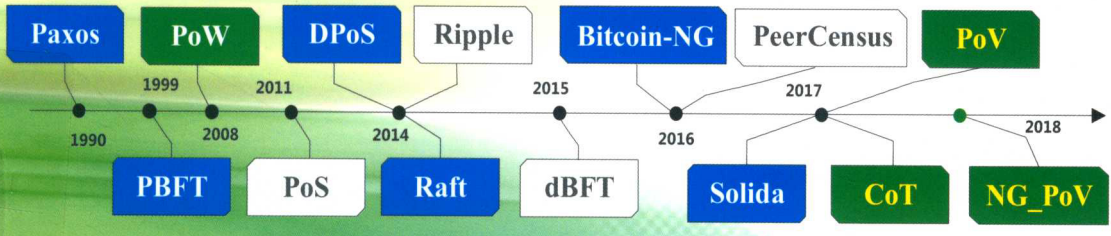
区块链

共识算法原理及应用

——以多标识网络体系管理系统为例

李挥　王菡　著



科学出版社

区块链共识算法原理及应用

——以多标识网络体系管理系统为例

李 挥 王 菡 著

科学出版社

北 京

内 容 简 介

区块链技术是一种全新的分布式基础架构和计算方式，本书着重阐述区块链系统中的共识算法理论及其场景应用。全书共分 7 章。第 1 章介绍区块链的发展过程和基本知识。第 2～5 章介绍传统分布式系统的一致性算法和典型区块链系统的共识机制，并详细介绍基于投票和信任的两种共识算法。第 6 章介绍融合区块链的拟态分布式安全存储系统。第 7 章介绍基于联盟链共识的共管共治多标识网络体系管理系统。

本书可作为高等院校计算机专业本科生、研究生的教材和参考书，也可作为计算机、软件工程等领域工程技术人员的参考书。

图书在版编目（CIP）数据

区块链共识算法原理及应用：以多标识网络体系管理系统为例 / 李挥，王菡著. —北京：科学出版社，2019.12

ISBN 978-7-03-063341-5

Ⅰ. ①区… Ⅱ. ①李… ②王… Ⅲ. ①互联网络-应用-研究 ②智能技术-应用-研究 Ⅳ. ①TP393.4 ②TP18

中国版本图书馆 CIP 数据核字（2019）第 256318 号

责任编辑：赵艳春 / 责任校对：王萌萌

责任印制：师艳茹 / 封面设计：迷底书装

科学出版社 出版

北京东黄城根北街 16 号

邮政编码：100717

http://www.sciencep.com

天津文林印务有限公司 印刷

科学出版社发行 各地新华书店经销

*

2019 年 12 月第 一 版 开本：720×1 000 1/16

2019 年 12 月第一次印刷 印张：13 1/4

字数：255 000

定价：119.00 元

（如有印装质量问题，我社负责调换）

此为试读，需要完整PDF请访问：www.ertongbook.com

序

区块链技术与比特币是“孪生姐妹”，今年是比特币系统诞生十周年。作为首个完全去中心化的公众链加密数字货币——比特币的底层技术是互联网诞生以来最大的一次技术革命，它将对人类社会产生全方位的冲击，包括人类经济、政治、社会的各个领域。回顾一下互联网的发展所经历的若干阶段，从最初只是专业人士用于科研圈的文件信息交流网，到发明 Web 技术用于老百姓的电子商务及门户网站消费型网络，再后来由人人互联到人物或物物互联的万物互联物联网，近年正向价值制造和价值创造的生产型网络——工业互联网进化；可以看出网络技术已经成为人类重要的生活和生产基础设施，但是到目前为止它们的一个共同特点是网络运营或管理模式都需要一个中心化的机构来管理运营，所以它们的重要共同特点是中心控制的网络。

