Contents
目录

第一章　区块链技术概述……1

1.1　区块链技术背景……1

1.2　区块链的基本概念……5

1.3　区块链技术发展历史……12

1.4　区块链系统总体架构……17

1.5　区块链技术应用概况……24

本章小结……27

练习题……28

第二章　比特币区块链系统……30

2.1　比特币区块链系统架构……31

2.2　比特币系统数据层……33

2.3　比特币系统网络层……44

2.4　比特币系统共识层……49

2.5　比特币系统激励层……52

2.6　比特币系统合约层……53

本章小结……59

练习题……60
第三章　以太坊区块链系统……62
3.1　以太坊区块链系统架构……63
3.2　以太坊系统数据层……66
3.3　以太坊系统网络层……73
3.4　以太坊系统共识层……80
3.5　以太坊系统激励层……82
3.6　以太坊系统合约层……84
本章小结……87
练习题……88
第四章　超级账本区块链系统……91
4.1　超级账本 Fabric 系统架构……91
4.2　超级账本 Fabric 系统数据层……95
4.3　超级账本 Fabric 系统网络层……99
4.4　超级账本 Fabric 系统共识层……109
4.5　超级账本 Fabric 系统激励层……113
4.6　超级账本 Fabric 系统合约层……113
本章小结……118
练习题……119
第五章　区块链信息安全技术……122
5.1　哈希算法……122
5.2　公钥密码体制……135
5.3　默克尔树……144

5.4 默克尔帕特里夏树……145
本章小结……151
练习题……152
第六章 区块链共识机制……154
6.1 共识基本原理与问题……154
6.2 非拜占庭容错类共识算法……161
6.3 拜占庭容错类共识算法……170
本章小结……181
练习题……181
第七章 区块链智能合约技术……184
7.1 智能合约概述……184
7.2 智能合约技术原理……188
本章小结……213
练习题……213
第八章 区块链 P2P 网络技术……216
8.1 P2P 网络基本概念……216
8.2 P2P 网络模型……218
8.3 结构化 P2P 网络分布式哈希表技术……226
8.4 非结构化 P2P 网络数据查询与分发技术……234
本章小结……236
练习题……236
第九章 BaaS 区块链即服务平台技术……239
9.1 BaaS 区块链即服务概述……239

9.2 BaaS 相关核心技术……241
9.3 BaaS 平台系统架构……258
本章小结……272
练习题……273
第十章 区块链技术的应用……275
10.1 基于区块链的应用系统……275
10.2 区块链 + 应用方向……282
10.3 区块链技术参考应用方案……292
本章小结……304
练习题……304
参考文献……307

第一章

区块链技术概述

区块链（Blockchain）从字面意思理解是“由区块组成的链”，这个概念最早出现于2008年10月31日（北美东部时间）署名“中本聪”（Satoshi Nakamoto）的作者发表的论文《比特币：一种点对点的电子现金系统》（Bitcoin：A Peer-to-Peer Electronic Cash System）中论文首次提出“区块链”（Chain of Blocks）是一种用于记录交易账本的数据结构。

随着区块链技术十多年的发展与应用，人们逐步加深了对区块链技术本质的认识。最初人们将区块链视为一种分布式账本系统，通过维护数据块的链式结构，可以维持持续增长的、不可篡改的数据记录。近年来，人们认识到，区块链作为新一代信息技术，与云计算、人工智能、大数据、物联网等技术一样，有利于人类生产能力与生产效率的提升，有利于开放数字经济社会环境下人类生产关系的优化与重构。

区块链技术也不是全新的技术，而是将分布式计算与存储、共识机制、智能合约、P2P网络、网络安全等多种计算机技术相互融合的应用技术创新。

本章将描述区块链技术背景、区块链的基本概念、区块链技术发展历史、区块链系统总体架构、区块链技术应用概况等内容。

1.1 区块链技术背景

1.1.1 区块链产生的背景

随着人类处理大数据的数量、质量和速度的能力不断增强，推动人类经济形态由工业经济向数字经济形态转化，数字技术被广泛使用并由此带来了整个经济环境和经济活动的根本变化。企业、消费者和政府之间通过网络进行的交易迅速增长，必须极大地降低社会交易成本，提高资源优化配置效率，才能提高产品、企业、产业附加值，推动社会生产

