Contents
目录

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。

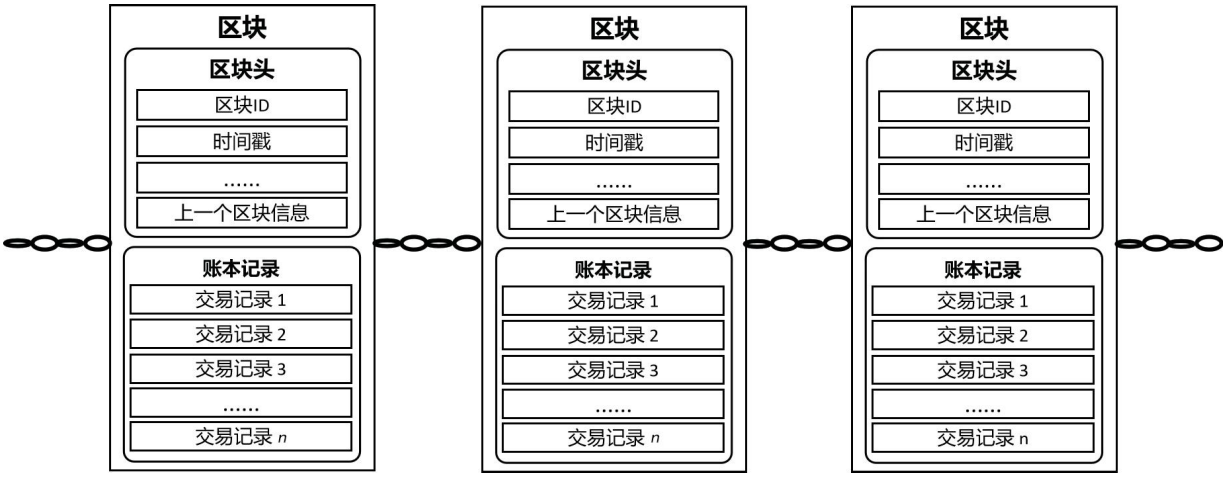

图 1-1　区块链“块 - 链”结构示意图

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。

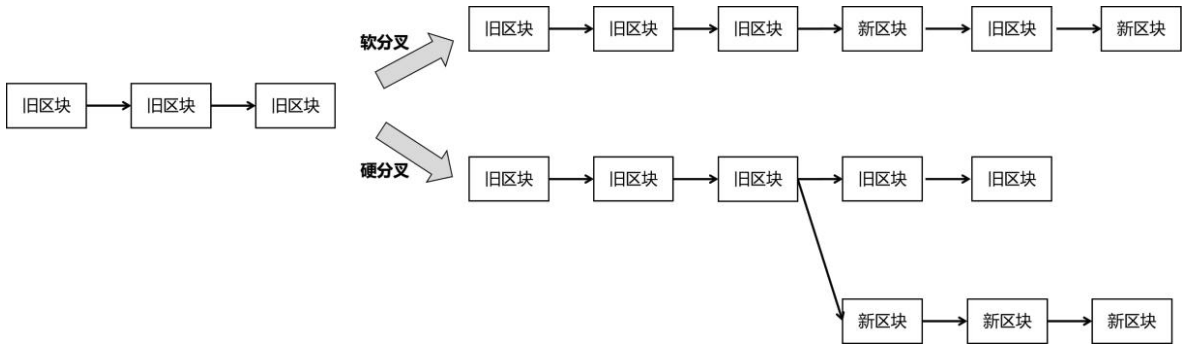

图 1-2　区块链软件升级分叉示意图

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）。

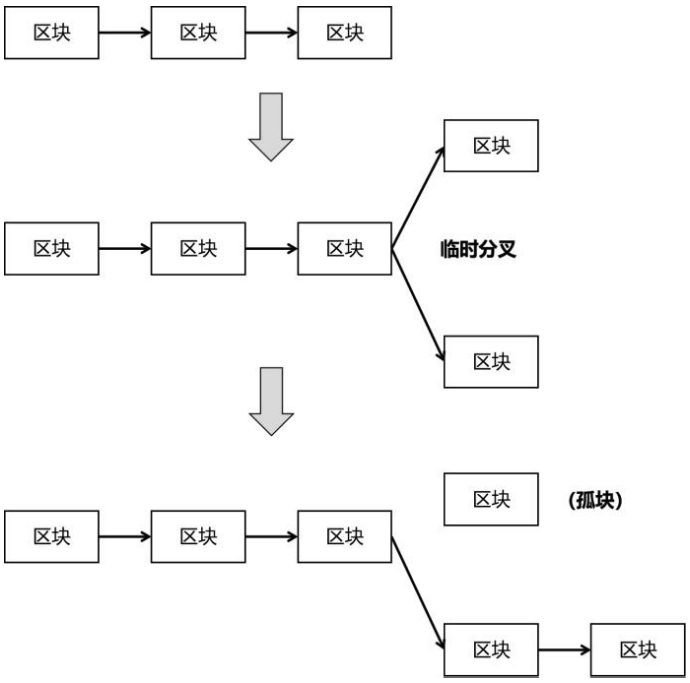

图 1-3　区块链出块冲突临时分叉示意图

1.3　区块链技术发展历史

区块链经过十多年的发展，随着人们对区块链技术逐步深入的研究与应用，业界普遍认为区块链技术已经过三个阶段的演化：第一阶段称为区块链 1.0 阶段，以基于区块链的去中心化的加密货币技术实现为代表；第二阶段称为区块链 2.0 阶段，以基于区块链的去中心化的智能合约交易处理技术实现为代表；第三阶段称为区块链 3.0 阶段，以基于区块链分布式账本处理技术的广泛的区块链应用实现为代表。