中心化网络的缺陷是维护其控制管理中心需要高额的成本；它使得行业的垄断骤然产生达到赢者通吃的地步；中心机构还可能泄露或滥用用户的数据或隐私信息。区块链技术正是构建去中心化不需要第三方的、很低成本或不需成本的信任关系，故是传递价值的互联网。

区块链共识算法是区块链的核心技术，目前专门介绍共识算法的专著并不多，该书填补了这个空缺，它介绍了分布式一致性技术的历史及今天。前 3 章作者先介绍了早期的传统分布式一致性算法，包括分布式同步系统和异步系统共识，进而介绍 20 世纪 90 年代提出的著名状态复制协议 Paxos；然后介绍了近十年来伴随比特币系统上线以来主流的共识算法，包括工作量证明 PoW，及其升级版本 PoS，DPoS；联盟链共识算法的基础算法 PBFT。第 4 章和第 5 章介绍了作者提出的并获得美国专利授权的基于投票的联盟链共识算法 PoV，基于信任的共识算法 CoT，并介绍算法组成及其共识流程，算法实现细节及其性能分析。第 6 章介绍了 PoV 在拟态防御分布式安全存储系统中的应用；第 7 章介绍了基于 PoV 提出的多边共治的多标识未来网络体系 MIN 及其在大规模运营商网络上原理验证，MIN 入选 2019 年乌镇世界互联网大会领先技术成果，从侧面印证了学术与产业界对该技术的期待。

该书对区块链共识技术从广度和深度上进行了叙述和探究，是该领域的决策者、从业者、研究生和高年级本科生极具新意和实用价值的参考资料。

郑纬民

2019 年 12 月初于清华园

前　言

区块链是一种在不可信网络中传输可信信息、实现价值传递的分布式账本，而其核心共识机制保证了众多分布式节点的数据达到一种较为平衡的状态，是保障区块链系统不断运行下去的关键。

本书对区块链共识领域进行全面的介绍，包括算法理论和场景应用。作为一类基于传统分布式一致性理论提出的、具有当前区块链系统特色的分布式共识，区块链共识发展至今，主要存在两个方向：一是 BFT 类共识及其在区块链系统中的应用；二是 PoX 类共识(包含著名的 PoW 共识)及其在区块链系统中的应用。本书侧重于介绍区块链系统中常用的共识算法的设计思想并从理论上进行分析。同时，为了有助于读者理解区块链共识的发展和应用，本书详细介绍区块链共识在拟态安全存储及多标识网络体系管理系统中的实践应用。

本书共分 7 章，李挥负责本书的规划、统稿及第 1、4、6、7 章的撰写，王菡负责第 2、3、5 章的撰写。国家重大科技基础设施未来网络北大实验室的李科浇、王贤桂、林志力、黄健森、徐睿、张昕淳、邢凯轩、王博辉等参与了其中部分章节素材的准备，张纪杨、林志力、黄健森、宁崇辉、黄婷、谢鹏程、刘馨蔚、綦九华、白永杰、于海洋等参与了系统开发工作，在此表示感谢！

本书的研究成果受到国家重点研发计划网络空间安全重点专项“拟态防御基础理论研究”(2016YFB0800101)、国家重点研发计划网络空间安全重点专项“先进防御设备与系统研制”(2017YFB0803204)、佛山市科技创新团队项目(2018IT100082)、国家自然科学基金面上项目“基于组合设计的高效分布式存储编码研究”(61671001)、国家重大科技基础设施——未来网络试验设施(发改高技【2016】2533 号，【2018】775 号)、广东省大数据计算与存储融合的关键技术研发(GD2016B030305005)、深圳市信息论与未来网络体系重点实验室(深科技创新【2016】86 号)(ZDSYS201603311739428)、深圳市融合网络播控关键技术工程实验室、深圳市 SDN 未来网络工程实验室、深圳市基础研究课题(JCYJ20170306092030521，JCYJ20150331100723974，JCYJ20140417144423192)和华为技术委托课题“未来网络 IDC 全域流量测量”(YBN2017125000)的资助。

