（3）只有持有 ASIC 的人才能执行连接区块链上区块的处理。

问题二

请选择关于区块链种类的一个正确的描述。

（1）公有链有最终确定性。
（2）联盟链有最终确定性。
（3）许多私有链都采用 PoW 来确保其最终确定性。

问题三

请选择一个正确的关于区块链历史的描述。

（1）比特币的创意是由中本聪提出的。
（2）平台型区块链是由中本聪开发的。
（3）所有的阿尔特币是由比特币分化出来的。

问题四

请列举 3 种区块链，并分别说明它们的特点。

问题五

请列举一个本书中没有介绍的区块链用例。

第2章 区块链的构成技术

构成区块链技术的核心技术有“加密技术”“P2P 网络”“共识算法”。下面我们来详细地讲解这些技术。

2.1 加密技术

区块链中到处都使用了各种密码技术。在这里我们重点对加密哈希函数、公开密钥加密方式、通用密钥加密方式、椭圆曲线密码学和电子签名等进行介绍说明。

2.1.1 加密哈希函数

加密技术的哈希函数是一种将输入的数值转换为按照一定的规则输出数据的函数。这种函数具有以下 4 个特征。

（1）只能进行单向运算，不具备行之有效的逆运算方法。（不可逆性）

（2）输入的数据哪怕仅有细微的变化，也会导致输出数据发生很大的变化。（机密性）

（3）不论输入数据的长度是多少，都将输出相同长度的数据。（固定长度）

（4）能够方便地从输入数据计算出输出数据。（处理速度）

通过利用这些特征，可以证明数据的正确性，节省数据的容量。

另外，通过哈希函数计算哈希值称为哈希处理，哈希处理也称为摘要（digest）。这是因为不仅仅返回输入数据，同样的会返回具有相同数据长度的输出值。再者，因为能够像指纹一样确认输出值和输入值是否具有一一对应的关系，又称为 Finger Print（指纹）。关于哈希函数，将在第 7 章中做详细介绍。

2.1.2 公开密钥加密方式

加密的过程分为加密和解密两个阶段，如图 2.1 所示。

图 2.1 加密和解密的过程

公开密钥加密方式是使用不同的加密密钥和解密密钥。通过使用私密密钥和公开密钥实现公开密钥加密方式。私密密钥和公开密钥分别发挥不同的作用，私密密钥是自己所持有并且绝对不能泄露给他人的密钥，公开密钥是广泛公开的密钥，如图 2.2 所示。

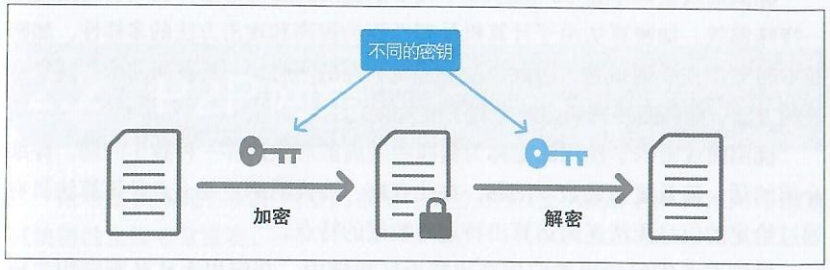

图 2.2 公开密钥加密方式

这里，私密密钥和公开密钥的重要特征是，通过公开密钥无法逆向运算得出私密密钥。否则，如果不告诉其他人的私密密钥信息，却能够通过任何人获得的公开密钥而进行推算确定，那么这种加密技术就没有意义了。

比特币区块链使用的是公开密钥加密方式，可用于地址的生成和交易数据的处理等各种各样的场合中。

2.1.3 通用密钥加密方式

通用密钥加密方式和公开密钥加密方式是不同的，通用密钥加密方式是使用相同的密钥进行加密和解密，如图 2.3 所示。由于在通用密钥加密方式中加密和解密的过程使用相同的密钥，密钥安全地和另一方共享是非常必要的。另外，由于存在多少共享数据的人就需要有多少个密钥，因此存在这样一个缺点即随着共享人数的增加，管理也将随之变得繁杂。为了克服这个缺点，开发了前面已经介绍过的公开密钥加密方式。

