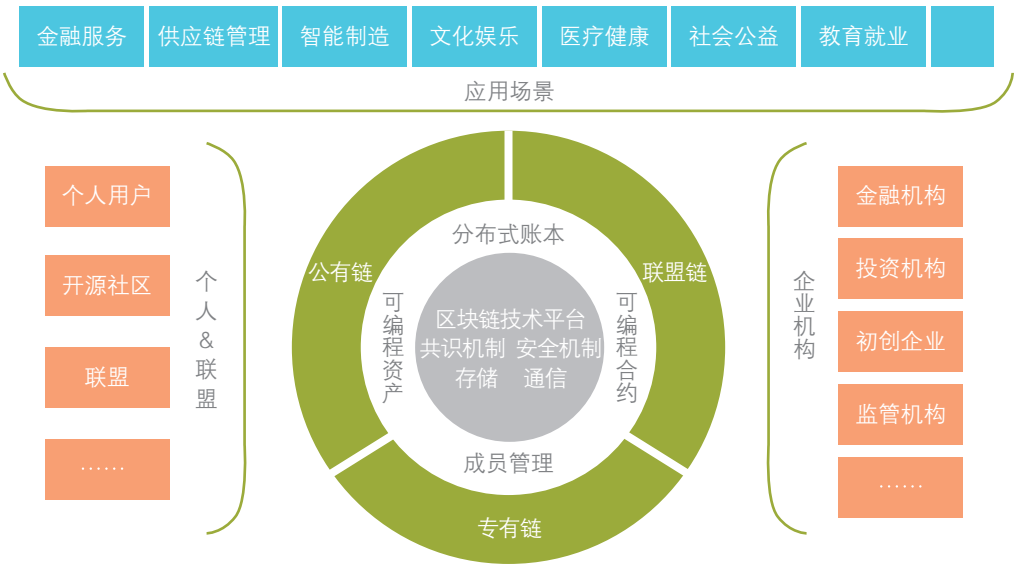


图2-8区块链生态系统

2.2.2 产业联盟

随着区块链技术的发展，其在各行业的应用潜力开始受到参与者的关注。为了协调推进区块链技术和应用发展，国内外先后成立各种类型的区块链产业联盟。例如，美国银行、花旗银行、纽约梅隆银行、德意志银行、法国兴业银行、摩根史丹利等国际大型金融机构参加的R3区块链联盟，万向控股、乐视金融、上海矩真等发起成立的分布式总账基础协议联盟（简称：Chinaledger），微众银行、平安银行、招银网络、恒生电子等共同发起成立的金融区块链合作联盟（简称：金联盟）。

2.2.3 骨干企业

目前，国内外互联网、IT等领域的大量企业开始涉足区块链行业，着

手研发或推出从基础设施到应用案例的一系列解决方案。其中，国内已经初步发展形成了一批区块链骨干企业。例如，万向控股于2015年9月成立了万向区块链实验室，开展区块链产业研究、开源项目赞助等活动，并建立了国内首个区块链云平台——万云（Wancloud）。此外，设立了专注于区块链领域的风险投资基金，已在全球范围内投资超过30个区块链初创公司，累计投资金额超3000万美金。2016年9月，万向集团宣布未来7年还将投资2000亿人民币在杭州建设以新能源汽车为核心产业的“万向创新聚能城”，该项目将全方位大规模应用区块链技术，成为迄今为止全球最大的区块链应用项目。蚂蚁金服在以公益为代表的普惠金融场景中利用区块链解决信任缺失的问题。万达网络科技积极加入国际区块链开源联盟，专注推动国内开源区块链技术发展，研发安全可控的自主区块链平台，同时将区块链技术融入智慧生活、物流网等领域，整合海量实体商业应用场景，实现实体产业的数字化转型升级，已内部试运行区块链征信及区块链资产交易所等应用。微众银行倡议发起金融区块链合作联盟，推出基于腾讯云的联盟链云服务，发布了基于联盟链技术的银行间联合贷款清算平台并已上线试运行。

2.2.4 初创公司

随着区块链技术的发展，区块链领域的初创公司也如雨后春笋般涌现出来。这些初创公司将区块链技术应用到包括金融与非金融在内的多个领域中。其中，金融领域包含支付汇款、智能债券、资产发行与交易后清结算等应用。在非金融领域包括数字存证、物联网、供应链、医疗、公益、文化娱乐等应用。此外，还出现了一些为区块链开发者提供开发平台的技术型公司。

2.2.5 投资机构

资金是推动区块链技术发展不可或缺的力量之一，各类投资机构也是

区块链生态的重要组成部分。由于区块链技术仍处于较为早期的阶段，风险投资机构则是区块链领域内的主要投资力量。另外，以高盛为代表的传统金融机构在区块链投资领域也占据重要地位。随着区块链技术的快速发展，区块链领域的投资金额一直在成倍的增长。自2009年以来，全球已有数十亿美元的资金投入到区块链行业中。2015年以前，主要的投资主要集中在与比特币相关的企业中，比如矿机芯片、交易平台、支付汇款、钱包服务等相关企业。随着区块链技术的发展，越来越多的资金投入在了区块链技术研发及行业应用上，包括交易后清结算、智能合约、供应链、物联网、医疗、身份认证、数据存证、数据分析等。这些项目相对来说还处于比较早期的阶段。

目前为止，区块链领域的投资金额仍处于线性增长阶段。其中，绝大多数的投资都集中在北美，其次是欧洲，最后是亚洲。由于区块链技术发源于欧美，相应的区块链初创公司数量也远高于亚洲。

2.2.6 金融机构

自2015年以来，全球主流金融机构纷纷开始布局区块链，以高盛、摩根大通、瑞银集团为代表的银行业巨头分别成立各自的区块链实验室、发布区块链研究报告或申请区块链专利，并参与投资区块链初创公司。其中，高盛不仅参与投资了区块链创业公司Circle，还在2015年11月提交了一份专利申请，描述了一种可以用于证券结算系统的全新数字货币“SETLcoin”。美国存管信托和结算公司DTCC、Visa、环球同业银行金融电讯协会SWIFT等金融巨头也相继宣布其区块链战略。其中DTCC于2016年1月发布了名为《拥抱颠覆》的白皮书，呼吁全行业开展协作，利用区块链技术改造传统封闭复杂的金融业结构，使其变得现代化、组织化和简单化。除此之外，上海证券交易所、纳斯达克、纽约证券交易所、芝加哥商品交易所等各国证券交易所也对区块链技术进行了深入的探索。其中，纳斯达克在2015年12月30日宣布通过其基于区块链的交易平台Linq

完成了首个证券交易。

2.2.7 监管机构

区块链涉及了包括金融在内的多个行业，各国监管机构在区块链技术的发展与落地中势必会发挥重要作用。当前，各国政府对与以比特币为代表的数字货币政策定义不一。但对于区块链技术，各国政府普遍采取积极支持的态度。英国、新加坡政府相继推出了沙盒计划，以促进区块链领域内的创新。中国互联网金融协会也成立了区块链研究工作组，深入研究区块链技术在金融领域的应用及影响。

2.3 部分国家和地区对区块链的态度

2015年下半年以来，“区块链”这个词开始成为全球各大监管机构、金融机构及商业机构如摩根斯丹利、英国政府、花旗银行等争相讨论的对象。从整体上看，参与讨论的金融机构普遍对区块链技术在改善其中后端流程效率及降低运作成本的可能性上有着较为积极的态度，部分国家政府对推动区块链技术和应用的发展也持积极态度。

2.3.1 中国政府：积极探讨推动区块链技术和应用发展

2016年2月，中国人民银行行长周小川在谈到数字货币相关问题时曾提及，区块链技术是一项可选的技术，并提到人民银行部署了重要力量研究探讨区块链应用技术。他认为，目前区块链存在占用资源过多的问题，不管是计算资源还是存储资源，还应对不了现在的交易规模。2016年9月9日，中国人民银行副行长范一飞在2015年度银行科技发展奖评审领导小组会议中提出，各机构应主动探索系统架构转型，积极研究建立灵活、可延展性强、安全可控的分布式系统架构，同时应加强对区块链等新兴技术的持续关注，不断创新服务和产品，提升普惠金融水平。

2.3.2 英国政府：区块链及分布式账本技术有着颠覆性潜力

英国政府首席科学顾问在其《分布式账本：超越区块链》报告中指出，区块链技术能够为多种形式的服务提供新型的信任机制。该国首席科学顾问认为，分布式账本技术能够为英国的金融市场、供应链、福利管理、土地所有权登记乃至英国国民健康保健制度等领域带来极大的好处。

此外，该国首席科学顾问指出，分布式账本技术凭借其技术特点，具有天然的抵御攻击的优势，认为这种网络中存在多个共享的数据库副本，网络的共识也能防止账本内容未经授权的恶意篡改行为。这样，就能够解决中心化数据管理方案中可能存在的单点失效风险。同时指出，分布式技术有可能改变数据管理体系中对个人信息隐私权的保护方式，让个人有权力决定个人记录的访问权，为不同的机构开放不同的信息访问权限。

政府首席科学顾问认为，英国在金融技术领域有着很强大的先发优势，若借助分布式账本技术并探索其对公共服务及经济体系所能带来的益处，则有利于英国在新一轮的金融技术革命中抢占先机。针对分布式账本技术使用过程中的监管问题，提出了“法律治理”与“技术治理”两大原则，认为新时代的金融体系既需要沿用已有的法律体系监管模式，也需要考虑如何使用技术要素对分布式账本技术系统进行管理。若能妥善处理“法律治理”与“技术治理”这两者之间的关系，分布式账本技术有利于降低金融机构的合规成本、降低系统性风险及提高金融机构运作的效率。

最后，政府首席科学顾问指出，不同的分布式账本体系都有各自的实施方案，这也带来了不同的安全性及隐私问题的差异，各机构在使用具体的分布式账本系统之前，应该从自身的业务流程及安全、隐私保护的角度出发，着重解决相关的问题并寻求最佳的技术解决方案。

2.3.3 美国特拉华州：区块链技术简化企业注册成本

美国的特拉华州因其宽松的企业管理环境和法律体系被誉为是“企业

注册圣地”。目前，在特拉华州注册的企业超过了100万，包括美国过半数的上市企业。美国特拉华州州长Jack Markell表示，区块链技术用于企业注册及股权管理等领域有着很大的潜力，并通过与特拉华州律师协会合作，探索将区块链技术与该州法律体系结合起来，择机开始将特拉华州的企业档案管理记录转移到分布式账本体系的尝试。

特拉华州政府在区块链上的一系列举措及计划，被统称为“特拉华州区块链倡议行动”。2015年成立的智能证券公司Symbiont是该行动的一个参与者，该公司将区块链技术与现有的金融市场基础设施结合起来，用于股东信息登记、股份登记、资本管理等领域，作为特拉华州区块链倡议行动的重要组成部分。Symbiont公司认为这个计划能够简化公司股权管理及股东权益管理等事项，从而让在特拉华州注册的公司受益。

2.3.4 俄罗斯央行：研究区块链在金融领域的潜在应用

2016年上半年，俄罗斯央行发布的一项研究计划表示将对区块链技术在金融领域的应用进行研究，这与其对比特币的态度有着较大的差距。

目前，俄罗斯央行发布的信息显示已成立了一个专门研究前沿科技及金融市场创新技术的工作小组，对分布式账本、区块链技术及多种金融科技领域的新成果展开调查和研究。俄罗斯央行行长Elvira Nabiullina表示，该国央行正在密切关注及监控区块链基础的发展，并对其创新金融领域的可能性表示关注。

2.3.5 欧洲证券及市场管理局：区块链技术可改进交易后流程

欧盟的最高证券监管机构——欧洲证券及市场管理局（ESMA）执行董事Verena Ross称，区块链及分布式账本技术有助于改进交易后流程。该机构认为，区块链可在结算、所有权记录、证券相关服务及抵押品管理等领域带来成本及效率上的改善。

