第一章 区块链概述

【学习目标】

1. 了解区块链技术的相关概念和基本原理。

2. 熟悉区块链的构成与区块链的形成过程。

3. 掌握区块链主要技术应用和未来发展前景。

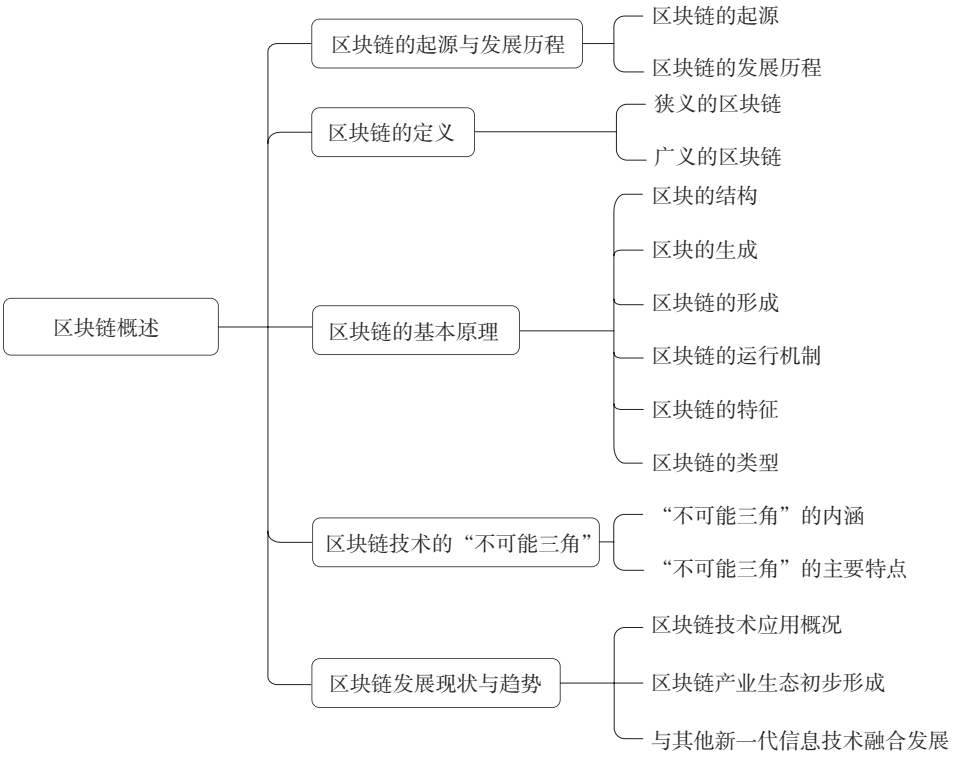
【能力目标】

1. 了解区块链技术的相关概念和基本理论，能自主查阅相关资料拓展知识。

2. 熟悉区块链技术的“不可能三角”，培养学生的系统思维和批判性思维能力。

3. 掌握区块链的应用方向和发展趋势，提高学生的创新意识和技术应用能力。

【思维导图】



【导入案例】

区块链技术随着数字货币的出现进入一般大众的视野，并得到广泛关注。作为一种去中心化技术，区块链技术有可能演变成为继蒸汽机、电力、信息和互联网技术之后的第五次颠覆式革命技术。区块链技术对人类社会已经产生了广泛的影响，它被广泛应用于金融、政务、司法存证、版权保护、产品溯源等多个领域。要想深刻地理解区块链技术对金融行业产生的深远影响，更好发挥它在金融领域的价值，就需要理解区块链技术。

本章主要介绍了区块链技术的起源与发展、区块链的概念与基本原理、特征、类型以及区块链技术发展现状与趋势。

第一节　区块链的起源与发展历程

一、区块链的起源

2008 年，一位化名中本聪（Satoshi Nakamoto）的学者首次提出了区块链的概念，他构建了一套完全基于点对点技术实现的电子现金系统，提出了“基于密码学原理而非信用，使达成交易（transaction）的双方可直接进行支付、不需要第三方中介参与”的交易系统，该系统解决了在没有中心机构的参与下数字货币的发行和流通问题。 2009 年 1 月 3 日，中本聪又将理论付诸实践，挖掘出第一个序号为 0 的创世区块，这标志着区块链的正式诞生。从那时起，区块链技术逐渐从一种数字货币的底层逻辑发展成为一项全球性的技术并迅速发展，被广泛应用于各种领域。它被认为是一种具有潜力的技术，可以应用于金融服务、供应链管理、智能合约、数字资产管理等领域，为实现去中心化、可信任和高效率的交易与数据管理提供了新的可能性。

二、区块链的发展历程

区块链专家梅兰妮·斯万[①]（Melanie Swan）在其著作《区块链：新经济蓝图及导读》中，根据区块链技术在不同阶段的应用场景与实现功能，把区块链的发展划分为区块链 1.0、区块链 2.0 和区块链 3.0 三个阶段，目前得到了业界广泛的认可。

（一）区块链 1.0：数字货币（2008—2014 年）

区块链 1.0 以加密数字货币的应用为主，目标是实现数字货币的去中心化以及解决数字货币的交易与支付问题。

区块链的出现开启了无须“第三方信任机构”的数字货币时代，这项技术使去中心化的数字货币得到了大规模试验。数字货币的快速兴起，催生了大量的数字货币交易平台，同时也引起了各国中央银行、金融机构的广泛关注，越来越多的国内外金融机构开始“拥抱区块链”。由于越来越多的人认知到了区块链技术的价值，对区块链的研究与应用热情不断高涨，投入区块链技术的资源

① 梅兰妮·斯万是区块链研究所（Institute for Blockchain Studies）创始人，她解释了区块链在本质上是一个公开账簿，拥有成为所有资产的登记、编册和转让的全球性的、去中心化记录的潜力——这些资产不仅仅包括资金，也可应用于诸如投票、软件、健康数据和思想等各类财产和无形资产。