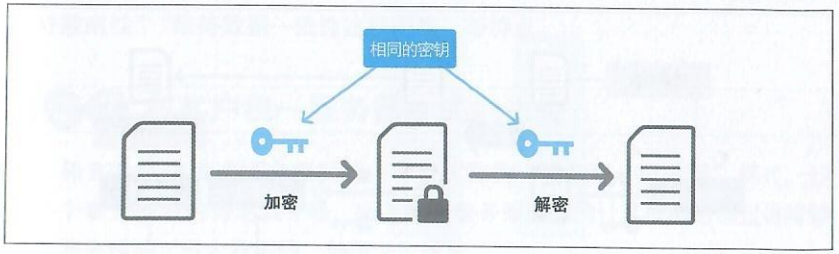

图 2.3 通用密钥加密方式

2.1.4 椭圆曲线密码学

椭圆曲线密码学是20世纪80年代中期提出的加密方法，利用椭圆曲线这一特殊曲线。加密算法由于计算机处理性能的提高和攻击方法的多样性，加密技术时刻都在受到威胁。因此，在保持便利性的同时，一直在研究维持高安全性的方法，椭圆曲线密码因此受到了极大的关注。

椭圆曲线密码学使用的是称为椭圆曲线离散对数这样一种数学问题。详细介绍的话，涉及复杂的数学问题，在此省略，要说明的重要一点是该算法具有通过给定的信息无法逆向运算出特定的数据的特点。

椭圆曲线密码学也被应用在比特币区块链中，并应用于从私密密钥生成公开密钥的情况。

2.1.5 电子签名

电子签名是用于验证数据确实是由特定作者生成的技术。在任何人都能够利用电子计算机的时代，任何人都可以复制数据或者修改数据，因此为了证明（签名）数据是由特定的人生成的，这种密码技术就成了必不可少的技术。电子签名的示例如图 2.4 所示。