区块链三个发展阶段对比如表 1–4 所示。

表 1-4　区块链的发展历史阶段对比

阶段	核心功能	共识机制	区块链类型	性能	实现语言
区块链 1.0	加密货币	PoW	公有链	低	简单脚本语言
区块链 2.0	智能合约	PoW/PoS	公有链	一般	专用语言
区块链 3.0	数字价值交换应用平台	PBFT/Raft 多种机制	公有链 联盟链 私有链	较高 可扩展	高级编程语言

1.3.1　比特币区块链系统的发展

区块链 1.0 阶段以基于区块链技术的加密货币系统为代表。在数量众多的加密货币系统当中，在全球最有影响力、应用范围最广的是比特币（Bitcoin）系统。比特币的概念最初由中本聪在 2008 年 11 月 1 日提出，并于 2009 年 1 月 3 日正式上线。比特币网络是世界上首个经过大规模、长时间检验的加密货币系统。

与人民币、美元、欧元、英镑、日元等法定货币相比，比特币没有一个集中的发行方，而是由区块链网络节点的计算生成，谁都有可能参与制造比特币，可以在任意一台接入互联网的电脑上买卖，不管身处何方，任何人都可以挖掘、购买、出售或收取比特币，并且在交易过程中外人无法辨认用户身份信息。

与法定货币相比，比特币具有如下特点：

（1）去中心化：意味着没有任何独立个体可以对网络中的交易进行破坏，任何交易请求都需要大多数参与者的共识。

（2）匿名性：比特币网络中账户地址是匿名的，无法从交易信息关联到具体的个体，但这也意味着很难进行审计。

（3）通胀预防：比特币的发行需要通过挖矿计算来进行，发行量每四年减半，总量上限为 2100 万枚，无法被超发。

1.3.2　以太坊区块链系统的发展

区块链 1.0 阶段，以比特币为代表的“加密货币”的成功应用，标志着由 P2P 网络、共识机制、加密算法等关键技术构成的区块链技术体系基本形成，但应用模式还比较单一。区块链 2.0 阶段，以太坊（Ethereum[①]）系统作为典型代表，在比特币区块链技术的基础上，引入新的智能合约机制，将区块链技术带向了更广阔的应用领域，使更多基于区块链的去中心化应用场景得以实现。

随着比特币借助互联网的快速扩散应用，比特币系统在设计上的一些先天缺陷也越来越明显。例如，PoW 工作量证明共识机制造成了巨大算力和能源的浪费，甚至造成环境污染，比特币系统的交易脚本机制十分简单，无法满足对于复杂应用场景的扩展支持等。俄罗斯人维塔利克（Vitalik Buterin）于 2013 年发布了以太坊（Ethereum）系统技术白皮书，决定基于区块链技术研发一个全新的区块链平台，改进比特币的发行机制，使算力不再是

① https://ethereum.org/en/

决定“出块权”的唯一优势，同时引入智能合约机制，使广大开发者能够基于以太坊专用虚拟机提供的智能合约接口，构建各种用途的去中心化 DApp（Decentralized Application）应用。

以太坊项目于 2014 年 6 月开始，以 42 天预售活动的形式，对以太坊系统中的第一批以太币进行了分配，这次预售活动共交换出 60102216 个以太币，在当时，价值大概 1800 万美元。2015 年 7 月 30 日，以太坊正式发布，到 2016 年年初，以太坊的技术得到越来越多的开发者和用户认可。2018 年 5 月 17 日，赛迪研究院正式发布首期全球公有链技术评估指数及排名，以太坊位列评估榜单第一位。

与比特币系统相比，以太坊的区块链平台具备以下的主要技术特点：

（1）支持图灵完备的智能合约应用（比特币采用的交易脚本开发语言是非图灵完备），设计了编程语言 Solidity 和虚拟机 EVM。

（2）哈希计算选用了同时需要计算性能和内存容量的哈希函数（比特币的哈希计算只依赖算力）。

（3）引入叔块（Uncle Block）激励机制，缩短区块产生间隔到 15 秒左右，提升了交易处理性能（比特币需要 10 分钟左右）。

（4）引入账户系统和世界状态，更容易支持复杂的业务逻辑（比特币采用 UTXO 模型，没有账户的概念）。

（5）引入燃料（Gas）机制，限制智能合约代码执行指令数，即在以太坊平台运行应用要支付成本，有效避免循环执行攻击（比特币系统对每个网络节点发出交易的行为没有任何限制）。

（6）最初仍然采用 PoW 工作量证明共识机制，未来计划支持效率更高的权益证明（Proof of Stake，PoS）共识机制。

1.3.3 超级账本区块链系统的发展

目前区块链发展到 3.0 阶段，如果说区块链 1.0 阶段是以去中心化的虚拟数字加密货币技术为标志，区块链 2.0 阶段以基于智能合约的去中心化 DApp 应用区块链平台技术为标志，那么区块链 3.0 阶段的标志就是区块链技术开始向社会经济各个领域应用延伸。人们逐渐意识到，区块链不仅是一种技术，更是一种代表公正透明、协作信任的模式，区块链思想与技术可以有效应用在政企管理、社会治理、供应链、物联网、权属管理、医疗健康等诸多领域，成为面向社会全行业的应用。

在区块链应用类型上，区块链 1.0 和 2.0 阶段主要以公有链为主，而区块链 3.0 阶段则是在公有链的基础上，联盟链和私有链得到更广泛的应用。区块链 3.0 阶段，超级账本（Hyperledger[①]）项目作为典型代表，是区块链技术中第一个面向企业级应用场景的开源分布式账本平台，可以运行以标准通用编程语言编写的分布式应用程序，使更多基于区块链的联盟链、私有链应用得以实现。

超级账本（Hyperledger）是一个由 Linux 基金会牵头创立的开源分布式账本平台项目，超级账本项目于 2015 年 12 月被正式宣布启动，由多个顶级项目构成。与以太坊区块链平台不同，超级账本项目的主要目标是开发一个开源的分布式账本框架，构建强大的行业特定应用、平台和硬件系统，以支持商业级交易，但并不发行加密货币。