力快速发展。而人类社会交易是个体或组织价值创造、价值交换与价值记录的过程。在这个过程中，所有环节的“可信”是有效社会交易活动的前提与基础，信任是确保人类社会交易甚至生产关系得以维系发展的核心要素。

根据信任主体之间的关系，可以把信任服务模式划分为无中介熟人信任、第三方信任和无中介陌生人信任等 3 种类型，如表 1–1 所示。无中介熟人信任，信任主体之间的信任关系构建在对相互身份、交往历史的了解和掌握的基础之上，信任主体之间为“熟人”关系；第三方信任，信任主体之间为“陌生人”关系，相互之间的信任依托于对第三方中介的信任，对第三方中介的信任程度直接影响对“陌生人”的信任程度；无中介陌生人信任，信任主体之间虽是“陌生人”关系，但相互之间构建信任关系并不依赖于第三方中介，信任的构建将依赖于软件算法与机器系统，如依托区块链系统。

表 1-1　信任服务模式的对比

信任服务模式	信任主体关系	是否第三方参与	信任依据
无中介熟人信任	熟人关系	否	熟人
第三方信任	陌生人关系	是	第三方可信度
无中介陌生人信任	陌生人关系	否	软件算法与机器系统

传统的信任服务模式包括无中介熟人信任、第三方信任等，在人类社会发展过程中，都发挥过重要作用，甚至使用至今，但均存在许多局限性。

无中介熟人信任是一种最早出现的信任服务模式，信任主体需要对价值交往对象的身份、交往历史进行了解和掌握，这种了解和掌握是构建在与交往对象的长期相识、相处及价值频繁交互的历史信息基础之上的，因而具有以下局限性：

（1）信任的基础是由特定原因形成的熟人社会关系，如亲戚、同乡、同学、同事等。

（2）信任的建立需要投入大量时间、精力，甚至情感等。

（3）信任形成范围十分有限，信任主体对象数量有限。

无中介熟人信任服务模式的特点决定了其信任范围、作用范围有限，并且信任成本高昂而低效，但是无中介熟人信任在现代社会中仍然在使用。

由于无中介熟人信任是一种落后的信任服务模式，已不适应人类社会经济活动快速发展的需要，因而出现了更具效率的第三方信任服务模式。与无中介熟人信任相比，第三方信任具有以下优势：

（1）信任主体的范围大大扩展，由原来极其狭窄的熟人群体扩展到广大的陌生人群体。

（2）由对个体的信任转变为对第三方中介平台的信任。

（3）第三方中介平台的信任服务能力决定了对个体的信任水平。

第三方信任是当前人类社会的主流信任服务模式，构成了现代社会经济活动的基础框架，但第三方信任体系仍有其局限性，主要表现在以下两个方面。

（1）第三方信任的构建成本仍然高昂。一个权威可信的第三方信任服务平台，必须具备大量资金投入与保障、规范的管理制度与严格执行、高水平高素质的运营团队，方可持续运营与服务，必然需要承担由此带来的高昂的交易成本。

（2）第三方信任的信任风险仍然广泛存在。由于第三方信任服务模式依赖于第三方中介平台，而第三方中介平台本身在资源投入、信息获取和运营管理能力方面的问题，以及自身潜藏的内部人员的作恶风险，均可能造成第三方信任的削弱甚至丧失。

21 世纪以来，数字化的技术、商品与服务不仅在向传统产业进行多方向、多层面与多链条的加速渗透，而且在推动诸如互联网数据中心建设与服务等数字产业链和产业集群不断发展壮大。比如，我国重点推进建设的 5G 网络、数据中心、工业互联网等新型基础设施，本质上就是围绕科技新产业的数字经济基础设施。数字经济发展使人类对“信息”的价值创造、传播与利用的时间与空间范围获得了空前的释放，企业、消费者和政府之间通过互联网进行的交易爆发式增长，第三方信任服务模式因其在成本、效率、风险等方面的局限性越来越跟不上数字经济发展的步伐，迫切需要发展全新的信任服务模式，进一步降低信任服务的成本和风险，提高服务效率，并打破互联网垄断格局，推动数字经济持续创新与高速发展。区块链作为一种创新的只依赖于软件算法与机器系统的无中介陌生人信任服务体系进入了学术界和产业界的视野。

