第一章 区块链原理

区块链（blockchain）是在点对点网络里，依赖现代密码学及共识规则，通过哈希算法将带有时间戳的交易数据块首尾相连，以实现数据不可篡改的一种分布式账本。本章主要介绍区块链各项技术构成，从介绍区块链的重要意义和作用开始，分析区块链的基本架构、密码技术、共识算法等。

第一节　区块链的重要意义

一、区块链技术推动经济高质量发展

区块链技术发展的情景如下。

第一，在国际竞争方面，努力让我国在区块链这个新兴领域走在理论最前沿，占据创新制高点，取得产业新优势，提升国际话语权和规则制定权。第二，在国内社会治理方面，发挥区块链在促进数据共享、优化业务流程、降低运营成本、提升协同效率、建设可信体系等方面的作用。例如，推动供给侧结构性改革，实现各行业需求有效对接，加快新旧动能接续转换，推动经济高质量发展。

高质量发展是中国式现代化建设的首要任务。产业升级和实体经济高质量发展对数字经济产生巨大需求。区块链技术与各产业结合形成数字生产力和数字经济，是现代经济体系发展的重要方向。新一代数字技术给产业发展与实体经济带来全面而深刻的影响。大力发展区块链技术，是数字经济建设的重要组成部分。

区块链技术已延伸到数字金融、物联网（internet of things，IoT）、智能制造、供应链管理、数字资产交易等领域。其在产业应用中的关键是“融合”，聚焦于具体场景，解决某一领域的具体问题，打通创新链、应用链、价值链。这是一个正在进行的过程，可以预见的是，随着区块链技术的发展和应用，它将成为推动产业转型升级、构建现代化产业体系、助力经济高质量发展的重要力量。

二、区块链的重要作用

新质生产力强调以新促质，以创新驱动新经济变革和高质量发展，这与区块链技术的特点非常契合。区块链技术是新一轮科技革命和产业变革中催生的关键性技术之一，为新质生产力发展提供了技术支撑。区块链技术是构建新质生产力的重要工具和驱动力，深化区块链技术的研究和应用，将进一步推动新质生产力的发展。

区块链是新基建信息基础设施中的重要部分，是推动数字经济发展的核心技术之一。

以信息网络为基础的信息基础设施是新基建的关键组成部分。区块链技术可以策略性地应用于多种信息技术基础设施中，包括云计算、大数据、物联网、人工智能（artificial intelligence，AI）等，帮助构建起安全、可信、高效的信息基础设施。区块链实现智能升级与融合创新，能够在金融、供应链、物联网等各个领域实现业务流程的智能化升级，并通过跨行业、跨领域的数据共享和协作，实现业务流程和服务的融合创新，缩短交易时间，提高数据安全性，保障用户隐私，使工作流程更为透明化。区块链技术可应用于政务、医疗、教育、版权等多个领域，推动各行业的数字化转型。实施区块链可以优化行业运作方式，推动转型创新升级，提高生产力和效率。

区块链技术带来的创新不仅仅在于技术层面，更在于模式层面。它改变了数据管理和交易的方式，这对于新质生产力中强调的科技创新有着重要的推动作用。区块链用数字及代码实现了数字信任，可以在无需中间第三方信任的情况下进行更安全、透明、高效的数据交易和管理。区块链技术能够通过复杂的加密算法确保数据的安全性。一旦数据被加到区块链之中，将非常难以被篡改和删除，提供了极高的数据安全保障。数据与信息的安全性和可信任性是数字经济最关键的一环。区块链数据透明的特性能够大大提高交易的公信力，减少欺诈和腐败。

区块链作为一种全球性技术，其发展对世界各国都产生深远且广泛的影响。随着区块链技术在全球范围内的应用逐渐普及，跨国合作将成为共建全球区块链生态的重要途径。我国在区块链技术发展上具备一定的优势，可以借助国际合作推动对外交流。

三、区块链是核心技术自主创新的重要突破口

区块链不仅在当下具有实际应用价值，还有潜在的无限发展空间。区块链以其去中心化、不可篡改、高度安全等特点，为现有技术领域带来了新的突破。同时，区块链技术还具有与互联网、大数据、人工智能等多领域交叉创新的潜力。因此，区块链被认为是一种具有自主创新潜力的核心技术。区块链技术在金融、供应链、版权保护、物联网等众多领域显示出巨大的应用价值。发展区块链技术可以推动产业升级，引领新的科技潮流，对各个产业形态产生全面影响。加大区块链技术创新力度，可以提高我国在区块链领域的国际竞争力和技术自主权。此外，通过研究和开发本土化的区块链技术，也有望降低我国对于外国核心技术的依赖，提高国家技术安全。

我国政府对区块链技术的支持和引导，为相关企业提供了有利的发展环境。政府对区块链技术的重视和投入，使得我国在区块链领域具备了较好的创新基础，为我国区块链技术的快速发展提供了有力支持。

区块链作为核心技术自主创新的重要突破口，具有独特的技术特点和广泛的产业影响力，在提高技术自主权的可能性与国家政策支持力度及国际合作机遇等多方面具有优势。全球主要国家都在加快区块链布局，希望通过区块链推动经济变革和社会发展。党和国家高度重视区块链技术，将其作为一项重大战略。在区块链技术发展上，我国正在抢占跑道。作为全球科技创新和经济实力的领导者，我国在推动区块链技术发展方面具备强大动力。未来，区块链技术将为我国经济社会发展带来革命性的变革，并创造显著的增长机遇。

第二节　区块链的起源

为了深入了解区块链技术及其应用，首先需要认识区块链的发展历程和演变脉络，这样不仅可以帮助我们更好地把握区块链技术细节，还可以洞悉其成长路径和潜在价值。

一、密码朋克的探索

区块链的概念是在 2009 年之后才被正式提出的，它的出现离不开此前几十年科技界在密码学、分布式网络及支付、货币等领域的研究成果。区块链的诞生与密码朋克运动有密切关系。密码朋克是一个由密码学专家、程序员和极客组成的组织。密码朋克宣言认为，在电子通信时代，人们要实现隐私权，隐私权是一个社会在数字时代维持其开放性的必要条件。基于数字科技的密码技术对健全的隐私权至关重要。密码朋克以开发匿名系统为使命，试图用密码学、匿名电邮系统、数字签名保护自己，创造支持匿名交易的系统。

早在 1982 年，大卫·乔姆发表了盲签名技术的论文，给出了在网络上匿名传递价值的方式，并将其命名为 Ecash。它可以让传统货币通过银行的加密签名，以数字形式存储货币，在网络上自由、匿名地传递，用户可以将这种“数字化的传统货币”自由转移，并且无须暴露身份，但这个体系是中心化且无法自洽的。

1997 年，亚当·巴克在密码朋克邮件中提出了哈希算法（Hash algorithm）：执行哈希现金程序的计算机，在发送邮件时，需要额外的几秒钟时间进行哈希运算，试凑出一个符合特殊规则的哈希函数值。

2004 年，密码学家哈尔·芬尼把哈希算法改进为可复用的工作量证明机制（reusable proofs of work），它被用于比特币出现之前的一系列数字资产实验。

2005 年，尼克·萨博（Nick Szabo）提出比特现金的设想，用户通过解决数学难题，并用加密算法认证公布结果来构建一个产权认证系统。该思路非常接近比特币的工作量证明算法。

从 Ecash 到比特现金，几代密码朋克努力做着加密价值的尝试，并使其能够在互联网环境中安全、私密地流通，然而最终都失败了。究其原因，密码朋克的探索并没有真正解决去中心化的问题，他们的构想仍然需要依赖某种形式的托管或交易验证机构，这显然和他们最初追求的去中心化思想是相悖的。在没有中央权威机构的情况下，如何防止“双花”是一个巨大的问题。“双花”指的是同一笔电子货币被重复使用，这在传统的中心化金融体系中可以通过银行的账务体系加以防范，但在去中心化环境中就显得非常困难。

尽管早期密码朋克的尝试不太成功，但这些探索经验为后来的区块链提供了宝贵的经验教训。这也是技术进步的常态，只有不断尝试，失败与成功才能交替上场，推动技术的进步。

二、区块链技术的诞生

先有比特币，后有区块链。中本聪提出使用首尾相连的用哈希值链在一起区块的账本

（block chain），后来叫区块链。

2008 年 10 月 31 日，中本聪在加密邮件组中说，他正在开发一个点对点的电子支付系统，称作比特币（bitcoin），并给出了《比特币：一种点对点的电子现金系统》的摘要和全文地址。比特币系统背后的设计者中本聪可能是一个人，也可能是一个组织，需要具有非常强的信息技术、金融学、博弈论、应用密码学等跨领域知识积累及实战经验。

中本聪发明的比特币是一个点对点的电子现金支付系统，用于对抗现实生活中通胀等一系列问题。它从数学上可以自证清白，是公平且高度自治的系统。正是因为这套系统能够遵循有贡献就有收益的原则，所以这个生态从一文不值发展到上千亿美元市值。

自中本聪 2008 年发布比特币白皮书以来，区块链技术已经走过了十多年的发展历程，其已从最初的密码学和技术底层概念，逐步演变为一个成熟的产业应用技术。

区块链技术主要具有去中心化、不可篡改、可追溯性、自动执行的特点。去中心化的区块链通过将数据分布存储在多个节点上，消除了数据的中心化风险；使用加密算法存储的数据具有不可篡改性，确保数据的真实性和安全性，这是区块链能得到大规模应用的基础；区块链上的每一笔交易都可以追溯来源和归宿，增加了数据的透明度。