超级账本项目由技术委员会、管理董事会和 Linux 基金会“三驾马车”协同领导发展。技术委员会（Technical Steering Committee）负责对技术相关的工作进行领导，下设多个技术工作组，具体对各个项目的发展进行指导。管理董事会（Governing Board）负责整体社区的组织决策，其代表座位成员从超级账本会员中推选。Linux 基金会（Linux Foundation）负责基金管理和大型活动组织，协助社区在 Linux 基金会的支持下健康发展。

如图 1–4 所示，超级账本项目已建立了 10 个子项目，其中包括 Burrow、Fabric、Indy、Iroha、Sawtooth 等 5 个框架平台类子项目，Caliper、Cello、Composer、Explorer、Quilt 等 5 个工具类子项目，开源代码规模已超过 360 万行。以上所有项目都遵守 Apache V2 许可，并约定共同遵守如下基本原则。

（1）重视模块化设计：包括交易、合同、一致性、身份、存储等技术场景。

（2）重视代码可读性：保障新功能和模块都可以很容易添加和扩展。

（3）可持续的演化路线：随着需求的深入和更多的应用场景，不断增加和演化新的项目。

① https://www.hyperledger.org/use/fabric

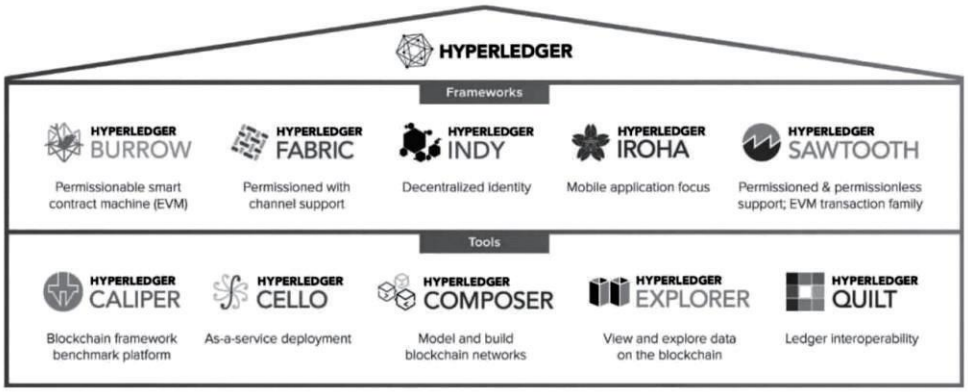

图 1-4　超级账本项目整体结构

Burrow 是最早由 Monax 开发的项目，它是一个通用的带有权限控制的智能合约执行引擎，同时也是超级账本项目大家庭里面第一个来源于以太坊框架的项目，智能合约引擎遵循 EVM 规范。

Indy 是一个着眼于解决去中心化身份认证问题的技术平台，该项目由 Sovrin 基金会牵头。Indy 可以为区块链系统或者其他分布式账本系统提供基础组件，用于构建数字身份系统，它可以实现跨多系统间的身份认证、交互等操作。

Iroha 可以简单方便地以模块的形式应用于任何分布式账本系统中，其设计理念之一便是项目中的很多组件可以为其他项目所引用，同时 Iroha 区别于其他超级账本项目的一大特点是主要面向于移动应用。

Sawtooth 是一个支持许可（permissioned）和非许可（permissionless）部署的区块链系统，是功能完整的区块链底层框架。它提出的共识算法——时间流逝证明（Proof of Elapsed Time，PoET），开创性地使用了可信执行环境（Trust Execution Environment，TEE）来辅助共识达成。PoET 可以在容忍拜占庭攻击的前提下，降低系统计算开销，是较为高效且低功耗的共识算法。

Caliper 是一个区块链性能基准测试工具（Benchmark Tool），开发者可以使用该工具内置的测试用例来测试区块链每秒执行交易数 TPS（Transactions Per Second）、延迟（latency）等性能。

Cello 是一个区块链的模块工具包，主要用于管理区块链的生命周期，在各种物理机、虚拟机、Docker 等基础设施上提供有效的多租户链服务，可用于监控日志、状况分析等。

Composer 是一个开发工具框架，协助企业将现有业务和区块链系统集成。开发人员可以借助 Composer 快速创建智能合约及区块链应用。通过强大的区块链解决方案，推动区块链业务需求的一致性。

Explorer 是一个区块浏览器，提供一个简洁的可视化 Web 界面。用户可通过该工具，快速查询每个区块的内容。它包括区块头中区块号、哈希值等信息，也包含每笔交易的读写集等具体内容。

Quilt 通过实施跨账本协议（Interledger Protocol，ILP）提供分类账系统之间的互操作。ILP 主要是支付协议，旨在跨分布式分类账和非分布式分类账中传输价值。

在超级账本项目的众多子项目中，Fabric 是一个功能完善的支持多通道（多链）的主要面向企业应用的区块链系统，是超级账本项目中的基础核心平台项目，它致力于提供一个能够适用于各种应用场景的、内置共识协议可插拔的、可部分中心化（即进行权限管理）的分布式账本平台，是首个面向联盟链场景的开源项目。

1.4　区块链系统总体架构

1.4.1　软件系统架构

软件系统架构相关知识与方法在软件工程领域中已有广泛的应用，不同学者与技术标准化组织对软件系统架构提出的定义有：

（1）软件系统架构是软件设计过程中的一个层次，这一层次超越计算过程中的算法设计和数据结构设计。系统架构包括总体组织和全局控制、通信协议、同步、数据存取，为设计元素分配特定功能，设计元素的组织、规模和性能，在各设计方案间进行选择等（Mary Shaw 和 David Garlan）。

