区块链白皮书

（2018 年）

中国信息通信研究院
可信区块链推进计划

2018年9月

版权声明

前言

2018 年 5 月，习近平总书记在两院院士大会上的讲话中指出，“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。”区块链凭借其独有的信任建立机制，成为金融和科技深度融合的重要方向。在政策、技术、市场的多重推动下，区块链技术正在加速与实体经济融合，助力高质量发展，对我国探索共享经济新模式、建设数字经济产业生态、提升政府治理和公共服务水平具有重要意义。

区块链作为点对点网络、密码学、共识机制、智能合约等多种技术的集成创新，提供了一种在不可信网络中进行信息与价值传递交换的可信通道。当前，基于区块链的应用探索一直在加速推进，跨链、隐私保护、安全监管等区块链关键技术也正在成为研究热点。然而，区块链技术仍处于社会实验阶段，各方对区块链的概念、架构、技术特点、发展路线及治理与监管等尚未形成共识。

为推动区块链技术与实体经济深度融合，形成发展共识，中国信息通信研究院和可信区块链推进计划共同组织编写了《区块链白皮书》（2018 年）。本白皮书深入解读了区块链内涵概念，提出了区块链技术体系架构，分析了区块链关键技术发展路线，剖析当前区块链在政策、产业、技术和标准方面的最新形势和发展机遇，探讨了区块链发展面临的挑战，并提出相应政策建议。

目录

一、区块链的概念和特征

（一） 区块链概念

区块链（Blockchain）是一种由多方共同维护，使用密码学保证传输和访问安全，能够实现数据一致存储、难以篡改、防止抵赖的记账技术，也称为分布式账本技术（Distributed Ledger Technology）。典型的区块链以块-链结构存储数据。作为一种在不可信的竞争环境中低成本建立信任的新型计算范式和协作模式，区块链凭借其独有的信任建立机制，正在改变诸多行业的应用场景和运行规则，是未来发展数字经济、构建新型信任体系不可或缺的技术之一。

典型的区块链系统中，各参与方按照事先约定的规则共同存储信息并达成共识。为了防止共识信息被篡改，系统以区块（Block）为单位存储数据，区块之间按照时间顺序、结合密码学算法构成链式（Chain）数据结构，通过共识机制选出记录节点，由该节点决定最新区块的数据，其他节点共同参与最新区块数据的验证、存储和维护，数据一经确认，就难以删除和更改，只能进行授权查询操作。按照系统是否具有节点准入机制，区块链可分类为许可链和非许可链。许可链中节点的加入退出需要区块链系统的许可，根据拥有控制权限的主体是否集中可分为联盟链[1]和私有链[2]；非许可链则是完全开放的，亦可称为公有链[3]，节点可以随时自由加入和退出。

[1]联盟链：根据一定特征所设定的节点能参与、交易，共识过程受预选节点控制的区块链。
[2]私有链：写入权限在一个组织手里，读取权限可能会被限制的区块链。
[3]公有链：任何人都能读取区块链信息，发送交易并能被确认，参与共识过程，是真正意义上的去中心化区块链，比特币区块链即是公有链最好的代表。

（二） 区块链的特征

相对于传统的分布式数据库，区块链体现了以下几个对比特征：**一是从复式记账演进到分布式记账。**传统的信息系统，每位会计各自记录，每次对账时存在多个不同账本。区块链打破了原有的复式记账，变成“全网共享”的分布式账本，参与记账的各方之间通过同步协调机制，保证数据的防篡改和一致性，规避了复杂的多方对账过程。**二是从“增删改查”变为仅“增查”两个操作。**传统的数据库具有增加、删除、修改和查询四个经典操作。对于全网账本而言，区块链技术相当于放弃了删除和修改两个选项[4]，只留下增加和查询两个操作，通过区块和链表这样的“块链式”结构，加上相应的时间戳进行凭证固化，形成环环相扣、难以篡改的可信数据集合。**三是从单方维护变成多方维护。**针对各个主体而言，传统的数据库是一种单方维护的信息系统，不论是分布式架构，还是集中式架构，都对数据记录具有高度控制权。区块链引入了分布式账本，是一种多方共同维护、不存在单点故障的分布式信息系统，数据的写入和同步不仅仅局限在一个主体范围之内，需要通过多方验证数据、形成共识，再决定哪些数据可以写入。**四是从外挂合约发展为内置合约。**传统上，财务的资金流和商务的信息流是两个截然不同的业务流程，商务合作签订的合约，在人工审核、鉴定成果后，再通知财务进行打款，形成相应的资金流。智能合约的出现，基于事先约定的规则，通过代码运行来独立执行、协同写入，通过算法代码形成了一种将信息流和资金流整合到一起的“内置合约”。

[4]用户可以对本地数据进行删除和修改，但不影响全网共识后的数据一致性。

（三） 区块链适用的场景条件

作为一项新兴技术，区块链具有在诸多领域开展应用的潜力。然而，区块链不是万能的，技术上去中心化、难以篡改的鲜明特点，使其在限定场景中具有较高的应用价值，可以总结为**“新型数据库、多业务主体、彼此不互信、业务强相关”**。

首先，源自于应用场景对数据库的需要。区块链本质上是一种带时间戳的新型数据库，从对数据真实、有效、不可伪造、难以篡改的组织需求角度出发，相对于传统的数据库来说，可谓是一个新的起点和新的要求。**其次，需要是一个跨主体、多方写入的应用场景。**多个主体各自维护账本，往往因为数据信息不共享、业务逻辑不统一等原因，导致“账对不齐”的现象。与之相反，区块链中每个主体都可以拥有一个完整的账本副本，通过即时清结算的模式，保证多个主体之间数据的一致性，规避了复杂的对账过程。**再次，适合于在不可信的环境中建立基于数学的信任。**区块链在技术层面保证了系统的数据可信（密码学算法、数字签名、时间戳）、结果可信（智能合约、公式算法）和历史可信（链式结构、时间戳），因此区块链提供了一种“机器中介”，尤其适用于协作方不可信、利益不一致或缺乏权威第三方介入的行业应用。**最后，根据系统控制权和交易信息公开与否进行归类。**公有链允许任一节点的加入，不对信息的传播加以限制，信息对整个系统公开；联盟链只允许认证后的机构参与共识，交易信息根据共识机制进行局部公开；相比而言，私有链范围最窄，只适用于限定的机构之内。

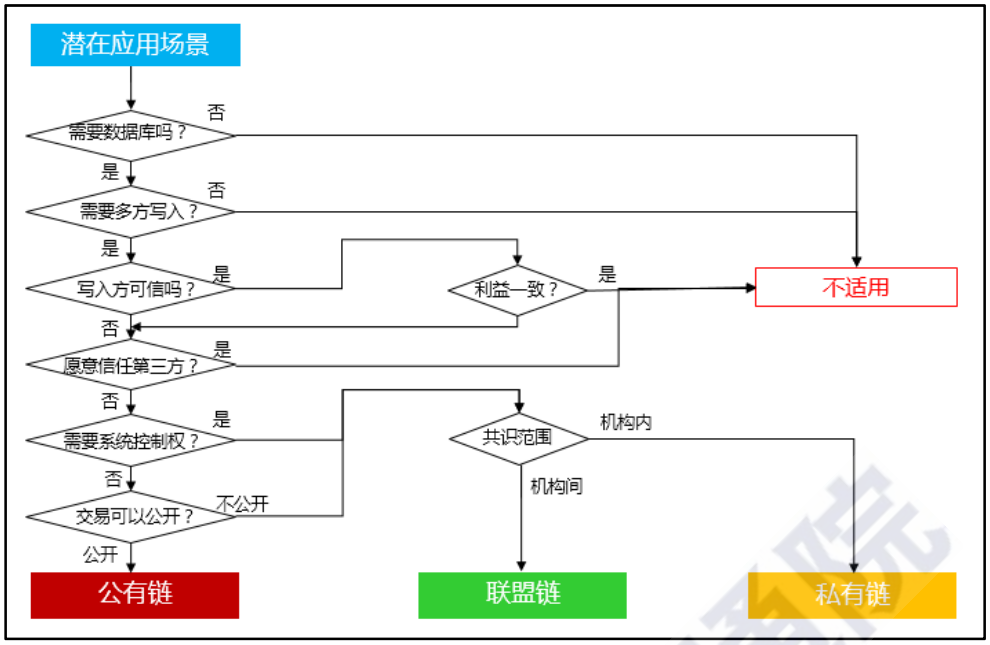
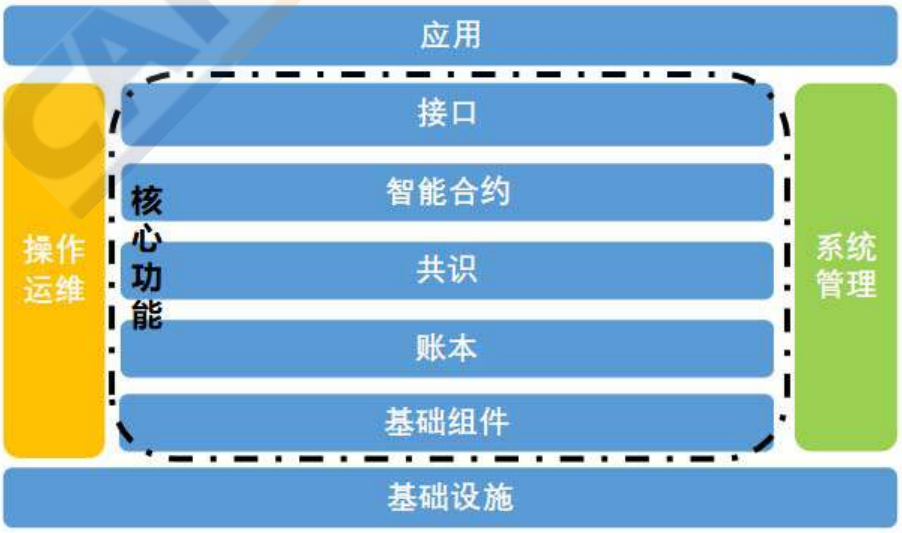