也开始不断增长。

从 2014 年开始，针对区块链技术的并购和投资便火热起来，包括巴克莱银行、桑坦德银行和摩根大通集团在内的全球众多金融机构开始积极开展区块链技术的研发和储备，为逐步将区块链技术应用到金融领域打下基础。2014 年，戴尔、微软等公司先后宣布加入开放式账本系统研发，区块链并购投资出现热潮。同时，许多国外大型金融机构和企业纷纷开展区块链技术的应用试验。分布式账本初创公司 R3 CEV、LLC 公司宣布与高盛、瑞士银行等几家银行结成联盟，共同开发区块链技术，共享区块链技术试验数据，共同探索区块链技术在金融领域的应用。同年，微软联合 R3 CEV 区块链联盟，共同研究并积极探索区块链技术，与全球 40 多家大型银行签署区块链合作项目。中国平安保险集团成为国内首家加入 R3 CEV 区块链联盟的金融机构。

（二）区块链 2.0：可编程金融（2015—2017 年）

2015 年被称为区块链元年，划时代的标志是《华尔街日报》刊文称“区块链是近 500 年以来金融领域最重要的突破”。2015 年 10 月 31 日，《经济学人》期刊刊登了《信任的机器》一文，该文提出“区块链是制造信任的机器”，区块链可以让人们在没有中央权威机构监督的情况下彼此之间建立起信任。并且其强调“区块链技术创新所承载的意义延伸价值远远超出了加密货币本身”。

进入 2016 年后，区块链价值的重要性开始被业界大规模地认识到。在这一阶段产生了运行在区块链上的智能合约，区块链技术应用进入可编程金融的区块链 2.0 阶段。智能合约作为区块链 2.0 时代的重要标志，是一种模块化、可重用、自动执行脚本的合约，其核心是应用程序算法替代人工来执行合约，其中，以太坊（Ethereum）是区块链 2.0 的典型代表，它实现了数字资产的编程应用，让一切有价物在技术上都可实现资产化。

通过应用智能合约区块链技术大大拓展了它的应用范围，其开始被应用于股权、债权和产权的登记、转让，以及延伸到保险、证券、租赁、征信、清算结算等金融合约的交易与执行等领域。2017 年世界经济论坛发布的区块链白皮书中预测，到 2025 年区块链产业的产值将占全球 GDP（国内生产总值）的 10%。

（三）区块链 3.0：可编程社会（2018 年至今）

区块链 3.0 被称为可编程社会，该阶段区块链技术突破了在金融领域的应用，作为一种泛解决方案开始被广泛应用在政府行政管理、金融、物流、物联网、企

业供应链、医疗、法律、版权保护、社交通信等其他众多领域。区块链的应用提高了整个社会各个行业运行效率，由于区块链具有底层开源和创新业务多方共识（consensus）等逻辑，因此区块链成为未来整个 IT（信息技术）架构和互联网转型的重要支撑，它是价值互联网的核心。区块链技术让人类生活建立在许多应用和工具中，社会进入“可编程”状态和智能化的时代。

实际上，区块链发展的三个阶段仅是区块链技术应用的范围不同，从区块链 1.0 到区块链 3.0 都处于平行发展状态，区块链 1.0 是区块链技术的萌芽和主要在数字货币上的应用，区块链 2.0 是区块链在数字资产、智能合约方向的技术落地，区块链 3.0 是为了解决各行各业的信任问题与数据传递安全性的技术实现。

第二节　区块链的定义

区块链是一项集成了计算机科学、数学、密码学、经济学等多学科领域研究成果的组合式创新技术。在工业和信息化部信息化和软件服务业司及国家标准化管理委员会指导下，2016 年由中国区块链技术和产业发展论坛编写的《中国区块链技术和应用发展白皮书（2016）》是我国关于区块链技术的第一份官方指导文件，其中对区块链从狭义和广义两个层面进行了诠释。

一、狭义的区块链

狭义的区块链是指“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数据难以篡改和不可伪造的分布式账本”。

狭义的区块链也被称为分布式账本技术（distributed ledger technology，DLT），在中国人民银行 2020 年 2 月发布的《金融分布式账本技术安全规范》中，将分布式账本定义为“可以在多个站点、不同地理位置或者多个机构组成的可分享资产数据库”。

从数据结构的角度看，区块链是一条由哈希指针串联起来的区块链表，每个区块（block）中包含一系列交易。从系统的角度看，区块链是由多个互不信任的节点共同维护全网一致账本的分布式系统。从应用的角度看，区块链可以被看作一个根据时间顺序记录了某一时间段内所有发生交易的相关信息的完整“账本”。该“账本”最大的特点是只能对数据进行添加而不能删除，也就是说，

区块链存储了所有的历史数据，并且以只增的方式进行维护。所有参与者共同记录、集体维护以保证账本的真实可信与安全。

分布式账本与中心化账本如图 1–1、图 1–2 所示，二者主要区别见表 1–1。

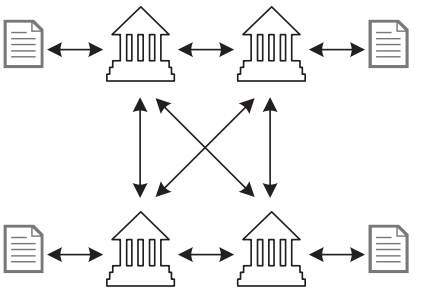


图 1-1 分布式账本示意图

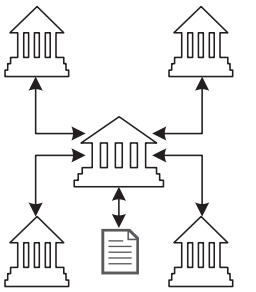


图 1-2 中心化账本示意图

表 1–1 分布式账本与中心化账本的主要区别

项目	分布式账本	中心化账本
存储方式	分布式存储	中心化存储
审核方式	参与者共同审核	中心集中审核
共享方式	所有节点共享数据	不能共享数据
数据记账权	共识算法获得	中心指定
保密方式	非对称加密技术 + 哈希算法	密码

二、广义的区块链

广义上，区块链是指“利用区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去中心化基础架构与分布式计算范式”。

从广义的区块链定义可以看出，区块链并不是“某一项技术”，而是“多种技术”的有机整合，它整合了链式数据结构、P2P 网络技术、共识算法、密码学、自动化脚本等多种技术。其中，基于时间戳的链式区块结构、分布式网络的共识机制、可编程的智能合约是区块链技术最具代表性的创新。区块链技术实现的所有功能都是由这些技术共同支撑的，缺一不可。