电子签名的程序如下。

（1）生成需要传送的数据。

（2）通过利用哈希函数，将需要传送的数据进行哈希处理。

（3）加密哈希值。

（4）将需要发送的数据以及加密的哈希值都发送给对方。

（5）接收数据的人对发送来的数据进行哈希处理以获得哈希值。

（6）通过解密将包含有加密数据而求得的哈希值和自己求得的哈希值进行比较，以确认是否是相同的数据。

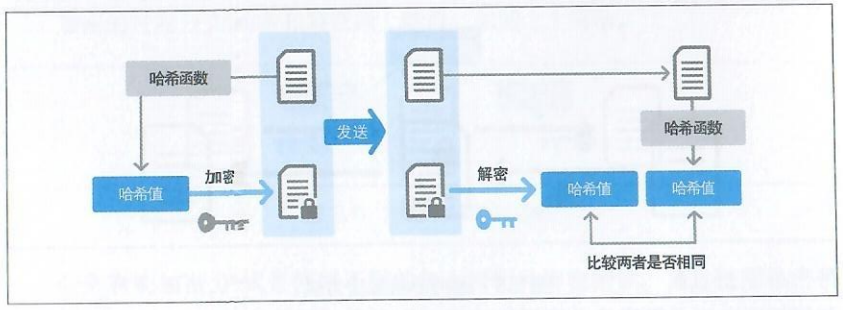

图 2.4　电子签名的原理

通过阅读上述内容，可以理解哈希函数以及公开密钥加密方式等各种加密技术的使用方法。比特币区块链中用它来证明汇款数据确实是由汇款人所生成的。

2.2 P2P 网络

区块链技术是在 P2P 网络的前提下建立的技术。理解 P2P 技术对于理解区块链的发展非常重要。

2.2.1 什么是 P2P 网络

P2P 网络是由被称为 Peer（对等者）的处于对等地位的计算机彼此连接而成的网络如图 2.5 所示。此时，P2P 网络上的计算机称为“节点”。

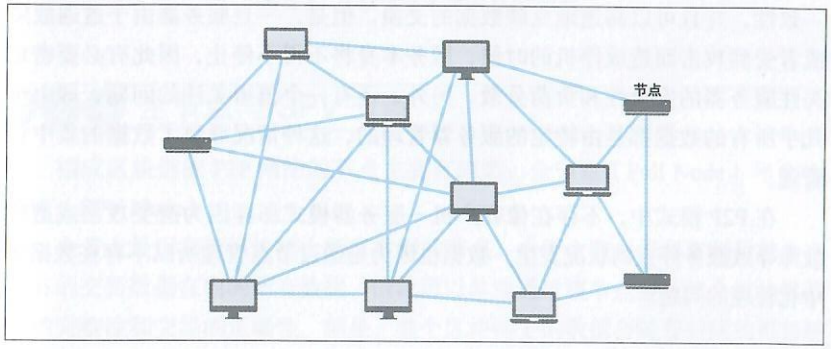

图 2.5　P2P 网络示意图

作为 P2P 的特点，这里可以列举出诸如“系统不会停机”“具有高度的网络分散耐性”“维持数据一致性比较困难”等特点。

2.2.2 与客户机—服务器模式的比较

和 P2P 网络模式完全相反的一种模式称为“客户机—服务器”模式。这是一个事先准备的特定服务器，所有接收服务器服务的计算机都是通过访问该服务器来读取 / 写入数据的，如图 2.6 所示。

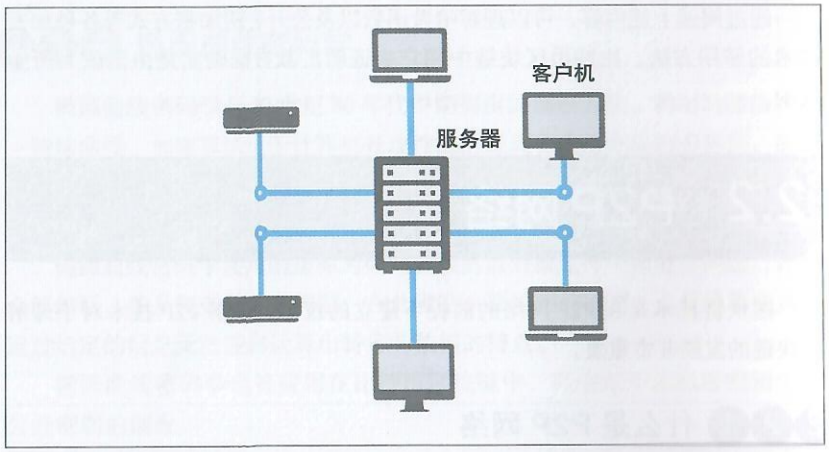

图 2.6　客户机—服务器模式示意图

由于特定的服务器承担了所有的数据处理的任务，因此能够保持数据的一致性，并且可以高速地反映数据的交换。但是，一旦服务器由于遭遇故障或者受到攻击而造成停机的时候，服务本身将不得不停止，因此有必要密切关注服务器的安全性和负荷分散。另外，还有一个值得关注的问题，即由于几乎所有的数据都是由特定的服务器管理的，这种情况导致了数据的集中化管理。

在 P2P 模式中，不存在像客户机—服务器模式那样因为遭受攻击或遭遇故障导致服务停止的状况发生，数据也因为是通过节点管理所以不存在数据集中化管理的问题。

2.2.3 区块链中的 P2P 网络

让我们仔细看看区块链技术中的 P2P 网络，如图 2.7 所示。

分布在世界各地的计算机都连接在区块链中。同样，就比特币而言，世界上每秒会产生数十笔交易数据，这些数据也同样不间断地在网络上传输。

区块链中的交易数据，像接力赛一样从一个节点传递到另外一个节点，并在整个网络上传输。此时，在节点之间进行着信息的交换，并且执行诸如连接确认和发送数据的内容的确认等通信。