由于作者能力有限，书中难免有不足之处，敬请广大读者不吝赐教。

作　者

2019 年 1 月

目　录

第 1 章　区块链基础

区块链是近年来最具革命性的新兴技术之一。区块链技术发源于比特币，具有以去中心化方式建立信任等突出特点，对金融等诸多行业来说极具颠覆性，有非常广阔的应用前景，受到各国政府、金融机构、科技企业、爱好者和媒体的高度关注。

1.1　区块链简介

区块链是由密码学串接并保存内容的串联交易记录(又称区块)。每一区块包含前一个区块的全部信息的散列(Hash，又称哈希)值，这样的设计使得区块内容具有难以篡改的特性。中本聪(Satoshi Nakamoto)于 2008 年，在“比特币白皮书”中提出区块链概念，并在 2009 年创立了比特币网络，开发出第一个区块，即创世区块。

1.1.1　区块链起源——比特币

2008 年 9 月，以美国投行雷曼兄弟(Lehman Brothers)的破产为开端，金融危机开始在美国爆发并迅速向全世界蔓延。为了应对危机，世界各国政府和中央银行采取了史无前例的财政刺激方案与扩张的货币政策，为由于自身过失而陷入困境的大型金融机构提供了紧急援助。但这些措施引起了大众对传统金融体系的广泛质疑，也动摇了大众对以国家信用为基础的货币体系的信任度。

2008 年 10 月，一位化名为中本聪的密码学研究者以电子邮件的形式向密码朋克(CypherPunk)联盟成员公开发表了一篇关于比特币的论文[1]，描述了一种无须第三方可信机构介入的点对点电子货币系统。中本聪首次提出了区块链的概念。2008 年 11 月，中本聪发布了比特币代码的先行版本。2009 年 1 月 4 日，中本聪在位于芬兰赫尔辛基的一个小型服务器上挖出了比特币的首个区块——创世区块，这也代表着比特币的诞生。中本聪将当天英国泰晤士报头版的标题“财政大臣站在第二次救助银行的边缘”写入了创世区块，不仅开创了货币非国家化理念的新纪元，同时表达了对旧金融体系的嘲讽。

从此，比特币成为区块链技术的第一个也是发展到目前规模最大、应用最广泛的系统。区块链技术作为比特币系统衍生出来的底层技术，被认为是有潜力颠覆金融服务、供应链管理、文化娱乐、智能制造、社会公益、教育就业等多个行业的一种综合性底层技术。

此为试读，需要完整PDF请访问：www.ertongbook.com

1.1.2　区块链定义

区块链指的是一种在对等网络(peer-to-peer networking，P2P networking，又称点对点网络)环境下，通过透明和可信规则，构建不可伪造、不可篡改和可追溯的块链式数据结构，来实现和管理事务(在比特币中称为交易)处理的模式[2]。根据人们早期对区块链的讨论，狭义上，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；广义上，区块链是利用块链式数据结构来验证和存储数据、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(smart contract)来编程和操作数据的一种全新的分布式基础架构与计算方式[3]。

1.1.3　区块链特点

在信息互联网时代，网络上的信息公开透明，但它们也因为可以被随意篡改而不能够完全地被信任，需要第三方可信机构为其真实性提供信任担保。一旦第三方平台倒闭，这种信任便化为泡沫，因此互联网上的数据难以有内生性的价值。但区块链的诞生为互联网上的数据重新赋予了一种可以被信任的价值，数据被存储于全球无数台机器节点之上，变得稳定、可信且不可篡改。区块链技术本质上是一种防篡改的、共享的分布式账本，网络中的所有成员节点共同维护账本，基于密码学技术而非外部信任，同时能够用链式数据结构完整地记录全部交易信息。因此，区块链被认为最有可能驱动实现信息互联网向价值互联网转变。区块链拥有三大显著特征：去中心化、不可篡改和去信任化。