1.1.2　区块链的起源

区块链技术起源于人类设计使用数字货币替代实体货币的长期探索和实践过程中。货币是人类社会商品交换的产物，是在商品交换过程中从商品中分离出来的固定地充当一般等价物的商品，其本质上是财产所有者与市场关于交换权的契约。在人类几千年的社会发展过程中，先后出现了实物货币（如贵金属货币）、代用货币（如银票）、信用货币（如纸币）、电子货币（如信用卡、储蓄卡）、数字货币（如央行数字货币）等货币类型。近代以来，在相当长的时间内，纸币一直是货币的主要形态，但是纸币的发行、印制、回笼和贮藏等环节成本较高，流通体系层级多，且携带不便、易被伪造、匿名不可控，存在被用于洗钱等违法犯罪活动的风险，虽然现代电子货币（信用卡、支付宝、微信等）弥补了纸

币的诸多问题，但电子货币依赖背后的集中式支付体系，一旦碰到支付系统故障、断网、缺乏支付终端等情况，就无法使用。同时，尽管集中式支付体系的结构带来了管理和监管上的便利，但系统安全性仍然存在很大挑战，诸如伪造、信用卡诈骗、盗刷、转账骗局等安全事件屡见不鲜。

从20世纪80年代开始，研究人员一直在探索设计实现一种新型数字货币，保持既有货币方便易用的特性，同时消除纸币和电子货币在使用上的缺陷。

1983年，大卫·乔姆（David Chaum）在其发表的论文《无法追踪付款的盲签名》（Blind Signatures for Untraceable Payments）中提出了基于盲签名技术的e-Cash数字加密货币方案。

1997年，英国著名的计算机科学家和密码学家亚当·巴克（Adam Back）在“加密朋克”（CryptoPunk）邮件列表发送了一封主题为“一种基于局部哈希冲突的邮资方案”（A Partial Hash Collision Based Postage Scheme）的邮件，提出了哈希现金（Hash Cash）技术方案，该方案中首次使用一种叫作工作量证明（Proof of Work）的技术来解决垃圾邮件问题。

1998年，华人密码学家戴维（Wei Dai）在“加密朋克”邮件列表发送一封关于B-money的技术设想，B-money的设计目标是一种采用PoW工作量证明机制和分布式记账的电子现金系统，但是B-money交易过程还是要依赖于第三方信任服务体系，PoW机制只能保证代表电子现金的一串数字的确对应了真实世界一定价值的资源消耗，但如果没有对分布式账本记录的第三方见证人，就不能防止同一串数字被同一个人多次使用，即存在对数字货币来说是致命的双花问题。可见，信任服务体系已成为制约数字货币技术实现的难题之一。

在前人工作的基础上，2008年10月31日，中本聪（Satoshi Nakamoto）在其发表的论文《比特币：一种点对点的电子现金系统》（Bitcoin：A Peer-to-Peer Electronic Cash System）中，提出了一种基于无中介陌生人信任服务体系的分布式账本技术的数字加密货币系统方案，并将这种用于记录交易账本的数据结构取名为“区块链”。2009年1月3日第一个序号为0的“创世区块”诞生，2009年1月9日出现序号为1的区块，并与序号为0的“创世区块”相连接形成了链，标志着区块链的诞生。因此，目前普遍认为区块链技术最早起源于比特币（Bitcoin[①]）开源项目。

比特币系统通过区块链在一个由陌生主体构成的开放网络中，生成和维护统一、可信的分布式账本的技术方案，用事实证明构建一个基于区块链的无中介开放信任服务体系，不仅在理论上可行，在实践上也是可行的。

① https://bitcoin.org/en/

基于区块链的信任服务模式与中心化网络第三方信任、实体第三方信任的对比如表1–2所示。

表 1-2　区块链信任与其他信任服务模式的对比

信任服务模式	信任依据	规模与范围	成本代价	影响因素
实体第三方信任	依据第三方中介的可信度	规模与范围较大	较高	受到少数人影响
中心化网络第三方信任	依据中心化网络第三方平台的可信度	规模与范围大	高	受到关键少数人影响
区块链信任	依据区块链的算法、共识机制	规模与范围大	很低	几乎不受人为因素的影响