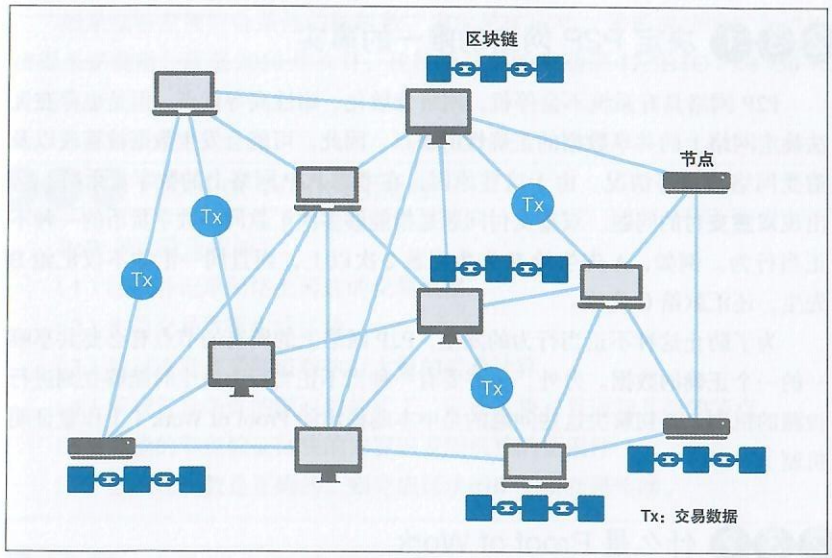

图 2.7　区块链技术中的 P2P 网络

2.2.4 全节点与 SPV 节点

构成区块链的 P2P 网络的节点主要有两类：**全节点**（Full Node）和 **SPV 节点**（SPV Node）。

全节点是保存有区块链上所有数据的节点。由于全节点保存有到目前为止所有的交易数据在内的所有数据，因此可以单独通过该节点验证整个区块链数据的完整性和交易的正确性。但是，整个区块链上的数据会随着时间的推移越来越多，截至 2019 年 9 月大约为 200GB，因此，除非计算机具有足够的容量，否则按当时现状很难成为全节点。另外，SPV 节点是仅仅保存有区块链的区块头的信息的节点。不足部分通过访问全节点来进行补充。由于数据容量可以减小到全节点的大约千分之一，因此在一般的终端上很容易进行处理。

2.3 共识算法

在 P2P 网络上决定数据正确性的过程称为共识算法（Consensus algorithm）。共识算法对于区块链技术的实现是必不可少的。

2.3.1 决定 P2P 网络的唯一的事实

P2P 网络具有系统不会停机，网络分散化、耐性高等优点，但是也存在无法确定网络上的共享数据的正确性的缺点。因此，可能会发生数据被篡改以及遭受网络攻击等情况。由于这些原因，在考虑 P2P 网络上的数字货币时，会出现**双重支付**的问题。双重支付问题是指能够多次汇款同一数字货币的一种不正当行为。例如，A 先生给 B 先生汇款 2 次以上，而且同一汇款不仅汇给 B 先生，还汇款给 C 先生。

为了防止这种不正当行为的发生，P2P 网络上的所有的节点有必要共享唯一的一个正确的数据。另外，还需要有一种当不正当行为发生时能够立刻进行检测的机制。最初解决这些问题的是中本聪提出的 Proof of Work（工作量证明机制）。

2.3.2 什么是 Proof of Work

Proof of Work（PoW）是指通过不确定多数的计算机进行运算以确保区块链整体的完整性和一致性的一种算法，如图 2.8 所示。具体来说，即汇总交易数据的摘要以及时间戳等数据。将该数据加上“随机数（Nonce）”，通过哈希函数计算哈希值。通过更改 Nonce 来执行计算，直到哈希值小于某个一定值（目标值）为止。执行这种计算的过程称为“**采矿**”，执行采矿的主体称为“**矿工**”。这里的时间戳和 Nonce 汇总起来成为区块头。