针对区块链技术的应用可能带来的风险问题，ESMA认为需要关注其

安全性。此外，该机构还意识到分布式账本技术与现有的中心化系统，如交易平台，在一段相当长的时期内可能是会共存的，因此也特别关注区块链技术与现有的各种关键金融系统之间的互操作性。另外，ESMA认为，一旦区块链及分布式账本技术能够解决交易量、可扩展性、隐私保护等问题，则会带来降低成本、提高市场效率的好处，并有助于降低中心化系统网络犯罪活动出现的概率。

ESMA对区块链及分布式账本技术的看法，与美国DTCC颇为一致。DTCC指出，当今的金融市场是建立在不同的服务提供商及市场基础设施所组成的庞大网络上的，在这个庞大的网络中，存在着各种互相孤立的数据系统及运作体系，这极大地影响了金融市场效率的进一步提升。DTCC认为，区块链及分布式账本技术有潜力降低金融机构数据管理、风险控制及清算、结算和对账的成本；同时，该机构也认为，分布式账本技术的发展需要引入金融产业参与者的沟通及协调机制，以免各种互不兼容的分布式账本技术标准与体系互相孤立，否则现有金融系统基础设施缺乏互操作性、互通性和孤立的问题也会再次在分布式账本技术体系中出现。

2.3.6 新加坡政府：银行应持续关注技术变革

新加坡总理李显龙表示，银行业正在面临着全新的挑战，而不断进化的技术所推动的新型商业模式将会对银行业原有的商业模式带来冲击，区块链技术就是其中的一个例子。他认为，区块链技术能够应用于全额结算、金融交易记录确认等领域，具有很大的应用潜力，因此新加坡的银行及监管机构必须对这项技术展开深入的研究，巩固新加坡的金融重镇地位。

目前，新加坡金融管理局宣布成立了金融科技和创新组，并针对与区块链及其他金融科技相关的企业推出了“沙盒”试验机制，只要预先在这个体系中进行登记，企业就能在金融科技创新等事项上获得极大的自由度。新加坡是截至目前为止亚洲范围内对区块链技术态度最为积极的国家之一。

2.4 区块链与新一代信息技术

随着新一轮产业革命的到来，云计算、大数据、物联网等新一代信息技术在智能制造、金融、能源、医疗健康等行业中的作用愈发重要。自“十二五”被确立为七大战略性新兴产业之一以来，我国新一代信息技术的发展迅速，逐步成为各行业深化信息技术应用的方向。从国内外发展趋势和区块链技术发展演进路径来看，区块链技术和应用的发展需要云计算、大数据、物联网等新一代信息技术作为基础设施支撑，同时区块链技术和应用发展对推动新一代信息技术产业发展具有重要的促进作用。图2-9说明了区块链与新一代信息技术的关系。

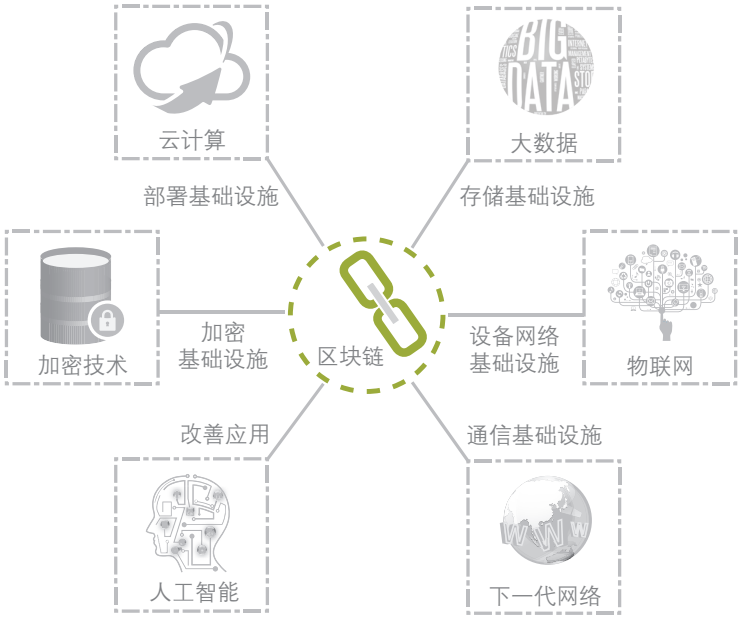


图2-9 区块链与新一代信息技术

2.4.1 区块链与云计算

区块链技术的开发、研究与测试工作涉及多个系统，时间与资金成本等问题将阻碍区块链技术的突破,基于区块链技术的软件开发依然是一个高门槛的工作。云计算服务具有资源弹性伸缩、快速调整、低成本、高可靠性的特质，能够帮助中小企业快速低成本地进行区块链开发部署。两项技术融合，将加速区块链技术成熟，推动区块链从金融业向更多领域拓展。

2015年11月，微软在Azure云平台里面提供BaaS服务，并于2016年8月正式对外开放。开发者可以在上面以最简便、高效的方式创建区块链环境。IBM也在2016年2月宣布推出区块链服务平台，帮助开发人员在IBM云上创建、部署、运行和监控区块链应用程序。

2.4.2 区块链与大数据

区块链是一种不可篡改的、全历史的数据库存储技术，巨大的区块数据集合包含着每一笔交易的全部历史，随着区块链的应用迅速发展，数据规模会越来越大，不同业务场景区块链的数据融合进一步扩大了数据规模和丰富性。区块链提供的是账本的完整性，数据统计分析的能力较弱。大数据具备海量数据存储技术和灵活高效的分析技术，极大提升区块链数据的价值和使用空间。

区块链以其可信任性、安全性和不可篡改性，让更多数据被解放出来，推进数据的海量增长。区块链的可追溯特性使得数据从采集、交易、流通，以及计算分析的每一步记录都可以留存在区块链上，使得数据的质量获得前所未有的强信任背书，也保证了数据分析结果的正确性和数据挖掘的效果。区块链能够进一步规范数据的使用，精细化授权范围。脱敏后的数据交易流通，则有利于突破信息孤岛，建立数据横向流通机制，并基于区块链的价值转移网络，逐步推动形成基于全球化的数据交易场景。

2.4.3 区块链与物联网

物联网作为互联网基础上延伸和扩展的网络，通过应用智能感知、识别技术与普适计算等计算机技术，实现信息交换和通信，同样能满足区块链系统的部署和运营要求。另外，区块链系统网络是典型的P2P网络，具有分布式异构特征，而物联网天然具备分布式特征，网中的每一个设备都能管理自己在交互作用中的角色、行为和规则，对建立区块链系统的共识机制具有重要的支持作用。

根据有关机构预测，2015年全球的物联网设备数量将达到49亿台，2020年将达到250亿台左右。随着物联网中设备数量的增长，如果以传统的中心化网络模式进行管理，将带来巨大的数据中心基础设施建设投入及维护投入。此外，基于中心化的网络模式也会存在安全隐患。区块链的去中心化特性为物联网的自我治理提供了方法，可以帮助物联网中的设备理解彼此，并让物联网中的设备知道不同设备之间的关系，实现对分布式物联网的去中心化控制。

2.4.4 区块链与下一代移动通讯网络

区块链是点对点的分布式系统，节点间的多播通信会消耗大量网络资源。随着区块链体量的逐步扩大，网络资源的消耗会以几何倍数增长，最终会成为区块链的性能瓶颈。

5G网络作为下一代移动通信网络，理论传输速度可达数十Gb每秒，这比4G网络的传输速度快数百倍。对于区块链而言，区块链数据可以达到极速同步，从而减少了不一致数据的产生，提高了共识算法的效率。另外，预计到2020年时，大约有500亿部设备将连接到5G网络，并且将融合到物联网之中。下一代通信网络的发展，将极大提升区块链的性能，扩展区块链的应用范围。

2.4.5 区块链与加密技术

现代信息的应用越来越趋于全球化和全民化,对于信息安全的要求除了防篡改、抗抵赖、可信等基础安全之外，更需要加强隐私保护、身份认证等方面的安全。从某种意义上看，区块链技术是因为现代密码学的发展才产生的，但今天区块链技术所用的密码学主要是二十年前的密码学成果，还存在很多问题需要解决。将区块链技术应用于更多分布式的、多元身份参与的应用场景，现有的加密技术是否满足需求，还需要更多的应用验证，同时更需要深入整合密码学前沿技术，包括目前国际国内在零知识证明、多方保密计算、群签名、基于格的密码体制、全同态密码学等最新前沿技术。

新兴的区块链技术有助于推动信息化沟通模式从多对多沟通发展到物联网沟通模式，密码学需要不断创新才能满足趋于复杂的通信方式的安全需求，从某种程度上说，区块链技术在推动密码体系创新的同时，也给现代密码学带来新的发展契机。同时在区块链治理过程中，身份认证系统是第一要务，数字证书对于区块链技术也是极其重要的，区块链技术的发展对数字证书的发展和应用也有极大的促进作用。

2.4.6 区块链与人工智能

基于区块链的人工智能网络可以设定一致、有效的设备注册、授权及完善的生命周期管理机制，有利于提高人工智能设备的用户体验及安全性。

此外，若各种人工智能设备通过区块链实现互联、互通，则有可能带来一种新型的经济模式，即人类组织与人工智能、人工智能与人工智能之间进行信息的交互甚至是业务的往来，而统一的区块链基础协议则可让不同的人工智能设备之间在互动过程中不断积累学习经验，从而实现人工智能程度的进一步提升。

三、区块链典型应用场景

3.1 区块链应用场景概览

目前，区块链的应用已从单一的数字货币应用，例如比特币，延伸到经济社会的各个领域，其应用的场景如图3–1所示。考虑到各个行业应用的可行性、成熟度和重要性，本白皮书列举了金融服务、供应链管理、文化娱乐、智能制造、社会公益、教育就业等6个行业的应用场景作为代表。另外，需要特别说明的是，除金融服务行业的应用相对成熟外，其他行业的应用还处于探索起步阶段。在后续工作中，我们将结合区块链技术和应用的发展不断丰富完善。

图3–1 区块链应用场景概览

3.2 区块链与金融服务

金融服务是区块链技术的第一个应用领域，不仅如此，由于该技术所拥有的高可靠性、简化流程、交易可追踪、节约成本、减少错误以及改善数据质量等特质，使得其具备重构金融业基础架构的潜力。

3.2.1 行业痛点

在支付领域，金融机构特别是跨境的金融机构间的对账、清算、结算的成本较高，也涉及了很多的手工流程，这不仅导致了用户端和金融机构中后台业务端等产生的支付业务费用高昂，也使得小额支付业务难以开展。

在资产管理领域，股权、债券、票据、收益凭证、仓单等资产由不同的中介机构托管，提高了这类资产的交易成本，也容易带来凭证被伪造等问题。

在证券领域，证券交易生命周期内的一系列流程耗时较长，增加了金融机构中后台的业务成本。

在清算和结算领域，不同金融机构间的基础设施架构、业务流程各不相同，同时涉及很多人工处理的环节，极大地增加了业务成本，也容易出现差错。

在用户身份识别领域，不同金融机构间的用户数据难以实现高效的交互，使得重复认证成本较高，也间接带来了用户身份被某些中介机构泄露的风险。

3.2.2 基于区块链的解决思路

区块链技术具有数据不可篡改和可追溯特性，可以用来构建监管部门所需要的、包含众多手段的监管工具箱，以利于实施精准、及时和更多维度的监管。同时，基于区块链技术能实现点对点的价值转移，通过资产数字化和重构金融基础设施架构，可达成大幅度提升金融资产交易后清、结算流程效率和降低成本的目标，并可在很大程度上解决支付所面