三、区块链的分类

区块链可按网络范围、对接类型、应用范围、开发阶段这 4 种方式进行分类，如图 1-1 所示。对区块链的多角度分类，能够帮助我们理解区块链的不同应用场景及面临的具体挑战。

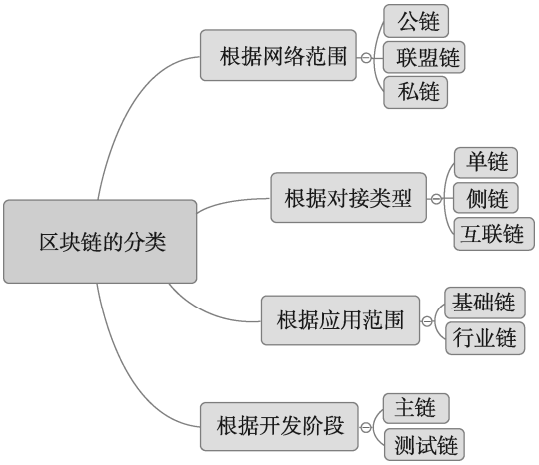

图 1-1　区块链的分类

（一）根据网络范围分类

按照网络范围，区块链可以被分为公链、联盟链和私链。公链代表了一种完全去中心化的区块链，对所有用户开放，任何人都可以参与其中。比特币和以太坊都属于这种类型的区块链。联盟链则是一种需要获得准入许可才能使用的区块链，它通常在发起联盟链的

组织间共享，如银行或者其他金融机构。国际商业机器公司（International Business Machines Corporation，IBM）的超级账本就是联盟链的一个例子，它将区块链的概念应用在商业场合，以协助公司处理交易和合同。私链则能更进一步中心化，它只在单一组织的内部使用。私链的应用场景包括企业内部的数据管理和审计，提供了高度的隐私性和安全性。

（二）根据对接类型分类

这种分类从链与链之间的关系和应用方式来进行。单链是最基本的一种形态。单链指的是只有一个主链，所有的交易和数据都在这一条链上进行，并且被存储。比特币就是一个典型的单链。侧链是指附属于主链的区块链，它可以实现与主链之间的资产互通。侧链可以有自己的独立规则和功能，它在主链上运行，可以提供主链所不能提供的服务，如更快的交易速度或者支持更多种类的资产类型。主链和侧链之间的关系可以类比为主干道和辅路的关系，侧链代表一种扩展性的解决方案。互联链，也被称为跨链，指的是不同的区块链之间可以实现信息的互通和交互。这个概念是区块链领域的一项新技术挑战，通过实现跨链，各个区块链网络间可以实现数据和资产的相互转移，这样可以实现区块链的互操作性，真正实现价值互联网的概念。Polkadot 和 Cosmos 都是致力于跨链技术研究的项目。

（三）根据应用范围分类

这是一个从区块链的实际应用级别和针对性来进行分类的视角。基础链，可以被理解为一个提供底层区块链技术支持和平台的系统。这种区块链主要提供了区块链的基本能力，如数据存储、共识算法、加密算法等，并且具有很高的通用性和可扩展性。比如，以太坊就可以看作是一种基础链，它开创了智能合约技术，并通过其开源特性，供其他开发者进行参考与创新。行业链在基础链的基础上，更加关注区块链技术在特定行业或特定场景下的应用。它是一种定制化的产品，专门为解决某一领域的问题或者满足某一领域的需求而设计和开发的。例如，贸易金融区块链、医疗健康区块链、供应链区块链等就是针对特定领域设计和应用的行业链。基础链关注的是区块链技术本身的广泛应用，而行业链更注重在特定领域内实现区块链技术的定制化与深度应用。

（四）根据开发阶段分类

主链，也被称为主网，是一个区块链项目正式运行后的网络环境。在主链上，所有的交易和操作都是真实、有效的，有真实的经济价值在其中转移。测试链则是开发者为了测试新的功能而创建的网络环境。在这个环境中，开发者测试交易或者验证网络功能的稳定性。任何在测试链上的操作和交易都不会影响到主链上的价值转移。

第三节　区块链中的密码技术

一、密码技术原理

密码技术是区块链得以构建的基石，是使其能够实现去中心化、安全共享的关键所在。

了解密码技术知识可以更好地理解区块链的机构与运作规则。通过密码技术，区块链在一个去中心化、任何人都可以参与的开放网络中，能够保证信息与数据的真实性、完整性和安全性。

在第二次世界大战前和第二次世界大战期间，军方主要通过应用密码技术来收集敌方情报，在加密和破解这两种技术的相互促进发展过程中，密码技术得到了充分的发展。但是，在 20 世纪 70 年代以前，密码技术一直处于保密的地位，尖端的技术往往被军方控制，很难被普通人了解。随着经济的发展和信息革命的来临，民间对密码应用的需求越来越多，从而促使民间的学术机构和商业机构对这一领域开展了广泛的研究，并最终推动密码技术走下神坛，成为与人们生活息息相关的应用技术领域。

简单地讲，密码算法就是通过某种方式对信息进行变换，使别人无法解读这些信息，通常的密码算法结构如图 1-2 所示。

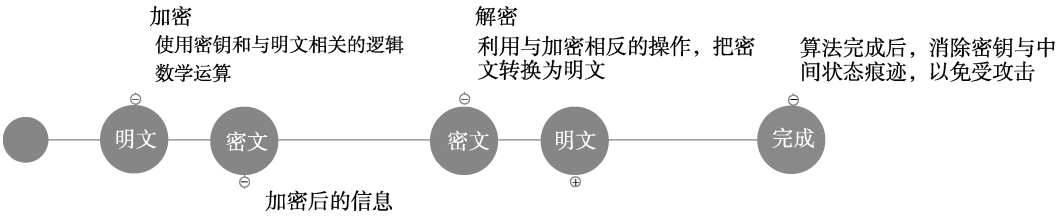

图 1-2　密码算法结构

明文（plaintext）是指原始的消息，密文（ciphertext）是指加密后的消息。明文通过加密（encrypt）得到密文，而密文经过解密（decrypt）得到明文。在一般人的印象中，加密密钥和解密密钥都是相同的。比如，使用“197321”作为密钥加密密文，一般都会期望使用“197321”作为密钥去解密密文。如果算法中使用的加密密钥和解密密钥相同（更严格地说，如果从加密密钥可以推算出解密密钥），则称这种算法为对称加密算法（symmetric algorithm）。而有些算法加密时使用的加密密钥和解密时使用的解密密钥并不是同一密钥，并且从加密密钥无法推算出解密密钥，这种算法被称为非对称加密算法（asymmetric algorithm）。对称加密算法和非对称加密算法在数学原理上有着根本不同的机理。在非对称加密算法中，从加密密钥无法推算出解密密钥这一特点为其带来了很多精彩的特性。

本节对区块链用到的密码技术进行简要介绍，包括密码哈希函数、非对称加密算法、数字签名等。关于密码技术的具体算法原理，读者可参阅应用密码学相关资料。

二、密码哈希函数

（一）密码哈希函数的特征

区块链技术的一个重要组成部分是密码哈希函数。哈希是一种对几乎任意长度的数据（可以是文档、文本、图像等）进行密码哈希运算处理并输出唯一结果（称为消息摘要或摘要）的方法。由于在这一过程中数据没有发生变化，不同个体可以独立地进行数据输入，对该数据进行哈希处理并得到相同的结果。即使输入数值发生了最细微的变化（如仅改变

了一个比特），都会导致最终的结果大相径庭。

密码哈希函数有以下几个重要的安全特性。

（1）抗预映射性，即它是单向的、不可逆的。通过给定的输出值来反推输入值几乎是不可能的，即给定一个 y，无法找到 x，使 $\text{hash}(x) = y$。

（2）抗第二预映射性，即无法找到一个对应特定结果的输入值。也就是说，给定一个输入，人们无法找到第二个可以输出相同结果的输入值。唯一的办法是找遍输入域，但从计算意义上讲，几乎没有成功的可能。即给定一个 x，无法找到 y，使得 $\text{hash}(x)=\text{hash}(y)$。

（3）强抗碰撞性。这意味着人们无法同时找到两个不同输入在经过哈希后得到相同的结果。即无法同时找到 x、y，使 $\text{hash}(x) = \text{hash}(y)$。

作为在许多区块链应用中被使用的密码哈希函数，安全哈希算法（secure hash algorithm，SHA）输出长度为 256 位的结果（secure hash algorithm-256，SHA-256）。许多计算机在硬件上支持这种算法，可以加快计算速度。SHA-256 输出结果为 32 字节，通常显示为一个 64 位的十六进制字符串。这意味着存在 2^{256}（约等于 10^{77}）种可能的输出值。SHA-256 哈希算法，还有其他一些哈希算法都是经过国际标准认定的安全哈希算法。

密码哈希函数既然存在无限多的输入值和有限可能多的输出值，就有极小的概率会出现碰撞，即发现两个不同的输入值生成了相同的结果。SHA-256 被认为具有抗碰撞性是因为在执行算法的过程中，平均每经过 2^{128} 次才可能遇到一次碰撞。