图 1　区块链适用的场景条件判定

二、区块链关键技术架构和发展趋势

（一） 区块链的技术架构

各类区块链虽然在具体实现上各有不同，其整体架构却存在共性，本白皮书建议了一种可划分为基础设施、基础组件、账本、共识、智能合约、接口、应用、操作运维和系统管理 9 部分的架构。



来源：中国信息通信研究院，2018 年 8 月

图 2　区块链技术架构图

1. 基础设施（Infrastructure）

基础设施层提供区块链系统正常运行所需的操作环境和硬件设施（物理机、云等），具体包括网络资源（网卡、交换机、路由器等）、存储资源（硬盘和云盘等）和计算资源（CPU、GPU、ASIC 等芯片）。基础设施层为上层提供物理资源和驱动，是区块链系统的基础支持。

2. 基础组件（Utility）

基础组件层可以实现区块链系统网络中信息的记录、验证和传播。在基础组件层之中，区块链是建立在传播机制、验证机制和存储机制基础上的一个分布式系统，整个网络没有中心化的硬件或管理机构，任何节点都有机会参与总账的记录和验证，将计算结果广播发送给其他节点，且任一节点的损坏或者退出都不会影响整个系统的运作。具体而言，主要包含网络发现、数据收发、密码库、数据存储和消息通知五类模块。

1）网络发现

区块链系统由众多节点通过网络连接构成。特别是在公有链系统中，节点数量往往很大。每个节点需要通过网络发现协议发现邻居节点，并与邻居节点建立链路。对于联盟链而言，网络发现协议还需要验证节点身份，以防止各种网络攻击。

2）数据收发

节点通过网络通讯协议连接到邻居节点后，数据收发模块完成与其他节点的数据交换。事务广播、消息共识以及数据同步等都由该模块执行。根据不同区块链的架构，数据收发器的设计需考虑节点数量、

密码学算法等因素。

3）密码库

区块链中多个环节使用密码学算法。密码库为上层组件提供基本的密码学算法支持，包括各种常用的编码算法、哈希算法、签名算法、隐私保护算法等。与此同时，密码库还涉及诸如密钥的维护和存储之类的功能。

4）数据存储

根据数据类型和系统结构设计，区块链系统中的数据使用不同的数据存储模式。存储模式包括关系型数据库（如 MySQL）和非关系型数据库（如 LevelDB）。通常，需要保存的数据包括公共数据（例如：交易数据、事务数据、状态数据等）和本地的私有数据等。

5）消息通知

消息通知模块为区块链中不同组件之间以及不同节点之间提供消息通知服务。交易成功之后，客户通常需要跟踪交易执行期间的记录和获取交易执行的结果。消息通知模块可以完成消息的生成、分发、存储和其他功能，以满足区块链系统的需要。

3. 账本（Ledger）

账本层负责区块链系统的信息存储，包括收集交易数据，生成数据区块，对本地数据进行合法性校验，以及将校验通过的区块加到链上。账本层将上一个区块的签名嵌入到下一个区块中组成块链式数据结构，使数据完整性和真实性得到保障，这正是区块链系统防篡改、可追溯特性的来源。典型的区块链系统数据账本设计，采用了一种按

时间顺序存储的块链式数据结构。

账本层有两种数据记录方式，分别是基于资产和基于账户。基于资产的模型中，首先以资产为核心进行建模，然后记录资产的所有权，即所有权是资产的一个字段。基于账户的模型中，建立账户作为资产和交易的对象，资产是账户下的一个字段。相比而言，基于账户的数据模型可以更方便的记录、查询账户相关信息，基于资产的数据模型可以更好地适应并发环境。为了获取高并发的处理性能，且及时查询到账户的状态信息，多个区块链平台正向两种数据模型的混合模式发展。

表 1 账本层两种模型对比

	基于资产	基于账户
建模对象	资产	用户
记录内容	记录资产所有权	记录账户操作
系统中心	状态（交易）	事件（操作）
计算重心	计算发生在客户端	计算发生在节点
判断依赖	方便判断交易依赖	较难判断交易依赖
并行	适合并行	较难并行
账户管理	难以管理账户元数据	方便管理账户元数据
适用的查询场景	方便获取资产最终状态	方便获取账户资产余额
客户端	客户端复杂	客户端简单
举例	比特币、R3 Corda	以太坊、超级账本 Fabric

4. 共识（Consensus）

共识层负责协调保证全网各节点数据记录一致性。区块链系统中的数据由所有节点独立存储，在共识机制的协调下，共识层同步各节

点的账本，从而实现节点选举、数据一致性验证和数据同步控制等功能。数据同步和一致性协调使区块链系统具有信息透明、数据共享的特性。

表 2　两类共识机制对比

	第一类共识机制	第二类共识机制
写入顺序	先写入后共识	先共识后写入
算法代表[5]	PoW、PoS、DPoS	PBFT及BFT变种
共识过程	大概率一致就共识 工程学最后确认	确认一致后再共识 共识即确认
复杂性	计算复杂度高	网络复杂度高
仲裁机制	如果一次共识同时出现多个记账节点，就产生分叉，最终以最长链为准	法定人数投票，各节点间P2P广播沟通达成一致
是否分叉	有分叉	无分叉
安全阈值	作恶节点权益之和不超过1/2	作恶节点数不超过1/3总节点数
节点数量	节点数量可以随意改变，节点数越多、系统越稳定	随着节点数增加，性能下降，节点数量不能随意改变
应用场景	多用于非许可链	用于许可链

区块链有两类现行的共识机制，根据数据写入的先后顺序判定，如上表所示。从业务应用的需求看，共识算法的实现应综合考虑应用环境、性能等诸多要求。一般来说，许可链采用节点投票的共识机制，以降低安全为代价，提升系统性能。非许可链采用基于工作量、权益证明等的共识机制，主要强调系统安全性，但性能较差。为了鼓励各节点共同参与进来，维护区块链系统的安全运行，非许可链采用发行 Token 的方式，作为参与方的酬劳和激励机制，即通过经济平衡的手段，来防止对总账本内容进行篡改。因此，根据运行环境和信任分级，选择适用的共识机制是区块链应用落地应当考虑的重要因素之一。

[5]共识算法代表包括：PoW（Proofof Work）工作量证明机制，PoS（Proofof Stake）股权证明机制，DPoS（Delegated Proof of Stake）授权股权证明机制，PBFT（Practical Byzantine Fault Tolerance）实用拜占庭容错算法，BFT（Byzantine Fault Tolerance）拜占庭容错算法等。

表 3 共识算法对比

特性	PoW	PoS	DPoS	PBFT	VRF
节点管理	无许可	无许可	无许可	需许可	需许可
交易延时	高（分钟）	低（秒级）	低（秒级）	低（毫秒级）	低（毫秒级）
吞吐量	低	高	高	高	高
节能	否	是	是	是	是
安全边界	恶意算力不超过 1/2	恶意权益不超过 1/2	恶意权益不超过 1/2	恶意节点不超过 1/3	恶意节点不超过 1/3
代表应用	Bitcoin、Ethereum	Peercoin	Bitshare	Fabirc（Rev 0.6）	Algorand
扩展性	好	好	好	差	差