从技术角度上，区块链主要解决了三个关键问题：①如何完整地存储数据并可实现数据追溯；②如何构建一个可以实现分布式共识的网络；③如何确保网络的安全运行。

区块链的本质是“一个去中心化的共享总账数据库”。作为公共的数据账本，区块链网络中每个节点都存有一个完整的数据备份，这意味着它存在高度的数据冗余。但这种数据冗余不只是为了保证系统的可靠性，甚至可以说基本不是为了确保系统的可靠性而作出的冗余，而是所有技术的设计与应用是为更好地维护好该分布式数据账本，以确保数据不可篡改、不可伪造，确保数据的高度透明与共享。

第三节　区块链的基本原理

“区块 + 链”的数据结构是区块链的核心技术之一。区块在区块链网络中承载交易数据，是一种标记有时间戳和前一区块的哈希值的数据结构；链是由区块按照发生的时间顺序，通过区块的哈希值串联而成的链式结构，是区块交易及状态变化的日志记录。

一、区块的结构

区块是构成区块链的基本单位，它主要由区块头和区块主体两部分组成，如图 1–3 所示。

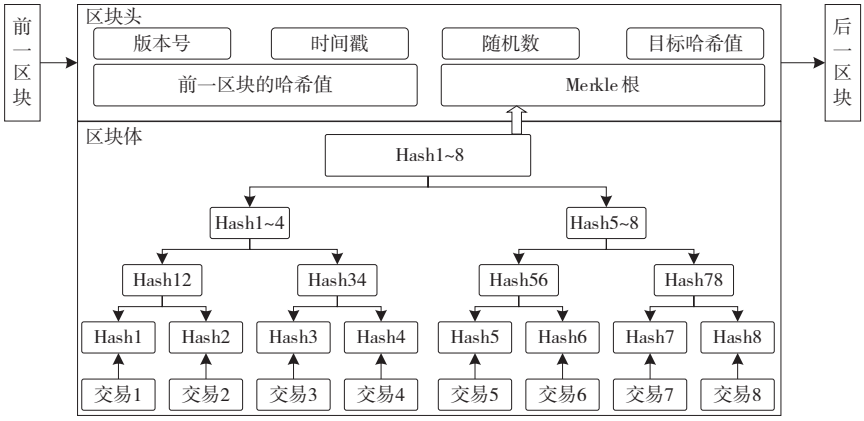


图 1–3　区块的结构

（一）区块头

区块头主要包括区块的版本号、前一区块的哈希值、时间戳、随机数、区块产生的难度值、目标哈希值、区块的 Merkle 根等信息，见表 1–2。

表 1–2 区块头的构成

字段	描述
区块的版本号	标识软件及协议的相关版本信息
前一区块的哈希值	本区块的父区块头的哈希值，将本区块与前一区块组成首尾相连的区块链
时间戳	本区块产生的时间，精确到秒
随机数	本区块工作量证明算法的难度值
目标哈希值	本区块的哈希值
区块的 Merkle 根	该值由所有交易的哈希值生成，如果其中一个交易被修改，该值就会变化

（二）区块主体

区块主体用来存储数据，一般包含一段时间内所有的交易信息。所谓交易，是一次针对数据账本的操作，它会导致账本状态的一次改变。一个区块主体要至少包括一个交易，如添加一条转账记录。

二、区块的生成

区块的生成过程如图 1–4 所示。

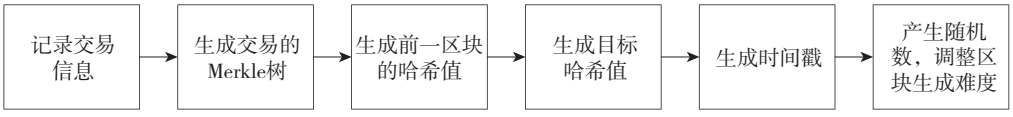


图 1–4 区块的生成过程

（1）记录交易信息。把网络上某个时间段的所有交易信息记录到区块体中。

（2）生成交易的 Merkle 树。在区块体中生成所有交易信息的 Merkle 树，并把 Merkle 树的根值存储在本区块的区块头中。

（3）生成前一区块的哈希值。把前一区块（父区块）的哈希值保存在本区块头的“前一区块的哈希值”字段中。

（4）生成目标哈希值。通过哈希算法将区块头中的数据生成哈希值，并保存

在本区块头中的“目标哈希值”字段。

（5）生成时间戳。把当前时间保存在本区块头的“时间戳”字段中，其中，时间戳是用来证实该区块在某特定时间是存在的。

（6）产生随机数，调整区块生成难度。其代表本区块产生的难度值。难度值会随着前一段时间区块生成平均时间进行调整，以应对整个网络不断变化的计算量。如果计算量降低，系统会提高数学题的难度值。

在当前生成的区块加入区块链后，则开始下一个区块的生成。

三、区块链的形成

从外观上看，区块链是以区块为基本单位连接形成的链状数据结构，它是一个线性的链表，这也是“区块链”名字的来源，如图 1–5 所示。其中“链”是通过应用时间戳机制以确保一个个“区块”按生成的时间顺序连接起来。同时，在当前区块的区块头中都存有前一个区块（父区块）的哈希值，这样就形成了区块链。

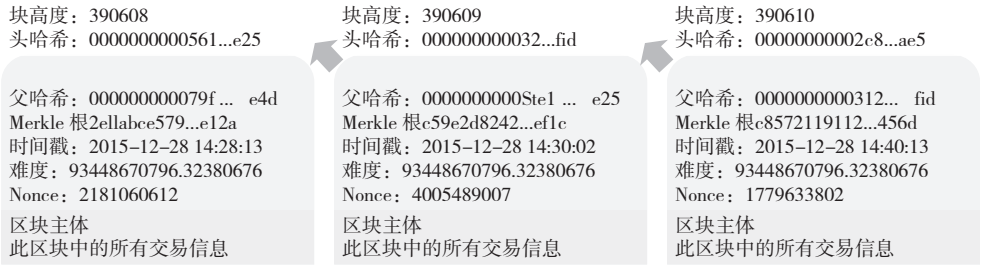


图 1–5　区块链示意图

四、区块链的运行机制

区块链中的每个区块就如同“总账”中的一页，都会记录从上一个区块生成后至本区块被创建的这段时间内所发生的全部交易信息，其中，交易信息可以是一条或者多条。生成添加一个新的区块就相当于账本上多了一页，从而保证了“总账”的完整性。网络中的任一节点都可以提议生成一个新的区块，但这个新的区块以及区块中的交易是否合法需要通过计算哈希值的方式进行检验，并经过共识机制对最终上链的区块达成一致。