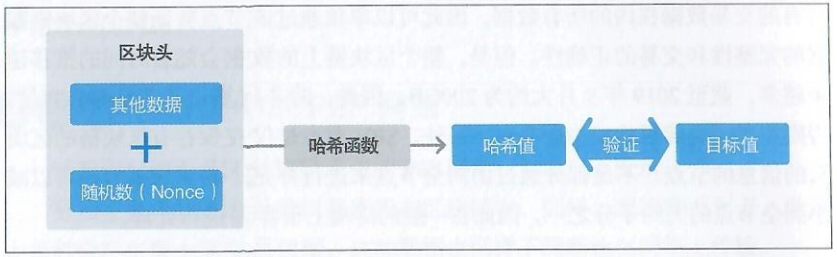

图 2.8　PoW 的流程

由于非随机数的数据是固定的，因此只能够通过一点点变更随机数进行计算。但是，由于哈希函数的特点，即使输入值发生很小的变化，也会使输出的哈希值发生很大的变化。因此，基本上无法推算出比一定值小的随机数。所以，“**矿工**”别无他法，只能使用“蛮力破解”的方式计算这一随机数。

如果能够发现符合条件的随机数，表示采矿成功，采矿成功的矿工可以获得采矿奖励。截至 2019 年 9 月，比特币采矿的奖励是 12.5BTC（约 750 万日元）。

2.3.3 Proof of Work 的流程

PoW 的大致流程如下。

（1）接收并记录网络上传送的交易数据。

（2）汇总交易数据生成区块。

（3）通过逐渐改变随机数执行大量的哈希计算。

（4）发现符合条件的随机数的矿工，完成区块并且通知其他的节点。

（5）其他的节点验证区块的内容以及随机数的正确性。

（6）如果随机数是正确的，则完成区块的矿工将获得奖励。

2.3.4 哈希能力与难易度调整

区块链网络上的计算能力称为哈希能力。以比特币为例，其哈希能力逐年增长，整个网络整体的计算能力超过了全球排名前 50 位的超级计算机的计算能力的总和，如图 2.9 所示。通过执行这样大量的计算，可以维持整个区块链的完整性。

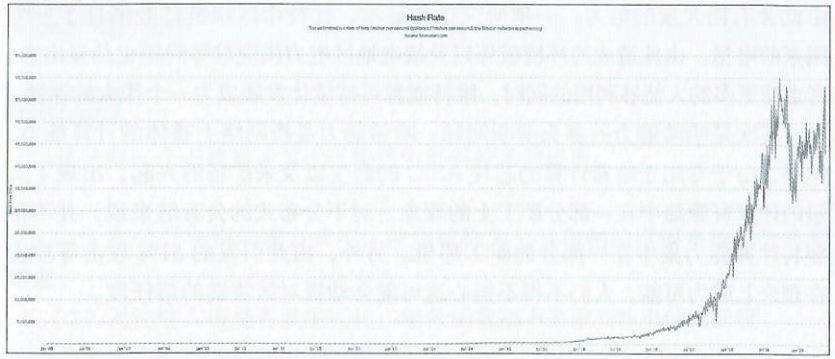

图 2.9　哈希能力的演变

另外，设置采矿的**难易度级别**（Difficulty），这样做是为了防止由于哈希能力提高而使得挖掘变得非常迅速，或者由于哈希能力变小导致挖掘速度变慢而设定的。PoW 中的难易度级别是指定一个包含随机数在内的区块头的很小的哈希值。由于值越小条件越苛刻，计算哈希值需要花费的时间越多。

以比特币为例，难易度级别被设定为挖矿每 10 分钟成功一次，并且每次成功生成的 2016 个区块都会自动进行调整。同时，由于难易度级别基本上是根据哈希能力进行调整的，因此哈希能力和难易度级别的增加程度是非常相似的，如图 2.10 所示。