5. 智能合约（Smart Contract）

智能合约层负责将区块链系统的业务逻辑以代码的形式实现、编译并部署，完成既定规则的条件触发和自动执行，最大限度的减少人工干预。智能合约的操作对象大多为数字资产，数据上链后难以修改、触发条件强等特性决定了智能合约的使用具有高价值和高风险，如何规避风险并发挥价值是当前智能合约大范围应用的难点。

智能合约根据图灵完备[6]与否可以分为两类，即图灵完备和非图灵完备。影响实现图灵完备的常见原因包括：循环或递归受限、无法实现数组或更复杂的数据结构等。图灵完备的智能合约有较强适应性，可以对逻辑较复杂的业务操作进行编程，但有陷入死循环的可能。对比而言，图灵不完备的智能合约虽然不能进行复杂逻辑操作，但更加简单、高效和安全。

[6]图灵完备（Turing completeness）：指一系列操作数据的规则（如指令集、编程语言、细胞自动机）可以用来模拟单带图灵机的可计算性系统。（Gannon, Paul, Colossus: Bletchley Park's Greatest Secret, London: Atlantic Books, 2006-01-10 [2006], ISBN 978-184-354-330-5）

表 4　部分区块链系统的智能合约特性

区块链平台	是否图灵完备	开发语言
比特币	不完备	Bitcoin Script
以太坊	完备	Solidity
EOS	完备	C++
Hyperledger Fabric	完备	Go
Hyperledger Sawtooth	完备	Python
R3 Corda	完备	Kotlin/Java

当前智能合约的应用仍处于比较初级的阶段，智能合约成为区块链安全的“重灾区”。从历次智能合约漏洞引发的安全事件看，合约编写存在较多安全漏洞，对其安全性带来了巨大挑战。目前，提升智能合约安全性一般有几个思路：一是形式化验证（Formal Verification）。通过严密的数学证明来确保合约代码所表达的逻辑符合意图。此法逻辑严密，但难度较大，一般需要委托第三方专业机构进行审计。二是智能合约加密。智能合约不能被第三方明文读取，以此减少智能合约因逻辑上的安全漏洞而被攻击。此法成本较低，但无法用于开源应用。三是严格规范合约语言的语法格式。总结智能合约优秀模式，开发标准智能合约模板，以一定标准规范智能合约的编写可以提高智能合约质量，提高智能合约安全性。

6. 系统管理（System Management）

系统管理层负责对区块链体系结构中其他部分进行管理，主要包含权限管理和节点管理两类功能。权限管理是区块链技术的关键部分，尤其对于对数据访问有更多要求的许可链而言。权限管理可以通过以下几种方式实现：1）将权限列表提交给账本层，并实现分散权限控制；2）使用访问控制列表实现访问控制；3）使用权限控制，例如评分/子区域。通过权限管理，可以确保数据和函数调用只能由相应的

操作员操作。

节点管理的核心是节点标识的识别，通常使用以下技术实现：1）CA[7]认证：集中式颁发 CA 证书给系统中的各种应用程序，身份和权限管理由这些证书进行认证和确认。2）PKI[8]认证：身份由基于 PKI 的地址确认。3）第三方身份验证：身份由第三方提供的认证信息确认。由于各种区块链具有不同的应用场景，因此节点管理具有更多差异。现有的业务扩展可以与现有的身份验证和权限管理进行交互。

7. 接口（Interface）

接口层主要用于完成功能模块的封装，为应用层提供简洁的调用方式。应用层通过调用 RPC 接口与其他节点进行通信，通过调用 SDK 工具包对本地账本数据进行访问、写入等操作。同时，RPC 和 SDK 应遵守以下规则：一是功能齐全，能够完成交易和维护分布式账本，有完善的干预策略和权限管理机制。二是可移植性好，可以用于多种环境中的多种应用，而不仅限于某些绝对的软件或硬件平台。三是可扩展和兼容，应尽可能向前和向后兼容，并在设计中考虑可扩展性。四是易于使用，应使用结构化设计和良好的命名方法方便开发人员使用。常见的实现技术包括调用控制和序列化对象等。

8. 应用（Application）

应用层作为最终呈现给用户的部分，主要作用是调用智能合约层的接口，适配区块链的各类应用场景，为用户提供各种服务和应用。

[7]CA:电子商务认证授权机构（Certificate Authority），也称为电子商务认证中心，是负责发放和管理数字证书的权威机构，并作为电子商务交易中受信任的第三方，承担公钥体系中公钥的合法性检验的责任。
[8]PKI：公钥基础设施（Public Key Infrastructure ），是一种遵循既定标准的密钥管理平台,它能够为所有网络应用提供加密和数字签名等密码服务及所必需的密钥和证书管理体系。

由于区块链具有数据确权属性以及价值网络特征，目前产品应用中很多工作都可以交由底层的区块链平台处理。在开发区块链应用的过程中，前期工作须非常慎重，应当合理选择去中心化的公有链、高效的联盟链或安全的私有链作为底层架构，以确保在设计阶段核心算法无致命错误问题。因此，合理封装底层区块链技术，并提供一站式区块链开发平台将是应用层发展的必然趋势。同时，跨链技术的成熟可以让应用层选择系统架构时增加一定的灵活性。

根据实现方式和作用目的的不同，当前基于区块链技术的应用可以划分为三类场景，如表 5 所示：一是价值转移类，数字资产在不同账户之间转移，如跨境支付；二是存证类，将信息记录到区块链上，但无资产转移，如电子合同；三是授权管理类，利用智能合约控制数据访问，如数据共享。此外，随着应用需求的不断升级，还存在多类型融合的场景。

表 5 区块链应用场景分类

类型	政府	金融	工业	医疗	法律	版权
价值转移		数字票据 跨境支付 应收账款 供应链金融	能源交易	医疗保险		
存证	电子发票 电子证照 精准扶贫	现钞冠字号 溯源 供应链金融	防伪溯源	电子病历 药品追溯	公证 电子存证 网络仲裁	版权确权
授权管理	政府数据共享	征信		健康数据共享		版权管理

9. 操作运维（Operation and Maintenance）

操作运维层负责区块链系统的日常运维工作，包含日志库、监视

库、管理库和扩展库等。在统一的架构之下，各主流平台根据自身需求及定位不同，其区块链体系中存储模块、数据模型、数据结构、编辑语言、沙盒环境的选择亦存在差异，详见表 6，给区块链平台的操作运维带来较大的挑战。

表 6 主流平台区块链技术体系架构对比

层级	平台差异	比特币	以太坊	Hyperledger Fabric	R3 Corda
应用		比特币	Dapp/ 以太币	企业级 分布式账本	CorDapp
智能合约	编程语言	Script	Solidity/ Serpent	Go/Java	Java/Kotlin
	沙盒环境		EVM	Docker	JVM
共识（数据准入）		PoW	PoW/ PoS	PBFT/SBFT/Kafka	Raft
账本	数据结构	Merkle 树/ 区块链表	Merkle Patricia 树/ 区块链表	Merkle Bucket 树/ 区块链表	无区块 连接交易
	数据模型	基于资产	基于账户	基于账户	基于资产
	区块存储	文件存储	LevelDB	LevelDB/CouchDB	关系数据库
基础组件层		TCP，P2P	TCP，P2P	HTTP2 P2P	AMQP(TLS) P2P

（二） 区块链的技术发展趋势

1. 架构方面，公有链和联盟链融合持续演进

联盟链是区块链现阶段的重要落地方式，但联盟链不具备公有链的可扩展性、匿名性和社区激励。随着应用场景日趋复杂，公有链和联盟链的架构模式开始融合，开始出现公有链在底层面向大众、联盟链在上层面向企业的混合架构模式，结合钱包、交易所等入口，形成一种新的技术生态。例如，在公有链中选取验证节点时，共识算法层

面存在 PoS 不确定性高、PoW 资源消耗严重、PBFT 无法支持大量节点进行共识等问题，Algorand 算法[9]通过密码学的方法，从大量节点中选出少量节点，再用 PBFT 算法在少量节点之间达成共识的方式，为公有链和联盟链的混合架构提供了可能。

2. 部署方面，区块链即服务加速应用落地

区块链与云计算结合，将有效降低区块链部署成本。一方面，预配置的网络、通用的分布式账本架构、相似的身份管理、分布式商业监控系统底层逻辑、相似的节点连接逻辑等被模块化、抽象成区块链服务，向外支撑起不同客户的上层应用。用云计算快速搭建的区块链服务，可快速验证概念和模型可行性。另一方面，云计算按使用量收费，利用已有基础服务设施或根据实际需求做适应性调整，可实现应用开发流程加速，部署成本降低，满足未来区块链生态系统中初创企业、学术机构、开源组织、联盟和金融机构等对区块链应用的服务需求。