1.2　区块链的基本概念

1.2.1　什么是区块链

在数据结构中，链是由多个节点（Node）相互连接构成的一种最基本的数据结构。区块链从字面上理解就是由多个记录数据的区块构成的链式数据结构。目前，区块链技术仍处于快速发展过程中，学术界、产业界从不同角度对区块链提出不同的定义和阐释。

从技术角度来看，区块链是一种基于P2P网络架构的分布式账本技术系统，以“块–链”式数据结构来验证与存储账本数据，由多方维护的分布式节点共识机制来生成无法篡改、无法抵赖的账本数据，使用密码学方法保证数据传输和访问的安全，可自动执行由高级语言或脚本语言编写的智能合约程序来查询或生成账本数据。

如图1–1所示，在一个区块链系统中，每过一段时间，各参与主体维护的分布式节点产生的交易数据会被打包成一个数据区块，数据区块按照时间顺序依次排列，形成数据区块的链条，各分布式节点中存放了一致的数据链条，且无法单方面篡改，并且只允许添加新的信息，无法删除或修改旧的信息，从而实现多主体间的信息共享和一致决策，确保各主体身份和主体间交易信息的不可篡改、公开透明。

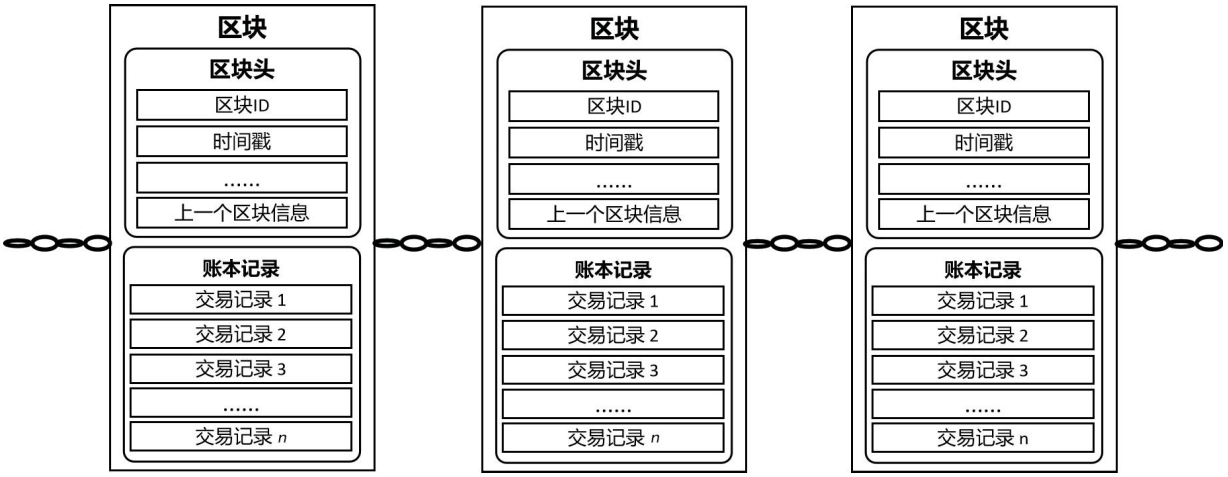

图 1-1　区块链“块 - 链”结构示意图

从应用角度来看，区块链面向由陌生主体构成的开放网络环境的价值创造、价值交换与价值记录过程，提供多方集体维护、不可篡改、可追溯、公开透明的分布式账本记账服务，大幅降低第三方信任服务的成本和风险，提高服务效率，是一种新型的无中介陌生人信任服务应用支撑平台系统。

1.2.2　区块链的特点

1.2.2.1　去 / 弱中心化

区块链不依赖中心化或第三方管理机构及硬件设施，去除或弱化中心管理，通过 P2P 网络构建分布式的结构体系和开源协议，让所有的节点都参与数据的记录和验证，再通过分布式传播发送给各个节点，即使部分节点受到攻击或者发生故障，也不会影响整个分布式账本数据的一致性和完整性，各个节点实现了信息自我验证、传递和管理。去 / 弱中心化是区块链最突出最本质的特点。