临的现存问题。

3.2.3 应用场景

应用场景1：支付领域

在支付领域，区块链技术的应用有助于降低金融机构间的对账成本及争议解决的成本，从而显著提高支付业务的处理速度及效率，这一点在跨境支付领域的作用尤其明显。另外，区块链技术为支付领域所带来的成本和效率优势，使得金融机构能够更处理以往因成本因素而被视为不现实的小额跨境支付，有助于普惠金融的实现。

应用场景2：资产数字化

各类资产，如股权、债券、票据、收益凭证、仓单等均可被整合进区块链中，成为链上数字资产，使得资产所有者无需通过各种中介机构就能直接发起交易。上述功能可以借助于行业基础设施类机构实现，让其扮演托管者的角色，确保资产的真实性与合规性，并在托管库和分布式账本之间搭建一座桥梁，让分布式账本平台能够安全地访问托管库中的可信任资产。此外，资产发行可根据需要灵活采用保密或公开的方式进行。

应用场景3：智能证券

金融资产的交易是相关各方之间基于一定的规则达成的合约，区块链能用代码充分地表达这些业务逻辑，如固定收益证券、回购协议、各种掉期交易以及银团贷款等，进而实现合约的自动执行，并且保证相关合约只在交易对手方间可见，而对无关第三方保密。基于区块链的智能证券能通过相应机制确保其运行符合特定的法律和监管框架。

应用场景4：清算和结算

区块链技术的核心特质是能以准实时的方式，在无需可信的第三方参与的情况下实现价值转移。金融资产的交易涉及两个重要方面：支付和证券。通过基于区块链技术的法定数字货币或者是某种“结算工具”的创设，与前文所述的链上数字资产对接，即可完成点对点的实时清算与结

算，从而显著降低价值转移的成本，缩短清算、结算时间。在此过程中，交易各方均可获得良好的隐私保护。

应用场景5：客户识别

全世界的金融机构都是受到严格监管的，其中很重要的一条就是金融机构在向客户提供服务时必须履行客户识别（KYC）责任。在传统方式下，KYC是非常耗时的流程，缺少自动验证消费者身份的技术，因此无法高效地开展工作。在传统金融体系中，不同机构间的用户身份信息和交易记录无法实现一致、高效的跟踪，使得监管机构的工作难以落到实处。区块链技术可实现数字化身份信息的安全、可靠管理，在保证客户隐私的前提下提升客户识别的效率并降低成本。

3.3 区块链与供应链管理

供应链是一个由物流、信息流、资金流所共同组成的，并将行业内的供应商、制造商、分销商、零售商、用户串联在一起的复杂结构。而区块链技术作为一种大规模的协作工具，天然地适合运用于供应链管理。

3.3.1 行业痛点

供应链由众多参与主体构成，不同的主体之间必然存在大量的交互和协作，而整个供应链运行过程中产生的各类信息被离散地保存在各个环节各自的系统内，信息流缺乏透明度。这会带来两类严重的问题：一是因为信息不透明、不流畅导致链条上的各参与主体难以准确了解相关事项的状况及存在的问题，从而影响供应链的效率；二是当供应链各主体间出现纠纷时，举证和追责均耗时费力，甚至在有些情况下变得不可行。随着经济全球化的快速推进，企业必须在越来越大的范围内拓展市场，因此，供应链管理中的物流环节往往表现出多区域、长时间跨度的特征，使得假冒伪劣产品这样的难题很难彻底消除。

3.3.2 基于区块链的解决思路

首先，区块链技术能使得数据在交易各方之间公开透明，从而在整个供应链条上形成一个完整且流畅的信息流，这可确保参与各方及时发现供应链系统运行过程中存在的问题，并针对性地找到解决问题的方法，进而提升供应链管理的整体效率。其次，区块链所具有的数据不可篡改和时间戳的存在性证明的特质能很好地运用于解决供应链体系内各参与主体之间的纠纷，实现轻松举证与追责。最后，数据不可篡改与交易可追溯两大特性相结合可根除供应链内产品流转过程中的假冒伪劣问题。

3.3.3 应用场景

应用场景1：物流

在物流过程中，利用数字签名和公私钥加解密机制，可以充分保证信息安全以及寄、收件人的隐私。例如，快递交接需要双方私钥签名，每个快递员或快递点都有自己的私钥，是否签收或交付只需要查一下区块链即可。最终用户没有收到快递就不会有签收记录，快递员无法伪造签名，因此可杜绝快递员通过伪造签名来逃避考核的行为，减少用户投诉，防止货物的冒领误领。而真正的收件人并不需要在快递单上直观展示实名制信息，由于安全隐私有保障，所以更多人愿意接受实名制，从而促进国家物流实名制的落实。另外，利用区块链技术，通过智能合约能够简化物流程序和大幅度提升物流的效率。

应用场景2：溯源防伪

区块链不可篡改、数据可完整追溯以及时间戳功能，可有效解决物品的溯源防伪问题。例如，可以用区块链技术进行钻石身份认证及流转过程记录——为每一颗钻石建立唯一的电子身份，用来记录每一颗钻石的属性并存放至区块链中。同时，无论是这颗钻石的来源出处、流转历史记录、归属还是所在地都会被忠实的记录在链，只要有非法的交易活动或是欺诈

造假的行为，就会被侦测出来。此外，区块链技术也可用于药品、艺术品、收藏品、奢侈品等的溯源防伪。

3.4 区块链与文化娱乐

文化娱乐是文化产业的重要组成部分，包括数字音乐、数字图书、数字视频、数字游戏等。文化娱乐产品涉及生产、复制、流通和传播等主要环节。随着“互联网+”时代的到来，文化娱乐将迎来新的发展机遇。

3.4.1 行业痛点

随着知识经济的兴起，知识产权已成为市场竞争力的核心要素。互联网应是知识产权保护的前沿阵地，但当下的互联网生态里知识产权侵权现象严重，网络著作权官司纠纷频发，侵蚀原创精神、行政保护力度较弱、举证困难、维权成本过高等问题成为内容产业的尖锐痛点。

3.4.2 基于区块链的解决思路

使用区块链技术，可以通过时间戳、哈希算法对作品进行确权，证明一段文字、视频、音频等存在性、真实性和唯一性。一旦在区块链上被确权，作品的后续交易都会被实时记录，文化娱乐业的全生命周期（如图3–2）可追溯、可追踪，这为司法取证提供了一种强大的技术保障和结论性证据。

另外，文化娱乐的起点是创意、核心是内容，利用区块链技术，能将文化娱乐价值链的各个环节进行有效整合、加速流通，缩短价值创造周期。其次，利用区块链技术，可实现数字内容的价值转移，并保证转移过程的可信、可审计和透明。最后，基于区块链的政策监管、行业自律和民间个人等多层次的信任共识与激励机制，同时通过安全验证节点、平行传播节点、交易市场节点、消费终端制造等基础设施建设，不断提升文化娱

乐行业的存储与计算能力，有助于文化娱乐业跨入全社会的数字化生产传播时代。

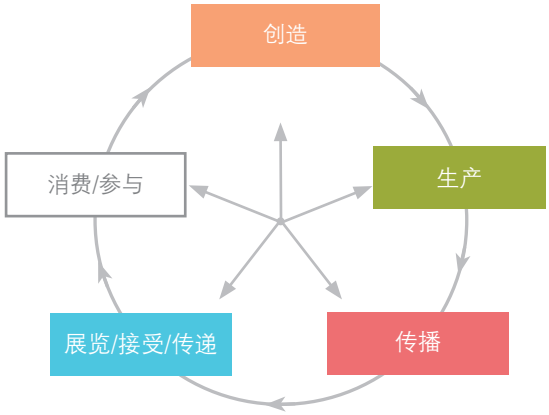


图3–2 文化娱乐周期

3.4.3 应用场景

应用场景1：改变音乐市场格局

音乐行业的市场规模巨大，但在传统模式下，音乐人很难获得合理的版税。利用区块链技术，使音乐整个生产和传播过程中的收费和用途都是透明、真实的，能有效确保音乐人直接从其作品的销售中获益。另外，音乐人跨过出版商和发行商，通过区块链平台自行发布和推广作品，不需要担心侵权问题，还能更好地管理自己的作品。

应用场景2：文化众筹

文化众筹不同于传统意义的民间集资或金融领域的债权和股权融资，基于区块链的文化消费端的众筹服务，具有在独特的泛金融和非金融特色，是围绕知识产权（IP）的新业态。基于区块链特性和虚拟市场规则，使得消费者能够参与IP创作、生产、传播和消费的全流程，而不需要依靠第三方众筹平台的信用背书。另外，利用区块链技术，添加信任的确权节

点，进行IP及其相关权利的交易，以及权益分配等功能，可解决交易不透明、内容不公开等问题。非公开融资也可以通过区块链实现跨地域建立人与人之间的信任关系。

3.5 区块链与智能制造

加快推进智能制造，是实施《中国制造2025》的主攻方向，是落实工业化和信息化深度融合、打造制造强国的战略举措，更是我国制造业紧跟世界发展趋势、实现转型升级的关键所在。当前，我国正在加快实施智能制造工程，积极推动制造企业利用新一代信息技术提升研发设计、生产制造、经营管理等环节的数字化、网络化水平，实现智能化转型，以重塑制造业竞争新优势。

3.5.1 行业痛点

实施智能制造，重点任务就是要实现制造企业内部信息系统的纵向集成，以及不同制造企业间基于价值链和信息流的横向集成，从而实现制造的数字化和网络化。在现实中，由于制造设备和信息系统涉及多个厂家，原本中心化的系统主要采用人工或中央电脑控制的方式，实时获得制造环节中所有信息的难度大。同时，所有的订单需求、产能情况、库存水平变化以及突发故障等信息，都存储在各自独立的系统中，而这些系统的技术架构、通讯协议、数据存储格式等各不相同，严重影响了互联互通的效率，也制约了智能制造在实际生产制造过程中的应用。

3.5.2 基于区块链的解决思路

利用区块链技术，可有效采集和分析在原本孤立的系统中存在的所有传感器和其他部件所产生的信息，并借助大数据分析，评估其实际价值，并对后期制造进行预期分析，能够帮助企业快速有效地建立更为安全的运营机制、更为高效的工作流程和更为优秀的服务。数据透明化使研发审

计、生产制造和流通更为有效，同时也为制造企业降低运营成本、提升良品率和降低制造成本，使企业具有更高的竞争优势。智能制造的价值之一就是重塑价值链，而区块链有助于提高价值链的透明度、灵活性，并能够更敏捷地应对生产、物流、仓储、营销、销售、售后等环节存在的问题。

3.5.3 应用场景

应用场景1：组建和管理工业物联网

组建高效、低成本的工业物联网，是构建智能制造网络基础设施的关键环节。在传统的组网模式下，所有设备之间的通信必须通过中心化的代理通信模式实现，设备之间的连接必须通过网络，极大提高了组网成本，同时可扩展性、可维护性和稳定性差。

区块链技术利用P2P组网技术和混合通信协议，处理异构设备间的通信，将显著降低中心化数据中心的建设和维护成本，同时可以将计算和存储需求分散到组成物联网网络的各个设备中，有效阻止网络中的任何单一节点的失败，而导致整个网络崩溃的情况发生。另外，区块链中分布式账本的防篡改特性，能有效防止工业物联网中任何单节点设备被恶意攻击和控制后带来的信息泄露和恶意操控风险。最后，利用区块链技术组建和管理工业物联网，能及时、动态掌握网络中各种生产制造设备的状态，提高设备的利用率和维护效率，同时能提供精准、高效的供应链金融服务。

应用场景2：生产制造过程的智能化管理

在传统的生产模式下，设备的操作、生产和维护记录是存储在单一、孤立的系统中，一旦出现安全和生产事故，企业、设备厂商和安全生产监管部门难以确保记录的真实性与一致性，也不利于后续事故的防范及设备的改进。

区块链技术能够将制造企业中的传感器、控制模块和系统、通信网络、ERP系统等系统连接起来，并通过统一的账本基础设施，让企业、设备厂商和安全生产监管部门能够长期、持续地监督生产制造的各个环节，