在云计算当前主要提供的 3 种类型服务（IaaS、PaaS、SaaS）基础之上，区块链与云计算结合发展出 BaaS（Blockchain as a Service，区块链即服务）。BaaS 服务供应商旨在为用户提供更好的区块链服务，因此 BaaS 服务商比区块链底层技术提供商更注重与垂直行业的对接，提供合理的智能合约模板、良好的账户体系管理、良好的资源管理工具和定制化的数据分析和报表系统。

[9] Algorand 共识算法由图灵奖获得者 Silvio Micali 教授提出。

来源：中国信息通信研究院，2018 年 8 月

图 3 BaaS 架构图

现阶段，在后台数据存储、应用数据分析、移动终端、应用发布、信息识别等方面都有 BaaS 服务供应商支撑。以云计算平台为依托，区块链开发者可以专注于将区块链技术应用到不同的业务场景，帮助用户更低门槛、更高效地构建区块链服务，同时推动自有产业转型升级，为客户创造全新的产品、业务和商业模式。

3. 性能方面，跨链及高性能的需求日益凸显

让价值跨过链和链之间的障碍进行直接的流通是区块链越来越凸显的需求之一。跨链技术使区块链适合应用于场景复杂的行业，以实现多个区块链之间的数字资产转移，如金融质押、资产证券化等。目前主流的跨链技术包括：公证人机制（Notary schemes）、侧链/中继（Sidechains/relays）和哈希锁定（Hash-locking）。

表 7 跨链技术对比

类别	公证人	侧链/中继	哈希锁定
跨链方向	双向	双向/单向	双向
资产交换	支持	支持	支持
资产转移	支持	支持	不支持
信任	需要第三方	不需要	不需要
类型	协议	技术架构	算法
难度	中等	困难	容易
案例	Ripple	BTC relay Poldadot COSMOS	Lightning network

为了提高区块链系统的吞吐量，区块链技术和学术专家提出多种高性能方案，如下表 8 所示。

表 8 高性能方案对比

类别	DAG	并行	减少共识节点数
优化层面	拓扑	架构	共识
安全性	高	高	可能降低
资源消耗	低	低	低
扩展能力	好	好	一般
难度	较难	中等	保证安全性方案较难
性能	高	高	中
案例	IOTA Byteball Hashgraph	Ethereum（分片） TrustSQL（子链） Fabric（多通道）	Algorand BitcoinNG PoS

第一类高性能方案是改变块链式拓扑结构为基于交易的有向无环图（Directed Acyclic Graph，简称 DAG）。在这种拓扑结构下，交易请求发起后，广播全网确认，形成交易网络，无打包流程，交易可以从网络中剥离出来或者合并回去。基于 DAG 的设计没有区块的概念，扩容不受区块大小的限制，其可伸缩性取决于网络带宽、CPU 处理速度和存储容量的限制[10]。这种拓扑结构可以应对安全问题、高

[10]IOTA 白皮书中首次提出了缠结（Tangle）区块链，它便是一种有向无环图（DAG），但其架构不仅存在双花的风险，还存在伪造数字签名的风险。字节雪球（Byteball）为了解决双花问题，在 IOTA 的 DAG 的基础上，提出了主链（Mainchain）的概念，并通过见证人的方式实现了主链选择算法，有效的解决了 DAG 的双花问题。

并发问题、可扩展性问题和数据增长问题，以及适应小额支付场景。

第二类高性能方案是改变共识策略，通过减少一次参与共识的节点数量以提高吞吐量。这类方案中，为了提高性能，尽量在不影响安全的前提下减少参与共识的节点数，用算法控制一次参与共识的节点不被提前预知。虽然这种方案可以提高性能，但保证安全性的策略实现起来难度较大。

第三类高性能方案是通过提高系统横向扩展能力来提高系统整体吞吐量，代表有分片、子链、多通道等技术。对于这类技术，片区内、子链内、通道内需保持数据同步，片区间、子链间、通道间则是异步的。分片技术（Sharding）是把整个 P2P 网络中的节点分为若干相对独立的片区，以实现系统水平扩展。分片的情况下，通过把交易导引至不同节点，多个网络片区并行分担验证交易的工作。目前的分片策略包括网络分片（Network Sharding）、交易分片（Transaction Sharding）和计算分片（Computational Sharding）。子链技术是在主链上派生出来的具有独立功能的区块链，子链依赖主链而存在，并且可以定义自己的共识方式和执行模块。通过定义不同的子链，系统的可扩展性、可用性和性能均得到提高。多通道技术是系统中多个节点组成一个通道，每个节点也可以加入不同的通道中，通道之间互相隔离，通过锚节点互相通信。多通道技术可以消除网络瓶颈，提高系统可扩展性。

4. 共识方面，共识机制从单一向混合方式演变

共识机制在区块链中扮演着核心的地位，决定了谁有记账的权利，

以及记账权利的选择过程和理由，因此一直是区块链技术研究的重点。常见的共识机制包括 PoW、PoS、DPoS、拜占庭容错等，根据适用场景的不同，也呈现出不同的优势和劣势。单一共识机制，各自有其缺陷，例如 PoS 依赖代币且安全性脆弱，PoW 非终局且能耗较高。为提升效率，需在安全性、可靠性、开放性等方面进行取舍。区块链正呈现出根据场景切换共识机制的趋势，并且将从单一的共识机制向多类混合的共识机制演进，运行过程中支持共识机制动态可配置，或系统根据当前需要自动选择相符的共识机制。

表 9　共识机制的适用场景

场景	共识机制	算法举例
不可信环境、节点数未确定	权益类	PoW，PoS，DPoS
不可信环境、节点数已确定	拜占庭类	PBFT 等
可信环境、节点数未确定	非拜占庭类	Raft 等
可信环境、节点数已确定	消息分发机制	Kafka 等

5. 合约方面，可插拔、易用性、安全性成为发展重点

智能合约应用是否丰富，取决于智能合约自身及其所在区块链对于智能合约应用的支撑能力，而智能合约的开发和执行效率则取决于开发语言和执行虚拟机。在目前的生态系统中，智能合约的开发语言不够规范，为了适应智能合约，需要创造新的合约语言或为现有语言增加形式更为严格的规范和校验。智能合约在轻量级的执行环境中将实现快速的启动时间和较高的执行效率。

智能合约的发展方向包括如下几点：1）可插拔的执行环境架构：默认的执行环境应该不提供持久化存储，让合约默认是一种类似于微

服务的无状态函数，从而直接进行并发处理。2）明示化的调用关系：即只提供静态调用的功能，从而使得程序的调用关系可以在运行它之前就整理清楚。3）可链外存储的合约代码：通过链上存储散列值、链外存储合约代码实现存储空间的扩展性。4）低耦合度的设计：降低合约语言、执行环境、区块链之间的耦合度，提高智能合约系统的通用性；5）完整安全的防护体系：代码定型与发布时的验证与检查，节点在执行合约中的动态验证，合约执行完毕的合理性判断，相关利益方的申诉机制与自动判决技术。

三、区块链发展现状

（一）各国竞相布局区块链产业制高点

区块链正在被各国认可，并在多领域积极探索技术的推广应用。2018 年 1 月 22 日英国技术发展部门（Innovate UK）相关人士表示，英国将投资 1900 万英镑用于支持区块链等新兴科技领域的新产品或服务。2018 年 2 月 14 日美国众议院召开第二次区块链听证会，“拥抱技术”与“不要封杀”成为共识。韩国央行鼓励区块链技术，韩国唯一的证券交易所 Korea Exchange（KRX）也宣布开发基于区块链技术的交易平台。澳洲在多领域积极探索区块链技术，澳大利亚邮政将区块链技术应用于身份识别。迪拜建立全球区块链委员会，并成立含 Cisco、区块链初创公司、迪拜政府等 30 多名成员的联盟。