（2）软件系统架构是一个抽象的系统规范，主要包括用其行为来描述的功能构件和构件之间的相互连接、接口和关系（Hayes Roth）。

（3）软件系统架构是一个程序 / 系统各构件的结构、它们之间的相互关系以及进行设计的原则和随时间进化的指导方针（David Garlan 和 Dewne Perry）。

（4）一个程序或计算机系统的软件系统架构包括一个或一组软件构件、软件构件的外部的可见特性及其相互关系。其中，“软件外部的可见特性”是指软件构件提供的服务、性能、特性、错误处理、共享资源使用等（Bass、Ctements 和 Kazman）。

（5）在标准《ISO/IEC 42010：2011 系统和软件工程——架构描述》（*Systems and Software Engineering——Architecture Description*）中，系统架构的定义为：一个系统在其所处环境中所具备的各种基本概念和属性，具体体现为其所包含的各个元素、它们之间的关系以及架构的设计和演进原则。

本书认为软件总体系统架构至少应从系统体系结构与逻辑架构两个方面对软件系统高层结构进行描述：系统体系结构，描述系统的主要构件及它们之间的关系；系统逻辑架构，描述系统主要功能分解与层次结构。

1.4.1.1 系统体系结构

随着计算机体系结构的发展，软件体系结构也从最初的大型中央主机（Mainframe）结构和单机体系结构，逐步发展出 C/S 体系结构、B/S 体系结构、P2P 体系结构等多种体系结构。

（1）C/S（Client/Server）体系架构是一种典型的客户端—服务器端两层架构，采用 C/S 体系结构的软件系统一般以数据库服务器端为中心，客户端通过数据库连接访问服务器端的数据，如图 1-5 所示。

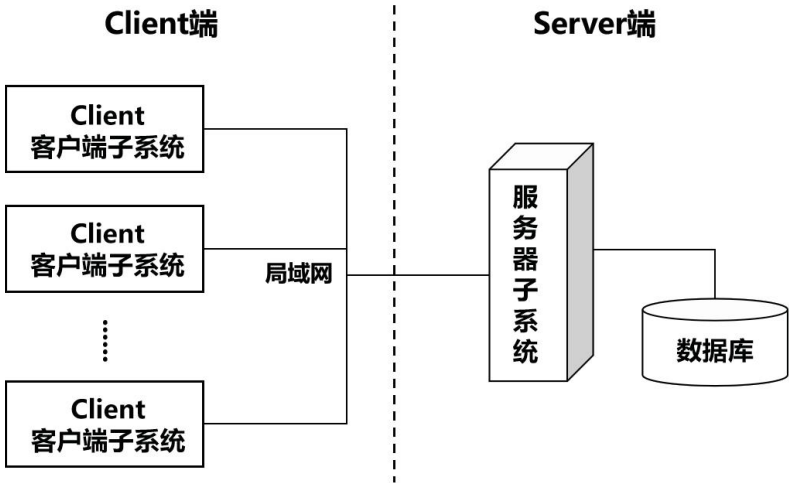

图 1-5　软件系统 C/S 体系结构示意图

（2）B/S（Browser/Server）体系结构，即浏览器端—服务器端结构。B/S 体系结构是随着互联网技术的快速发展，对 C/S 结构的一种变化或者改进的结构。在这种结构下，软件系统用户交互界面通过 Web 浏览器来实现，极少部分事务逻辑在浏览器端实现，主要事务逻辑在服务器端（Server）实现。基于 B/S 体系结构的软件，系统安装、修改和维护全在服务器端完成，用户在使用系统时，客户端仅需要浏览器就可运行系统全部的模块，真正实现了“零客户端”的效果。

如图 1–6 所示，B/S 体系结构一般可由 Browser 浏览器前端、Web 服务器中间层和数据库后端构成所谓的三层架构。采用 B/S 体系结构的软件系统，Web 浏览器前端负责显示交互逻辑，Web 服务器中间层负责事务处理逻辑，因为客户端需要处理的逻辑较少，因此也被称为“瘦客户端”。

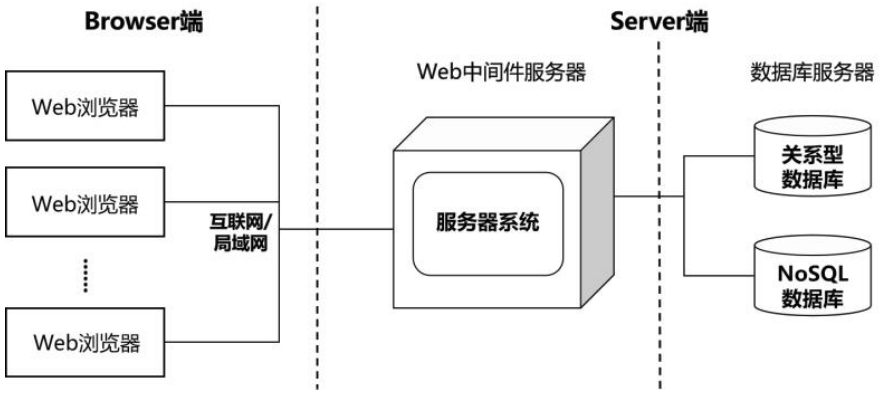

图 1-6　软件系统 B/S 体系结构示意图

（3）P2P（Peer to Peer）体系结构，即对等网络结构。在 P2P 体系结构中，取消了作为中心的服务器，系统内各个客户端节点都可以通过交换直接共享计算机资源和服务。在 P2P 体系结构中，计算机可对其他计算机的要求进行响应，请求响应范围和方式都根据具体应用程序不同而有不同的选择。与 C/S 体系结构相似，P2P 体系结构要求用户使用专门的软件系统客户端，如图 1–7 所示。