为了避免哈希碰撞的发生，区块链网络通常会选择增加难度，使哈希函数更难产生相同的哈希值。以目前的网络算力，数百亿年才会出现一次碰撞。而即便存在 x 和 y，可以得到相同的哈希值，也几乎没有可能会在区块链网络中同时有效。这意味着，在区块链网络中进行交易记录时，可以保证任何两笔不同的交易都有不同的哈希值，从而避免区块链网络因哈希碰撞而拥堵。

在一个区块链网络内，密码哈希函数有多种用途，如地址推导、创建唯一身份标识符（identity document，ID）、保护区块数据的安全等。

以保护区块头为例，一个出块节点会对区块数据进行哈希处理，并创造出一个摘要存储在区块头。如果区块链网络使用了工作量证明模型，那么出块节点在哈希块头时需要不同的随机数（nonce），直到出块计算难题被解除。当前区块头的哈希值会被包含在下一个区块头内，这保证了当前区块头的数据安全。因为区块头包含了代表区块内数据的哈希值，因此当区块头哈希值被存储在下一个区块时，此区块数据本身也得到了保护。

很多密码哈希函数在区块链技术中得到了应用（SHA-256 只是其中一种），如 Keccak（SHA-3 哈希加密函数标准）、RIPEMD-160 及我国自主设计的密码算法 SM3。依据国内商用密码管理法规，国内项目一定要用国密算法。

（二）哈希算法

哈希函数能接受任意的输入，产生固定长度的一个唯一输出。它特别设计成了不能反向运算，也就是说无法从输出中获取输入。

哈希算法可以作为一个很小的计算机程序来看待，不论输入数据的大小及类型如何，

它都能将输入数据转换成固定长度的输出。加密哈希（散列）值被称为数据的指纹，在区块链中被广泛使用。哈希算法在任何时候都只能接受单条数据的输入，并依靠输入数据创建哈希值。根据最终产生哈希值的长度不同，密码学专家设计了多种哈希算法。其中一类重要的哈希算法被称为加密哈希算法（密码哈希函数），它能够为任何类型的数据创建数字指纹。

通过向哈希函数输入一段数据，可以产生对应的哈希值。这意味着每个独立的数据块，都将有自己独特的哈希值。哈希函数只能在给定的时间接受一个数据。没有哈希算法能够一次接受一堆独立的数据。实际上，我们经常需要为一组数据生成一个哈希值。区块链必须一次处理许多交易数据，并且还需要对同一批数据产生一个哈希值。因此哈希值的生成具有多重方式。

（1）独立哈希。独立哈希指的是将哈希算法单独应用在每一个数据块上。每一个单词都可以生成自己独有的哈希值。

（2）重复哈希。密码哈希函数可以将任意数据块转换为哈希值。哈希值本身也可以被认为是一个数据块，因此也就可以将哈希值输入（密码哈希函数）来获得这个哈希值的哈希值。

（3）组合哈希。组合哈希的目标是尝试一次为多个数据块生成单个哈希值。将所有独立的数据块组合成一个总数据块并计算哈希值，就是组合哈希的实现方法。它在为给定有效时间存在的数据块集合创建一个单独的哈希值时特别有用。由于组合哈希需要消耗计算能力、时间和存储空间，所以它只能在单个数据块较小时使用。组合哈希的另一个缺点是单个数据片段的哈希值不可用，因为只有组合后的数据才会被交给哈希函数。

（三）哈希在现实世界中的应用

根据哈希值进行数据对比，是哈希值最直观的应用。在数据对比的过程中不用去一一对比其中具体的数据内容，直接对比它们的哈希值即可。这让任何数据对比都像比较两个数字那样简单。如果对应的哈希值不同，那它们对应的数据也就不同；如果两个或两个以上的哈希值相同，那么它们对应的输入数据也相同。通过对比哈希值来对比数据的原理是建立在哈希计算的防碰撞性之上的。

哈希算法被广泛用于验证文件完整性和创建区块链的链接。哈希数据比对，在区块链数据上链、数字作品溯源、版权存证等应用之中经常会提到。

三、非对称加密算法

非对称加密技术产生于 20 世纪 70 年代，它依赖于数学算法。加密和解密使用的是两个相关联但不同的密钥，分别称为公钥和私钥。公钥是公开的，任何人都可以获得；私钥则是私有的，只有密钥的所有者才能使用。一般而言，公钥用于加密，私钥用于解密。代表算法有 RSA 算法、椭圆曲线等。

1978 年，麻省理工学院的罗恩·李维斯特（Ron Rivest）、阿迪·萨莫尔（Adi Shamir）和伦纳德·阿德曼（Leonard Adleman）提出了非对称加密算法——RSA 算法，它是首个既

可用于数据加密也可用于签名的算法，是目前最流行的公钥加密算法。

区块链技术使用了非对称加密算法，算法包含一对密钥：数学上彼此关联的公钥和私钥。公钥可以公开，不影响密码处理安全；但私钥则关系到账户安全，必须妥善保管。尽管公钥和私钥之间有一定的关联，但知道公钥的信息并不意味着可以推导出私钥。个人可以用私钥加密然后用公钥解密；相应地，也可以用公钥进行加密然后用私钥解密。

相比之下，对称加密算法中加密解密均用单一密钥完成。使用对称加密算法的用户必须建立信任关系，从而交换预共享的密钥。对称加密的速度快，计算量相对较小，但密钥管理和分发较为复杂，因为密钥需要在通信双方之间进行预先分享。并且，一旦密钥被泄露，信息的安全将面临威胁。实际应用中经常混合使用对称加密算法和非对称加密算法。

四、数字签名

日常生活中，人们经常需要签署各种信件和文书，传统上都是用手写签名或印章。签名的作用是认证、核准和生效。随着信息科技的迅猛发展，人们越来越希望可以进行迅速、远距离的签名，于是数字签名就诞生了。对于个人网上交易、公司间沟通，数字签名提供了快速验证的手段与信源的保护。

数字签名与传统签名的主要区别在于是否为电子形式，并且依赖于加密技术和一个公开的验证算法来生成和验证。这个过程增强了数字签名的可依赖性，因为数字签名的生成及验证都是基于数学原理的，并且可以跨越物理距离。不同于手写签名，数字签名无论对于发送者还是接收者来说，它们都是易于存储和复制的，身份验证的准确性也得到了极大提高。

数字签名的使用也面临一些挑战。一方面，人们需要防止数字签名的重复使用，以避免被恶意利用。这意味着数字签名需要建立一定的存储和管理系统，可以在签名被使用后进行相应的记录或删除动作。另一方面，数字签名的法律效应必须被获取确认，由第三方进行仲裁，将使流程更为公正。

当前，非对称加密算法已是数字签名主流的技术之一。在非对称加密算法中，私钥和公钥是一对，私钥用于签名，而公钥则用于验证，这样就能实现一种即便是接收方，也无法伪造或篡改签名的机制。这一机制确保了签名的真实性，并且使签名者不能否认其签名操作。

在交易公开化的情况下确保交易的完整性和授权性，非对称加密算法为非互信用户创造了信任关系。交易是被数字签名的，这意味着私钥被用来对交易进行加密，拥有公钥的人可以相应地解密。公钥是可以任意获取的，但被私钥加密后的交易数据，只有签名者才拥有私钥。相应地，个人可以用公钥对数据进行加密，只有拥有对应私钥的人才可以解密数据。

在区块链网络中，数字签名算法经常在以下场景被使用：私钥被用来对交易进行数字签名，用于区块链账户、个人信息的保护；公钥用来导出地址并验证由私钥生成的数字签名；非对称加密算法可以用来验证，只有拥有私钥的用户才能对交易进行签名，从而完成数字资产的价值转移。

在区块链网络（尤其是公链）中，用户必须妥善保管自己的私钥。他们通常使用软件进行私钥的安全存储，而非人工记录，这个软件被称为“钱包”。钱包可以存储公钥、私钥及相对应的地址。

第四节　区块链的结构

区块链的基本结构是：用户把一段时间内的信息，包括交易数据或代码打包成一个区块，盖上时间戳，与上一个区块衔接在一起，每一个新区块的页首都包含了上一个区块的哈希值，然后再在页中写入新的信息，从而形成新的区块，首尾相连，最终链接起来。任何一个区块内信息的轻微修改，都会导致哈希值的改变，而因为各区块环环相连，修改一个区块中一个字节信息都必须相应地修改下面整条链的信息，成本极高，因此区块链存储的信息事实上是无法篡改的。区块里的有效载荷不仅仅是狭义的交易，它可以是被打上时间烙印（时间戳）的任何信息。

用户加入区块链时，是默许了区块链系统的初始状态。而这个初始状态是被唯一的预配置区块记录的，它叫作创世区块。每个区块链网络都有其创世区块，链上每个区块都需要基于共识算法的认可，接续添加在创世区块链之后（见图 1-3）。

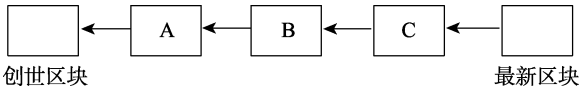

图 1-3　区块链的基本结构

区块链技术看上去非常复杂，但如果单独分析它的每个组成要素就会容易些。简言之，区块链技术使用了一般的计算机科学及密码技术，并结合记录保存的理念（如只可追加的账本）。本节对区块链主要组成要素分别进行讨论，即交易、地址、账本、区块，以及区块如何被链到一起。