1. 去中心化

区块链的网络体系采用了对等网络架构，节点之间地位对等，不存在超级管理节点，因而区块链具有去中心化的特点。不同于中央网络架构的客户端/服务器(client/server，C/S)服务架构，在对等网络中，每个节点既是服务器也是客户端，依靠用户群而不是中心服务器来交换信息。所有节点共同维护网络中的资源和服务，信息的传输和服务的实现都直接在节点之间进行，可以做到不需要中间节点和中间服务器介入。由于服务是分散在各个节点之间进行的，部分节点或网络遭到破坏对其他部分的影响很小，整个系统具有耐攻击、高容错的优点。另外，在对等网络中，数据价值交换的中间成本非常低，降低了中心化导致的资源成本和时间成本。

2. 不可篡改

区块链的数据组织结构采用了块链式数据结构并结合了纯数学加密算法，具有不可

篡改、不可伪造的特点。后写入的数据区块包含了先写入的数据区块的标识信息，任何数据都可以通过链式结构追本溯源地进行校验。链上任意数据的变化均会连锁式地引发后续数据的改变并以此来保证链上数据的正确性。同时，区块链使用密码学中的散列算法，利用 Hash 函数的不可逆向破解特性使得数据的伪造过程不可实现。因此，这样的结构不允许篡改或伪造已经被写入链上并确认过的数据，否则将触发连锁效应导致链上的数据无法通过校验，保证了整条区块链上数据的完整性、真实性和安全性。

3. 去信任化

区块链的信任机制基于密码学中的非对称加密(a symmetric encryption)原理，具有去信任化的特点，任意两个节点之间建立连接无须信任彼此的身份，双方交换数据也无须互相信任的基础。非对称加密是一种纯数学的加密方法，使用一对非对称的公钥和私钥完成加密与解密的过程。例如，当网络中的 Alice 对 Bob 发起一笔转移资产的交易时，Alice 使用 Bob 的公钥对交易进行加密，然后将交易信息向全网公开，该信息只有使用 Bob 的私钥才可解密。当 Bob 使用只有自己拥有的私钥对加密信息进行解密时，即可证明自己是资产的接收者，并得到全网的认可和记录。严谨的加密算法和完善的认证体系保证了区块链网络中交易一方不需要知道对方节点的身份，也不需要第三方机构的信任担保，就可以在陌生模式下进行可信任的交易。网络中所有节点都可以扮演监督者的身份，保证了数据背后交易者的个人隐私安全。

1.2　区块链发展演进路径

区块链技术起源于对等网络、非对称加密、数据库和分布式系统等已发展成熟的技术，通过对这些现有技术的组合和创新，实现了前所未有的功能。至今为止，区块链技术大致经历了 3 个发展阶段：可编程货币、可编程金融和可编程社会[4]，区块链的演进路径如图 1.1 所示。