1.2.2.2　数据不可篡改

信息一旦经过验证并添加到区块链，就会被永久地存储起来，在系统任何节点上对数据的修改都是无效的，除非有人能同时控制超过半数以上的系统节点，但是区块链系统的节点是由多方公共维护的，要控制超过半数以上的节点，需要付出的代价可能远远大于篡改数据获得的收益。因此，区块链技术从根本上改变了中心化的信用创建方式，并通过数学算法与博弈论原理而非中心化信用机构来低成本地建立信用，比特币、以太坊等系统

已充分证明了区块链的这一特点。

1.2.2.3　数字价值唯一性

在信息世界中，最基本单元是比特（bit），数字比特序列是可复制的，但是数字价值不能被复制，数字价值必须是唯一的，这本身就是矛盾的。在区块链技术出现之前，要让一个文件在全世界范围内是唯一的，需要花费巨大的代价。区块链采用共识机制和密码学方法，以很小的代价实现数字化表达唯一性，真正使数字价值变得唯一，可以模拟真实世界中的实物唯一性。

1.2.2.4　智能合约

区块链通过可编程的智能合约，让机器系统自动执行双方所达成的契约或一些无法预见的交易模式，排除了传统交易过程中人为单方不完全履约或毁约等干扰因素，从制度上确保合约的全面执行，防止任何一方的抵赖。区块链有助于推动价值传递过程进入智能化状态，实现数字经济发展的质的飞跃。

1.2.2.5　开放性

区块链技术基础是开源的，除了对交易各方的私有信息进行加密外，区块链数据对所有人公开，任何人都能通过公开的接口，对区块链数据进行查询，并能开发相关应用，整个系统的信息高度透明。

1.2.2.6　去信任

传统的互联网应用系统是通过可信任的中央服务器节点或者第三方信任平台（如微信）进行信息的匹配验证和信任积累。区块链基于自身去 / 弱中心化、数据不可篡改、数字价值唯一性等特性，系统所有节点都能在去信任的环境中自由安全地交换数据，交易各方不用通过公开身份的方式让对方对自己产生信任，让对“人”的信任改变为对机器系统与公开算法的信任，更有利于由陌生主体构成的开放网络环境中信用的积累。

1.2.3　区块链的类型

根据区块链系统的节点归属、节点加入方式、共识范围、数据公开范围、应用范围等

差别，可以将区块链分为公有链、联盟链与私有链 3 种不同类型，如表 1–3 所示。

表 1-3　区块链的类型

类型	节点归属	节点加入方式	共识范围	数据公开范围	应用范围
公有链	任意陌生主体	自由加入	所有节点	完全公开	公众
联盟链	联盟成员主体	联盟成员自由加入	联盟通道节点	联盟范围内	联盟范围内 / 公众
私有链	单一主体	受控加入	单一主体节点	不公开	单一主体内部

1.2.3.1　公有链

公有链（Public Blockchain）中的“公有”就是任何人都可以参与区块链数据的维护和读取，数据完全开放透明。公有链即区块链共识建立的范围是面向全社会，公共账本及软件代码完全公开，任何个体与组织均可在认同公有链相关共识机制的条件下，自由参与公有链网络的建设与运营，参与区块数据的产生、传播与维护，以及各类区块链应用的开发、部署与服务运营。公有链由于完全开放，参与主体众多，特别是对具有应用开发支持能力，即支持智能合约的区块链而言，就具备了围绕相关主题，构建自治、闭环生态系统的能力，这对打破垄断型的互联网生态系统而言，具有特别重大的意义。

目前全球最有影响力的公有链是比特币和以太坊系统。例如比特币系统，使用者只需下载相应的客户端，就可以创建钱包地址、转账交易、参与挖矿，这些都是免费开放的。比特币系统的成功充分验证了区块链技术的可行性和安全性。

公有链系统完全没有中心机构管理，依靠事先约定的规则来运作，并通过这些规则在不可信的网络环境中构建起可信的网络系统。通常来说，需要公众参与、需要最大限度保证数据公开透明的系统，都适合选用公有链。