区块链的运行机制理解起来并不复杂，它实际上就是针对整个交易状态变化的日志记录。如果把区块链看作一个状态机，那么每次交易就是试图改变一次状态；每次通过分布式网络共识机制生成的区块，就是参与者对区块中交易导致的状态改变结果进行的一次确认。

下面举例说明区块链如何运行，如图 1–6 所示。

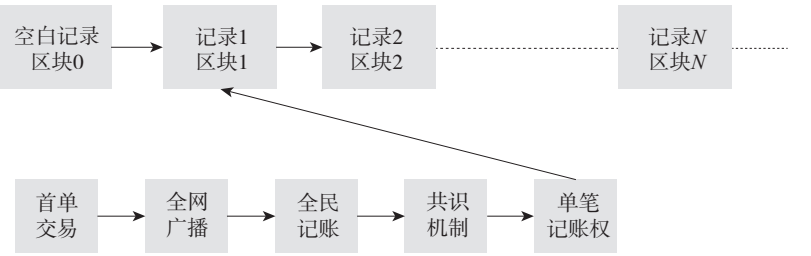


图 1–6　区块链的运行机制

假设当前网络中还没有进行过任何的交易，也就是账本为空。

（1）首单交易。网络中的节点 1 与节点 2 进行了一次交易。

（2）全网广播。新的交易将向全网进行广播，也就是节点 1 与节点 2 的交易信息发送至网络中的每个节点。

（3）全民记账。所有节点在收到这条新的交易信息后都需要记账，也就是每个节点都要对本次交易进行记账。

（4）共识机制获得记账权。由于每个节点都在记账，那么以谁的记账为准就需要有一个共识机制，网络节点获得记账权，可以简单理解为按某种标准进行评比后择优录用，如以又快又准作为标准。经过共识机制后，假设网络所有节点都认为节点 3 对这笔账记得最快最准，那么就会把这笔交易的记账权授予节点 3。

（5）写入区块并更新账本。节点 3 对这次交易的记录被确认为第 1 条记录写入区块。同时，由节点 3 对交易记录信息进行全网广播，其他节点就相当于获取了账本副本。

随着交易继续进行，以上（1）至（5）过程就会周而复始地进行下去。这样一条条的记录也就生成了网络中唯一的账本，形成了一个合法记账的区块链。

五、区块链的特征

区块链技术具有去中心化（decentralized）、防篡改性（untampered）、可追溯性

（traceability）、去信任（trustless）和自治性（autonomy）等主要特征。

（一）去中心化

去中心化是相对于中心化而言的，区块链系统采用的是分布式存储和计算，网络中没有中心化的服务器或管理机构。网络中每个节点都可以成为中心独立运行，每个节点权利与义务均等，任意两个节点之间都可以进行点对点交易而无须第三方机构介入。即使有节点出现故障或者遭受攻击，也不会影响整个网络的运行。

（二）防篡改性

防篡改性是指在区块链中每个节点都记录并保存了一个完整的历史交易数据账本，并由全网所有节点对数据进行集体维护，一旦交易数据经过全网节点的验证并添加到区块链就很难被修改或删除。这主要是因为区块链的数据结构保证了区块链数据的不可篡改。前面讲过，每个区块的区块头中都储存有上一个区块的哈希值，一旦链上某一区块记录的数据发生变动，该区块的哈希值就会随之改变，这就意味着后续所有区块内容都会发生变动，因此所有节点都能发现数据被篡改过并选择不认可丢弃该无效数据。

当然，区块链中的分布式账本也不是绝对不能被篡改，但篡改的难度很大。由于所有节点都拥有一个完整统一的账本，对单个节点账本的修改无效，只有控制了网络中超过 51% 的节点才能实现篡改数据。并且当区块链延伸到一定长度的时候，要想攻击 51% 以上的节点技术上是非常困难的，所以区块链的数据稳定性和可靠性较高。

（三）可追溯性

可追溯性是指由于区块链是带有时间戳的链式区块结构，区块链上发生的任何一笔交易都有完整记录，时间戳技术保证了交易信息按时间顺序全程可追溯至起始区块。同时，区块的区块头中都包含前一个区块的哈希值的设计，使数据也可追溯至起始区块。数据的可追溯在间接上也保证了数据的公开透明性。

（四）去信任

去信任是指区块链在去中心化的前提下实现了点对点的直接交易。去信任并不是说不需要信任，完整地描述应该是“去第三方信任”。区块链技术通过自身一套独特的信任机制创造了信任，网络中的节点交易无须建立预设的信任机制，如交易双方因熟悉产生的信任、依赖第三方中介产生的信任等。

（五）自治性

自治性是指区块链是基于共同协商一致的规范和协议，使网络所有节点能够在去信任环境中按照共识规则来记录、共享分布式账本。区块链技术的自治性还体现在智能合约的应用上。密码学家尼克·萨博（Nick Szabo）1994 年首次提出了智能合约，它是指一旦条件触发合约就会不受干扰自动执行，从而实现从对“人的信任”到对“机器信任”的转变。

六、区块链的类型

根据应用场景与设计体系不同，区块链可分为公有链、私有链和联盟链三类。

（一）公有链

公有链是指网络中不存在任何中心化的节点，任何节点均可自由加入、退出区块链系统，并参与链上数据的读写。所谓“公有”就是指数据完全公开透明，节点没有权限设定，也没有身份认证，任一节点都可查看。公有链中节点的数量是不固定的，节点是否在线也无法控制，甚至某一节点是不是恶意节点也不能保证。由于没有第三方管理，公有链需要依靠一组事先约定的规则，该规则确保在不信任的网络环境中每个节点能发起可靠的交易。