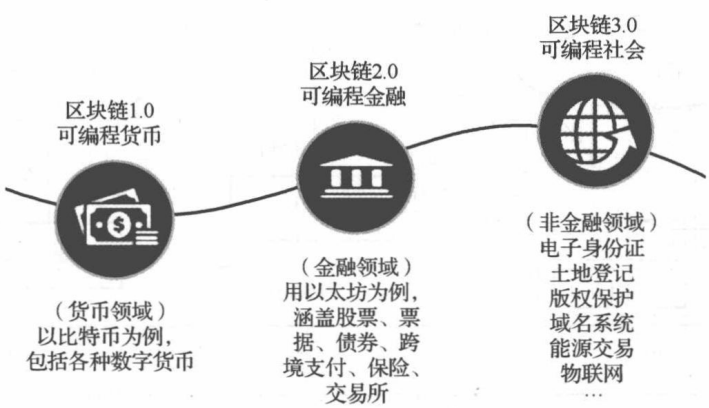


图 1.1　区块链的演进路径

1.2.1　可编程货币

区块链技术的基本应用场景是与转账、汇款和数字化支付相关的密码学货币应用，其中的典型代表就是比特币。

2009 年初，比特币的第一版实施系统正式上线运行。它为人们勾勒了一幅理想的愿景——全球货币的统一。比特币的总量是由网络中的共识协议限定的，不再依赖于各国的中央银行，没有任何个人或机构能够随意修改其中的供应量及交易记录。比特币因其有限的储量也被认为是互联网上的黄金、未来数字货币的价值衡量标准。随着以比特币为代表的数字货币被欧美市场大幅度接受，部分金融机构开始意识到，比特币系统的底层支撑——区块链技术实际上是一种非常巧妙的去中心化的分布式共享账本技术，通过节点间的通信共识来实现数据的交易和媒介、记账、存储的功能，对金融市场有着极大的冲击潜力。

基于区块链的数字货币应用弥补了传统数字货币的弊端。在传统的货币体系中，数字货币和数字资产具有无限可复制性，人们必须依赖第三方可信机构(如银行和支付宝等)来管理和确认某笔资产的归属权。而在区块链中，货币的拥有权是由公共总账本来记录的，并由全网节点来确认。节点每收到一个新的交易，都会向前遍历检查此交易所用的数字货币是否属于当前交易发起方，若发现这个数字货币已经被使用则投反对票否决此交易，最终这笔交易将无法被记录到区块链上。因此，区块链的账本管理权属于网络中的全部拥有账本副本的节点，而无须依赖某一可信的中心化机构。用户在发起交易时不需要考虑交易对方是否可信，区块链的信任规则建立在一个公开透明的数学算法之上，能够实现在不可信网络中进行可靠的支付和交易。

比特币凭借其先发优势，目前已经形成图 1.2 中体系完备的涵盖发行、流通和

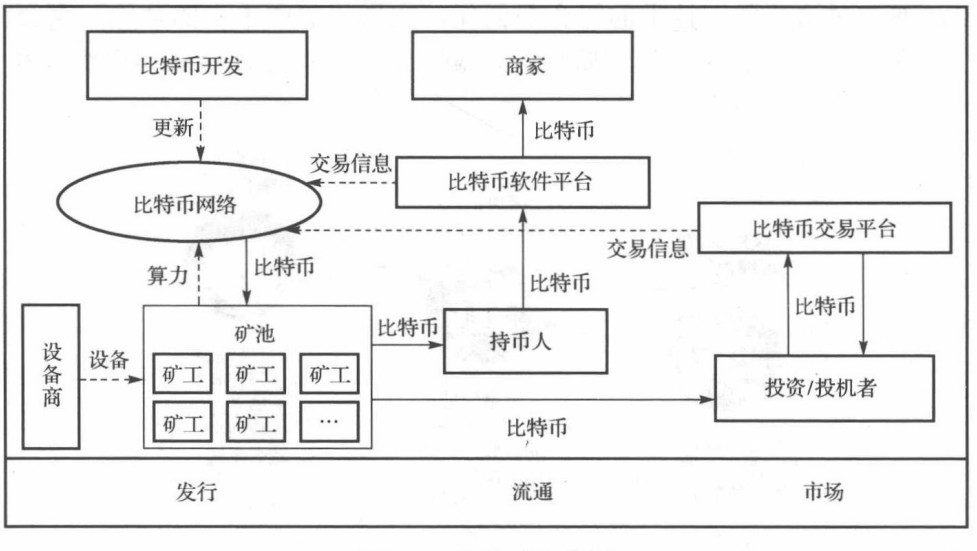


图 1.2　比特币生态圈

金融衍生市场的生态圈与产业链[3]，占据了绝大多数数字加密货币的市场份额。至此，以比特币为代表的数字货币构成了区块链的可编程货币阶段。但是由于最初的区块链架构只是比特币系统的底层支撑，它的功能设计主要围绕数字货币的实现来考虑，具有一定的局限性。因此，区块链在发展的下一阶段——可编程金融中加入了智能合约的概念。