一、交易

交易代表着主体间的互动。在区块链上，一次交易就意味着加密数字权益（token，通证）在区块链网络用户间的一次转移。在商业场景中，交易可能是记录数字资产或现实资产变化的一种方式。图 1-4 描述了一个区块链上的虚构交易。区块链上每个区块包含 0 个或多个交易记录。对有些区块链网络而言，新块的持续发布（即使不包含交易）对维持区块链网络的安全也是至关重要的。新块的不断发布，可以防止恶意用户“赶上”并制造出更长的分叉链。

（一）交易过程

虽然记录交易的数据因区块链实现的差异而有所不同，但交易机制大体上一致。用户向区块链网络内发送信息，信息中要包含发送方地址（或其他相关 ID）、发送方的公钥、数字签名、交易输入及交易输出。

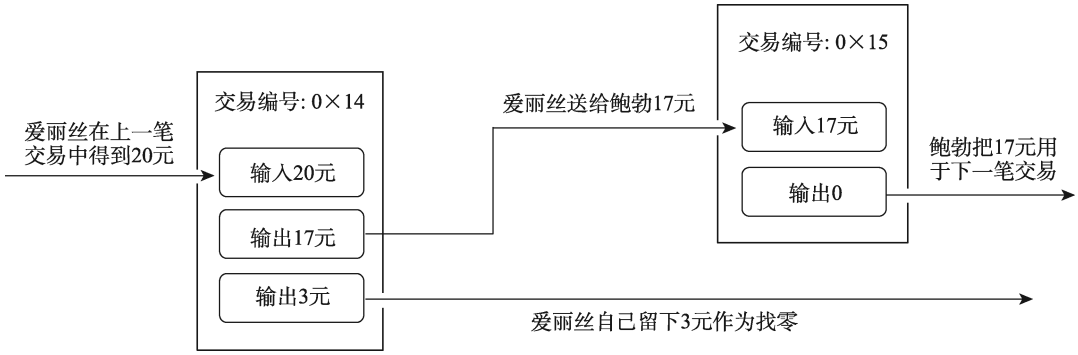

图 1-4　区块链交易示例

通常，区块链一次交易至少需要但不仅限以下的信息。

输入——通常指一组将被转移的数字资产。交易会引用数字资产的来源：发送方从过往的历史交易中获得，或是源于初始生成的新数字资产。由于交易的输入引用参考了过往发生的活动，因此数字资产不会变化。在区块链中，这意味着手中数字资产的价值无法被更改。一份数字资产可以被拆分成多份新的数字资产，同时多份数字资产也可以合并成为具有更大点的数字资产。资产拆分或合并的内容将在后续介绍交易输出时具体阐述。发送方通常利用私钥对交易进行数字签名来证明相关交易输入的可获取性。

输出——通常指接收方账户及即将接收多少数字资产。每个交易输出都包含了新用户即将获得的数字资产的具体数额、新用户的 ID 及花费这些资产所需要的条件。如果转移过程中数字资产供大于求，多出来的部分将被返还到发送方的账户（“找零”机制）。

交易除了转移数字资产的基础功能外，还可以用于数据的传输。简言之，个人可以在链上永久且公开地发布数据。在智能合约中，交易被用来发送数据、处理数据，并在区块链上存储结果。比如，在基于区块链技术的供应链系统中，一个交易可以用来改变数字化资产的属性，如货物物流的位置数据。

不论数据如何被产生和转移，交易的有效性和授权性始终是至关重要的。交易的有效性确保了交易符合区块链内的协议要求、数据格式化要求及智能合约的要求。交易的授权性也很重要，它决定了发送方是否有权操作这些数字资产。交易一般由发送方用私钥进行数字签名，可以随时用其相关联的公钥进行验证。

（二）地址

区块链将用户的公钥进行哈希运算，得出的结果连同一些附加数据（如版本号、校验和等），由此形成一个由字母和数字组成的字符串作为地址。绝大多数区块链在交易中用“to”和“from”标识地址的起止。地址的长度比公钥短且无需保密。生成地址的一种办法是，创建一个公钥并对其进行哈希处理，然后将哈希值转成文本格式。

不同的区块链可采取不同的方法生成地址（见图 1-5）。对允许匿名账户创建的公链网络而言，用户可以随意生成任意多组公私钥对，继而生成任意多的地址，而这可以带来一定程度的匿名的好处。对用户而言，地址在区块链中扮演着公共 ID 的角色，地址常常会被

转换成二维码以便移动端设备的使用。

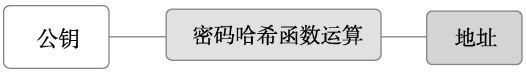

图 1-5　从公钥生成地址

在区块链网络中，用户不是唯一的地址来源。智能合约在被部署到区块链上的时候需要有一个调用的方法。在以太坊中，智能合约是通过一个叫合约账户的特殊地址被调用的。合约地址在智能合约被部署时自动创建（合约地址是算法通过合约创建人的地址确定性地计算出来的）。一旦合约账户接收到交易，合约立即被执行，当然它也可以创建其他智能合约。

（三）账本

人类的记账方式随着时间推移经历了几个阶段的演变。起初，人们采用的是单式记账法，该方法仅涉及记录个体的收入和支出，个人维护自己的私人账本。随后，复式记账法的出现将记账带入一个新的维度，它不仅记录收入和支出，还包括资产和负债，然而这仍然是在个体的账本中进行。在现代社会中，账本则用数字化的方式保存在大型数据库中，并由中心化的第三方信任主体（账本的所有者）代表社区的用户运维，而这些中心化属性的账本可以用中心化或者分布式的方式实现。

账本是链上数据的汇总。区块链技术用账本所有权的分布式及物理架构的分布式来提供一个分布式账本。数据的存储和管理分布在网络的多个节点上，每个节点都包含了完整的账本副本，并通过共识机制来保持账本的一致性。区块链网络的分布式物理架构通常需要比中心化网络架构有更多的计算机支持。

相比于中心化账本，分布式账本的优势在于可信任、安全、可靠。区块链作为分布式账本，为数字经济和网络价值交换提供了一个可靠的基础设施。

（四）区块

用户通过软件（如桌面应用、手机应用、数字钱包、网页服务等）向区块链网络提交交易申请，软件随即向一个或多个节点发送交易信息。被选中的节点有可能是没有出块功能的全节点或者可以出块的节点。已提交的交易在网络中扩散，但这并不等于交易上链。在许多区块链中，悬置的交易一旦被扩散到各节点就必须排队等候，直到交易被出块节点打包并记录到链上。

当节点发布一个区块时，交易记录即上链。一个区块包含了区块头和区块数据。区块头包含了该区块的元数据，区块数据则包含了一系列被验证且已提交至区块链网络的真实交易记录。通过两方面的检查确保了交易的有效性和真实性，即交易记录格式是否正确，以及是否每笔数字资产的交易上均附有加密数字签名。这说明交易中数字资产的发起方可以获取私钥对数字资产进行签字移交。其他全节点会验证已发布区块中所有交易的真实性和有效性，如果出现无效交易便拒绝接收该区块。

需注意，每个区块链可以自行定义数据字段，但通常大部分区块链都采用以下数据字段。

- 区块头。
- 区块号，有些区块链也称为“区块高度”。
- 前一区块头的哈希值。
- 区块数据的哈希值（可以用很多方式实现。例如，生成一个默克尔树，存放一个根哈希值或者对整个区块进行哈希计算）。
- 时间戳。
- 区块大小。
- 随机数（nonce）。对于工作量证明“挖矿”的区块链，随机数是出块节点用来解决哈希难题的；其他类型的链可能没有随机数或者另作他用。
- 区块数据。
- 区块内的交易列表和账本事件。
- 其他可能用到的数据。

每个区块均包含前一区块头的哈希值，区块依次上链从而形成区块链。如果之前的区块发生变化，将会得到一个不同的哈希值。相应地，此区块往后序列中所有区块的哈希值均会发生变化，这就很容易识别并拒绝发生改动的区块。

二、共识算法

区块链一个核心要点是确定谁来发布下一个区块，这可以通过选择一种共识算法来解决。共识算法是多方就网络系统状态达成共识的，该决定将被添加到区块链中，然后被视为不可辩驳的单一真相来源。现在主流的区块链共识算法有以下几类。

第一类是工作量证明（proof of work，PoW）算法。工作量证明算法基于解决一个复杂的数学难题来竞争获得记账权。这个数学难题通常是哈希碰撞，即找到一个特定输入的哈希函数输出值满足一定条件。为了解决这个问题，“矿工”需要进行大量的哈希运算尝试，通过调整输入参数不断计算哈希值，直到找到有效的解决方案。因此，谁拥有更强的计算能力就可以进行更多的尝试，从而增加获得记账权的机会。工作量证明算法主要应用于区块链网络中的“挖矿”过程。“挖矿”是指验证交易并将其打包成一个新的区块，然后将该区块添加到区块链中的过程。“矿工”通过解决数学难题来验证新的区块，并且通过提供有效的工作量证明，获得记账权和相应的奖励。这种机制确保了新的区块得到有效验证，并防止恶意节点篡改交易记录。工作量证明算法可谓是久经考验，它使得修改大量区块的成本极高，迄今为止，发生 51%攻击篡改数据的案例极少。