凡是需要公众参与，需要最大限度保证数据公开、透明的系统都适用公有链，如数字货币系统、众筹系统、金融交易系统等。

（二）私有链

私有链与公有链相对，它也被称为专有链。所谓“私有”就是指不对外开放。私有链的节点来自机构内部，且节点只有经过认证、授权后才能加入私有链系统，并共同维护区块链的正常运行。私有链仍具有区块链多节点运行的通用结构，但在使用中除了有注册和身份认证要求外，还具备一套权限管理体系。每个节点的写入权限由内部控制，而读取权限可视需求有选择地对外开放。在私有链系统中，节点数量、节点状态通常可控，因此私有链一般不需要通过竞争的方式获取对区块的写入权限，可以更节能环保。

适用私有链的主要场景有特定机构内部的数据管理与审计，如企业的票据管理、账务审计、供应链管理，或某些政务管理系统等。

（三）联盟链

联盟链是指各节点通常有与之对应的实体机构，经过授权后才能加入和退出

联盟链系统。联盟链中的各机构组成利益相关的联盟，共同维护区块链的运转。联盟链的网络范围介于公有链与私有链之间，与私有链一样，联盟链系统一般也具有身份认证和权限设置，且节点的数量往往也是确定的。

联盟链通常被用在明确的机构之间，可用于机构之间的事务处理，如银行间的支付结算与清算、企业间的物流信息交换等。

表 1–3 列出了公有链、联盟链和私有链三类链的主要不同。因公有链和私有链都存在一定的技术限制，在应用中存在一定的缺陷，所以采用部分中心化的联盟链代表区块链未来的应用趋势。

表 1–3　不同类型的区块链比较

项目	公有链	联盟链	私有链
参与节点	所有节点进入或退出不受限制	节点必须经授权才可进入	通常在一个组织机构内部
匿名性	节点通常是匿名的	节点身份需要审核	节点身份需要审核
共识机制	PoW/PoS/DPoS 等	分布式一致性算法	分布式一致性算法
记账人	所有参与者	联盟成员协商确定	自定义
激励机制	需要	可选	可选
中心化程度	去中心化	多中心化	中心化
突出特点	信任的自建立	效率与成本优化	效率高
数据写入能力	3~20 次 / 秒	1 000~1 万次 / 秒	1 000~20 万次 / 秒

【案例】基于联盟链的机构间对账平台

第四节　区块链技术的“不可能三角”

一、“不可能三角”的内涵

在传统货币银行学中存在“不可能三角”，也称为“三元悖论”，即开放经济下，一国无法同时实现货币政策独立、汇率稳定与资本自由流动，最多只能同时实现两个目标，而放弃另一个目标。类似地，当前的区块链技术也存在“不可能三角”。所谓区块链技术“不可能三角”，就是指当前的区块链技术无法同时满足去中心化、安全性和高效性三个条件。选择应用区块链技术时需要在三者中进行权衡，最多只能同时满足其中两项。

二、“不可能三角”的主要特点

（一）满足“去中心化”与“安全性”无法完全实现“高效性”

去中心化和安全性被认为是区块链技术的最大优势，但因它主要依赖于分布式账本技术，区块交易数据需要在全网广播并需要被所有网络节点进行验证，因此效率低成为区块链技术应用中的最大缺陷，具体表现在以下四个方面。

（1）在数据结构上，虽然区块链基于时间戳的区块链式结构在交易数据的可追溯、防篡改上具有安全优势，也易于分布式系统中的数据同步，但当需要对数据信息进行查找、验证时，会涉及对整个链的遍历操作，而遍历是一种较低效率的查询方式。

（2）在数据存储上，区块链每个节点都存储所有数据包，通过强冗余性实现强容错、强纠错，使得网络实现民主自治。但每个节点存储所有交易数据致使对存储空间的高消耗。随着区块链所承载信息内容的不断增加，这对单个节点的存储能力也提出了挑战。

（3）在内容验证上，区块链的每个节点都有完整的交易数据，同时还要对区块内的所有交易数据进行哈希运算，虽然提高了安全性，但对大量数据处理会影响效率。

（4）在并发处理上，区块链只允许网络中的一个节点获得记账权并建立区块，实质上是对整个链进行串行的“写”操作。虽然它能有效保证网络运行的安全性和稳健性，但效率远低于我们常用的关系数据库。因为关系数据库是将数据分为若干表，仅仅根据操作涉及的数据锁定表或表中记录，其他表仍能实现并发处理。

目前主流的私人数字货币的区块链技术是一种追求“去中心化”和“安全性”而无法达到“高效性”的典型技术组合代表。国际清算银行（Bank for International Settlements）研究发现：与在线支付、PayPal（贝宝）相比，主要私人数字货币的交易效率与传统支付方式仍然有巨大差距，见表 1–4。

表 1–4　主要私人数字货币与传统支付方式的交易效率比较

类型	VISA	MASTER	PayPal	以太币	莱特币
交易效率 /（次 / 秒）	3 526	2 061	241	3.18	0.26

资料来源：Bank for International Settlements. BIS Annual Economic Report 2018[EB/OL].（2018–06–24）. https：//www. bis. org/publ/arpdf/ar2018e.htm.