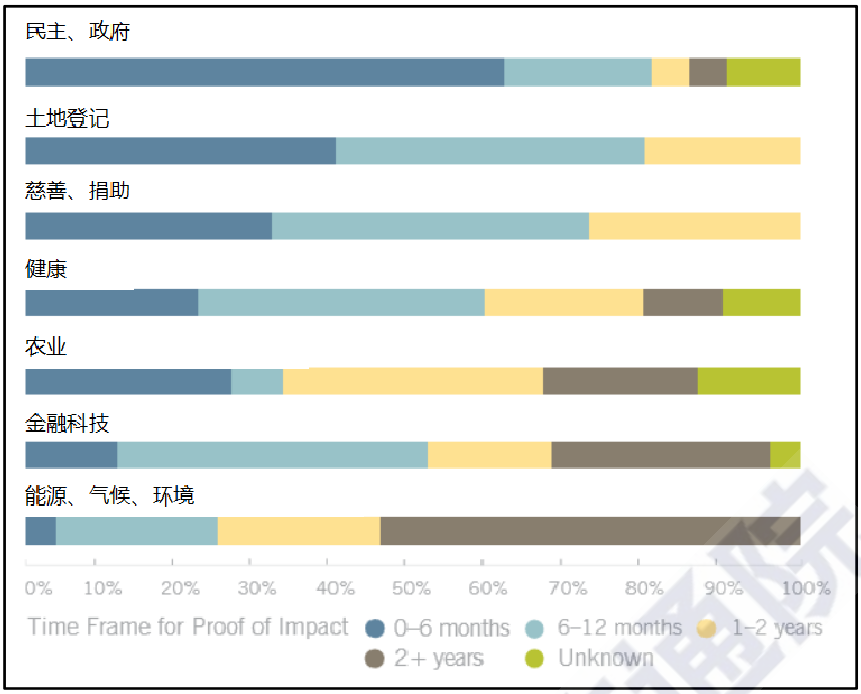
我国超前布局前沿阵地，积极探索基于区块链的行业应用。2016 年区块链首次被列入国务院印发《“十三五”国家信息化规划》。2018 年 6 月，工信部印发《工业互联网发展行动计划（2018-2020 年）》，

鼓励推进边缘计算、深度学习、区块链等新兴前沿技术在工业互联网的应用研究。2018 年 5 月 28 日，习近平总书记在两院院士大会上的讲话中指出，“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。”

各地纷纷推出鼓励政策，区块链项目竞相上马。截至 2018 年 5 月底，北京、上海、广东、河北（雄安）、江苏、山东、贵州、甘肃、海南等 24 个省市或地区发布了区块链政策及指导意见，多个省份将区块链列入本省“十三五”战略发展规划，开展对区块链产业链布局。随着区块链技术在应用层面的不断拓展,各地纷纷推出区块链鼓励政策，越来越多区块链技术企业选择到落户政策优惠地区发展。

（二）区块链与实体经济融合成为主旋律

从行业发展看，区块链的技术正在走向融合，这使得区块链产业逐渐走向细分。按照区块链产业上下游结构，区块链产业自下而上可以划分为四类：底层基础设施及平台开发、技术扩展及通用型服务、行业应用、产业周边服务。相应的产品归属，可进一步细分为链、客户端、应用等不同类型。继以数字货币为代表的区块链 1.0 之后，区块链 2.0 所加入的智能合约等相关技术基础已具备承载部分垂直行业应用及通用应用开发的能力。随着区块链革新升级，与云计算、大数据等前沿技术深度融合、集成创新，将促进区块链技术在医疗、司法、工业、媒体、游戏等各个细分领域的商业探索应用。区块链“脱虚向实”趋势明显，行业生态链已经初步成形，正在从各个领域助力实体经济高质量发展。



来源：斯坦福大学《区块链项目研究报告》，2018 年 7 月

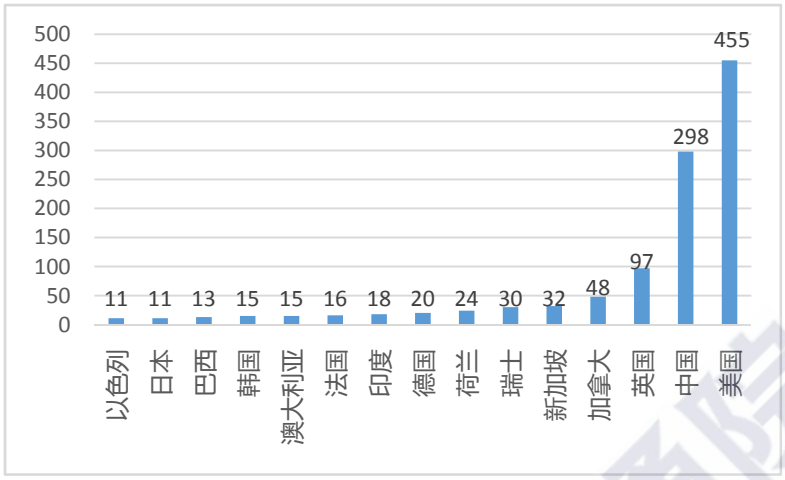
图 4 区块链应用成熟时间[11]

从公司数量看，中国的区块链企业数量仅次于美国。根据中国信息通信研究院调查，如图 5 所示目前全球共有 1242 家公司[12]活跃在区块链产业生态中，美国、中国、英国区块链企业数量分列前三位。从行业分类来看，如图 7 所示从事加密货币相关技术与服务的公司数量最多（467 家，占比 37.60%），随后是区块链技术和软件平台研发公司（201 家，占比 16.18%）。根据公开资料显示，截至 2018 年 6 月我国区块链企业数量排名前五的城市依次为北京、上海、深圳、杭州、广州，其中北京以 175 家区块链企业排名第一，详见图 6。值得关注的是，通过政府支持、社区协作的方式，一批东南亚（新加坡、越南、泰国等）区块链新势力在区块链 2.0 时代陆续崛起，在监管沙盒的创

[11]斯坦福大学对全球 193 个区块链项目研究显示，34%的项目在 2017 年及以后启动，74%的项目仍然处于试验或验证阶段，55%的社会类项目预计最早在 2019 年能产生效益。

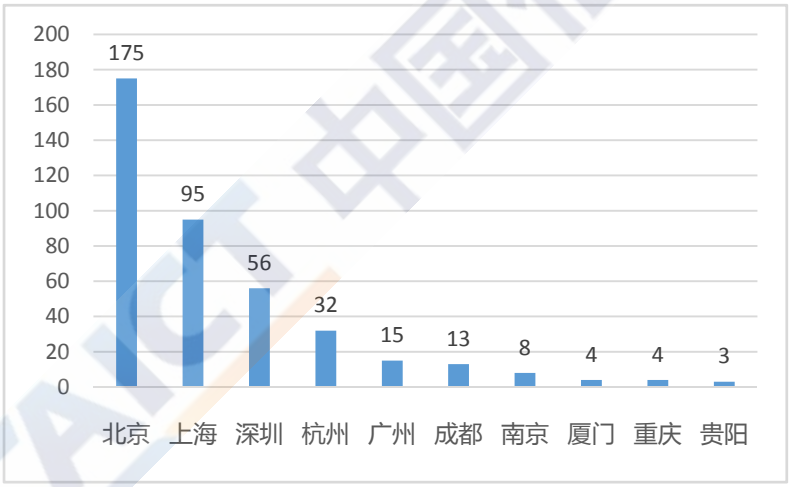
[12]区块链公司范围：1）以区块链技术、平台为主要产品和服务；2）核心业务主要依靠区块链技术的公司；3）业务专注于区块链产业的其他公司，如：培训、媒体、投资等。