第二类是权益证明（proof of stake，PoS）算法。权益证明是区块链网络在不需要大量计算能力、能源消耗也较少的情况下，验证交易和添加新的区块至区块链的机制。在权益证明共识中，不是所有的网络节点都能创建新的区块，而是要有一定的“权益”（或资源）才可以成为验证者（创建新区块的节点）。“权益”通常以持有和投注某种特定的网络资源数量来定义。权益证明共识机制的优势主要表现在能源效率更高、安全性强，并且可以抵抗“51%攻击”。这些优势主要得益于其不再需要以竞争解决复杂计算问题（如工作量证明

算法）来决定区块链的添加权。

第三类是拜占庭容错（Byzantine fault tolerant，BFT）算法。有的地方在 BFT 签名加个“x”，也称为 xBFT 算法，因为它们都源于拜占庭容错算法，都是拜占庭容错算法的变种，如 PBFT 之类的。拜占庭是古代东罗马帝国的首都，由于地域宽广，守卫的将军需要通过信使传递消息，以达成一致的决定。但将军中可能有人叛变，他们可能会发送错误的信息来扰乱大家的决策，这就是拜占庭将军问题。拜占庭将军问题的提出是为了解决在这种情况下，怎样让忠诚的将军们达成一致的决议。这个问题映射到计算机领域中，就是如何让网络中不同的计算机通过互相通信达成一致。在实践过程中，有些计算机可能出现错误，有些计算机可能被黑客攻击。计算机网络上的“拜占庭将军问题”是指在存在信息丢失的不可靠信道上试图通过消息传递的方式达到一致性的问题。就区块链而言，其实就是系统节点的识别问题，存在诚实节点和欺诈节点，信道有可能畅通，也有可能不通，因此区块链需要严格的共识来保证信息一致性。拜占庭容错算法设计的容错上限是 1/3，可以保证系统节点达成共识。

第四类是代理权益证明(delegated proof of stake，DPoS)算法。它的意思是我们先用手中权益投票选出若干个节点，然后让这几个代表性节点来决定出块。这类似于公司股东用权益选举董事，组成董事会来决策。DPoS 算法形成共识的节点少，因此出块效率很高，相较于权益证明算法，DPoS 能大幅度提升效率，在牺牲一部分去中心化特性的情况下得到性能的提升。最早使用 DPoS 算法的是 Bitshares 项目，但真正让 DPoS 算法流行起来的是 EOS（enterprise operation system，EOS）项目，现在已经有越来越多的公链采用 DPoS 算法。

三、分叉

区块链网络的用户分布在世界各地，并由用户间的共识实现自治，任何变动都是极其困难的。区块链上软件更新，新的区块生成出现分歧，造成区块链网络协议和数据结构的改变，形成两个出块方向。分叉可以分为两类：硬分叉和软分叉。对软分叉而言，改动对于没有升级的节点是向后兼容的；对硬分叉而言，如果节点不更新，就会拒收改动后的区块，因此硬分叉的改动不向后兼容。这导致了同一区块链可能出现多个不同版本，如以太坊和以太坊经典的分叉。主要公链均被多次分叉，产生许多分叉链。对联盟链而言，出块节点和用户信息是已知的，定期软件升级可以减少分叉的影响。

第五节　时间服务器

经过上一节对区块链结构的介绍，读者对区块链的轮廓有了一个总体认识。区块链整合了应用密码学、分布式账本、共识算法等技术。本节将对区块链运行规则进行讨论。

区块链的本质，可以用“时间服务器”来描述。与时间相关的五个概念共同构成了时间服务器，其他的数据可以放在链外。交易频次（transactions per second，TPS）并不是区块链的重点。关于时间服务器，有几个概念需要厘清，先用一幅图来说明这几个概念（见图 1-6）。

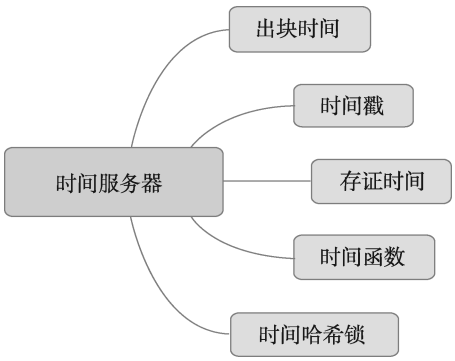

图 1-6　时间服务器

图 1-6 中的五个时间概念为出块时间、时间戳、存证时间、时间函数和时间哈希锁。这些时间概念在区块链技术中有重要应用，如密码学、信用管理、存证等方面。通过这些时间概念，区块链系统能够实现一个不可篡改、可验证的历史记录，进而满足文化、创意、金融等领域的应用需求。

一、出块时间

比特币是众多区块链里最著名的一个应用。比特币是基于工作量证明的公链区块链，也叫非限制准入区块链，或者非许可链（permissionless blockchain）。

比特币有个巧妙的设计，那就是著名的抗摩尔定律的挖矿难度值调整，遇强则强。参与工作量证明的设备越多，算力越大，这个难度值就越大。那比特币链自身怎么知道有多少设备参与竞争呢？答案是出块时间，也就是写死在代码里的每 10 分钟出块这个参数。这是个负反馈设计，10 分钟是反馈的参考点。当出块时间大于 10 分钟时，挖矿难度下调，区块链感知到算力不足；反之，当出块时间少于 10 分钟时，挖矿难度调高。在比特币系统里，每 10 分钟，确切说，大概 10 分钟，一个新的出块周期开始。这个 10 分钟不需要太精确，是一个相对的时间段，这是区块链上第一个“时间”。

二、时间戳

比特币的白皮书题目叫“比特币：一种点对点的电子现金系统”，中本聪用每个块的奖励来激励“矿工”们去竞争记账权，记的什么账？交易数据，就是谁给谁转了多少比特币及找零多少。每个区块都有数量不等的这类交易，“矿工”除了获得出块奖励，还获得交易手续费，足够公平。这个过程中有个很重要的东西，即时间戳。

在比特币的创世区块，中本聪写入了一则与 2008 年金融危机有关的新闻，新闻是有时间戳的。时间戳对金融系统、信用管理非常重要，它是时间轴上的点，是历史痕迹参考点。时间戳证明了数据一定在那时存在。每个时间戳在哈希中包括先前的时间戳，形成了一条链，每个新增的时间戳都验证了它之前的所有时间戳。时间戳存在于几乎所有区块链系统里，时间戳组成了历史。这是区块链上第二个“时间”。

三、存证时间

区块链虽然是天然的金融系统，但区块里的有效载荷不仅是狭义的交易，它还可以是被打上时间烙印（时间戳）的任何信息。一个典型的应用就是存证。存证是为了在事件发生的时候存下证据，在未来使用的时候，调取并使用证据。这里强调两个时间，发生时间和未来时间。用证据的场景是：找一个事件（需要唯一 ID 的）在某个时间点或者时间段的记录。

四、时间函数

区块链用到的各种密码技术几乎都可以认为是时间的函数。这些保护措施确保区块链在相当长的时间内不被破解。尤其是各类哈希算法，它们无法通过并行计算加速，虽然可以用空间换一定的时间，但时间还是省不掉。各类区块链底层，不分共识模式，都会以某个时间作为一个出块节奏，或者说，记账周期。区块链是被每个块有效载荷的哈希值“链”起来的，也是被时间串起来的“历史”。

五、其他时间概念

区块链里还有很多“时间”，如时间哈希锁。这些时间锁、时间点、时间段、时间戳让区块链变成一个“到点做加加减减”的服务。

记录在区块链上的时间不会撒谎，不可篡改。这个特性对于版权管理非常有意义。区块链是进行知识产权（intellectual property，IP）、版权及各种电子合同存证的理想工具。记录在区块链上知识产权的时间戳序列，可以有效确权，防止抄袭和盗版。数字作品的所有者把版权存证信息和版权交易信息记录在区块链上。版权信息可以在区块链上被追踪和查询，并被充分证明。区块链让数字版权记录、交易的时间真实，可查可追溯，让分布式公共账本准确可靠。

区块链本质上是一个时间服务器。也就是说，可以把区块链视为一个后台系统。在这个后台系统上可以做各种各样的用户接口，如数字藏品、数字资产。普通用户可以不了解后台系统是什么样的。区块链的特点是自带确定性的清结算，这是它与现有的金融系统不太一样的地方。买股票和基金的朋友应该知道，在股票和基金市场中有所谓的“T + 1”，也就是说交易成功后要等一天才能结算完成，但在区块链中是即时清算的，当下即完成，交易确认与清结算一体同步完成。

第六节　智 能 合 约

一、什么是智能合约

智能合约（smart contract）是指一种执行合约条款的计算机交易协议，由尼克·萨博（Nick Szabo）于 1993 年首次提出，他将其定义为“一组以数字形式为表征的承诺