（二）满足“安全性”与“高效性”无法完全实现“去中心化”

从共识机制的角度，在确保区块链安全性的前提下，为解决区块链技术所使用的工作量证明机制的低效性，出现了权益证明机制、股份授权证明机制。但无论是基于网络权益代表的权益证明机制，还是利用受委托人通过投票实现的股份授权证明机制，实际上都是对完全“去中心化”的退让，最终形成“部分去中心化”。

如私有链中，为确保安全与高效，其已经完全演化成为一种“中心化”的技术。联盟链只允许预设的节点进行记账，加入的节点需要申请和身份验证，实质上也是在确保安全与提高效率的基础上进行的“部分去中心化”或“多中心化”的妥协。还有如作为区块链 3.0 的代表，商用分布式区块链操作系统 EOS（enterprise operation system，企业运营系统）方案，就是一种旨在追求分布式应用性能的“高效性”与“安全性”，却牺牲“去中心化”的技术组合。

（三）满足“去中心化”与“高效性”无法完全实现“安全性”

一个极端的例子就是基于 P2P 的视频播放软件。在过去，一旦在线观看人数增加，基于中央服务器设计的视频服务器会因承载压力变大而导致播放速度缓慢。为了提高效率，P2P 视频播放软件被设计为：①资源的分享采用不再依赖于中央服务器的“去中心化”模式。网络中的每个节点不仅是下载者同时也是服务器，一个节点在下载、观看视频文件的同时，也能将数据传输给其他节点。去中心化网络中参与节点越多，数据传输越快、效率越高。② P2P 视频播放软件牺牲安全性，允许传输的数据出现少量错误。视频中少量图片的局部数据损坏并不影响正常的视觉感官，但因数据校验而出现的图像延迟是不可接受的。当然，金融业数据错误是不可接受的，安全性是首要考虑的目标。

“不可能三角”的重要意义在于：当前的技术条件尚无法同时满足三者的需求，区块链技术设计中不能完全抛开“三角”中的其他两者而孤立地去谈其中之一。倘若能对这三者中的一个或两个条件进行妥协，所产生的新技术集合就可能因更符合实际需求，在应用中的吸引力更大。

第五节　区块链发展现状与趋势

一、区块链技术应用概况

作为数字经济发展的重要支撑，区块链在推动经济转型、产业升级方面发挥的支撑作用愈加明显。在政策、技术、市场的多重推动下，区块链技术的创新应用加速，全球区块链产业也处在快速扩张中。据统计，2021 年全球区块链产业共有 1 812 笔融资事件，其中，1 433 笔公开披露具体融资总额，总计达 486.74 亿美元、平均单笔融资额达 3 396.65 万美元；3 月的融资数量为全年最高，有 239 笔；8 月的融资金额为全年最高，合计达 73.07 亿美元，如图 1–7 所示。

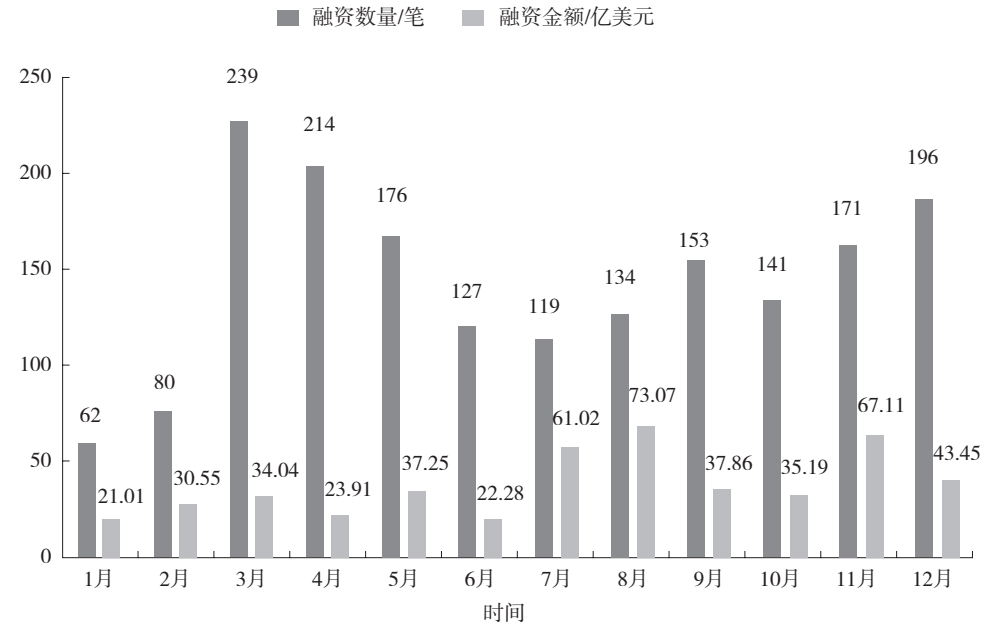


图 1–7　2021 年全球区块链产业融资数量及金额

资料来源：零壹智库 . 全球区块链投融资报告（2021）[EB/OL].（2022–02–16）. https://www.01caijing.com/article/311093.htm.

截至 2022 年 9 月，全球共有区块链企业 6 900 余家，其中，中美两国区块链企业合计占比超过 50%，处于全球领先水平；新加坡、英国均超过 400 家，位于第二梯队；印度、加拿大、瑞士、韩国、德国、中国香港等国家和地区均超过 100 家，位于第三梯队。①

① 中关村区块链产业联盟 . 全球区块链产业图谱报告 [R]. 2022.

目前，全球区块链应用主要通过组建区块链联盟模式来推进，国际上共有五个区块链联盟组织（表 1–5）。组织成员通过合作开展相关技术和场景应用的探索，并通过发挥区块链联盟组织的辐射效应，吸引更多企业加入相关联盟组织。

表 1–5　区块链联盟组织基本信息

发起时间	联盟名称	发起机构	现有成员数	联盟宗旨
2015 年 9 月	R3	R3 CEV 公司联合巴克莱银行、高盛、J.P. 摩根等 9 家机构	近 400 家	推动全球金融市场中加密技术和分布式总账智能协议的应用，帮助区块链技术的落地应用、商业化
2017 年 8 月	Blockchain in Transport Alliance（区块链货运联盟）	行业发起	近 400 家	降低成本、提高运输效率。推动新兴技术落地，发展区块链行业标准、交流与推广区块链应用、解决方案及分布式账本技术
2015 年 12 月	Hyperledger（超级账本）	Linux 基金会	近 300 家	让成员共同合作、共建开放平台。满足来自多个不同行业各种用户的需求，并简化业务流程。实现区块链的跨行业发展与协作，并着重发展性能和可靠性，使之可以支持全球商业交易
2017 年 3 月	Enterprise Ethereum Alliance（企业以太坊联盟）	摩根大通、微软、英特尔等 30 家企业	200 余家	致力于合作开发标准和技术，提高以太坊区块链的隐私性、安全性和扩展性，使其更加适用于企业应用
2019 年 4 月	INATBA（国际可信区块链应用协会）	欧盟	150 余家	制定规范，促进标准统一和监管融合，以支持创新型区块链技术的开发和应用