1.2.2　可编程金融

比特币的出现给金融业带来了一种全新的货币体系，区块链技术在可编程货币阶段体现的价值担保和价值传递属性，为以信用为基石的金融行业带来了颠覆性的机遇。人们逐渐将目光转向了泛金融领域，试图利用区块链技术来转换不同的资产，例如，股票、债券、期货、贷款、抵押和产权等，而不仅仅是数字货币，可编程金融阶段随之到来。其中的核心代表就是智能合约。

智能合约的概念最早是由 Nick Szabo 于 1994 年提出的，是一套以数字形式定义的承诺[5]。以太坊项目首次将智能合约应用在区块链中，该项目也是智能合约在区块链的本阶段最成功的应用。按照 Vitalik Buterin 在白皮书[6]中的设计，以太坊的目标是构建一个开源的图灵完备的智能合约平台，所有开发者都可以依据自身需求在以太坊上建立自己的应用和发行自己的代币。在以太坊区块链中，智能合约是存放在合约地址上的数据和代码的集合，该地址上的代码在一定条件下会自发执行，因此它允许合约双方在没有第三方担保的情况下进行可追踪且不可逆转的可信交易。

相较于传统合约，智能合约提供的可信度能够最大限度地替代纸质签字所能够保证的合约可信度。传统合约是双方或者多方在互相信任彼此会履行义务的前提下，共同协商在不同的条件下执行不同的流程；而智能合约利用区块链去信任化的特点，实现可信的合约流程在线自动化执行。首先，智能合约完全是由代码定义执行的，一旦启动就会自动根据判决条件而运行，无须线下的人为干预。其次，智能合约是分布式的，不依赖于第三方可信机构的服务器提供担保，可以在区块链网络节点中自动达成共识和运行，不需要提前信任中心服务器。

以以太坊智能合约为标志的可编程金融阶段，代表着区块链开始广泛地应用于金融领域。但仅在金融场景应用已经不能充分施展区块链技术的潜力，随着区块链技术的发展，应用开始从金融全面下沉到各个领域，区块链同时迈入了新的阶段——可编程社会。

1.2.3　可编程社会

随着研究和应用的不断深入，区块链技术逐渐超越金融领域，扩展到政府、健康、科学、工业、文化和艺术等社会领域，能够支持广义资产、广义交换和行业应用，进而作为一种能够实现万物互联的底层协议驱动信息互联网向价值互联网转变。

价值互联网的核心是由区块链构造的一个全球性的分布式记账系统，记录的内容可以是任何有价值的能以代码形式进行表达的事物，例如，对共享汽车的使用权、信号灯的状态、出生和死亡证明、教育程度、财务账目、保险理赔、投票和能源状态等。区块链对互联网中每一个代表价值的信息和字节进行认证、计量和存储，从而实现资产在区块链上可被追踪、控制和交易[7]。

同时，区块链平台开始具备企业级属性以支持行业应用，并且增加了适用于不同应用场景的权限控制功能。互联网行业巨头纷纷拓展区块链业务，加入到区块链的技术研究与场景应用中来。腾讯开发了企业级的区块链基础服务平台 Trust SQL，已经落地供应链金融、医疗、数字资产、物流信息、法务存证和公益寻人等多个场景。阿里巴巴将区块链技术去中心化和防篡改的特性应用在公益、正品追溯、租赁房源溯源和互助保险等场景内，共申请了约 80 项区块链专利。百度金融(度小满科技(北京)有限公司)先后与华能信托(华能贵诚信托有限公司)和长安新生(长安新生(深圳)金融投资有限公司)等合作了国内首单区块链技术支持证券化项目以及基于区块链技术的交易所资产支持证券化(asset backed securitization，ABS)项目。

如图 1.3[8]所示，目前，我国的区块链产业链条已经形成。从上游的硬件制造、平台服务、安全服务，到下游的产业技术应用服务，到保障产业发展的行业投融资、媒体、人才服务，各领域的公司基本完备，协同有序，共同推动产业不断前行。