新孵化模式下，孕育出一系列以跨链、多链-子链等新技术为主的区块链互操作体系，有可能争夺未来区块链领域话语权。



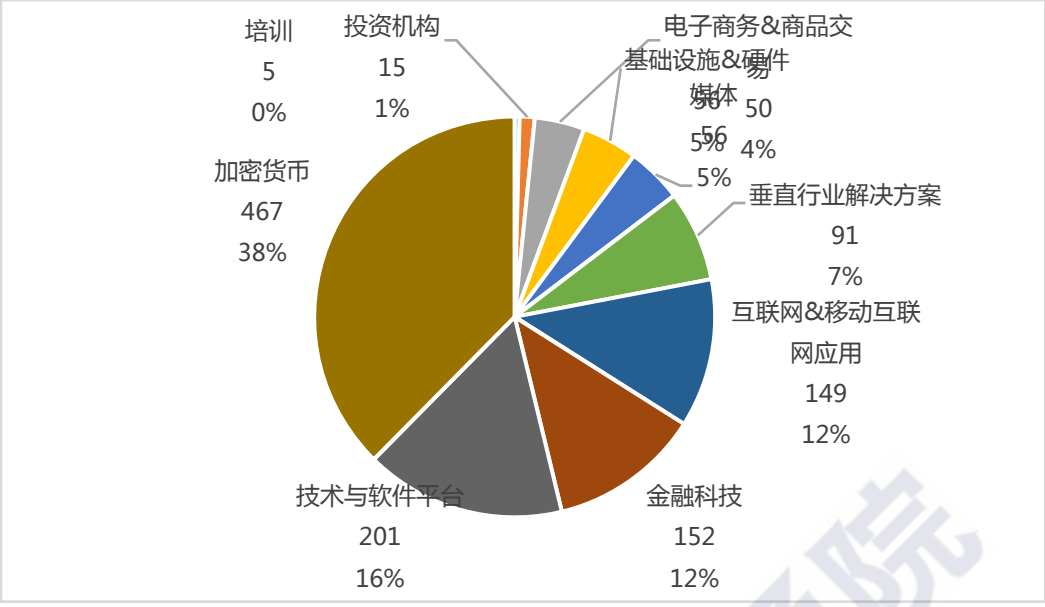
来源：中国信息通信研究院整理，2018 年 6 月

图 5　全球各国区块链企业数量



来源：中国信息通信研究院整理，2018 年 7 月

图 6　我国区块链企业数量分布图



来源：Cbinsight&Crunchbase，2018 年 7 月

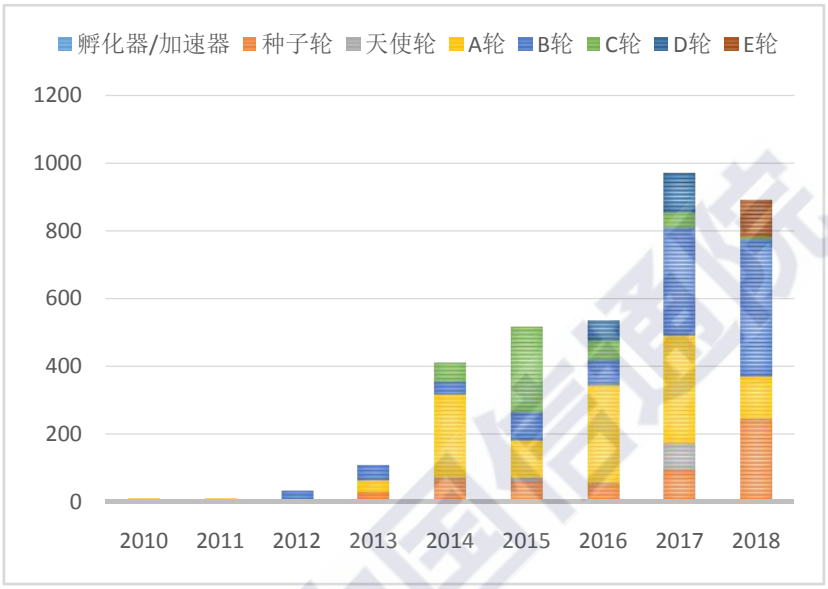
图 7 各行业区块链企业数量

从投融资看，全球区块链产业融资加速，国内监管政策加码。一方面，如图 8 所示 2009 至 2018 年，区块链初创企业融资（非 ICO[13]融资）总额达到 48.1 亿美元。从地域分布来看，美国共有 25.42 亿美元融资，中国 6.02 亿美元位居第二位，加拿大 2.47 亿美元居第三位。另一方面，ICO 成为新的融资渠道，2018 年上升势头依旧不减。2014 至 2018 年，ICO 累计融资达到 180.9 亿美元，远超过同期区块链企业通过传统途径融资金额。其中，区块链初创公司 EOS 在 2018 年 6 月 1 日完成 42 亿美元融资，成为迄今为止最大规模 ICO 融资。在中国监管部门 2017 年 9 月 4 日明令禁止 ICO[14]、关闭国内虚拟货币交易所几个月后，2018 年年初 ICO 又以“出口转内销”或花样变形的方式暗度陈仓，通过代理投资等中间商进行相关募资活动。针对这类情况，

[13] ICO：Initial Coin Offering，源自股票市场的首次公开发行（IPO）概念，是区块链项目首次发行代币，募集比特币、以太坊等加密数字货币的行为。

[14]为防范系统性金融风险，中国人民银行等七部委于 2017 年 9 月 4 日发布《关于防范代币发行融资风险的公告》，将代币发行融资定性为一种未经批准的非法公开融资行为。

央行营业管理部、中国互联网金融协会等机构频频发声，国内的监管措施持续加码，2018 年 8 月 24 日中国银保监会与公安部等五部委发布《关于防范以“虚拟货币”“区块链”名义进行非法集资的风险提示》。“规范币，鼓励链”，是当前我国区块链发展的主旋律。

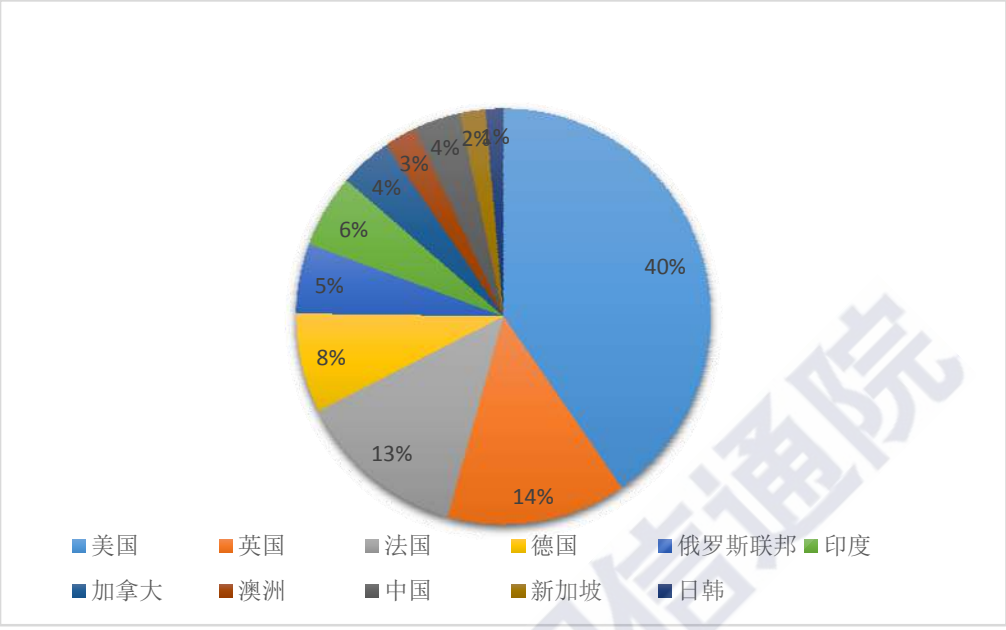


来源：Cbinsight&Crunchbase，2018 年 7 月

图 8　区块链各阶段融资轮次分布

从人才供给端看，区块链人才增长速度尚不能满足市场需求。根据领英 2018 年 2 月数据显示，全球对于区块链人才的需求量从 2015 年开始出现增长，在 2016-2017 年经历了爆发式的显著增长，但目前来看，其占全球人才市场需求总量的比重还非常低。近年来对于区块链人才需求增长最快的行业是计算机软件行业，其次是金融服务及保险行业。从 2015 年到 2017 年，在领英档案上标注有区块链相关技能的人才数量增长了近 19 倍，但人才总量仍然较少，仅相当于领英平台上全球 AI 人才数量的 2%左右。从当前区块链人才的全球分布来看，美国占据 25%，其次是印度 7%以及英国 6%。美国的相关人才更多集中在大纽约地区 24%，旧金山湾区 21%及大洛杉矶地区 10%。而

中国相关人才基数还较小，从目前的分布来看，主要集中在北京、上海、深圳和杭州。



来源：领英，2018 年 2 月

图 9 全球主要国家对区块链人才需求比例

（三）区块链技术创新日趋活跃

越来越多国外公司开始加入区块链源代码的开发和贡献，根据 GitHub 平台数据显示，从 2010 年各个公司开发的区块链项目占所有项目的比例不超过 1%，到 2017 年各个公司开发的区块链项目占比达到 11%，形成了围绕比特币(Bitcoin)、以太坊（Ethereum）、超级账本（Hyperledger）、瑞波（Ripple）等多个核心开源平台的公司及个人合作开发生态，同时国际上多个区块链行业联盟也应运而生，例如 R3 区块链联盟（Corda）、Linux 基金会支持的超级账本 Hyperledger 区块链联盟、企业级以太坊联盟（EEA）等。