提高生产制造的安全性和可靠性。同时，区块链账本记录的可追溯性和不可篡改性也有利于企业审计工作的开展，便于发现问题、追踪问题、解决问题、优化系统，极大提高生产制造过程的智能化管理水平。

3.6 区块链与社会公益

随着互联网技术的发展，社会公益的规模、场景、辐射范围及影响力得到空前扩大，“互联网+公益”、普众慈善、指尖公益等概念逐步进入公益主流。这些模式不仅解构了传统慈善的捐赠方式，同时推动公众的公益行为向碎片化、小额化、常态化方向发展。同时，各式各样的公益项目借助互联网，实现丰富多彩的传播，使公益的社会影响力被成百倍地放大。

3.6.1 行业痛点

慈善机构要获得持续支持，就必须具有公信力，而信息透明是获得公信力的前提。公众关心捐助的钱款、物资发挥了怎样的作用。既要知道公益机构做了什么，也要知道花了多少，成本有多高。这种公信度的高低和公益的成效决定了公益机构能否获得公众的认同和持久支持。然而，在过去几年里，公益慈善行业时不时地爆发出一些“黑天鹅”事件，极大地打击了民众对公益行业的信任度。公益信息不透明不公开，是社会舆论对公益机构、公益行业的最大质疑。公益透明度影响了公信力，公信力决定了社会公益的发展速度。信息披露所需的人工成本，又是掣肘公益机构提升透明度的重要因素。

3.6.2 基于区块链的解决思路

区块链从本质上来说，是利用分布式技术和共识算法重新构造的一种信任机制，是用共信力助力公信力。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。

为了进一步提升公益透明度，公益组织、支付机构、审计机构等均可加入进来作为区块链系统中的节点，以联盟的形式运转，方便公众和社会监督，让区块链真正成为“信任的机器”，助力社会公益的快速健康发展。

区块链中智能合约技术在社会公益场景也可以发挥作用。在对于一些更加复杂的公益场景，比如定向捐赠、分批捐赠、有条件捐赠等，就非常适合用智能合约来进行管理。使得公益行为完全遵从与预先设定的条件，更加客观、透明、可信，杜绝过程中的猫腻行为。

3.6.3 应用场景

区块链与公益的结合，有很多的应用场景和想象空间，目前已经有真实的应用案例投产上线。2016年7月，支付宝与公益基金会合作，在其爱心捐赠平台上线设立了第一个基于区块链的公益项目，为听障儿童募集资金，帮助他们“重获新声”。在这次的项目中，捐赠人可以看到一项“爱心传递记录”的反馈信息，在进行了必要的隐私保护基础上，展示了自己的捐款从支付平台划拨到基金会账号，以及最终进入受助人指定账号的整个过程。以上所有的信息，都来源于区块链上的数据，既从技术上保障了公益数据的真实性，又能帮助公益项目节省信息披露成本，充分体现出了区块链公益的价值。

3.7 区块链与教育就业

教育就业作为社会文化传授、传播的窗口，需要实现学生、教育机构以及用人就业单位之间的无缝衔接，以提高教育就业机构的运行效率和透

明度。区块链系统的透明化、数据不可篡改等特征，完全适用于学生征信管理、升学就业、学术、资质证明、产学合作等方面，对教育就业的健康发展具有重要的价值。

3.7.1 行业痛点

学生信用体系不完整、未建立历史数据信息链、数据维度有限，导致政府、企业无法获得完整有效信息，这直接导致学生无法便捷、公平地享受应有的服务。学历造假、论文造假、求职简历造假，用人单位、院校缺乏验证手段，蒙受信息不对称产生的损失，降低了学校与企业间、院校与院校间的信任。另外，针对一些学术性实验、跨校组织的公开课以及多媒体教学资源，在网络上往往存在版权纠纷与学术纠纷，对学者以及研究人员缺乏相应的知识产权保护，影响了高等学府对学术研究的积极性。

3.7.2 基于区块链的解决思路

利用区块链技术对现存运行方案不足之处进行优化，能有效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。利用分布式账本记录跨地域、跨院校的学生信息，方便追踪学生在校园时期所有正面以及负面的行为记录，能帮助有良好记录的学生获得更多的激励措施，并构建起一个良性的信用生态。

利用区块链技术，可为学术成果提供不可篡改的数字化证明，为学术纠纷提供了权威的举证凭据，降低纠纷事件消耗的人力与时间。同时，这种数字化证明可以与已有的应用无缝整合，为每一个文字、图片、音频、视频加盖唯一的时间戳身份证明，交叉配合生物识别技术，从根本上保障了数据的完整性、一致性，保护了知识产权。

3.7.3 应用场景

应用场景1：教育存证

在教育存证场景上，基于区块链的学生信用平台可创建含有关基本

信息的数字文件，然后使用用户的私钥对证书的内容进行签名，再对证书本身附加签名。依赖于创建的哈希值，可以验证证书内容是否被篡改。最后，再用私钥在区块链上创建一条数字记录，保证用户信息和证书内容的一致性。教育机构利用自己的私钥签署一份具有完整信息记录的数字证书，将其哈希值存储在区块链中，在每一次发放和查询时，都会由智能合约触发相应的多重签名校验，确保不会被恶意查询，交易输出将数字证书分配给需求方，如学生或者用人单位。

应用场景2：产学合作

产学合作是教育机构与用人企业之间多赢的机制，现在教育存在的问题之一就是封闭办学，即学生的技能信息、知识体系未与用人企业的技能需求、市场趋势保持信息对称。通过引入区块链技术，实现学生技能与社会用人需求无缝衔接，可精确评估人才录用、岗位安排的科学性和合理性，能有效促进学校和企业之间的合作。

3.8 区块链应用展望

尽管区块链技术还存在可扩展性、隐私和安全、开源项目不够成熟等问题，但是已有的应用充分证明了区块链的价值。未来一段时间内，随着区块链技术不断成熟，其应用将带来以下几个方面的价值：

一是推动新一代信息技术产业的发展。随着区块链技术应用的不断深入，将为云计算、大数据、物联网、人工智能等新一代信息技术的发展创造新的机遇。例如，随着万向、微众等重点企业不断推动BaaS平台的深入应用，必将带动云计算和大数据的发展。这样的机遇将有利于信息技术的升级换代，也将有助于推动信息产业的跨越式发展。

二是为经济社会转型升级提供技术支撑。随着区块链技术广泛应用于金融服务、供应链管理、文化娱乐、智能制造、社会公益以及教育就业等经济社会各领域，必将优化各行业的业务流程、降低运营成本、提升协同

效率，进而为经济社会转型升级提供系统化的支撑。例如，随着区块链技术在版权交易和保护方面应用的不断成熟，将对文化娱乐行业的转型发展起到积极的推动作用。

三是培育新的创业创新机会。国内外已有的应用实践证明，区块链技术作为一种大规模协作的工具，能推动不同经济体内交易的广度和深度迈上一个新的台阶，并能有效降低交易成本。例如，万向将结合“创新聚能城”建设，构建区块链的创业创新平台，既为个人和中小企业创业创新提供平台支撑，又为将来应用区块链技术奠定了基础。可以预见的未来是：随着区块链技术的广泛运用，新的商业模式会大量涌现，为创业创新创造新的机遇。

四是为社会管理和治理水平的提升提供技术手段。随着区块链技术在公共管理、社会保障、知识产权管理和保护、土地所有权管理等领域的应用不断成熟和深入，将有效提升公众参与度，降低社会运营成本，提高社会管理的质量和效率，对社会管理和治理水平的提升具有重要的促进作用。例如，蚂蚁金服将区块链运用于公益捐款，为全社会提升公益活动的透明度和信任度树立了榜样，也为区块链技术用于提升社会管理和治理水平提供了实践参考。

四、我国区块链技术发展路线图

4.1 区块链通用技术需求

通过对第三章总结归纳的应用场景进行系统分析，提炼出针对区块链应用的技术需求，除分布式系统、密码学算法、成员管理等通用技术外，还包括以下技术需求：

1、模块化与插件化：为了提高区块链应用的研发效率、可维护性和可移植性，区块链系统的核心功能应实现模块化、可配置和可扩展，以便捷地构建上层应用。

2、高性能：突破现有区块链技术的性能瓶颈，提升区块链系统的吞吐量，以满足主流交易网络高并发的性能要求。

3、数据一致性：采用科学合理的数据算法，降低数据同步延迟，保证数据的一致性，避免造成数据混乱和失准，并减少意外分叉带来的风险。

4、互操作：实现不同区块链间的互操作，需要采用有效的通信协议、统一的API和区块数据格式，以及高效的连接机制。

5、经济合理：技术选型时，在满足需求的前提下，一般尽可能降低技术复杂度，规避高能耗的技术方案。

6、安全和隐私：区块链技术的普及应用需要保障数据存储、数据传输和数据应用等多个方面的安全和隐私保护。

7、安全可靠：积极贯彻落实国家网络安全和信息化战略部署，优先采用安全可靠的软硬件产品。

4.2 区块链技术架构

通过研究分析现有的区块链系统的技术方案和需求，提出典型的区块

链技术架构，如图4–1所示。

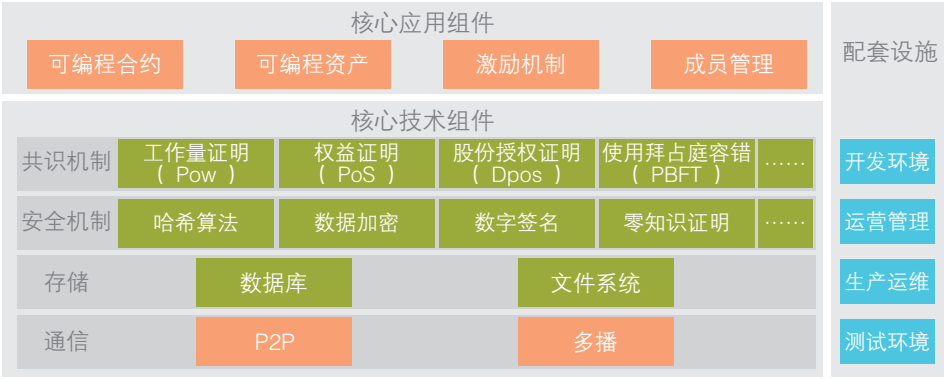


图4–1 区块链技术架构

4.2.1 核心技术组件

核心技术组件包括区块链系统所依赖的基础组件、协议和算法，进一步细分为通信、存储、安全机制、共识机制等4层结构。

1、通信：区块链通常采用P2P技术来组织各个网络节点，每个节点通过多播实现路由、新节点识别和数据传播等功能。

2、存储：区块链数据在运行期以块链式数据结构存储在内存中，最终会持久化存储到数据库中。对于较大的文件，也可存储在链外的文件系统里，同时将摘要（数字指纹）保存到链上用以自证。

3、安全机制：区块链系统通过多种密码学原理进行数据加密及隐私保护。对于公有链或其他涉及到金融应用的区块链系统而言，高强度高可靠的安全算法是基本要求，需要达到国密级别，同时在效率上需要具备一定的优势。

4、共识机制：是区块链系统中各个节点达成一致的策略和方法，应根据系统类型及应用场景的不同灵活选取。

4.2.2 核心应用组件

核心应用组件在核心技术组件之上，提供了针对区块链特有应用场景的功能，允许通过使用编程的方式发行数字资产，也可以通过配套的脚本语言编写智能合约，灵活操作链上资产。通过激励机制维系区块链系统安全稳定运行。对于联盟链和专有链，还需要有配套的成员管理功能。