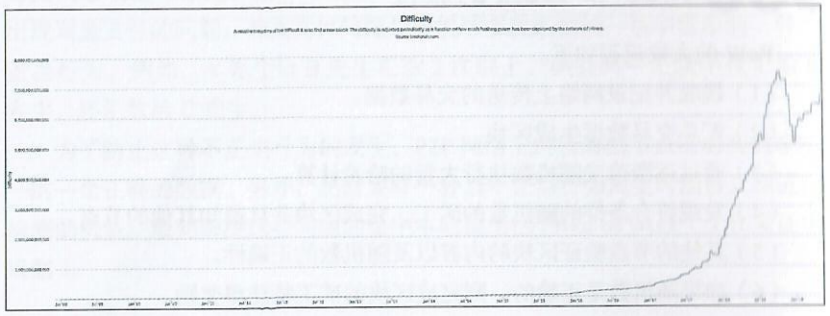

图 2.10　难易度级别（Difficulty）的演变

2.3.5 Proof of Work 的弱点

PoW 通过不确定数量的多台机器进行哈希计算以维持区块链整体的完整性，防止不正当行为的发生。但是这里存在两大弱点。

首先是过度用电。由于执行哈希计算的计算机需要运行大量的计算程序，由此会消耗大量的电力。一项研究报告显示，比特币区块链已经消耗了一个国家的电量。由此造成的环境破坏以及缺电地区电力供应难等问题也凸显出来。考虑使更多的人能够利用的同时，维持能源可持续化发展成为一个很大的课题。

其次是哈希能力的寡头垄断问题。哈希能力是指网络上整体的计算能力。但是，由于专用于哈希计算的芯片 ASIC 的诞生以及采矿场的兴起，出现了大量的计算资源集中在一部分矿工上的现象。对于分布式的公有链来说，并不希望将计算能力集中在一部分的矿工那里。另外，由此引发的 51% 攻击等攻击在理论上成为可能，人们不得不担心这可能会动摇对区块链的信任度。

说明

51% 攻击

怀有恶意的个人或者组织，通过控制网络整体的 51% 的计算能力，从而进行拒绝正当的交易等网络攻击的行为，目前还没有有效的解决方案。

2.3.6 其他的共识算法

PoW 解决了 P2P 网络上的问题，但同时引发了电力的过度使用以及哈希能力的寡头垄断问题。为了克服这些弱点而开发出了各种各样的共识算法。每种算法都有各自的优点和缺点，没有哪种是完美无缺的，但是都有一个共同的目标，即维持区块链的完整性，见表 2.1 所示。

表 2.1　其他的共识算法

	PoS	DPoS	PoI	XRP LCP
概要	根据代币数量的变化，PoW 的成功概率也随之发生变化	根据节点投票决定批准哪个节点	根据代币数量和交易量进行评价	通过指定的组织进行批准
优点	低成本	低成本、高速	确保流动性	批准的高速化
缺点	流动性低、持有代币量大者有利	可能造成集中化管理	需要持有一定量的代币	可能造成集中化管理
例	ADA	EOS	NEM	Ripple

本章习题

问题一

请选择一个正确描述关于区块链中密码技术的选项。

（1）在公开密钥加密方式中，使用被称为公开密钥的密钥来执行加密和解密。

（2）无论输入值是否发生变化，哈希函数都不会改变输出值的长度。

（3）采矿时需要使用电子签名。

问题二

请选择一个正确描述关于区块链中 P2P 技术的选项。

（1）网络上分布着包含交易数据的各种各样的数据。
（2）参与比特币的网络的所有节点都是全节点。
（3）网络上的数据始终通过特定节点进行分发。

问题三

请选择一个关于 PoW 的错误的描述。

（1）在 PoW 中，成功进行采矿的矿工将获得采矿奖励。
（2）在 PoW 中，采矿成功率根据所拥有的代币数量而变化。
（3）在 PoW 中，不确定多数的矿工努力寻找满足条件的随机数。

问题四

请选择一个正确描述在 EOS 中使用共识算法的选项。

（1）PoW
（2）PoS
（3）DPoS

问题五

请选择一个正确定义参与 P2P 网络的各个计算机的术语。

（1）客户机
（2）节点
（3）服务器

第

2

篇

Python 的基本原理

在本书中，我们将使用 Python 来运行程序。在正式学习区块链的内容之前，我们先来学习一下 Python 语言。