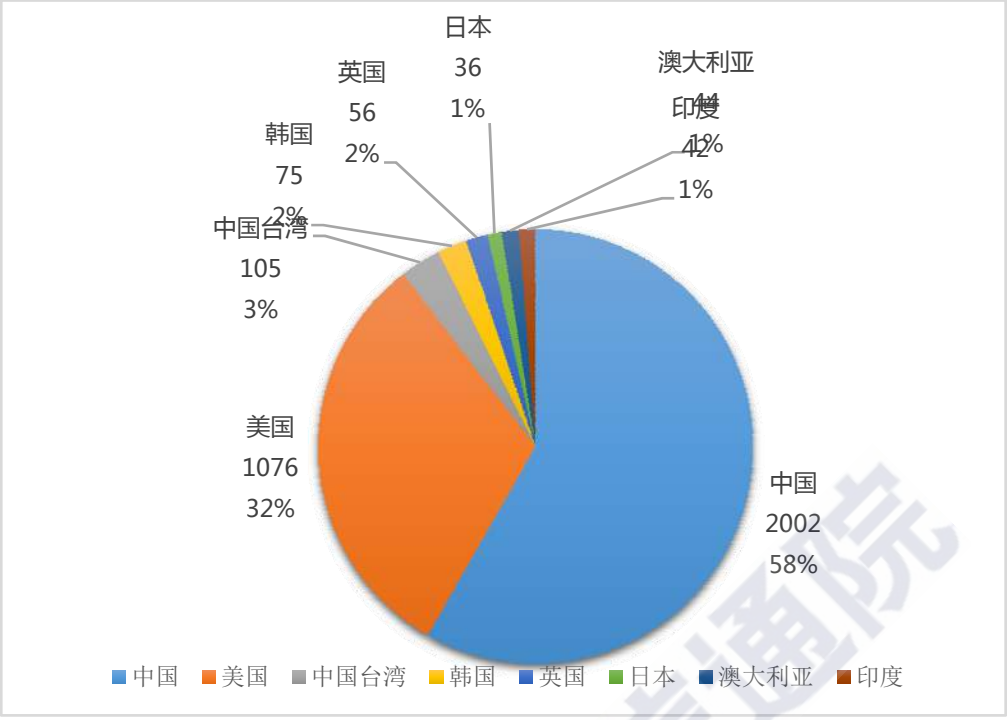
开源代码方面，中国的代码贡献量仅是美国的三分之一。美国作为传统的科技高地，围绕跨链技术、多方可信计算、可信预言机、数字身份、隐私保护、智能合约语言等领域在全球开源社区引领技术走

向。中国自主技术平台不多，超过 90%的区块链技术平台是使用国外开源技术（如超级账本、以太坊）的产品或者衍生产品。与专利数量增长势头不同的是，如表 9 所示相比 2016 年，中国 2017 年开源代码贡献量显著地下滑，美国 2016 年的区块链开源项目数为 2538 个，2017 年仅有 1728 个；中国 2016 年的区块链开源项目数为 834 个，2017 年仅有 527 个，均不及美国的 1/3。由此可见，我国的区块链发展更多关注在应用层面，在开源代码核心算法方面仍与国际领先水平存在明显差异。

表 10 中美区块链项目数量对比（单位：个）

国家/地区		2014 年	2015 年	2016 年	2017 年
中国	全国	263	274	834	527
	北京	67	76	225	137
	上海	62	35	134	119
美国	全国	1906	1920	2538	1728
	旧金山	389	318	227	150
	纽约	150	161	208	147

专利申请方面，我国在区块链领域的专利申请数量已居全球首位。根据对 Incopat 平台数据的整理分析，截止 2018 年 7 月，全球区块链相关专利申请量达到 3731 件，2017 年区块链专利申请量较 2016 年增长 87%。其中如图 10 所示，中国是目前区块链专利申请量最多的国家，累计区块链专利申请量达到 2002 件，美国为 1076 件。目前，全球区块链专利申请中加密货币相关专利申请量达到 376 项，智能合约专利申请量为 286 项。在几项共识算法中，PoW 算法研发最早，专利申请量多于其他算法。从地区分布来看，美国在加密货币、智能合约、PoW 算法领域专利申请量较多。我国在智能合约领域专利申请量最多。

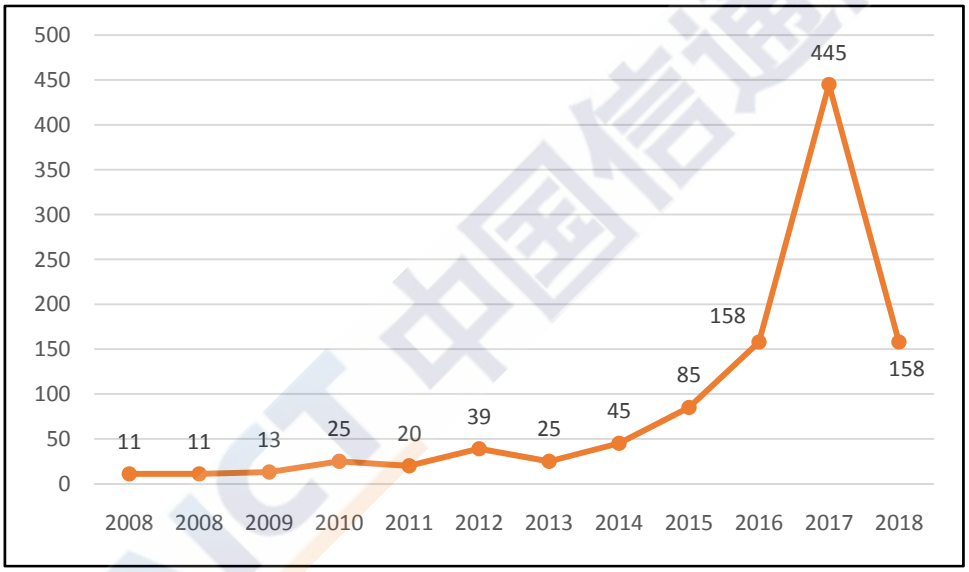


来源：Incopat，2018 年 7 月

图 10　各国区块链专利分布

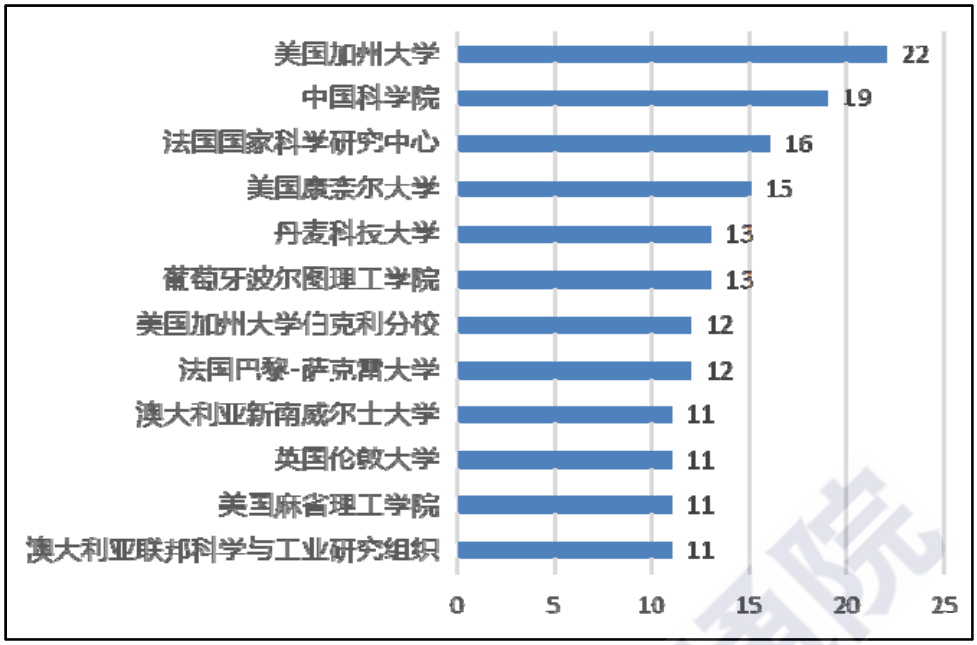
科研方面，国外研究更加重视核心问题的技术突破，而国内更加关注区块链应用的业务场景。根据 2018 年 7 月中国信息通信研究院调查数据显示，全球科研机构对区块链的关注度从 2015 年开始提升，2017 年 Web of Science 收录的有关区块链的核心论文数量达到 445 篇，比 2016 年增长 181.6%，如图 11 所示。但从绝对数量来看，总体数量仍然较低，区块链在学术研究领域仍处于早期阶段。从核心论文发布机构分布来看，现阶段各国研究机构进展相差不大，美国加州大学、中国科学院发布论文数量暂时领先于其他机构。法国、丹麦、葡萄牙、澳大利亚、英国的科研机构也在积极开展研究。截至 2018 年 4 月，如图 12 所示，全球已有包括美国麻省理工学院（MIT）、加州大学伯克利分校、英国帝国理工等在内的 27 所大学明确设立区块链相关课程或开设相关培训班，开展区块链的相关研究。国外主流的院校围绕性能、技术、应用等多个视角涌现了一批学术机构项目团

队，产学研一体化的形式形成良性的循环造血能力。国内方面，除部分行业机构开展区块链训练营、区块链总裁班等围绕科普、应用为主题的教育工作外，各高校也逐步在区块链领域发力。中央财经大学于 2016 年 7 月，设立了国内第一个区块链实验室，并开设区块链相关课程。2018 年 4 月，西安电子科技大学开设《区块链技术原理与开发实战》课程，同期浙江大学计算机学院开设区块链研究中心。目前我国在关键技术、核心问题方面仍缺少系统性的研究，尚未形成产学研用联动的学术生态。