4.2.3 配套设施

区块链作为典型的分布式系统，在研发阶段需要具备与之配套的开发测试工具和环境。在生产阶段，需要建立相应的运维体系和运营管理功能。

在部署层面，区块链系统可以部署于单台服务器上，以单台服务器作为区块链网络中的一个节点加入。也可部署于多台服务器上，以服务器集群为单位作为区块链网络中的一个节点加入。后者可以提升节点的稳定性和吞吐量，更适用于那些对节点可用性有较高要求的共识机制。

4.3 区块链核心关键技术

4.3.1 共识机制

常用的共识机制主要有PoW、PoS、DPoS、Paxos、PBFT等。另外，基于区块链技术的不同应用场景，以及各种共识机制的特性，本白皮书建议按照以下维度来评价各种共识机制的技术水平：

- 合规监管：是否支持超级权限节点对全网节点、数据进行监管。
- 性能效率：交易达成共识被确认的效率。
- 资源消耗：共识过程中耗费的CPU、网络输入输出、存储等计算机资源。
- 容错性：防攻击、防欺诈的能力。

1、PoW：依赖机器进行数学运算来获取记账权，资源消耗相比其他共识机制高、可监管性弱，同时每次达成共识需要全网共同参与运算，性能效率比较低，容错性方面允许全网50%节点出错。

2、PoS：主要思想是节点记账权的获得难度与节点持有的权益成反比，相对于PoW，一定程度减少了数学运算带来的资源消耗，性能也得到了相应的提升，但依然是基于哈希运算竞争获取记账权的方式，可监管性弱。该共识机制容错性和PoW相同。

3、DPoS：与PoS的主要区别在于节点选举若干代理人，由代理人验证和记账。其合规监管、性能、资源消耗和容错性与PoS相似。

4、Paxos：是一种基于选举领导者的共识机制，领导者节点拥有绝对权限，并允许强监管节点参与，性能高，资源消耗低。所有节点一般有线下准入机制，但选举过程中不允许有作恶节点，不具备容错性。

5、PBFT：与Paxos类似，也是一种采用许可投票、少数服从多数来选举领导者进行记账的共识机制，但该共识机制允许拜占庭容错。该共识机制允许强监管节点参与，具备权限分级能力，性能更高，耗能更低，该算法每轮记账都会由全网节点共同选举领导者，允许33%的节点作恶，容错性为33%。

4.3.2 数据存储

1、数据结构

在区块链技术中，数据以区块的方式永久储存。区块按时间顺序逐个先后生成并连接成链，每一个区块记录了创建期间发生的所有交易信息。区块的数据结构一般分为区块头（header）和区块体（body），如图4–2所示。其中，区块头用于链接到前一个区块并且通过时间戳特性保证历史数据的完整性；区块体则包含了经过验证的、区块创建过程中产生的所有交易信息。

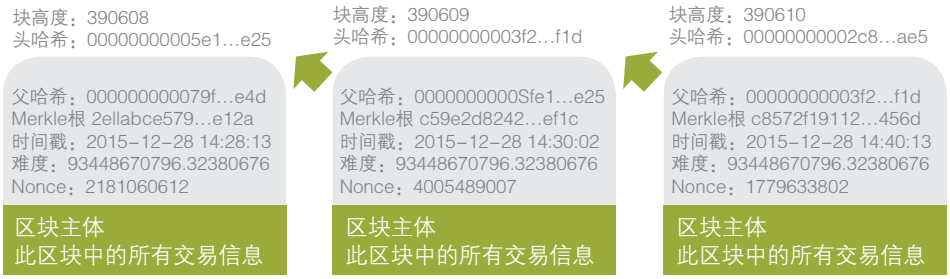


图4-2 区块链数据结构

2、数据库

按照数据库的数据结构组织形式来看，一般分为Key-Value型和关系型两种。其中，Key-Value型数据库的数据结构组织形式比较简单，读写性能很高，能支持海量并发读写请求，而且可扩展性强，操作接口简单，支持一些基本的读、写、修改、删除等功能，但不支持复杂的SQL功能和事务性。关系型数据库采用关系模型来组织数据，支持各种SQL功能，功能性强，支持事务性，读写性能一般，可扩展性弱。

按照数据库的部署形式来看，一般分为单机型和分布式两种。其中，单机型数据库保证强一致性和较好的可用性。分布式数据库在物理部署上遵循了分布式架构，能提供高并发的读写性能和容错，有很强的可用性和分区容错性，但由于需要进行数据同步，分布式架构的数据一致性较弱，只能保证最终一致性。

4.3.3 网络协议

区块链网络协议一般采用P2P协议，确保同一网络中的每台计算机彼此对等，各个节点共同提供网络服务，不存在任何“特殊”节点。不同的区块链系统会根据需要制定独自的P2P网络协议，比如比特币有比特币网络协议，以太坊也有自己的网络协议。

4.3.4 加密算法

1、散列（哈希）算法

散列算法也叫数据摘要或者哈希算法，其原理是将一段信息转换成一个固定长度并具备以下特点的字符串：

（1）如果某两段信息是相同的，那么字符也是相同的。

（2）即使两段信息十分相似，但只要是不同的，那么字符串将会十分杂乱随机并且两个字符串之间完全没有关联。

本质上，散列算法的目的不是为了“加密”而是为了抽取“数据特征”，也可以把给定数据的散列值理解为该数据的“指纹信息”。典型的散列算法有MD5、SHA1/SHA2和SM3，表4–1对比了这些算法的特点。

表4–1 典型散列算法的特点

加密算法	安全性	运算速度	输出大小（位）
MD5	低	快	128
SHA1	中	中	160
SHA256	高	比SHA1略低	256
SM3	高	比SHA1略低	256

总体上看，SHA256和SM3这两种算法效率和安全性大致相当，目前区块链主要使用SHA256，国内某些特定业务场景使用国密SM3，亦是比较符合国家安全和监管的选择。但由于不同业务场景的安全性标准有别，未来不排除还需要探索更优算法的可能性。

2、非对称加密算法

非对称加密算法由对应的一对唯一性密钥（即公开密钥和私有密钥）组成的加密方法。任何获悉用户公钥的人都可用用户的公钥对信息进行加密与用户实现安全信息交互。由于公钥与私钥之间存在的依存关系，只有用户本身才能解密该信息，任何未受授权用户甚至信息的发送者都无法将

此信息解密。

在近代公钥密码系统的研究中，其安全性都是基于难解的可计算问题的，常用的非对称加密算法特点及其比较如表4–2和表4–3所示。

表4–2 非对称加密算法的特点

保密级别	RSA密钥长度	ECC/SM2密钥长度
80	1024	160
112	2048	224

表4–3 RSA、ECC/SM2总体比较

加密算法	成熟度	安全性	运算速度	资源消耗
RSA	高	低	慢	高
ECC	高	高	中	中
SM2	高	高	中	中

4.3.5 隐私保护

目前区块链上传输和存储的数据都是公开可见的，仅通过“伪匿名”的方式对交易双方进行一定的隐私保护。对于某些涉及大量的商业机密和利益的业务场景来说，数据的暴露不符合业务规则和监管要求。目前，业界普遍认为零知识证明、环签名和同态加密等技术比较有希望解决区块链的隐私问题。

4.3.6 智能合约

智能合约可视作一段部署在区块链上可自动运行的程序，其涵盖的范围包括编程语言、编译器、虚拟机、事件、状态机、容错机制等。

虚拟机是区块链中智能合约的运行环境。虚拟机不仅被沙箱封装起来，事实上它被完全隔离。也就是说运行在虚拟机内部的代码不能接触到网络、文件系统或者其他进程。甚至智能合约之间也只能进行有限的调用。

智能合约本质上是一段程序，存在出错的可能性，甚至会引发严重问题或连锁反应。需要做好充分的容错机制，通过系统化的手段，结合运行环境隔离，确保合约在有限时间内按预期执行。

4.4 区块链治理

4.4.1 区块链治理规则

区块链的治理规则总体由区块链参与者设定的规则组成，规则本身又分为两大层面：一是技术层面的治理规则，由软件、协议、程序、算法、配套设施等技术要素构成。二是技术外部的、监管法规层面的治理规则，由法规框架、条文、行业政策等组成。兼顾两者，才更有利于保护参与者乃至全社会的广泛利益，以及推进在区块链技术之上的商业应用场景的落地，最终构建由监管机构、商业机构、消费者等共同参与的完整商业体系。

4.4.2 区块链治理模式

有效的治理规则是区块链关键技术得以成功实施的关键，而在不同的区块链部署结构（公有链、专有链、联盟链）下，其治理模式也有较明显的差异。

1、开源社区运行模式

公有链的第一个成功应用——比特币，其核心代码正是用开源社区的方式维护代码的。除此之外，在技术平台，分布式账本，公证鉴证，物流跟踪，以及其他各种应用都出现了不少开源项目，如定位为提供区块链基础技术平台、支持智能合约的以太坊，Linux基金会开源项目Hyperledger等。开源体系下，大量的技术项目不断得到孵化和成长，优秀项目逐渐成为行业标准。

2、技术服务提供商模式

随着区块链技术的进步和应用的发展，出现了大量构建不同业务领

域的区块链的需求，不少技术实力较强的企业因此进入区块链技术服务提供商领域。这些企业专注在技术领域，研究区块链技术的底层架构、业务构建方式、安全风险控制等，以提供成熟可用的区块链技术解决方案。国外的IBM、微软都是类似的模式。例如，2015年微软与ConsenSys合作建立了Ethereum区块链技术服务，并将其作为微软Azure服务的一部分（EBaaS），为企业客户、合作伙伴和开发人员提供分布式总账技术试验。技术服务商一般还会申请自己的专利，除了提供软硬件系统、人力外包、基础服务之外，也可以通过出让、授权专利获得利润。

3、联盟模式

多家有共同商业或技术进步诉求的企业机构联合在一起，在互惠互利、共同贡献的前提下共同推动区块链领域的商业和技术进展，可以称为联盟模式。联盟模式有一定的准入标准，需要审核机构身份、资质、评估投入程度，缴纳会费，有共同的章程，有合法组织形式，共享技术研究成果，一起构建商业模式。对大多数行业及大型商业机构而言，是比较切实可行的区块链发展运作模式。国外著名的区块链联盟中，R3联盟研究的是区块链在金融细分领域的应用，Hyperledger则是更偏技术探索的区块链联盟。国内的ChinaLedger和金链盟都是首先关注区块链在金融领域的应用，目前同处于底层技术平台构建与关键需求提取阶段。

4.5 区块链安全

区块链系统面临的风险不仅来自外部实体的攻击，也可能有来自内部参与者的攻击，以及组件的失效，如软件故障。因此在实施之前，需要制定风险模型，认清特殊的安全需求，以确保对风险和应对方案的准确把握。

4.5.1 区块链技术特有的安全特性

1、写入数据的安全性

在共识机制的作用下，只有当全网大部分节点（或多个关键节点）都同时认为这个记录正确时，记录的真实性才能得到全网认可，记录数据才允许被写入区块中。

2、读取数据的安全性

区块链没有固有的信息读取安全限制，但可以在一定程度上控制信息读取，比如把区块链上某些元素加密，之后把密钥交给相关参与者。同时，复杂的共识协议确保系统中的任何人看到的账本都是一样的，这是防止双重支付的重要手段。

3、分布式拒绝服务（DDOS）攻击抵抗

区块链的分布式架构赋予其点对点、多冗余特性，不存在单点失效的问题，因此其应对拒绝服务攻击的方式比中心化系统要灵活得多。即使一个节点失效，其他节点不受影响，与失效节点连接的用户无法连入系统，除非有支持他们连入其他节点的机制。

4.5.2 区块链技术面临的安全挑战与应对策略

1、网络公开不设防

对公有链网络而言，所有数据都在公网上传输，所有加入网络的节点可以无障碍地连接其他节点和接受其他节点的连接，在网络层没有做身份验证以及其他防护。针对该类风险的应对策略是要求更高的私密性并谨慎控制网络连接。对安全性较高的行业，如金融行业，宜采用专线接入区块链网络，对接入的连接进行身份验证，排除未经授权的节点接入以免数据泄漏，并通过协议栈级别的防火墙安全防护，防止网络攻击。