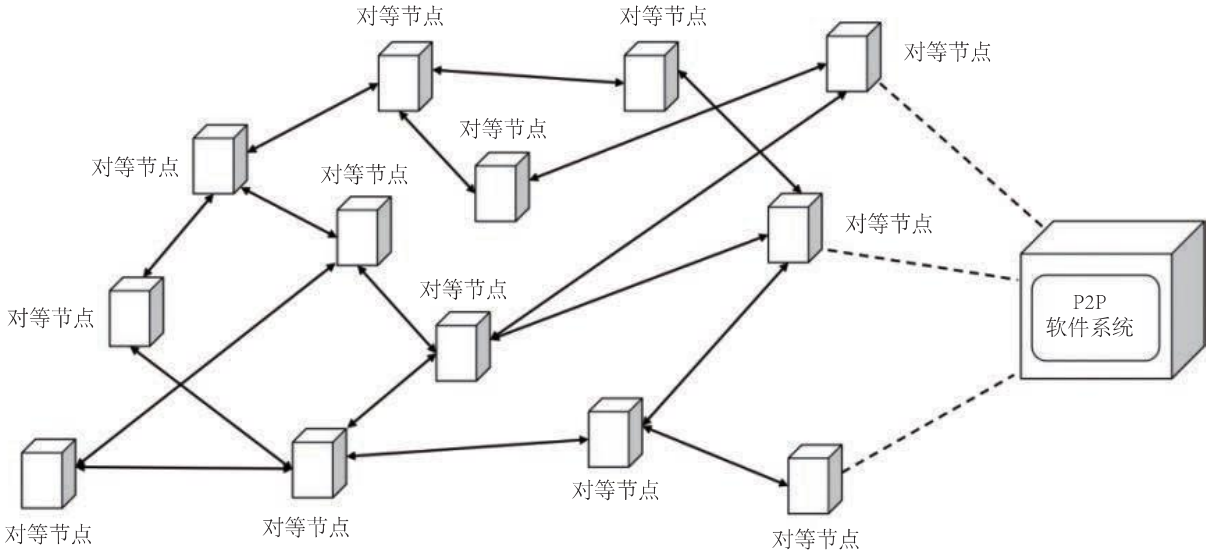

图 1-7　软件系统 P2P 体系结构示意图

1.4.1.2 系统逻辑架构

系统逻辑架构的目的是设计软件系统的逻辑层次结构，将系统功能和组件分成不同的功能层次，一般而言，最上层的组件和功能可以被系统外的使用者访问，相邻的层次之间能够直接相互调用。

系统逻辑架构常被划分为多个逻辑单元，称为“层”。每个层级都可包含多个功能组件，提供了一组高内聚的服务，并具有以下特点：

（1）每层都有特定的角色和职责。例如，展现层负责处理所有的用户界面。

（2）分层架构是一个技术性的分区架构，而非一个领域性的分区架构。

（3）分层架构中的每一层都可被标记为封闭或者开放。封闭层意味着请求必须按顺序通过每一层，不能跳过任何层。

OSI（Open System Internetwork）开放系统互连参考模型（如图 1-8 所示）具有最典型的分层逻辑架构，通过将开放系统的功能和组件划分成不同层次，通过层次之间定义清晰的接口，实现复杂的互操作性。

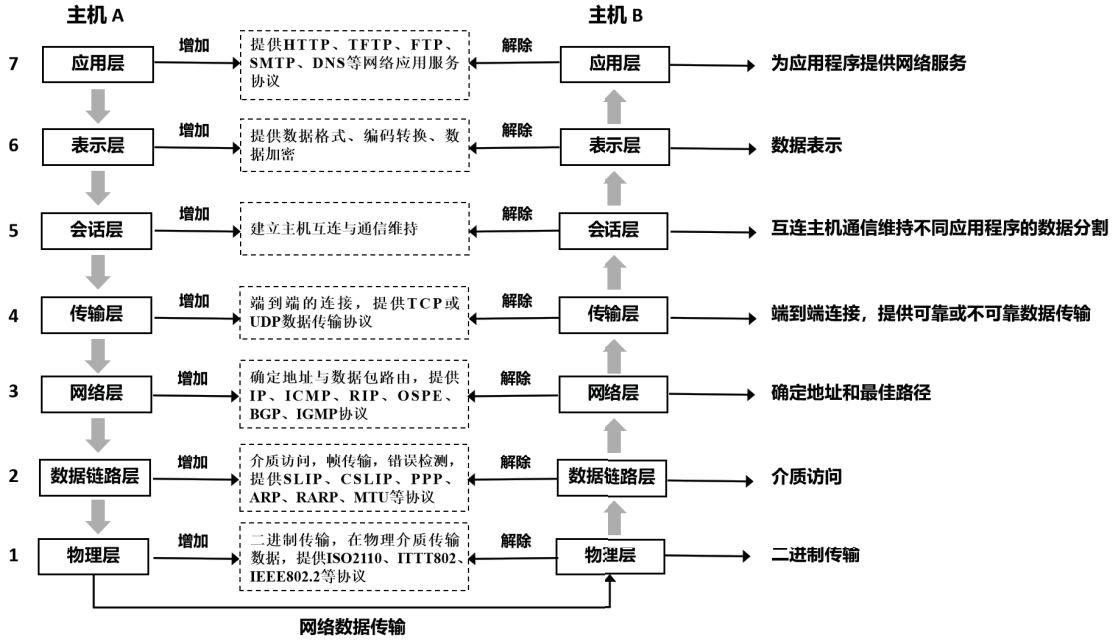

图 1-8　OSI 开放系统互连参考模型分层逻辑架构

以 OSI 开放系统互连参考模型为例，在其分层逻辑架构中，自上而下分为应用层、表示层、会话层、传输层、网络层、数据链路层、物理层，每一层实现各自的功能和协议，并完成与相邻层的接口通信。