来源：Web of Science，2018 年 7 月

图 11　各年度区块链核心论文发布数量



来源：Web of Science，2018 年 7 月

图 12　区块链核心论文发布量机构排名

（四）区块链标准体系加速构建

来自世界经济论坛调查报告的预测，7 年后全球 GDP 总量的 10%将基于区块链技术保存。为推动区块链行业良性发展，多个国际组织纷纷积极探索区块链标准体系的建设。2017 年 2 月国际电信联盟标准化部门（ITU-T）决定启动 F.DLS（分布式账本服务需求）标准研究，2017 年 5 月成立了 ITU-T FG DLT 焦点组，2018 年 7 月 ITU-T SG16 全会成立了新的研究课题 Q22（Distributed ledger technologies and e-services，分布式账本技术和电子服务）。中国是 ITU-T 区块链标准研究的主要贡献者，中国信息通信研究院等单位牵头设立的区块链需求、参考架构、评测基准等四项国际标准，得到世界各国积极支持。国际标准化组织（ISO）也于 2016 年 9 月成立了区块链和分布式记账技术委员会（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区块链和分

布式记账技术领域的标准化相关问题。此外，万维网联盟（W3C）、电气和电子工程师协会（IEEE）、国际互联网工程任务组（IETF）等组织也在积极关注区块链的标准化问题。

来源：BSI &RAND Europe，2017 年 5 月

图 13　区块链标准 SWOT 分析

区块链技术标准将成为加速推动整个区块链产业发展的突破口，然而各方对区块链标准体系尚未达成一致共识。正如英国标准协会与兰德公司 2017 年联合发布的《分布式账本与区块链标准所面临的挑战、机会与展望》报告[15]中所述，可信安全已经成为区块链技术标准未来发展的关键要素，详见图 13。当前，我国正在积极推动区块链产业透明度，构建包含可信区块链标准在内的标准化体系建设。经过长期跟踪研究，结合在云计算、大数据等方面已有的标准化思路，中国信息通信研究院提出了国内首个可信区块链系列标准，在中国通信

[15]《Distributed Ledger Technologies/Blockchain：Challenges, opportunities and the prospects for standards》，BSI & RAND EUROPE, May 2017

标准化协会（CCSA）启动 2 项行业标准。目前已经发布 3 个可信区块链评测标准，同时正在开发 TrustedBench 区块链基准测试工具。可信区块链评测标准包含 19 类指标和 95 个评测点，涵盖功能、性能、安全等各个方面。2018 年 4 月，中国信息通信研究院联合 158 家单位发起“可信区块链推进计划”，共同推动区块链技术研发与应用落地，促进行业良性发展。

四、区块链面临的挑战

（一） 技术成熟层面存在隐患

目前，区块链技术在系统稳定性、应用安全性、业务模式等方面尚未成熟，主要存在五类问题：从性能上看，无法同时满足“高效低能”、“去中心化”和“安全”这三个要求，区块链上可进行的交易吞吐量不高，高频次业务需求难以得到满足；从能耗上看，工作量证明等共识算法能源消耗大、成本高，使得区块链浪费大量全网计算力和财力；从生态上看，目前区块链产品不成熟，缺乏相关的开发、集成和运维体系，标准缺失，我国在区块链开源平台上缺少话语权和影响力；从安全上看，隐私保护、有害信息上链、智能合约漏洞、共识机制和私钥保护、51%算力攻击、密码学算法安全等问题，令区块链面临着平台安全、应用安全的严峻形势；从监管上看，加密技术对合法监听、客户识别、反洗钱等监管手段带来不小挑战，同时区块链的多方协同治理也对监管提出更高要求。

（二） 应用场景模式尚不明确

伴随着“区块链”风口正盛，不仅 BAT 这样的产业科技巨头纷纷加码，越来越多的传统企业也宣布正式涉足区块链；与此同时，由于创业成本低，投资门槛也不高，大量创业公司也争相进入市场。然而，一方面，技术的不成熟制约了商业的应用落地，目前隐私保护算法、共识机制等区块链核心技术虽种类较多，但是普遍来说还不具备商业可用性。另一方面，区块链的应用模式仍在探索中，还没有找到真正的“杀手级”应用，区块链的“不可替代”优势还未体现。区块链不是必须的，并不适用于所有领域，其技术的突出特点使其对无风险、高价值、易实现的场景具有更高的应用价值。

（三） 行业专业人才相对稀缺

区块链技术是一门多学科跨领域的技术，包含了操作系统、网络通讯、密码学、数学、金融、生产等，我国目前在交叉学科、领域方面尚有不足。区块链的技术研发主要集中在 Go、JavaScript、C 和 C++ 等编程语言，新型的智能合约采用 Haskell、Ocaml、Rholang 等新型函数式编程语言，全球人才市场中具有相关语言资深研发经验的技术人才有非常大的缺口。与研发技术人才相比，区块链底层系统架构设计人才要掌握多项交叉学科的专业技能，并深入理解区块链底层设计原理，兼备系统架构设计的经验，更要懂应用场景的具体业务逻辑，可谓“一将难求”。虽然目前已有部分高等院校展开交叉学科教育、区块链专项技能学科设定，但专业人才在市场上仍十分稀缺。

（四） 相关法律法规有待完善

虽然比特币、以太坊已成为讨论热点，但该领域尚缺乏明确法律

法规，对区块链技术的治理、监管和标准等仍不健全，主要体现在两方面：一是法律主体不明确。区块链中系统维护和治理主体不明确，在区块链系统中不存在一个为整个系统承担责任的中心机构，缺乏中心化的法律实体，也使得传统法律规则难以在事后对分布式账本系统进行监管，要实现有效监管必须围绕事前的技术规则来推进。二是链上规则不明确。在区块链参与者的语境中，代码即“法律”，但法律不是代码。与法律上规定权利义务的方式不同，区块链技术规则直接决定了区块链系统的安全性和稳定性，并直接影响着每一个参与者的权利和义务。由于链上规则的不明确，会引发关于智能合约漏洞、Token 发行合规性、个人信息保护等的系列问题。

五、发展措施和建议

（一）引导社会客观理性认识

积极引导社会和公众，客观理性地看待区块链价值，一方面要充分认识到区块链技术对于建立信任机制、传递信息和价值的重要意义，另一方面要避免盲目夸大区块链技术对于传统行业的颠覆作用，警惕泡沫日趋膨胀。注意防范因为区块链应用可能引发的对传统机构管理、商业运营等模式的冲击，以及操作陷阱、技术垄断等潜在风险。促进区块链相关媒体声音的正本清源，营造行业风清气正的氛围，为区块链等颠覆技术营造良好的传播环境。

（二）加强核心关键技术研究

加快推进包括共识机制、密码学算法、跨链技术、隐私保护等在内的区块链核心关键技术研发，开展产品开发和集成测试。支持和培

育开源软件，打造自主开源社区，构建软硬件协同发展的生态体系。顺应技术产业实际需求，适度推进标准制定。搭建基础研究和交叉学科研究的创新平台，培养学科交叉、知识融合、技术集成的复合型人才。建立健全高校、研究机构、行业协会、智库等的协同推进机制，加强在技术攻关、瓶颈突破、标准制定等方面的协调配合。

（三）推动与实体经济深度融合

推动区块链技术与实体经济深度融合，在融合过程中要善于发掘、突出区块链技术在建立信任关系、提高协作效率、促进数据共享、提升政府穿透式监管能力等方面不可替代的作用。探索数字经济创新模式，实现行业供需对接，服务实体经济转型升级。选择重点领域，组织开展区块链应用的概念验证、试验平台、先导应用示范和评估，培育行业龙头、领军企业和产业生态。结合良好应用案例示范，面向行业机构、企业开展区块链技术与应用培训，推广应用落地经验，规避潜在应用风险。

（四）完善区块链发展政策环境

遵循技术发展规律，从政策层面做好体系化布局。深入研究区块链对个人信息保护、数据跨境流动等方面的影响，探讨区块链在底层核心技术、中层应用逻辑和上层信息管控等方面的监管问题。积极促进区块链系统中参与主体的信息披露，构建智能合约的合规审查和审计机制，推动行业自律。同步开展区块链相关政策和法律法规研究，探索制定区块链技术和应用的监督机制和认证体系，为产业健康发展营造良好环境。

中国信息通信研究院

地址：北京市海淀区花园北路 52 号

邮政编码：100191

联系电话：010-62304839

传真：010-62304980

网址：www.caict.ac.cn

可信区块链推进计划

地址：北京市海淀区花园北路 52 号

邮政编码：100191

联系电话：010-62300249

传真：010-62304980

网址：www.trustedblockchain.cn