1.2.4　区块链底层平台

在区块链产业，底层平台是目前很多公司的布局方向。其中主流的平台模式有公有链、联盟链和区块链即服务(blockchain as a service，BaaS)[9]，它们的应用场景和设计体系各不相同。

1. 公有链

公有链是指向全世界所有人开放，每个人都能成为系统中的一个节点参与记账的区块链。任何节点都可以无须许可地自由加入或退出公有链系统，并在其中读取数据、竞争记账、发送和转发待确认事务。它通常将激励机制和加密数字验证相结合来保证参与者竞争记账的活跃性，以确保数据的安全。公有链被广泛地认为是完全去中心化的，公开的共识过程决定了可以被写到链上的区块以及确切的当前状态，任何人或者机构都不能恶意控制数据的读写或篡改数据。

公有链是目前应用最为广泛的区块链，它的优点包括：程序开发者无权干涉用户，保护用户免受开发者的影响；所有数据默认公开，每个参与者可以看到所有的账户余额和交易活动，系统运作过程公开透明；访问门槛低，任何拥有足够技术能力的人都可以访问；通过社区激励机制更好地实现大规模的协作共享等。

公有链的典型平台有比特币[1]、以太坊[6]等，国内的领先平台有小蚁[10]等。

图 1.3　2018 年中国区块链产业生态图

2. 联盟链

联盟链是指若干个机构共同参与记账的区块链，每个机构运行一个或多个节点，联盟成员之间通过对多中心的互信来达成共识。链上块的创建由预选的记账节点共同决定，而且只允许成员节点进行读写、记录和发送交易。与公有链不同，联盟链被认为是部分去中心或者是多中心的。它在某种程度上只属于联盟内部的成员所有，链上的数据仅限联盟里的机构和成员有权限地进行访问。

相比于公有链，联盟链在高可用、高性能、可编程和隐私保护上更有优势，主要体现在：精简了节点数，使得系统的运行效率更高，成本更低；系统更加灵活，只要大部分机构达成共识，就能够很容易地在链上进行修改规则、还原交易和修改余额等操作；实施节点准入控制，制定符合要求的监管规则，保证了联盟链的可信安全。

联盟链的典型平台有超级账本(Hyperledger)等，国内的领先平台有 BCOS (blockchain open source)[10]等。

3. 区块链即服务

区块链即服务[8]参考了云计算领域的软件即服务(software as a service，SaaS)的概念，通常是一个基于云服务的企业级的区块链开放平台，配有权限管理功能，能够支持私有链、联盟链或多链。BaaS 在云端为中小企业或个人用户提供搭建区块链所需的资源，帮助用户快速地建立自己所需的开发环境。它还提供了基于区块链的搜索查询、交易提交和数据分析等一系列操作服务，该操作服务集合可能是中心化的，也可能是去中心化的。此外，在 BaaS 服务商提供的标准服务的基础上，开发者也可以根据自己的产品和业务特点，通过在线配置和上传代码功能来扩展自定义的个性化需求。

作为一种应用开发的新模式，BaaS 因其一键式快速部署接入、私有化部署、完善便捷的区块链开发体验和丰富的运维管理等特色能力，受到越来越多的开发者的青睐。

BaaS 的典型平台有 Microsoft Azure BaaS、IBM Blockchain 等，国内的领先平台有腾讯云区块链服务(tencent blockchain as a service，TBaaS)[11]、华为云区块链服务(blockchain service，BCS)[12]等。

总体来说，公有链与联盟链、区块链即服务虽然采取了不同的发展路径，但是现在我们仍无法断定哪个更优，三者依然会长期共存。大胆预测，有些平台最后将殊途同归，或者未来会通过跨链技术将分散的联盟链系统连接在底层公有链之上，形成更大范围的价值互联网产业生态。

此为试读，需要完整PDF请访问：www.ertongbook.com