（1）应用层是 OSI 参考模型中的最顶层，是为计算机用户提供应用接口，也为用户直接提供各种网络服务，如 HTTP、HTTPS、FTP、POP3、SMTP 等。

（2）表示层提供各种用于应用层数据的编码和转换功能，确保一个系统的应用层发送的数据能被另一个系统的应用层识别。数据压缩和加密也是表示层可提供的转换功能之一。

（3）会话层就是负责建立、管理和终止表示层实体之间的通信会话。该层的通信由不同设备中的应用程序之间的服务请求和响应组成。

（4）传输层负责建立主机端到端的链接，传输层的作用是为上层协议提供端到端的可靠和透明的数据传输服务，包括处理差错控制和流量控制等问题。该层向高层屏蔽了下层数据通信的细节，使高层用户看到的只是在两个传输实体间的一条主机到主机的、可由用户控制和设定的、可靠的数据通路。通常说的 TCP、UDP 协议就工作在传输层。

（5）网络层通过 IP 寻址来建立两个节点之间的连接，为源端的传输层送来的分组，选择合适的路由和交换节点，正确无误地按照地址传送给目的端的传输层。通常说的 IP 协议就工作在网络层。

（6）数据链路层将比特组合成字节，再将字节组合成帧，使用链路层地址（以太网使用 MAC 地址）来访问介质，并进行差错检测。

（7）物理层负责实现最终信号的传输，通过物理介质传输比特流。常用传输介质有集线器、中继器、调制解调器、网线、双绞线、同轴电缆。

1.4.2　区块链系统架构

1.4.2.1　区块链系统体系结构

区块链作为一种分布式计算软件系统，在体系结构上没有采用传统具有中心化服务器节点的 C/S 或 B/S 架构，而是采用无中心化节点的 P2P 体系结构，如图 1–9 所示。在区块链系统中，每个存储区块链与账本数据的网络节点都是对等关系，节点之间会共享区块链与账本数据，无论新区块从哪个节点生成，都会通过特定的 P2P 网络协议以广播的形式向其他节点进行传播，所有节点对区块进行验证后，新区块才能被添加到链上。尽管比特币、以太坊、超级账本等不同的区块链系统，在 P2P 体系结构的具体实现技术上并不完全相同，但是 P2P 体系结构是所有区块链系统必须具备的基本技术特征。

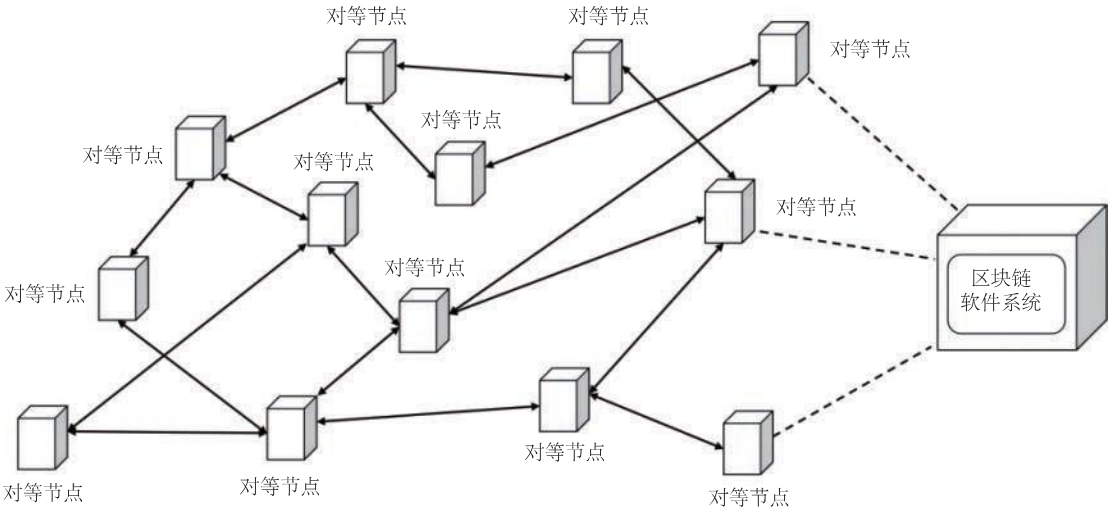

图 1-9　区块链 P2P 体系结构示意图

1.4.2.2　区块链系统逻辑架构

区块链技术经过比特币、以太坊、超级账本等几个阶段的发展，区块链系统的逻辑架构与功能层次已越来越完善和规范，从系统逻辑架构方面看，区块链系统自下而上可以分为存储层、数据层、网络层、共识层、激励层（可选）、合约层、接口层、应用层，每层又包含相应的功能组件，区块链系统参考逻辑架构如图 1–10 所示。

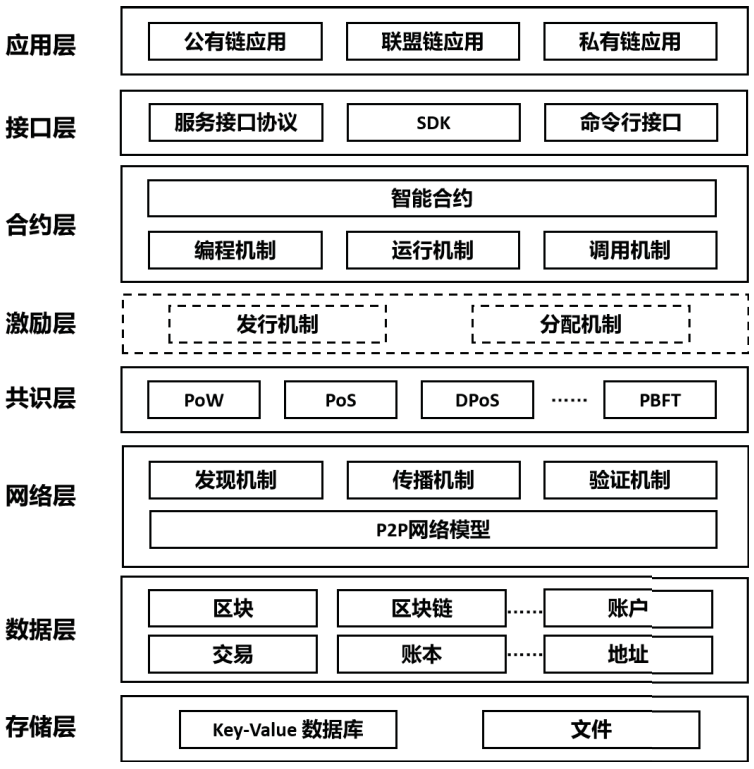

图 1-10　区块链系统参考逻辑架构

存储层为区块链系统相关的区块链、分布式账本、智能合约、X.509 数字证书、日志、配置文件等数据提供高效、可靠持久化存储服务。区块链系统一般采用的底层数据存储机制包括 Key-Value 数据库和文件系统。