2、隐私

公有链上交易数据全网可见，公众可以跟踪这些交易，任何人可以通

过观察区块链得出关于某事的结论，不利于个人或机构的合法隐私保护。针对该类风险的应对策略是：第一，由认证机构代理用户在区块链上进行交易，用户资料和个人行为不进入区块链。第二，不采用全网广播方式，而是将交易数据的传输限制在正在进行相关交易的节点之间。第三，对用户数据的访问采用权限控制，持有密钥的访问者才能解密和访问数据。第四，采用例如“零知识证明”等隐私保护算法，规避隐私暴露。

3、算力

使用工作量证明型的区块链解决方案，都面临51%算力攻击问题。随着算力的逐渐集中，客观上确实存在有掌握超过50%算力的组织出现的可能，在不经改进的情况下，不排除逐渐演变成弱肉强食的丛林法则。针对该类风险的应对策略是采用算法和现实约束相结合的方式，例如用资产抵押、法律和监管手段等进行联合管控。

4.5.3 区块链的安全体系构建

针对现有区块链技术的安全特性和缺点，需要围绕物理、数据、应用系统、加密、风控等方面构建安全体系，整体提升区块链系统的安全性能。

1、物理安全

运行区块链系统的网络和主机应处于受保护的环境，其保护措施根据具体业务的监管要求不同，可采用不限于VPN专网、防火墙、物理隔离等方法，对物理网络和主机进行保护。

2、数据安全

区块链的节点和节点之间的数据交换，原则上不应明文传输，例如可采用非对称加密协商密钥，用对称加密算法进行数据的加密和解密。数据提供方也应严格评估数据的敏感程度、安全级别，决定数据是否发送到区块链，是否进行数据脱敏，并采用严格的访问权限控制措施。

3、应用系统安全

应用系统的安全需要从身份认证、权限体系、交易规则、防欺诈策

略等方面着手，参与应用运行的相关人员、交易节点、交易数据应事前受控、事后可审计。以金融区块链为例，可采用容错能力更强、抗欺诈性和性能更高的共识算法，避免部分节点联合造假。

4、密钥安全

对区块链节点之间的通信数据加密，以及对区块链节点上存储数据加密的密钥，不应明文存在同一个节点上，应通过加密机将私钥妥善保存。在密钥遗失或泄漏时，系统可识别原密钥的相关记录，如帐号控制、通信加密、数据存储加密等，并实施响应措施使原密钥失效。密钥还应进行严格的生命周期管理，不应为永久有效，到达一定的时间周期后需进行更换。

5、风控机制

对系统的网络层、主机操作、应用系统的数据访问、交易频度等维度，应有周密的检测措施，对任何可疑的操作，应进行告警、记录、核查，如发现非法操作，应进行损失评估，在技术和业务层面进行补救，加固安全措施，并追查非法操作的来源，杜绝再次攻击。

4.6 区块链技术发展路线

4.6.1 区块链技术发展趋势

1、核心关键技术发展趋势

从区块链现阶段的技术和应用来看，其核心是分布式数据存储、点对点传输、共识机制、加密算法等已有计算机技术。随着区块链应用的不断深入，对这些核心技术也将不断提出新的和更高的要求。在共识机制、安全算法、隐私保护等相关技术领域的研究成果会对区块链技术和应用的跨越式发展起到重要作用，对这些技术的持续创新和突破将非常关键。

（1）共识机制发展趋势

公有链方面，目前常用的共识机制存在性能低、能耗高的缺点。“侧

链”技术也只能在某些特定条件下解决部分问题。联盟链目前的主流共识机制大多基于PBFT及其变种，虽然加入权限控制能获得性能的大幅提升，但是同时也牺牲了一部分共识的效率、约束、容错率等方面的性能。可以预见，针对一些典型场景的、具有普适性的、更优的共识算法及决策，将会不断出现。

（2）安全算法方向发展趋势

安全性对于以金融级应用系统为代表的系统中尤显重要。一方面，目前采用的大多数传统的安全类算法，存在潜在的“后门”风险，需要逐步替换成更加安全的国密算法，算法的强度也需要不断升级；另一方面，还要防止一些新技术，如量子计算，对传统安全算法的冲击甚至颠覆。

（3）隐私保护发展趋势

目前，区块链相关的隐私保护环节还比较薄弱。尤其是对敏感数据需要平衡隐私保护和合规监管。信息隐私保护技术，如零知识证明、同态加密等，也是后续发展的一个重要方向。

以上核心技术偏计算机底层技术，其发展需要相当大的人员和时间投入，将是一个不断递进的过程。相关企业、科研机构、高等院校等在这些领域的研究成果和相互间的协作贯通对区块链技术发展十分重要。

2、通用开发平台发展趋势

目前，已有众多的IT企业、咨询公司、社区及技术联盟已投入区块链的应用研发，建立通用开发平台并不断完善，对整个区块链技术应用具有很大推动作用。

类似于云计算的IaaS（基础设施即服务）、PaaS（平台即服务），由基础设施支撑层、区块链核心组件服务层，以及相应的开发测试套件组成的区块链通用开发平台，能够完整地提供一站式、低成本搭建和部署区块链应用的技术服务。目前已有部分这样的平台出现，随着区块链应用的迅速发展和各相关参与者的大力投入，其服务覆盖度、研发便利度、运维智

能度，以及高稳定性、大容量、低成本，均是可以预见的发展方向。

4.6.2 区块链技术发展路线图

为促进我国区块链技术的发展，为区块链技术创新活动提供方向，推进区块链核心技术的研发和应用，通过对区块链技术的成熟程度、应用需求和发展趋势的综合分析，提出区块链的技术发展路线，建议划分为4个阶段：需求分析和技术体系研究、关键技术方案选型和平台建设、技术开源与优化、应用试点，如表4–5所示。

表4–5 区块链技术发展路线

阶段	工作重点	主要任务
需求分析和技术体系研究	广泛收集需求，充分考虑可行性高的核心技术及其可能的扩展或改变，需要将区块链系统的开发经验与对传统业务模式的理解这两者相结合。	1.研究典型应用场景需求及用例。 2.研究提出通用的区块链技术架构。 3.攻关解决区块链的核心关键技术。 4.完善区块链技术的治理方案与安全机制。 5.形成安全可靠的区块链技术和产品体系。
关键技术方案选型和平台建设	对目标系统和底层技术平台需形成完整、准确、清晰、具体的要求，充分进行可行性验证，确保多个参与者形成一致认可。	1.对区块链各类关键技术的适用性与成熟性进行评估。 2.进行技术方案选型与可行性验证。 3.形成区块链技术解决方案。 4.构建满足共性需求的区块链底层技术平台。
技术开源与优化	通过开源社区促进区块链生态的形成与完善，增强企业间的技术交流和合作，应对区块链技术的快速升级换代。	1.推动底层技术平台开放共享。 2.推动技术解决方案的代码开源。 3.建立开源社区，协作优化底层技术平台和技术解决方案。
应用试点	促进技术与平台充分接受市场的检验，推动商用级、企业级或金融级的应用场景诞生，最终实现促进产业变革、切实为实体经济服务的目标。	1.推进典型应用场景在区块链开源底层技术平台之上的测试与试运行。 2.根据应用场景试运行的需求与问题，持续迭代更新技术平台与技术方案。 3.选择具备条件的行业开展应用试点，持续提升应用的成熟度。

五、我国区块链标准化路线图

5.1 区块链标准化需求分析

目前国内外在区块链领域还没有通用的标准，在标准化方面尚属空白。区块链应用面临一系列现实问题：一是市场上出现的各种DAPP兼容性和互操作性较差；二是区块链开发和部署缺乏标准化引导；三是区块链应用已经出现一些安全风险，如何有效防范这些风险，也是一个必须思考和解决的问题；四是由于对区块链规范的缺乏，使其容易被经济犯罪活动利用。

区块链标准化能打通应用通道，防范应用风险，提升应用效果，对于解决区块链发展问题、推进区块链应用起到重要作用。因此，为促进区块链应用的有序、健康和长效发展，很有必要及早推动开展区块链的标准化工作。

区块链标准化的好处——基于国际标准化组织（ISO）的分析：

按照ISO分析，标准对促进经济社会发展的贡献是巨大的。例如，在英国，标准每年对GDP的贡献高达82亿美元；在加拿大，自1981年以来，标准的应用为经济增长贡献了910亿美元。因此，开展区块链标准化工作，其好处主要体现在以下方面：

一是对企业来说，标准是解决区块链商业化应用过程中面临最大挑战的战略工具和指南，并能确保业务高效运营，提高生产率和帮助企业拓展新的市场。具体体现在：

- 降低成本：通过标准统一社会对区块链的认识，统一底层开发平台和应用编程接口（API），促进不同区块链系统的互操作和改进业

务流程，从而实现降低成本的目的；

- 增加客户满意度：通过标准提高区块链系统的安全和服务质量，优化服务流程，从而提高客户满意度；
- 拓展新市场：通过标准提高区块链相关产品和服务的通用性，能有效拓展企业市场。

二是对用户来说，区块链相关的产品和服务符合标准，意味着是安全的、可靠的和高质量的。

三是对政府来说，标准是制定政策和加强市场监管的重要依据，对提高政策水平和对外开放水平，具有重要作用。

5.2 区块链标准体系建议

标准体系是特定标准化系统为了实现本系统的目标而必须具备一整套具有内在联系的、科学的、由标准组成的有机整体。标准体系是一个概念系统，是人为组织制定的标准而形成的人工系统。另外，从国家信息技术服务标准（ITSS）、云计算、大数据、智能制造等一系列标准体系建设的思路来看，标准体系应具有发现问题、解决问题，以及指导标准研制和应用等作用。围绕标准体系建设要求，区块链标准体系主要针对以下问题提出：

- 构建区块链的标准化语言，统一对区块链的认识。
- 统一区块链底层开发平台和应用编程接口，为区块链的开发、移植和互操作提供支持。
- 统一不同区块链间的链接、实现信任和交换数据的标准，建立区块链间互操作基础。
- 构建安全和可信环境，规范基于区块链的服务，营造良好的应用环境。

基于上述问题的考虑，同时结合区块链的技术和应用全景图，从过程和方法、可信和互操作、信息安全等3个方面考虑，提出如图5–1所示的区块链标准体系框架，将标准分为基础、过程和方法、可信和互操作、业务和应用、信息安全等5个大类。

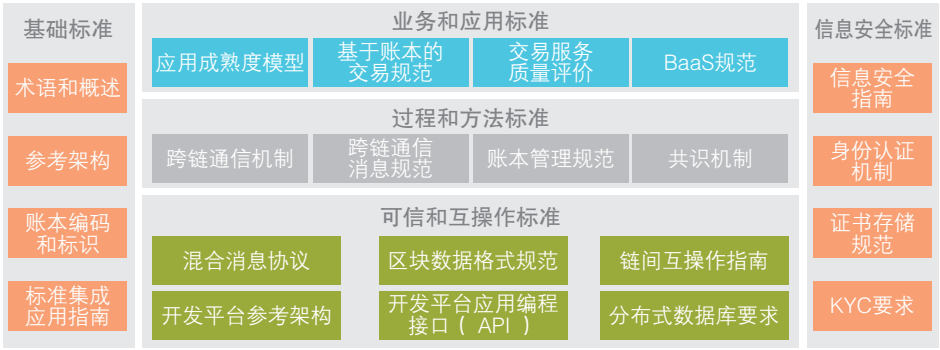


图5–1 区块链标准体系框架

1、基础标准：用于统一区块链术语、相关概念及模型，为其他各部分标准的制定提供支撑。主要包括术语、参考架构、账本编码和标识等方面的标准。

2、业务和应用标准：用于规范区块链应用开发和区块链应用服务的设计、部署、交付，以及基于分布式账本的交易。主要包括应用成熟度、基于分布式账本的交易、BaaS和服务质量评价等方面的标准。