公有链环境中，由于节点数量众多且不定，节点实际身份未知、在线与否也无法控制，仍然存在效率、隐私保护等问题。

（1）效率问题。由于在公有链中，区块的传递需要时间，为了保证系统的可靠性，大多数公有链系统通过提高一个区块的产生时间来保证产生的区块能够尽可能广泛地扩散到所有节点处，从而降低系统分叉（同一时间段内多个区块同时被产生，且被先后扩散到系统的不同区域）的可能性。因此，在公有链中，区块的高生成速度与整个系统的低分叉可能性是矛盾的，必须牺牲其中的一个方面来提高另一方面的性能。同时，由于潜在的分叉情况，可能会导致一些刚生成的区块回滚，因此在公有链中，每个区块都需要等待若干个基于它的后续区块的生成，才能够以可接受的概率认为该区块是安全的。例如，比特币中的区块在有 6 个基于它的后续区块生成后才能被认为是足够安全的，而这大概需要一个

小时，对于大多数企业应用来说根本无法接受。

（2）隐私保护问题。目前公有链上传输和存储的数据都是公开可见的，仅通过“地址匿名”的方式对交易双方进行一定隐私保护，相关参与方完全可以通过对交易记录进行分析从而获取某些信息。这对于某些涉及大量商业机密和利益的业务场景来说也是不可接受的。另外在现实世界的业务中，很多交易业务（如银行交易）都有实名制的要求，因此在实名制的情况下当前公有链系统的隐私保护问题很难有效解决。

（3）激励合法性问题。为促使参与节点提供资源，自发维护网络，公有链一般会设计激励机制，以保证系统健康运行。但现有的大多数激励机制，需要发行类似于比特币、以太币等数字代币，有可能违反不同国家的法律规范，如 2020 年 10 月我国央行已在《中华人民共和国中国人民银行法（修订草案征求意见稿）》中明确任何单位和个人不得制作和发售数字代币。

1.2.3.2　联盟链

联盟链（Consortium Blockchain）以区块链共识建立的范围及公共账本的公开对象为有限主体，如行业联盟成员之间，联盟成员平等参与区块链网络构建、公共账本创建与维护。联盟链使参与主体的共识边界由原来主体私有范围扩展至整个联盟范围，由于共识边界扩大，联盟成员之间具有了共同的信任基础——联盟链公共账本，因而联盟链成员之间在无须第三方中介参与的条件下，就可提升相互的价值交换效率。

联盟链通常在多个互相已知身份的组织之间构建，如多个银行之间的支付结算、多个企业之间的物流供应链管理、政府部门之间的数据共享等。因此，联盟链系统一般都需要严格的身份认证和权限管理，节点的数量在一定时间段内也是确定的，适合处理组织间需要达成共识的业务。区块链典型的联盟链代表技术是开源的超级账本（Hyperledger Fabric）系统。与公有链相比，联盟链具有以下优点：

（1）效率较公有链有很大提升。联盟链参与方之间互相知道彼此在现实世界的身份，支持完整的成员服务管理机制，成员服务模块提供成员管理的框架，定义了参与者身份及验证管理规则；在一定的时间内参与方个数确定且节点数量远远小于公有链，对于要共同实现的业务在线下已经达成一致理解，因此联盟链共识算法较比特币 PoW 的共识算法约束更少，共识算法运行效率更高，如 PBFT、Raft 等，从而可以实现毫秒级确认，吞吐率有极大提升，每秒执行交易数（Transactions Per Second，TPS）可达到几万。

（2）更好的隐私保护。数据仅在联盟成员内开放，非联盟成员无法访问联盟链内的数据。即使在同一个联盟内，不同的业务之间的数据也进行一定的隔离。比如，超级账本Fabric 系统的多通道机制将不同业务的区块链进行隔离，并支持对私有数据的加密保护。不同的联盟链厂商又做了大量的隐私保护增强，如对交易金额信息进行加密保护；通过零知识证明，对交易参与方身份进行保护等。

（3）无激励问题。联盟链中的参与方为了共同的业务收益而共同配合，因此有各自贡献算力、存储、网络的动力，一般不需要通过发行代币进行激励。

1.2.3.3 私有链

私有链（Private Blockchain）与公有链是相对的概念。所谓私有就是指不对外开放，仅仅在组织内部使用。私有链以区块链共识建立的范围及公共账本的公开对象为单一主体，单一主体对区块链的网络运行及数据处理、交换与存储具有全部权利。显然，除了利用区块链的技术特性来增强数据的安全性与网络运行的可靠性外，私有链应用与传统的中心化技术相较并无特别优势，反而由于区块链技术自身固有的一些性能弱点，如同步时延较大、高并发处理能力不强等，使私有链的应用场景受到限制。