数据层是区块链系统的核心功能层级之一，负责定义区块链系统相关的区块、区块链、交易、账本、账户、地址等关键数据结构，并基于底层的存储服务提供对区块链数据的安全读写访问管理。

网络层是区块链系统的核心功能层级之一，负责定义区块链系统相关的 P2P 网络模型与通信协议，为区块链系统各网络节点之间提供节点发现与安全连接通信机制，为交易、区块信息在区块链网络所有节点之间提供高效传播与有效性验证机制。

共识层是区块链系统的核心功能层级之一，为区块链系统提供一种或多种可选的公平、高效、安全、可靠的共识算法机制，让所有的区块链网络节点都认可每次计算产生的新区块，并且协调保证所有区块链网络节点数据记录一致性，使区块链系统的整体状态达成一致。

激励层是区块链系统可选的功能层级，以比特币、以太坊为代表的区块链系统，在共识层的功能基础上，提供了奖励加密货币的激励机制，对于加入区块链网络的节点，都有一定机率在区块链状态改变（如产生新区块、部署智能合约、智能合约被调用等）时被区块链系统增发奖励一定数量的加密货币。但是，以超级账本为代表的联盟链系统更多用于解决联盟内跨组织的信任服务问题，不需要类似奖励加密货币的激励机制。

合约层是区块链系统的核心功能层级之一，智能合约是将基于区块链的应用系统业务逻辑以可编程脚本或高级语言代码的形式开发后，由区块链系统的合约层负责对智能合约代码进行动态部署运行，并由系统根据既定规则的条件触发和自动执行，智能合约的源代码、调用过程与执行结果都会被记录到区块链上，杜绝合约篡改和抵赖。智能合约机制使区块链从最初单一的加密货币应用，延伸到政务服务、金融服务、征信管理、供应链管理、物联网等多个应用领域。

接口层定义了区块链系统对应用层和外部的服务 API 和管理接口。服务 API 对区块链系统的功能进行封装，采用如 RESTful、gRPC 等远程调用协议，为应用层或外部系统提供跨平台、便捷的区块链系统服务调用机制。区块链系统一般还提供命令行或 Web 服务接口，方便客户端或节点与区块链系统进行交互。

应用层包括基于区块链的各类应用，与区块链系统的类型密切相关。对于公有链来说，最普遍的应用就是比特币、以太币等加密货币与相关的支付、交易、结算、工具等应

用，以及基于智能合约的去中心化 DApp 应用；对于联盟链来说，更多的应用是实现跨组织或组织与个人之间的对等信任服务与数字资产化，如跨行业联盟的征信管理、供应链上下游溯源管理、跨多个政府单位的政务协同等；对于私有链来说，更多的应用是实现政府、企业内部重要业务数据的不可篡改，降低内控监督成本。

1.5 区块链技术应用概况

1.5.1 区块链的价值

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，提供一种在不可信环境中，由多方集体维护、不可篡改、可追溯、公开透明的分布式账本记账服务，在大幅降低第三方信任服务的成本和风险的前提下，实现信息与价值传递交换，提高服务效率，是一种创新的服务网络，是发展数字经济、构建变革性的价值生态系统的重要基础设施，具有重大的应用价值，体现在以下几个方面：

（1）区块链作为新一代信息技术，已逐步从金融领域延伸到实体领域，包括政务数据共享、征信、医疗、教育、电子信息存证、版权管理和交易、产品溯源、数字资产交易、物联网、智能制造、供应链管理等领域，正在迅速成为驱动各行业技术产品创新和产业变革的重要力量。

（2）区块链作为一种新型的去中心化或多中心化的信任服务工具，可以减少中间环节，让传统的高成本的中间机构成为过去，具有安全准入控制机制的联盟链和私有链已逐步成为国内应用的主趋势。区块链将促进各行业传统业务模式的创新，加速企业资产数字化和数据资产化的发展。

（3）区块链将推进数据记录、数据传播和数据存储管理模式的转型升级。区块链更像是一种互联网底层的开源协议，有望在现有互联网底层之上，逐步构建一个新的中间层，把信任机制固化到互联网底层协议中，甚至取代现有的互联网底层的基础协议，这将会是一个很重大的创新。

（4）区块链正在与云计算相融合，通过云链融合，使区块链获得云资源的开放性和易获得性，利用云计算服务模式，让基于区块链的应用系统快速进入市场，获得先发优

势。区块链与云计算的结合越发紧密，有望成为公共信用的基础设施。

（5）区块链将法律、经济、信息技术融为一体，有望促进社会的监管和治理模式的优化，社会治理组织形态也会因此发生一定的变化。区块链与集中化监管本质上并不存在冲突，区块链有望会成为构建基于合约的法治社会的有效工具之一。

1.5.2　区块链思维方式

在数字经济社会活动中，所有关系、交易关系、历史关系是三个重要关系，数字经济社会活动要良好、有效运行，其核心要素是这三个关系均要“可信”，因此“可信”是这三大根本关系的关键要素。