德国在 2019 年 9 月 18 日发布了“德国区块链战略”，明确区块链国家战略，认为区块链技术在未来是互联网的组成部分，可以有效助力德国数字经济的发展。美国在 2020 年 10 月公布了“国家关键技术和新兴技术战略”，将区块链纳入管制技术以保护国家基础设施的安全。澳大利亚于 2020 年 2 月 7 日发布了“国家区块链路线图”，强调区块链技术的潜力，同年发布《数字经济战略 2030》，进一步强调要在区块链等新兴技术领域保持前沿地位。日本于 2022 年 5 月将以区块链基础设施为技术支撑的新一代互联网框架 Web 3 发展上升为国家战略，并于同年 6 月批准了日本《2022 年经济财政运营和改革的基本方针》，提出将努力为实现一个去中心化数字社会进行必要的环境改善。

在我国，区块链于 2019 年被提升至国家战略层面，2020 年被列入新基建范畴，2021 年被列入“十四五”规划成为数字经济重点产业之一。区块链产业正呈

现出健康发展的态势，除了在金融领域的广泛应用外，区块链技术正在加速与实体经济融合，助力实体经济高质量发展。数据显示，自 2016 年开始，我国区块链企业注册数量快速增长，2020 年有 2 万多家。其中，广东的注册企业最多，其次是山东、海南。2021 年，我国区块链产业规模由 2019 年的 10.7 亿元增长至 65 亿元，市场规模在两年内扩张了五倍，行业发展趋势向好，如图 1–8 所示。根据预测，中国区块链市场将保持高速增长，2021—2026 年市场规模年复合增速达 73%，2026 年的市场规模将达到 163.68 亿美元，且在未来 20 年，中国区块链行业市场规模有望达万亿级别。

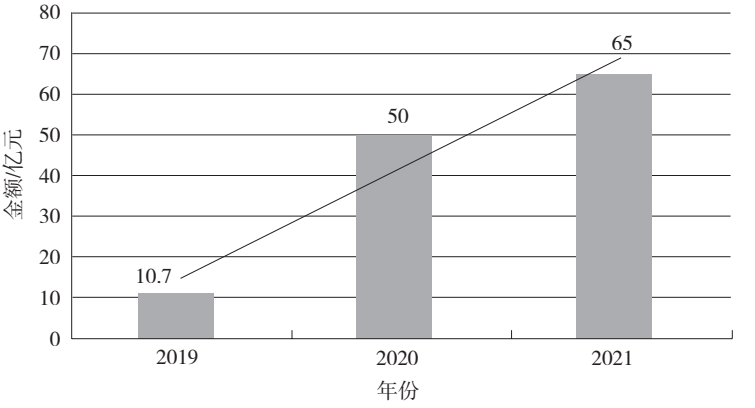


图 1–8　2019—2021 年中国区块链产业规模统计

资料来源：零壹智库 . 全球区块链投融资报告（2021）[EB/OL].（2022–02–16）. https://www.01caijing.com/article/311093.htm.

2021 年 5 月，为准确把握区块链发展的机遇和挑战、注重区块链产业与国家整体发展战略的协同，工业和信息化部、中央网络安全和信息化委员会办公室联合发布《关于加快推动区块链技术应用和产业发展的指导意见》，首次为区块链产业制定明确的发展路线图和时间表。明确了未来 5 年和 10 年区块链产业的发展目标，这意味着区块链技术应用和产业发展按下了“加速键”。该指导意见中提出从标准体系、技术平台、质量品牌、网络安全、知识产权等方面着力提升区块链产业基础能力；进一步明确了赋能实体经济、提升公共服务、夯实产业基础、打造现代产业链、促进融通发展等发展区块链的重要任务。可以说，该指导意见的出台，标志着我国区块链产业顶层设计的进一步完善，主要的区块链技术标准和行业标准见表 1–6 与表 1–7。

表 1–6　区块链技术标准相关文件

序号	标准编号	标准名称	标准状态
1	GB/T 42752—2023	《区块链和分布式记账技术 参考架构》	现行
2	GB/T 43579—2023	《区块链和分布式记账技术 智能合约生命周期管理技术规范》	现行
3	GB/T 43580—2023	《区块链和分布式记账技术 存证通用服务指南》	现行
4	GB/T 43572—2023	《区块链和分布式记账技术 术语》	现行
5	GB/T 42571—2023	《信息安全技术 区块链信息服务安全规范》	现行
6	GB/T 42570—2023	《信息安全技术 区块链技术安全框架》	现行
7	GB/T 43582—2023	《区块链和分布式记账技术 应用程序接口 中间件技术指南》	现行
8	GB/T 43575—2023	《区块链和分布式记账技术 系统测试规范》	现行

资料来源：赛迪区块链研究院。

表 1–7　主要的区块链行业标准

序号	标准编号	发布单位	标准名称	行业标准类型	日期	标准状态
1	JR/T 0193—2020	中国人民银行	《区块链技术金融应用 评估规则》	金融行业标准	2020 年 7 月	现行
2	YD/T 3747—2020	工业和信息化部	《区块链技术架构安全要求》	通信行业标准	2020 年 8 月	现行
3	YD/T 3905—2021	工业和信息化部	《基于区块链技术的去中心化物联网业务平台框架》	通信行业标准	2021 年 5 月	现行

资料来源：赛迪区块链研究院。

二、区块链产业生态初步形成

目前，形成的区块链产业主要由区块链上游、区块链中游、区块链下游三个部分构成。

（一）上游的硬件、技术及基础设施

上游主要是提供区块链应用所必备的硬件、通用技术以及基础设施支持。其中，硬件设备包括矿机、矿池、芯片厂商等；通用技术包括分布式存储、去中心化交易、数据服务、分布式计算等相关技术。

（二）中游的区块链应用及技术服务

中游主要包括基础平台建设和提供技术服务支持。其中，基础平台建设分为通用基础链和垂直领域基础链；技术服务支持包括技术支持和服务支持，技术支持与上游相关技术类似，负责为购买者提供区块链安全防护等一系列基于区块链