（promises），并涵盖合约参与主体执行这些承诺的协议”。当时的智能合约就是一个黑盒子，后来萨博又把它完善了，并给它取名智能合约。

尽管智能合约的概念早于区块链概念的诞生，但直到区块链技术出现，智能合约的作用才真正被付诸实践。2013 年，以太坊系统启动，针对比特币区块链存在的问题，为了实现诸如众筹、溯源等应用场景，以太坊做了如下改进：支持用户自定义的业务逻辑，即引入了智能合约，极大增强了区块链的功能，同时也为区块链赋予了可编程性。智能合约成为部署在区块链上的去中心化、可信息共享的程序代码。有了智能合约的支持，区块链应用范围从单一的数字通证领域扩大到涉及合约共识的其他信用管理领域，在股票、清算、私募股权等场景现身。

维塔立克·布特林（Vitalik Buterin）的智能合约理念，乃至以太坊项目，均受到尼克·萨博几篇论文的影响。智能合约是自动执行的合约机制，使区块链技术成为各种应用场景的基础。智能合约和区块链的相互嵌入为打造去中心化、自组织化的创意产业投融资智能平台提供了可能性。

就其本质而言，智能合约是传统软件的一个插件，是一个扩展功能。如果智能合约是通用功能，它就可以直接写在链上，内置在协议层，因此不需要做一个智能合约。因为智能合约有些功能不具有通用性，只是有些人要用，因此在底层链的基础上又做了一些插件。以太坊智能合约的 ERC（Ethereum requests for comments，ERC）标准是一套提案机制，可以让人们参与以太坊网络的更新和修正过程。比如，ERC721 协议，以太坊就用智能合约形式实现。ERC721 是专门为非同质化通证（non-fungible token，NFT）而构建的，可以跟踪区块中单个通证的所有权及其转移路径。ERC721 定义了 NFT。因为并不是所有人都需要 NFT，所以以太坊使用智能合约形式操作这部分功能。再如，ERC20 协议，其功能在以太坊上是最明显的，它定义了同质化通证。它们不是所有人都需要，但是有些人需要这个功能，又不能做成公有设施，因此开发者就在上面做了一个插件。所以，智能合约其实是一个插件的功能。IBM 的说法是链上代码（chain code），这个概念更符合智能合约的定义，就是一些对链扩展的功能。

当前的智能合约大致包括三类：一是比特币的未花费交易输出模型（unspent transaction outputs，UTXO），它基于堆栈，是一个很简单的脚本，没有循环，也是非图灵完备的；二是以太坊虚拟机（Ethereum virtual machine，EVM），它是图灵完备的，用的编程语言是 Solidity；三是超级账本（hyperledger）平台，智能合约程序通常是用链码来编写的，用的编程语言是 Golang、Java 或者 Node.js。超级账本提供了一个链码开发环境，可以利用容器来模拟网络并执行链码。

二、合约容器

智能合约需要一个容器，这个容器不是类似应用容器引擎（docker）这种狭义的容器。这个容器是一个广义的东西。当程序员需要一个插件的时候，需要把它包进去，要决定在什么容器里面跑这段代码。现在用得最广泛的是虚拟机，有不同的虚拟机，但很多都是以太坊的虚拟机衍生出来的；还有一个就是比特币这种堆栈的形式。

因此，智能合约需要一个容器来运行。虽然智能合约是运行在出块节点上，但是它需要一个容器来运行，需要一个独立的空间。

三、合约语言

智能合约语言接口的关键是对高级语言友好。其实理论上说，智能合约用汇编语言写也没有问题，毕竟对于计算机来说，它不必区分高级语言或汇编语言，它只处理 0 或 1 的数位。

目前，大约 40%的区块链从业者在以太坊社区，因为以太坊的合约接口对高级语言比较友好，让开发者能很快地融入进去，所以智能合约需要一个高级语言接口。

这些高级语言包括什么呢？比如，EOS 用的就是 C++，以太坊的 Solidity 用的是基于 Javascript 的语言，也有其他区块链项目基于 Python、Lua 等程序语言做智能合约。比特币使用的是一个功能简单的脚本语言，出错率稍低。

以太坊智能合约存在一些问题：首先，当初做以太坊虚拟机的时候，开发过程是比较匆忙的，没有经过太多的时间去验证；其次，以太坊编程语言 Solidity 是从 Javascript 改进的，它也是一个比较新的东西，新的东西放在一起运行就容易有各种各样的问题。所以，以太坊发展过程中出现了一些安全问题。比较著名的是 2016 年 The DAO 攻击事件。2016 年 6 月 17 日，一名匿名黑客利用构建 The DAO 的智能合约代码中的错误，从隔离的钱包地址中提取了约 6000 万美元的以太币。鉴于无法追回被盗资金，以太坊社区决定于 2016 年 7 月 20 日进行一次硬分叉，大部分人切换到分叉链上，而一些坚持区块链不可篡改信念的人坚守原来的以太坊链，形成以太坊和以太坊经典网络共存的生态。

四、预言机

智能合约还有一个重要的原理是预言机（oracle）。预言机的原理非常简单，但是其实现很难，难到今天都没有一个合意的实现案例。预言机是区块链智能合约一个非常好的发展方向。读者有兴趣可以去研究一下。

简单解释一下预言机的原理。跑在区块链上的智能合约，它是机器中的一段程序。智能合约有时候需要外部的数据，需要专门把数据传进来。最经典的例子就是在合约里面打赌。两个人赌明天天气好不好：明天 12 点下雨，你方赢；明天 12 点不下雨，另一方赢。一定要定义好是 12 点，不能说明天下午，它需要明确的条件。那智能合约怎么知道 12 点下不下雨？就得有人告诉它下不下雨。当然它也可以自己去调外部数据，程序员设计调用外部数据。比如，到 12 点的时候调用气象局的应用程序编程接口（application programming interface，API）数据。

预言机原理看起来比较简单，但是它在实践应用中也有困难点。预言机的实现难点在于人性。两个人打赌，打一块钱的赌，基本上不会有什么动机作弊，但是如果这个赌约是 1 亿元人民币，就像赌世界杯的时候，当赌注够大的时候，用户无论是自己出去调数据，还是采用串通的手段，都有作弊动机。这就是预言机难以实现的地方，也就是人性或者说激励机制。

第七节　个人信息安全管理

一、个人信息保护

大数据的流动有利于数字产业的发展，个人信息保护需求同样引发社会持续关注。互联网平台持续收集和利用消费者数据，从而进一步巩固其市场实力。由于在线持久的数据收集通常是隐蔽的，因此比较不同产品和服务的隐私成本更加困难。消费者基本上不清楚平台企业的数据收集做法。操纵性设计界面也已成为一种普遍的工具，推动在线跟踪和在线广告市场的发展，以增强平台企业的市场实力和竞争力。

互联网平台对用户数据的收集和滥用屡屡发生，各种网站和手机应用程序（application，App）后台不断收集用户上网行为的数据、身份信息、位置信息。部分 App 未经许可使用手机上的麦克风、盗取手机里的通信地址。用户隐私数据泄露后，骚扰电话、消息不断。这些体验并不是用户想要的，但是因为互联网平台的统治力，用户不得不接受这样的糟糕体验。如何加强隐私数据保护，是数字经济发展过程中的关键问题。

数字身份已有应用雏形。例如，很多 App 或者小程序支持用微信账号、QQ 账号、电话号码甚至人脸信息授权登录。现有的数字身份认证方式大多是由某一家公司或服务提供者来管理和控制的。这种方式虽然方便，但用户往往需要用失去自己对数据的控制权的代价来换取这个便利，可能存在隐私泄露的风险。

相比于日常生活中的实体信息收集装置，App 的安全性其实算比较好判断的。比如，小区里新安装的识别摄像头，要求每个人必须提交人脸信息，人们虽然会觉得不舒服，但也拿不准这个装置到底是不是必要的。严格来说，不应该由个人来判断，而是应当由物业企业主动地说明这个问题。但现在的企业不仅不做说明，反而是将能收集到的数据统统收集了。企业收集了这些数据后，往往直接把数据作为一种财产。对于个人来说，我们也可以做判断。比如，风景区入园、小区门卫人脸识别。如果没有人脸识别，访客能不能进入？显然，是可以的，看个身份证核对一下名字也行，只是麻烦一点罢了，但还是能进去的。显然，收集人脸数据并不是进入景区、小区所必需的。所以说，企业必须一开始就把数据处理的目的告诉用户：出于什么目的收集数据，以及收集了什么数据。这样公众就很容易判断安装这个摄像头进行人脸识别到底是不是必需的。平台企业在收集和使用数据的时候，需要对公众透明，让公众了解数据的用途，以确保数据使用的合理性。

针对这些需求，区块链技术加强个人数据管理，可以更加有效地保护用户的数字身份信息，避免隐私泄露的风险。

二、基于区块链的数字身份解决方案

数字身份（digital identity）包含标识符、属性、凭证等数据要素。传统互联网 Web1.0 和 Web2.0 的身份模型中，用户没有统一的标识符，数据身份无法互通，并且有隐私泄露的安全隐患，数字凭证也因为数据孤岛的问题难以大规模使用。这种身份模型在互联网早期

比较适用，但随着数字经济的深化，它反而成为阻碍数字世界互通的问题；登录各种网络平台都需要记住一堆用户名和密码，而且不同平台的数据无法通用。

区块链系统采用非对称加密形式以解决链上参与者的身份认证与标识。非对称加密算法使用了一对密钥：数学上彼此关联的公钥和私钥。私钥被用来进行数字签名，公钥用来验证由私钥生成的数字签名，进而完成参与者的身份验证，实现确权、交易、流转环节上链。用户在链上登记、存证数字艺术品及权利交换，依托公私钥密码机制解决，并实现信息的脱敏与不可篡改。