（1）所有关系。所有关系是人类社会生产关系的根本关系。所有关系是人类个体、组织之间建立交互关系的前提与基础，也是区分个体、组织的根本属性。人与人之间、组织与组织之间的不同，就是所有关系的不同。个人与组织可通过历史继承与生产创造活动形成所有关系，并通过交易活动进行所有关系的变更。

（2）交易关系。在所有关系之上，人类活动中所发生的所有交互关系，不管是从事一项互通有无的买卖，还是一次简单的谈话沟通，均可称为一次交易关系。交易关系与人类生产创造活动一起构成了人类活动的基本内容，人类社会活动的本质就是交易活动。交易活动可以让所有关系发生变更。

（3）历史关系。在人类价值创造、交易变更等活动过程中，形成了按时间顺序且不可逆的活动过程记录，即为历史关系。历史关系对评价个人、组织活动过程价值，以及基于已有过程价值再创新、再利用具有重要意义。人们以历史数据为基础，对活动主体的价值给出客观评估，并基于这些历史经验进一步优化和创新未来主体的活动。

区块链作为一种新型的信任体系，以一种新的模式和机制解决人类数字经济发展中迫切需要的去中心化信任服务体系问题。区块链与云计算、大数据相似，不仅是一种新的技术模式，也是一种创新的思维方式，更重要的是我们在学习、研究、应用区块链技术过程中，要逐步建立区块链思维方式。基于区块链的思维方式体现在以下几个方面：

（1）去 / 弱 / 多中心化。中心化是第三方中介信任体系的特征，而区块链是一种去 / 弱 / 多中心化的信任体系。因此，去中心化是研究应用区块链技术首先要建立的一种思维方式。开展一项涉及信任构建的工作，首先要思考，如果使用去中心化怎样来解决？不仅高价值数据资产及其相关计算能去中心化，普通 Web 数据访问存储也可以去 / 弱 / 多中心化。通过去 / 弱 / 多中心化思考，可能会获得中心化信任体系下难以获取的诸多新特性、

新能力。

（2）透明开放。研究应用区块链技术，在所属的共识范围内，需要机制、规则、代码的完全透明、开放，透明、开放是让共识群体积极参与的前提和基础；黑箱运行、潜藏规则或独有专利，在区块链中难以获得更大范围的共识，并难以被更多参与者所拥护。

（3）协同合作。不要试图一个人或一个机构独自完成所有工作和享有所有回报，要习惯人与人之间、团队与团队之间的协同合作，共定游戏规则，共建生态，共同发展产业，共获回报。

1.5.3 区块链应用现状

目前，区块链技术的应用领域不断扩大，从最初单一的加密货币应用，逐步从金融领域延伸到实体领域，包括政务、征信、医疗、教育、电子存证、版权保护和交易、产品溯源、数字资产交易、物联网、智能制造、供应链管理等领域，正在迅速成为驱动数字经济社会各行业技术创新和优化变革的重要力量，区块链应用的实际效果愈发明显。

根据中国信通院的研究数据，截至 2019 年 8 月，由全球各国政府推动的区块链项目数量达 154 项，其中荷兰、韩国、美国、英国、澳大利亚等国的政府推动项目数排名前五。中国在探索区块链技术研发、应用落地和人才培养方面表现更加积极。

2017 年 10 月 13 日，国务院办公厅发布的《国务院办公厅关于积极推进供应链创新与应用的指导意见》中提到，“研究利用区块链、人工智能等新兴技术，建立基于供应链的信用评价机制”。这份指导意见具有里程碑式的意义。全国各地方政府也都开始重视区块链技术，例如，杭州市的区块链产业园正式启动，河北省雄安新区上线区块链租房应用平台，无锡市成立“物联网 + 区块链”联合实验室，成都市批准成立区块链专委会，青岛市发力建设中国“链湾”等。同时，国内各互联网企业也早已开始布局区块链技术。据“2017 年全球区块链企业专利排行榜（前 100 名）”显示，前 100 名中国入榜的企业占比 49%，其次为美国，占比 33%。

2019 年 10 月 24 日下午，中共中央政治局就区块链技术发展现状和趋势进行第十八次集体学习。中共中央总书记习近平在主持学习时强调，区块链技术的集成应用在新的技术革新和产业变革中起着重要作用。我们要把区块链作为核心技术自主创新的重要突破口，明确主攻方向，加大投入力度，着力攻克一批关键核心技术，加快推动区块链技术和产业创新发展。

为了加快区块链专业技术应用人才的培养，2020 年 2 月 21 日，教育部发布的《关于

公布 2019 年度普通高等学校本科专业备案和审批结果的通知（教高函〔2020〕2 号）》批准成都信息工程大学开设全国首个“区块链工程”本科专业。同时，已有包括清华大学、北京大学、浙江大学、同济大学、武汉大学、中央财经大学、北京邮电大学、西安交通大学、上海财经大学、上海交通大学、电子科技大学在内的几十所高校都在积极推进区块链人才培养工作，开设了区块链相关课程。

中国的区块链应用发展方向与欧美国家不同。在欧美国家，区块链项目以代币发行 ICO（Initial Coin Offering）为主，有大量的 ICO 项目涉嫌从事非法金融活动，严重扰乱了经济金融秩序。与欧美国家不同，在中国区块链的 ICO 项目被明令禁止，区块链技术向着落地应用方向发展。随着区块链应用的纷纷落地，中国区块链的底层技术研发也正在走向全球，中国将有巨大潜力推动全球区块链产业的发展。

本章小结

通过对本章内容的学习，读者应该全面了解区块链技术产生的背景及其技术起源，掌握区块链的相关基本概念、特点和类型，了解区块链技术发展的三个阶段及每个阶段的典型代表性区块链系统，即比特币、以太坊和超级账本区块链系统；初步认识区块链系统的总体架构，包括区块链系统的体系结构、逻辑分层架构；同时，学会理解区块链的价值与思维方式，了解区块链技术国内外发展应用情况。