3、过程和方法标准：用于规范区块链的更新和维护，以及指导实现不同区块链间的通信和数据交换。主要包括跨链通信机制、跨链通信消息规范、账本管理规范和共识机制等方面的标准。

4、可信和互操作标准：用于指导区块链开发平台的建设，规范和引导区块链相关软件的开发，以及实现不同区块链的互操作。主要包括开发平台、应用编程接口（API）、数据格式、混合消息协议和互操作等方面的标准。

5、信息安全标准：用于指导实现区块链的隐私和安全，以及身份认证。主要包括信息安全指南、身份认证机制、证书存储和KYC等方面的标准。

5.3 区块链标准化重点方向

以标准体系框架为基础，通过研究分析信息技术和通信领域已有标准，结合区块链技术和应用发展趋势，提出直接反映区块链特征，并能引导和规范区块链相关的技术和产品研发以及服务设计、部署和交付，有效解决数据交换、供应商绑定、信息安全和隐私保护等问题的21个标准化重点方向，以指导具体标准的立项和制定。对尚未纳入标准研制方向但在综合标准化体系框架中列出的，是下一步开展标准化工作的重点研究方向。

5.3.1 基础标准

基础标准对区块链技术研发和应用发展的核心作用是统一认识、建立标准语言，同时指导其他标准的研发。如图5–2所示。

依据图5–2示例的内容，基础标准包括4个方向：

1、区块链术语和概述：主要制定区块链术语、定义和概念，以及关键特征、服务类型和部署模式等方面标准，用于统一对区块链的认识，指导其他标准制定。

2、区块链参考架构：主要制定参考架构标准，规定区块链生态系统涉及的角色、活动，以及区块链的功能视图，为区块链技术开发和使用提供技术支撑。

3、账本编码和标识：主要规定账本编码格式和标识方式，为区块链建设，特别是账本使用监管提供支持，也是实现互操作的基础。

4、标准集成应用指南：主要结合公有链、联盟链和链的建设，以及不同类型的区块链应用场景，开发标准集成应用方案，支持实现标准配套应用。

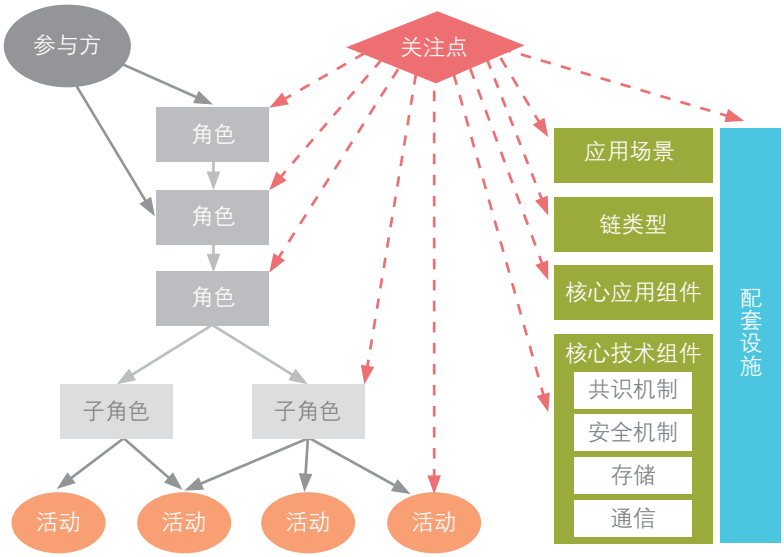


图5–2 基础标准的作用

5.3.2 业务和应用标准

业务和应用标准重点关注区块链即服务（BaaS）平台、不同类型的区块链应用，以及基于区块链的各类服务的标准，主要解决BaaS平台不统一、应用和服务质量无法保障等问题。如图5–3所示。

根据图5–3示例的内容，业务和应用标准包括3个方向：

1、应用成熟度模型：主要制定应用成熟度模型标准。为用户选择和评价、第三方开展区块链应用测评提供依据。

2、基于账本的交易规范：主要制定基于账本的交易要求和交易的业务程序。用于规范基于账本的交易。

3、交易服务质量评价：主要规定服务模型、指标体系与评价方法等方面的标准。用于对基于区块链的交易服务质量进行评价。

5.3.3 过程和方法标准

过程和方法标准重点关注规范区块链的更新和维护，以及不同区块链

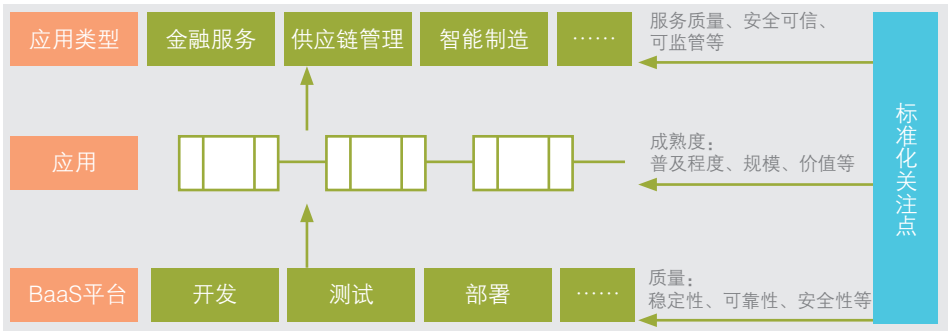


图5–3 业务标准化方向分析

间的通信和数据交换等方面的标准，主要解决账本维护和更新、不同区块链间通信问题。

根据图5–4示例的内容，过程和方法标准包括4个方向：

1、跨链通信机制：主要制定不同区块链间通信的场景、方式、流程等方面的标准。用于指导实现不同区块链间的互联互通。

2、跨链通信消息规范：主要制定不同区块链通信过程中的消息类型和格式方面的标准。用于指导实现不同区块链间通信的内容。

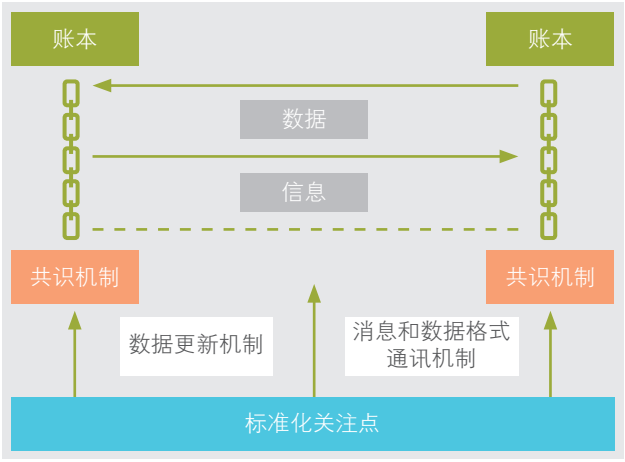


图5–4 过程与方法标准化方向分析

3、账本管理规范：主要规定账本发布、维护、使用和回收等方面的标准。用于指导和规范分布式账本的管理。

4、共识机制：主要制定区块链共识机制的类型、操作方法、技术要求和测试方法等标准。用于指导区块链系统的开发、分布式数据库运维和参与者之间的互动等。

5.3.4 可信和互操作标准

可信和互操作标准主要关注区块链开发平台的设计、建设和使用，以及实现区块链可移植、兼容和互操作等方面的标准。主要解决开发平台不统一，以及不同区块链的可移植性、兼容性和互操作性等方面的问题。如图5–5所示。

根据图5–5示例的内容，信任与互操作标准包括6个方向：

1、混合消息协议：制定不同区块链间互操作的消息头定义和格式，以及技术要求、测试方法等标准。用于规范区块链间的实现数据交换。

2、区块数据格式规范：主要制定区块的数据结构、数据类型等方面的标准。用于分布式账本的研发、管理和维护。

3、链间互操作指南：主要制定不同区块链间互操作的规程、方法和技术要求。用于支持区块链系统和应用的设计、开发、测试和使用等过程。

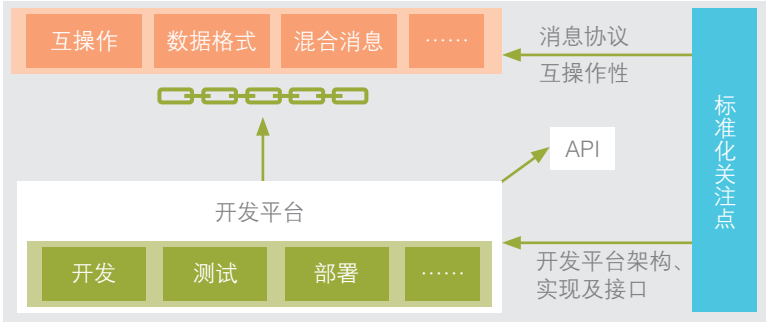


图5–5 信任与互操作标准化方向分析

4、开发平台参考架构：主要制定区块链开发平台的参考架构，规定了在开发平台中参与活动的角色之间的关系及角色的行为，以及区块链开发平台可提供的功能及可包含的组件。为区块链开发平台的设计、实现、部署和使用提供参考。

5、开发平台应用编程接口（API）：规定区块链开发平台提供的应用编程接口，确定开发平台设计应用编程接口的一般原则。用于区块链开发平台的设计、实现、测试、升级等。

6、分布式数据库要求：主要制定关于分布式数据库的架构、组成要素和功能要求等方面标准。用于指导分布式数据库产品的研发，以及分布式数据库的建设、管理和维护。

5.3.5 信息安全标准

信息安全标准旨在通过对区块链开发者提出信息安全能力要求和对区块链使用者提供信息安全指南和依据。信息安全标准包括4个方向：

1、信息安全指南：主要规定区块链可能面临的信息安全风险，提出采用区块链服务的安全管理基本要求和技术要求等。用于为采用区块链服务的用户提供全方位的信息安全指导。

2、身份认证机制：主要制定关于区块链系统中身份认证的类型、要求、方法、服务框架和技术要求等的标准。

3、证书存储规范：主要制定区块链证书在链内、侧链或链外存储的要求、存储格式、维护方法和检测技术等。主要用于支持区块链中证书存储。

4、客户识别要求：制定关于客户接受政策、客户身份识别、对高风险账户的持续监管和风险管理等方面的标准。用于指导实现安全识别客户要求。

5.4 区块链标准化实施方案

区块链标准化的实施方案主要以标准体系建设为核心，由4个环节组成，即体系预研、标准研制、试点推广、体系改进，这4个环节将促进标准体系不断完善和改进。如图5–6所示。

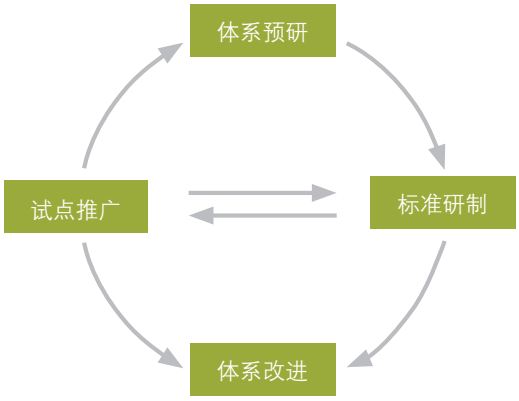


图5–6 区块链标准体系建设环节

在上述环节的工作中，主要包括区块链标准体系研究、重点标准研制、标准试点推广和标准体系持续改进等工作任务。各项任务的内容如下所述，具体推进计划如表5–1所示。

标准体系预研：系统分析区块链技术和产业发展趋势，以及应用要求，并根据引导和规范区块链技术和产业发展的事中事后监管要求，开展标准体系预研，指导成体系成系统开展标准研制工作。主要成果为《区块链标准体系研究报告》。