在区块链系统中，用户通过私钥签名认证身份和控制资产，他人可以通过公钥（地址）验证用户的身份。而“地址 + 私钥”无需注册，通过密码学规则由用户自行生成，验证身份的过程也无需任何机构参与。用户在完全去中心化下掌控着身份标识号，从而实现对数字身份的控制。

基于区块链的数字身份，不仅可以确保身份安全，还可以提升数字身份的可信程度，避免伪造、冒用、盗窃身份，有效保护隐私，实现身份可验而不可见。用户成为自己数字身份的控制者。用户可以控制自己的身份数据，允许什么信息被记录，什么信息被谁读取和使用，什么信息可以跨平台转移使用。随着数字经济的发展，网络空间中的实体都需要拥有数字身份，包括人、设备、组织、应用，这些实体通过数字身份来被区分和辨认。各类数字身份融合并且锚定现实身份，形成统一的新型身份体系。

作为一个分布式账本，区块链信息存储在网络的各个节点中，不由任何一方独立控制。在新一代互联网 Web3.0 中，区块链信息存证有利于提升人们对个人数据的控制权，用户掌握着对应个人数据账户的私钥，可以更为自由地选择将个人数据在何时披露；用户的数字身份信息可以被可靠地保护，避免了中心化存储可能带来的风险。相比之下，目前中心化网络 Web2.0 的个人信息管理方式，如身份证号、医疗记录等，则有更多的被非授权披露的风险。数字身份解决了 Web2.0 阶段个人信用无法跨平台互通的痛点，将数字画像从基于应用收集数据的封闭型转为基于开放数据和可信凭证的开放型，而链上数据的开放可信性也让 Web3.0 简历、Web3.0 社交名片、无抵押借贷得到更好的应用。

三、分布式数字身份

分布式数字身份（decentralized identity，DID）试图解决 Web2.0 目前的发展瓶颈，使更丰富的数字经济活动能够实现。现实世界中，身份系统是社会运行和经济活动不可缺少的一部分。身份证、学历、驾照等证明人们的身份和资质；同时，声誉和信用更是商业和金融得以拓展的关键。区块链数字身份将个人信息、资产、数据统一管理，可以有效确保数字资产安全。一套可以跨越平台的身份记录，使互联网下一阶段 Web3.0 的发展成为可能。分布式数字身份的一个重要功能是用户可以在 Web3.0 的不同平台之间凭借私钥形成身份的迁移，从而统合不同平台上同一主体的不同数字身份。

分布式标识符是一种可验证的分布式数字身份新型标识符。分布式标识符标准构建了一套多平台互通的身份系统，由用户控制标识符及对应的数据，控制应用对数据的读写范围和时间，从基础设施上支持了可验证凭证的大规模应用。

隐私计算在数字身份体系中发挥着基石作用。隐私计算可以在多方利用个人数据的

过程中增强对数据的保护，从而实现最小化信息披露，让数据“可用而不可见”。在“区块链 + 隐私计算”所搭建的生态里，每个人都可以基于数字身份拥有自己的数据权益，在保护个人隐私的同时充分释放数据价值。

第八节　区块链的应用

一、区块链的应用范围

区块链相关的技术经过十几年的发展，其共识算法、应用密码学等底层技术已经比较成熟。弄懂区块链技术原理是第一步，看看它适用于什么场景，接下来才是寻找系统和区块链的结合点。在区块链应用落地过程中，把大量信息在区块链上处理并不是高效的方式。采用“ + 区块链”或者“区块链 + ”，是更为务实的项目管理思路。

区块链适用于非信任环境的价值交互场景。传统的网络交易通常需要通过第三方机构来提供信任担保，但这些机构可能存在欺诈或破产的风险。而区块链技术的交易是基于密码学的，每笔交易都会被网络中的节点验证，成为区块链的一部分，这意味着一旦交易完成，就无法篡改或撤销，从而在无需第三方的情况下实现了信任。

现在有很多企业已经开始使用区块链来做解决方案，但在那些传统行业中，区块链就只是一种技术方案，只能降低运营成本。举个例子，假设业务需要运用区块链做一个 Airbnb 搭车软件，这个新搭车软件跟现有的 Airbnb 相比，其唯一的优势可能就是运营成本更低，在其他方面没有任何区别。如果没有什么特别的理由，传统的解决方案可以胜任，也可以做得很好，因为这些方案往往更加成熟。

区块链技术方案适用于多主体参与、分布式的系统。对于业务场景，区块链比较适合的应用方式可列举如下。

（1）全球化的唯一数字化标识：在区块链中，每个参与者都有一个唯一的公钥和私钥构成的数字身份，可以通过这个数字身份进行交易或访问其拥有的资产，这是全球通用且无法被篡改的。

（2）去中心化的命名服务或有序登记：由于区块链技术的去中心化特性，它可以构建一个公开透明的、有序的登记系统，使每个参与者都可以参与并对该系统进行监督。

（3）所有权的密码学安全系统：区块链技术采用了先进的加密算法来保护资产和交易的安全，只有持有相应私钥的人才能访问和操作其拥有的资产。

（4）减少或消除解决争议纠纷时的人为干预：区块链通过智能合约技术，能够在合约条件触发时自动执行，这极大地减少了争议纠纷的可能性，降低了依赖人为干预的需求。

（5）实时监控管理者对被管理者的行为：因为区块链上的一切操作都是可以追溯的，所以可以实时监控管理者对被管理者的行为，确保管理者的行为公开透明。

（6）多主体间共享数字资产和交易历史的完整记录：区块链的一个重要特性在于它是一个公开透明的账本，任何人都可以查看上面的交易记录，这为多主体间的数字资产共享提供了可能。

二、区块链的产业应用

区块链技术的发展和成熟，催生了许多具有革命性意义的产业应用，主要体现在以下几个方面。

在金融领域，区块链应用最为广泛，它可以一次性实现钱、账清结算，不像传统的金融系统需要花费大量的财力、物力去做第三方清算、结算。区块链技术应用于支付结算、跨境汇款、证券交易等金融领域，降低了交易成本，提高了交易速度，使金融领域步入新的信任时代。

在版权保护领域，通过区块链技术，可以实现数字内容的确权、保护和管理，降低版权纠纷的风险，保护创意产权。

在数字身份领域，通过区块链实现身份认证，可以大大降低诈骗风险，提高在线交流的安全性。为新一代互联网跨平台身份认证、数字分身、数字人应用提供基础技术。

在物联网方面，将区块链应用于物联网，可使设备彼此之间能够更加安全和可靠地进行信息交换和执行操作，从而产生更加可靠的机器协作体系。物联网区块链提高了物流供应链的真实性、透明度和安全性，为供应链管理提供了更为有效的解决方案。

区块链技术的广泛应用，正在对金融、身份认证及物联网等领域产生深远影响，推动各个行业不断发展与创新。

三、区块链的应用发展阶段

自 2008 年中本聪发表《比特币：一种点对点的电子现金系统》（*Bitcoin*: *A peer-to-peer Electronic Cash System*）以来，区块链技术经历了从理论到实践，从金融到各行业的发展历程。区块链不断完善的技术特点使其应用前景广阔。区块链作为一种技术架构，从应用发展阶段来看，其概念内涵不断演化，经历了五个阶段：分布式账本、去中心化计算平台、去中心化金融、非同质化通证、元宇宙。这几个阶段可以用一幅图来展示（见图 1-7）。

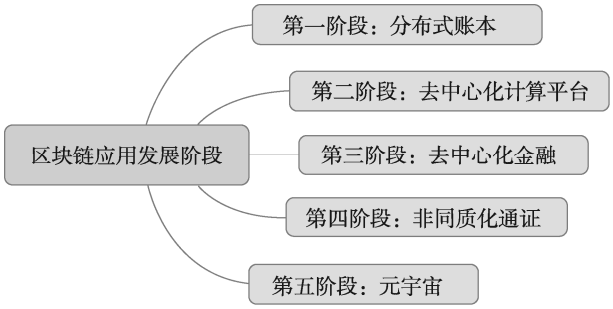

图 1-7　区块链应用发展阶段

（一）第一阶段：分布式账本

中本聪在 2008 年首次提出了比特币的概念，其背后的核心技术就是区块链。比特币成为第一个基于区块链技术的金融交易系统。比特币提出了一套有效的经济激励模型，运用

分布式账本解决了电子现金的“双花”问题，其去中心化、安全性等特点引起了广泛关注。

（二）第二阶段：去中心化计算平台

比特币底层 UTXO 模型虽然稳定地运行了多年，但 TPS 太慢。每秒 10 次以下的 TPS 响应速度，跟中心化互联网平台的 50 万次以上的 TPS 有云泥之别。以太坊作为一个支持智能合约的开放式区块链平台的诞生，丰富了区块链的功能，使区块链技术不仅可以应用于金融领域，还可以广泛应用于其他领域。2013 年，以太坊系统启动。以太坊支持用户自定义的业务逻辑，即引入了智能合约，极大增强了区块链的功能，同时也为区块链赋予了可编程性；以太坊还引入了权益证明的共识机制，提高了区块链响应速度。2015 年，IBM 开发了超级账本（hyperledger），作为联盟链，是区块链及分布式记账系统的跨行业发展与协作，并着重发展性能和可靠性，使之可以支持主要的技术、金融和供应链公司中的全球商业交易，在企业层面有广泛的应用。有了智能合约的支持，区块链应用范围从单一的数字通证领域扩大到涉及合约共识的其他信用管理领域，在股票、清算、数字身份等场景现身。