产品的技术支持；服务支持包括数字资产交易场所、数字资产存储、媒体社区等系列服务。

（三）下游的区块链产业应用领域

下游主要包括应用区块链技术与现有行业的结合，主要面向金融行业、物流行业、版权保护与交易、工业、能源、医疗、公益、大数据交易、数字营销、电子政务等众多领域，区块链作为新兴技术，下游应用领域众多，发展潜力巨大，如图 1–9 所示。

图 1–9　下游的区块链产业应用领域

德勤《2020 年全球区块链调查报告》通过对涵盖 14 个国家和地区约 1 500 位企业高管的调查发现，55% 的受访者将区块链视为前五大战略优先重点；超过 4/5 的受访者认为，如果不采用区块链，他们将失去竞争优势；63% 的受访者表示在区块链领域向前发展至关重要。

2021 年，我国区块链应用落地项目共计 336 个，其中政务服务领域区块链应用是 2021 年我国区块链技术落地项目最多的领域，共计 87 个，占比 25.89%。金融仍然是应用场景最为丰富的行业领域，金融领域全年应用落地项目数量达 82 个，如图 1–10 所示。2021 年以来，银行与金融部门进一步主导数字人民币、数字藏品等新兴市场，市场潜力不断扩大。

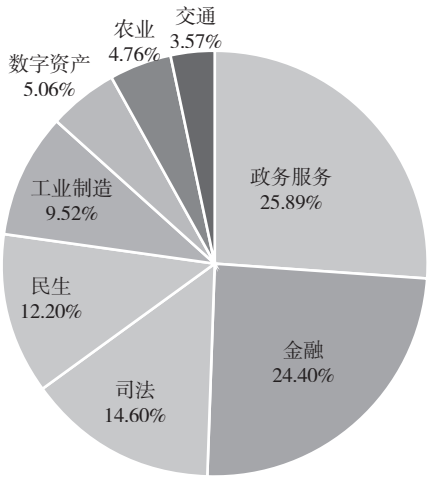


图 1–10　2021 年我国区块链应用落地占比分布

资料来源：2021 年中国区块链年度发展白皮书 [EB/OL].（2022–06–14）. https://dsj.guizhou.gov.cn/xwzx/gnyw/202206/t20220614_74881576.html.

三、与其他新一代信息技术融合发展

区块链与云计算、大数据、物联网、人工智能和 5G（第五代移动通信技术）等高新技术共同构成的现代科技集群，已经成为数字经济发展的驱动性技术。区块链在与产业融合过程中，将面临重构产业发展模式、重塑商业模式的挑战。因此在规划设计之初，它需要和大数据、云计算、物联网以及 5G 等多种技术实现底层耦合，才能真正解决产业转型升级的问题。

从国内外发展趋势和区块链技术的发展演进路径来看，区块链技术与应用的

发展需要云计算、大数据、物联网、人工智能等新一代信息技术作为基础设施支撑，同时，区块链技术与应用的发展也对推动新一代信息技术产业发展具有重要的促进作用，它们之间互相渗透、共同促进。

（一）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。两种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。如 2015 年 11 月，微软在 Azure 云平台里面提供 BaaS（blockchain as a service，区块链即服务），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（国际商业机器公司）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。

（二）区块链与大数据

（1）区块链是一种不可篡改的、全量的数据库存储技术，巨大的区块数据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。同时，因为区块链的可信任性、防篡改、安全性等特点，更多数据被解放出来，推进数据的海量增长。但由于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，极大提升与增加了区块链数据的价值和使用空间。

（2）区块链的可追溯特性使得数据从采集、交易、流通到计算分析的每一步记录都可以留存在区块链上，数据质量获得前所未有的强信任背书，保证了数据分析结果的正确性和数据挖掘的效果。

（3）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。

（三）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，有利于提升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，即人类与人工智能设备、不同人工智能设备之间进行信息的交互甚至是业务的往来。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，从而实现人工智能水平的进一步提升。

（四）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。

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。

（五）区块链与新一代移动通信网络

区块链是点对点的分布式系统，节点间的广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 网络作为新一代移动通信网络，理论传输速度可达 10 Gb/s，这比 4G（第四代移动通信技术）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。新一代通信网络的发展将极大提升区块链的性能和扩展区块链的应用范围。

（六）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 20 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，同时需要深入整合密码学前沿技术，

包括目前国际国内零知识证明、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模式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应用与发展也有极大的促进作用。

【本章小结】

1. 区块链在本质上是一种分布式账本技术，但它并不是单一的技术，而是各种技术的有机结合。区块链包含基于时间戳的链式数据结构、P2P 网络技术、共识算法、密码学、自动化脚本等计算机技术。

2. 区块链具有去中心化、防篡改性、可追溯性、去信任和自治性等主要特征。

3. 区块链以区块为基本单位连接形成，其中，区块是一种记录交易信息的数据结构，主要由区块头和区块主体两部分构成。

4. 当前的区块链技术存在着“不可能三角”，即无法同时满足去中心化、安全性和高效性，因此应用区块链技术时需要在三者之间作出权衡。

5. 根据应用场景与设计体系不同，区块链可以分为公有链、联盟链和私有链三类。应用场景不同对区块链的需求侧重不同，其中公有链和私有链都有一定的技术限制，应用中存在一定的缺陷，而采用部分中心化的联盟链代表了未来区块链的应用趋势。

6. 区块链技术发展主要经历了以数字货币为代表的区块链 1.0、以智能合约为代表的区块链 2.0 和以提高整个社会行业运行效率为代表的区块链 3.0 三个阶段。

7. 从区块链产业发展的角度来看，其主要由上游的硬件、技术及基础设施，中游的区块链应用及技术服务和下游的区块链产业应用领域三部分构成。区块链在与产业融合过程中，将面临重构产业发展模式、重塑商业模式的挑战。因此在区块链规划设计之初，需要与大数据、云计算、物联网以及 5G 等多种技术实现底层耦合，才能真正解决产业转型升级面临的问题。

【复习思考题】

1. 什么是区块链？简述区块链的基本特征。

2. 简述区块的构成和形成过程。

3. 简述区块链“不可能三角”的主要内容。

4. 简述公有链、私有链、联盟链的特点及适用场合。