重点标准研制：按照“急用先行、成熟先上”的原则，开展术语和概述、参考架构等重点标准的研制工作。主要成果为具体标准。

标准试点推广：根据标准研制进展情况，由区块链技术和产业发展论坛成员单位按照自愿原则，在区块链底层开发平台建设、区块链应用研发以及业务拓展过程中，开展标准验证工作。条件成熟时，选择具备条件的

省市或行业开展试点工作。主要成果为《标准验证试点报告》。经过验证试点后的标准，可视情况进行应用推广，应用推广方式包括论坛、专题讲座、媒体宣传、年会、支持政府采购等。在此过程中将收集到具体的应用需求，为区块链标准体系的持续改进提供必要的支持。

标准体系改进：主要是定期向区块链标准应用组织收集与区块链标准体系有关的意见建议。通过分析、寻求并证实问题产生或潜在的原因，提出改进区块链标准体系的措施办法并跟踪评估区块链标准体系改进成效。

表5–1 区块链标准化工作进度计划

阶段	主要工作任务	进度计划
标准体系预研	1．研究分析区块链发展现状及趋势； 2．研究分析区块链标准化需求； 3．明确区块链标准化工作思路； 4．确定标准化工作内容及工作机制。	2016.10—2017.4
标准研制	1．按照“急用先行、成熟先上”的原则开展标准研制工作； 2．优先开展术语和概述、参考架构等基础标准研制，针对过程和方法、可信和互操作、信息安全等领域，按照“成熟先上”的原则启动标准研制工作； 3．主导或参与国际标准化工作。	2016.10—
标准试点推广	1．对于已形成征求意见稿的标准草案，区块链技术和产业发展论坛成员单位按照自愿原则，开展标准验证工作； 2．对通过验证的标准，选择具备条件的省市和行业开展标准应用推广试点工作； 3．结合国务院要求，及时探索贯彻标准的机制和模式。	2017.4—
标准体系改进	结合下列情况对标准体系进行改进： 1．工信部、国标委等政府主管部门的相关政策要求； 2．标准研究制定及标准验证和试点的情况； 3．区块链技术和产业要求； 4．深入开展区块链标准化工作的要求。	2017.10—

最后，考虑到区块链技术和应用尚处于发展阶段，国际标准化工作也仅处于起步阶段，区块链标准研制的策略将积极贯彻落实国务院《深化标

准化工作改革方案》（国发〔2015〕13号），优先依托区块链技术和产业发展论坛，制定和推广团体标准，同步推进国际标准化工作。待条件成熟时，及时转化制定为国家标准或行业标准，从而建立政府主导制定与市场自主制定的标准协同发展、协调配套的区块链标准体系。

5.5 区块链国际标准化

5.5.1 国际标准化进程

目前，区块链标准化在国际上已经引起广泛关注和讨论，并且出现一些标准化工作的筹备和标准研制的实践。以下是区块链标准相关国际组织在区块链标准化方面的工作和相关分析：

1、万维网联盟（W3C）

（1）基本情况

2016年7月，万维网联盟（简称W3C）在针对区块链的专题会议（First Blockchain Workshop）中，明确提出W3C达成的共识是区块链需要标准来消除冗余的同时促进竞争。

（2）对标准化的认识

W3C认为，数据标准化是区块链标准化工作的第一步，最重要的标准化工作结果为APIs和关键的数据格式标准，其次是身份识别和授权标准，最后是软件许可和来源标准。

2、国际标准化组织/国际电工委员会 第一联合技术委员会（ISO/IEC JTC1）

2016年8月底，ISO/IEC JTC1咨询组（Advisor Group）在爱尔兰都柏林召开会议，向JTC1提出了分布式账本技术的标准化建议。主要内容如下：

一是分布式账本技术（DLT）是一种革新技术，具有广泛的应用，包括金融服务、健康信息学、房地产、电子政务、身份管理、分布式电网计

费、协议以及游戏等领域。

二是DLT本质上是信息技术，其标准化工作也应由JTC1负责。JTC1在安全和隐私技术、数据库技术、云计算、分布式平台等方面具有很深的标准化专业基础，这些技术都是与DLT标准化紧密相关的。

三是建议JTC1尽快成立一个新的DLT分技术委员会。在成立这个新的分技术委员会过程中，需要处理好与ISO/TC68（金融服务）、ISO/TC 125（健康信息学）、IEC SyC智能能源、IEC TC65（工业过程测量、控制和自动化）、ISO/TC 84（自动化系统和集成）以及ISO/TC 251（资产管理）的关系。

3、国际标准化组织区块链和电子化的分布式账本技术技术委员会（ISO/TC 307）

2016年9月12日，ISO成立了ISO/TC 307（区块链及电子化的分布式账本技术），负责区块链及分布式账本技术的标准研制，以支持用户、应用和系统间的互操作和数据交换。通过分析ISO/TC 307成立的背景资料发现：

（1）对区块链技术的理解

区块链和电子化的分布式账本技术是一种管理和记录交易的点对点（P2P）数据库工具，其后台技术是开源。ISO认为区块链是一种新的颠覆性技术，使得国家和国际之间能便利地共享政府到商业、商业到商业（B2B）的金融、法律、物理的或电子化的信息。

（2）区块链类型

ISO按照读写数据的权限，将区块链分为公有链和专有链，其中公有链是允许任何人在没有得到授权的情况下，都能够读写账本数据；而专有链则是区块链网络中的所有参与方都是公开和可信的。

（3）区块链的治理

ISO认为类似现有的金融交易，应该为区块链的治理制定标准化的

方法。

通过上述方面的分析，ISO认为，区块链标准化主要涉及术语、过程和方法、可信和互操作、隐私和安全、身份认证。

4、其他实践

除上述国际标准化组织外，还有以下相关的标准化实践。具体包括：

2015年，摩根大通、巴克莱银行、高盛集团、西班牙BBVA银行、澳洲联邦银行、瑞士信贷集团、道富银行、苏格兰皇家银行集团和瑞士银行达成了一项合作，将为区块链技术在银行业中的使用制定行业标准和协议。

2016年4月，澳大利亚非政府组织澳大利亚标准协会（Standards Australia）针对区块链和分布式账本技术提出了全新的国际标准化方案，并且提交给了ISO。

2016年5月，区块链技术提供商Chain公开发布一种开源区块链协议——Chain开放标准。Chain开放标准，由硅谷公司和全球金融服务机构合作开发，能支持大规模金融应用，在运行获得许可的区块链网络的同时，达到关于金融服务行业的严格监管、安全和隐私要求。

2016年7月，机构贸易交流国际证券协会（ISITC）欧洲分部提出了10项区块链基准，分为技术标准和监管标准两大类，涉及了区块链的弹性、可扩展性、时延、数据结构、审计、治理、法律管辖、调节；软件版本控制和网络；目标是帮助市场上可用的日渐多样化的区块链工具的标准化。目前该机构正在筹备相关标准制定工作，之后会向ISO标准机构提交审核。

5.5.2 国际标准化策略

区块链国际标准化目前还处于初期研究阶段，我国在国际标准化进程中能否发挥重要的作用，以及能否提高参与度和影响力，很大程度上取决于前期能否迅速反应，合理布局。为此，我们提出以下几点策略建议：

- 跟踪国际标准化新进展和新成果，研究国际标准体系，识别区块链标准化的新动向、新需求和新机会。
- 积极参与区块链领域国际标准化权威组织的工作，争取更多话语权。
- 加快制定参考架构、区块数据格式等基础标准，主导或实质参与区块链国际标准制修订工作，推动我国优势技术转化为国际标准。
- 加大力度构建具有国际先进水平的区块链标准体系，并向国际推广。

六、推动区块链发展的相关建议

当前，区块链技术和应用正处于快速发展阶段。在技术研发方面，以太坊（Ethereum）、超级账本（Hyperledger）等开源社区先后成立，万向控股、蚂蚁云、微众银行、乐视金融、万达网络科技等重点企业，正在加大资金投入，推动成立了分布式总账基础协议联盟、金融区块链合作联盟，建设联合实验室，加快研发通用的区块链平台，支持中小企业和个人创业创新。在应用方面，除数字货币领域的规模化应用外，区块链在新能源、社会公益、银行间联合贷款清算、文化娱乐、房地产等领域的应用正处于快速发展阶段。为了有效推动我国区块链技术和应用发展，培育形成具有全球竞争力的区块链产业，提出以下建议，供各级政府主管部门出台区块链技术和产业相关的扶持政策、各类企业和科研机构开展核心关键技术研发以及各类行业用户应用区块链技术提供参考。

（一）出台区块链相关的扶持政策

未来工作中，我们将继续紧密跟踪联合国、国际货币基金组织等国际组织对推动区块链应用的政策走向，加大力度研究欧盟、美国、英国、日本等地区和国家对推动区块链发展的政策措施。建议各级政府主管部门借鉴发达国家和地区的先进做法，结合我国区块链技术和应用发展情况，及时出台区块链技术和产业发展扶持政策，重点支持关键技术攻关、重大示范工程、“双创”平台建设、系统解决方案研发和公共服务平台建设等。同时，建议结合深入推进简政放权、放管结合、优化服务改革等，放宽市场准入限制，加强事中事后监管，提升为企业服务的能力和水平，营造有利于加快区块链发展的环境。最后，建议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、“双创”平

台和公共服务平台建设。

（二）加快核心关键技术攻关和平台建设

建议国内重点企业、科研、高校和用户单位加强联合，加快共识机制、可编程合约、分布式存储、数字签名等核心关键技术攻关。未来工作中，我们将学习借鉴国际开源社区建设和运用模式，通过论坛成员单位加强合作，建设我国区块链开源社区，提高区块链技术的安全可靠水平，并为各级政府扶持中小企业发展提供支持。建议大企业加大研发投入力度，建设区块链通用开发平台，降低区块链技术研发和应用成本。建议具备条件的省市，推动具备条件的软件和信息服务业示范基地，建设面向中小企业创业创新的孵化平台。

（三）组织开展区块链应用示范

建议各级政府结合《中国制造2025》、“互联网+”行动指导意见、制造业与互联网融合发展等系列国家战略的实施，聚焦典型应用需求，组织重点企业，研究提出区块链应用示范方案。围绕智能制造、新能源、供应链管理、数字资产管理等领域，支持大企业牵头、产学研用联合，选择有条件的地区和行业，开展区块链应用示范，探索形成区块链应用推广模式，营造应用环境。

（四）加快建立人才培养体系

建议鼓励和支持重点高校设置区块链专业课程。推动重点企业和高校联合，建设区块链人才实训基地，加快培养区块链专业技术人才。结合国家专业技术人才知识更新工程、企业经营管理人才素质提升工程、高技能人才振兴计划等，加强区块链专业技术人才和高端人才培养。支持和推动国内重点培训机构，加强与重点企业合作，积极培训区块链技术开发人才。

（五）加强国际交流与合作

建议鼓励和支持重点企业、中小企业积极参与国际区块链开源社区，提升影响力和话语权。借助中美、中欧战略对话机制，支持大企业围绕关

键技术攻关、“双创”平台建设、标准制定以及应用示范等，开展技术交流与合作。鼓励和支持具备条件的大企业充分利用市场、资金和人才优势，建立多种形式的国际民间交流合作机制，积极推动我国具有竞争优势的区块链技术和产品走出去。

参考文献

[1] 区块链技术发展现状与展望，自动化学报，2016年04期.

[2] 区块链：从数字货币到信用社会，中信出版集团，2016年7月.

[3] 分布式账本技术：超越区块链，英国政府首席科学顾问报告，2016年1月.

[4] 国家智能制造标准体系建设指南（2015年版），工业和信息化部、国家标准化管理委员会，2015年12月.

[5] 区块链和电子化的分布式账本技术，ISO/TSP_258，2016年6月.

[6] 区块链社会：解码区块链全球应用与投资案例，中信出版集团，2016年8月.