（三）第三阶段：去中心化金融

去中心化金融（decentralized finance，DeFi）的目标是构建透明化的金融系统，向所有人开放，并且无须许可，不用依赖第三方机构即可满足金融的需求。去中心化金融的应用场景非常广泛，目前涉及资产管理、基础设施、借贷、金融衍生品等业务。

（四）第四阶段：非同质化通证

2017 年，以太猫游戏催生了非同质化通证（non-fungible token，NFT），标志着区块链发展到第四阶段。运用 NFT，区块链可覆盖任何数字创意产品。在区块链加持下，加密艺术崛起，购买加密艺术品的人拥有数字资产，并附有真实性的数字证书。NFT 为加密艺术品、数字藏品、版权存证提供了重要支撑，引领了一个数字创意快速繁荣的阶段。NFT 的出现创造了一个非常好的经济确权机制，保证在这个架构中经济系统的稳定。去中心化金融和 NFT 融合，发展出区块链游戏创新模式。

（五）第五阶段：元宇宙

在第五阶段，元宇宙崛起，区块链为元宇宙建设提供重要基础设施。元宇宙作为虚实互动空间，需要以区块链作为桥梁，并综合运用 NFT、游戏化金融、智能合约等技术。

基于区块链五个应用发展阶段的认识，本书章节安排大体对应于区块链应用发展各个阶段，聚焦区块链在数字创意和元宇宙领域的应用。第一章主题是区块链原理，介绍了分布式账本和密码学基础知识；第二章主题是区块链与创意管理的融合，介绍了去中心化计算平台建立的信任机制；第三章主题是加密艺术与创意管理；第四章主题是版权区块链管理，这两章介绍了区块链应用的 NFT 阶段；第五章、第六章、第七章主题是元宇宙及其各种产品形态，介绍了作为元宇宙基础设施的区块链；第八章主题是 Web3.0 数字创意产品；第九章介绍区块链在文化创意金融领域的应用；第十章主题是区块链发展趋势展望。

如果对区块链发展脉络感兴趣，读者可以在阅读本书第一章、第二章之后，跳转到第

九章阅读，了解区块链金融应用阶段，然后再阅读第三章到第八章，这样对区块链应用各个阶段发展情况会有更加清晰的认识。

本章提要

区块链是在点对点网络里，依赖现代密码学及共识规则，通过哈希算法将带有时间戳的交易数据块首尾相连，以实现数据不可篡改的一种分布式账本。区块链技术通过其去中心化、不可篡改和高度安全的特性，改变了数据管理和交易方式，为科技创新提供了重要推动力。区块链被视为新质生产力的重要工具，对于促进经济变革和高质量发展具有显著作用，对推动数字经济的发展至关重要。

密码学是一种保护信息不被未经授权的方式访问的理论和实践，它在区块链中起着重要作用。密码技术包括密码哈希函数、非对称加密算法和数字签名等。哈希算法保证了数据的不可逆性和抗碰撞性。数字签名是一种使所有的交易公开，但又能保护交易双方隐私的机制，确保了交易的完整性和授权性。非对称加密算法使用一对公钥和私钥提高安全性。每个用户都有专属的一对私钥和公钥。私钥被安全地存储在用户的设备上，用于对交易进行签名，证明这个交易是由持有私钥的人发送的；公钥则用来加密信息，并且每个人都可以用它来验证签名的真实性。

区块链是一种用密码技术建立的分布式账本，通过加密算法实现数据不可篡改和数据共享的功能。区块链原理是将数据以区块的形式链接起来，每个区块包含先前区块链的哈希值和新的交易信息，这样形成一个不可篡改的数据链接。区块链的延伸和生长，是依靠新的块源源不断地生成。在区块链上，分布式账本记录每一笔交易并由共识协议来全网确认，从而避免了“双花”问题。

区块链作为时间服务器，利用时间戳、存证时间、时间函数等概念，为数据提供了不可篡改的历史记录。出块时间、时间戳和存证时间等都是区块链中重要的时间概念，它们共同构成了区块链的时间视图，对于版权管理、信用管理和存证等方面具有重要意义。

自 2008 年以来，区块链技术经历了从理论到实践，从金融到各行业的发展历程。区块链可以分为五个应用发展阶段：分布式账本、去中心化计算平台、去中心化金融、NFT、元宇宙。

从本章讨论可以看到，区块链用全新的方式结合了现有网络、密码学机制和数据存证技术，通过这样的组合技术体系，实现分布式体系，确保数据安全。区块链技术正在以前所未有的速度发展和变革，它的出现让我们看到一个全新的、充满创意的数字世界。随着区块链技术的发展及其应用领域的拓展，区块链将发挥越来越重要的作用。

思考题

1. 区块链在技术创新和产业发展中有什么重要作用？
2. 从密码技术的角度看，区块链是怎样实现数据和隐私安全的？
3. 软分叉和硬分叉的区别是什么，它们对区块链网络有什么影响？

4. 工作量证明算法和权益证明算法在区块链中如何实现，它们有何不同？

5. 出块时间、时间戳和存证时间在区块链中扮演什么角色，它们如何共同构成区块链的时间服务器功能？

6. 区块链应用经历了几个发展过程？随着区块链技术的不断发展，它将如何塑造未来的数字经济和社会组织结构？

案例

“链上清镇·智慧城乡”智能诚信管理平台

一、案例背景

随着我国社会经济的发展，诚信体系建设的重要性不断提升。自 2009 年以来，贵州省清镇市不断探索农民致富的新路子，在全市开展“诚信农民、诚信村组、诚信乡镇”创建活动，取得了不俗的成绩。清镇市以“链上清镇”为载体，充分结合区块链技术落地应用试点任务，开发基于区块链技术的诚信管理平台，夯实诚信体系建设的信息基础设施建设工作，全力打造公平的共享创新型数智城市。

在传统的第三方集中征集诚信数据的模式下，数据信息被视为企业商业秘密，数据被封闭在个别数据源垄断性企业中，诚信数据的使用从源头上就缺乏可信度，直接影响诚信评价效果。传统集中式管理数据，并提供诚信服务的模式，个人与机构诚信信息呈现跨区域、跨部门、跨行业、相对独立又纵横交叉的特点，导致原本具有公共产品或准公共产品属性的诚信信息数据被视为商业秘密而难以共享，因此形成数据孤岛。

二、技术方案概述

智能诚信管理平台由区块链监测支撑系统、统一接口服务系统、分布式数字身份管理系统、区块链浏览器、诚信平台数据上链工具、Spark 系统定制开发六个部分构成。

智能诚信管理平台不集中元数据，而是对数据哈希提取存证，所有元数据本地化、分布式存储。在使用中，元数据或计算后的指标根据场景单点授权，数据使用记录进行区块链存证，并实现从授权、认证、访问控制到共识与数据共享及各类特定业务场景的密码协议，形成可配置的综合安全机制，有效实现信息的安全防护、保障诚信管理服务，真正有效地保护用户的知情权、隐私权。

智能诚信管理平台促进信用数据的可信采集，为信用数据共享共用打好基础。运用区块链不可篡改的技术特征来记录、归集、完善和整合公共管理部门信用信息，以及农村根据村民规约采集的信息。智能诚信管理平台为清镇市全体居民、企业、机构打造了“链上清镇”身份标识符，为清镇市在互联网环境下进行经济活动、社会治理、民生服务提供高效、可信、安全的入口。分布式数字身份管理系统包括分布式数字身份的生成和销毁，通过密码学算法保证分布式数字身份不重复且具有唯一性。

本项目的核心是将链网上的公有价值共识定义为诚信积分，通过身份链的映射，在链网上捕捉同一诚信主体在不同身份下的各类诚信痕迹，并将同一诚信主体对应的不同场景下（不同身份）的诚信积分在唯一的诚信账户内实现便捷管理，再分场景个性化地进行点

对点的授权应用，拓展诚信应用产品。

实践证明，该项目的实施能够为清镇市居民提供更好的社会信用服务，具体包括以下四个方面：第一，诚信主体基础档案管理，基础档案分为诚信农民、诚信市民、诚信职工、诚信企业、诚信机构五大类；第二，诚信标准细则管理，标准涵盖基础档案五大类主体；第三，诚信征信信息采集、审核管理；第四，诚信评定结果管理。

三、案例评析

智能诚信管理平台在链上存证同一个诚信主体不同场景下的各类诚信痕迹，并对同一个诚信主体在不同场景下（也是不同身份）的诚信信息在唯一的诚信账户内实现便捷管理，实现了诚信评价场景化、个性化精准应用，变被动为主动，更好地向清镇市居民提供社会信用服务。

资料来源：中国信息通信研究院. “链”接未来：可信区块链应用实践[M]. 北京：人民邮电出版社，2019.

【案例讨论】

1. 在智能诚信管理平台中，如何通过区块链技术实现数据安全防护和用户隐私权保护的？

2. 为什么智能诚信管理系统更适合采用区块链技术方案？