私有链也可以看作是联盟链的一种特殊形态，即联盟中只有一个成员，如企业内部的票据管理、账务审计、供应链管理，或者政府部门内部管理系统等。私有链通常具备完善的权限管理体系，要求使用者提交身份认证。

在私有链环境中，参与方的数量和节点状态通常是确定的、可控的，且节点数目要远小于公有链和联盟链。私有链与联盟链相比，具有更好的处理性能和敏感数据的安全保护能力，在某些应用场景下甚至可以替代传统的数据库系统。

1.2.4 区块链分叉

区块链分叉是指由于某种原因，从区块链的某个区块开始，后续的区块构成了两条子链，如图 1–2 所示。造成区块链分叉的原因主要有两种。

1.2.4.1 区块链软件升级

区块链不管是开源还是闭源系统，系统软件本身都在不停地迭代开发，每过一段时间都会发布新的软件版本，区块链系统节点众多且由不同的主体维护，节点系统升级有先有后，不可能实现所有节点同时升级到最新版本。区块链系统的节点被划分为已升级的新

节点和未升级的旧节点两大阵营，旧节点拒绝验证新节点产生的区块，然后新、旧节点各自延续自己认为正确的链，区块链发生永久性分歧，所以分成两条链。

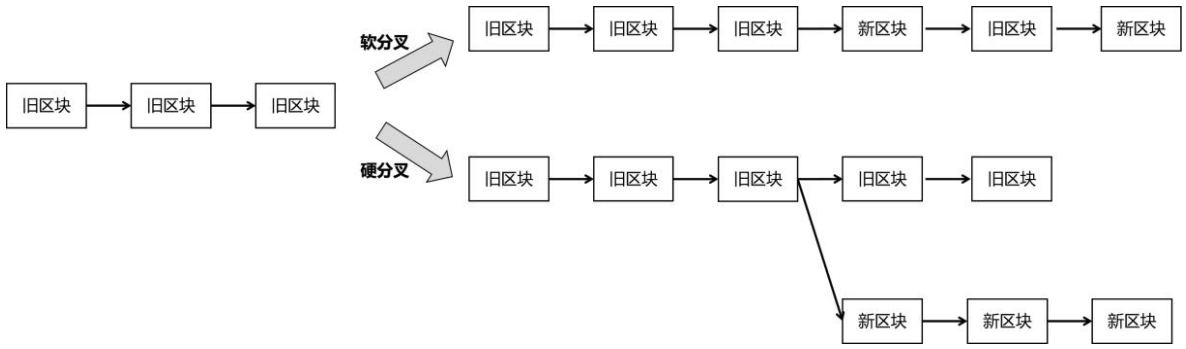

图 1-2　区块链软件升级分叉示意图

由区块链软件升级造成的分叉又可以分为两种情况：第一种情况是如果旧节点可以继续接收新节点产生的区块，只是旧节点无法读取新节点产生区块中的部分扩展属性，则称为“软分叉”；第二种情况是旧节点不能继续识别新节点产生的区块，则称为“硬分叉”。比特币、以太坊等区块链系统在运行过程中都发生过硬分叉，其中影响较大的硬分叉事件如 2016 年 6 月以太坊遭受黑客攻击，以太坊团队通过回滚的方式“追回”了被黑客盗取资产，但一部分社区成员认为此举有违区块链不可回滚、不可窜改的基本精神仍旧坚持维护旧链，从此以太坊分裂为“以太坊 ETH”和“以太经典 ETC”两个独立的区块链系统；2017 年 8 月，为解决比特币系统的性能问题，由于采用两种不同的升级方案，在位于比特币区块高度 478558 时，比特币系统分叉形成“BTC”与“比特币现金 BCH”两个独立的区块链系统。

1.2.4.2　区块链出块冲突

区块链系统（如比特币、以太坊等公有链）在运行过程中，如果采用 PoW 工作量证明之类的需要节点竞争计算新区块出块权的共识机制，有可能出现两个独立的节点同时求解出满足要求的哈希值结果，其都生成了一个新区块，导致出块冲突，使区块链发生临时分叉（见图 1–3）。

区块链系统处理上述临时分叉问题的方法十分简单，就是只承认分叉中最长的链，不是最长链的分叉中的区块将被抛弃成为孤立的区块（Orphan Block）。