第 1 篇

区块链概要及构成技术

区块链技术是由各种技术结合而成的。首先让我们来认识一下区块链技术的概要及其技术的构成。

第 1 章　区块链概要及学习意义
第 2 章　区块链的构成技术

第1章 区块链概要及学习意义

自从区块链概念出现以来，随着各种技术上的改进，很多行业及领域都开始探讨区块链的应用。这里让我们针对区块链的概要逐一进行学习理解。

1.1 分布式系统及区块链

区块链并不是突然产生的技术。对于这一点只要看一下分布式系统的特点及其发展历史就会明白了。

1.1.1 集中式系统和分布式系统

软件系统的构造（架构）总体上分为**集中式系统**和**分布式系统**两类，如图1.1所示。集中式系统是有一个中心，其他的计算机通过连接这一中心的形式而组成，分布式系统是通过多台计算机互相连接而组成的。根据系统的不同，也有分布式系统和集中式系统共同组合而成的情况，根据各种状况的不同选用合适的系统构造。

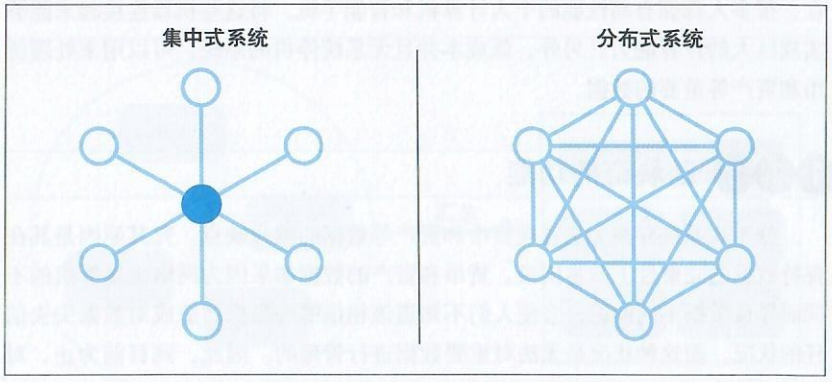

图1.1 集中式系统和分布式系统

集中式系统和分布式系统的优缺点见表1.1。通过比较，可以看出这两个系统构造有着正好相反的特点

表1.1 集中式系统和分布式系统的优缺点

	集中式系统	分布式系统
优点	• 灵活对应设计式样的变化 • 快速处理的能力 • 简化设计	• 降低成本 • 不易发生系统故障 • 高度的计算能力

（续表）

	集中式系统	分布式系统
缺点	• 存在单点故障的问题 • 信息收集集中，存在信息安全问题 • 维护管理的技术要求和成本高	• 必须拥有网络 • 协作及通信的成本高 • 程序复杂

在集中式系统中，有着被称为单点故障的问题，即作为中心的计算机不能运行的话，系统整体就会停止（**系统停机**），并且存在维护管理需要消耗高成本的缺点，但是又具有比较容易维护系统的灵活性、一致性的优点。最重要的是在系统中易于维护数据的完整性。数据的完整性是指数据不存在缺失、错误的特性，这是在系统中拥有可信数据的前提条件。

在分布式系统中，由于系统中的处理任务是由多台计算机共同分担，可以降低成本；又由于不存在单点故障的问题，可以大大降低系统停机发生的可能性。同时，计算能力也能够得到很大的提高。随着计算机整体的计算能力提高的同时，可以通过增加连接的计算机数量，不断地提高系统的计算能力。现在，很多人都拥有高性能的个人计算机和智能手机，将这些机器连接起来能够实现巨大的计算能力。另外，低成本并且无系统停机的系统，可以用来处理货币和资产等重要的数据。

1.1.2 区块链的功能

分布式系统存在无法管理货币和资产等数据的致命缺点。究其原因是其在保持数据的完整性上非常困难。货币和资产的数据如果因为网络上计算机的不同而导致数据不同的话，会使人们不知道该相信哪些数据，造成对数据失去信任的状况，而这种状况是无法对重要数据进行管理的。因此，到目前为止，对于货币和资产等重要数据的管理都是采用易于维护数据完整性的集中式系统管理。

正如前面所述，集中式系统中信息是集中在一起进行管理的，存在单点故障这样的弱点。尽管信息的集中管理是集中式系统管理的优点，但是为了系统的维护管理所必需的技术难度以及成本也是不断提高的，由于信息管理的集中化而造成的信息安全问题也因此凸显出来。

所以，在信息安全问题较少，成本低，计算能力强的分布式系统中，如果能拥有像集中式系统那样的便利性，就能使用两者的优点。由此诞生了区块链技术。区块链技术，可以被认为是具有诸多优点的分布式系统，同时，又像集中式系统那样作为维护数据完整性的技术而开发出来的。从这个意义上看，它是进一步扩展分布式系统可用性的技术，并且因为打开了一扇新技术的大门而受到热切的关注。

1.2 区块链的构造

区块链是将称为区块的数据以串珠的形式连接起来，通过区块的摘要数据将下一个区块接收进来的方式取得数据的完整性。

1.2.1 区块以及链的构造

收集多个交易数据并将其整合在一起，组合成为一个区块进行管理。此时，区块中同时存放了相互关联的多个数据。这些数据称作区块头，如图 1.2 所示区块头是在同一个区块中存储交易数据的摘要数据以及时间戳等标签数据。

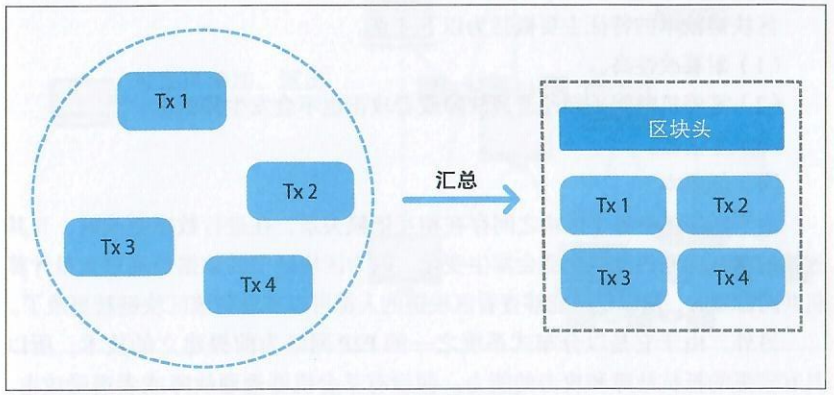

图 1.2 区块生成示意图（Tx 为交易数据）

将这个区块头中被摘要的数据，存储在下一个区块的区块头中后，就生成了从一个区块到前面一个区块的链接。通过这种对所有区块的链接操作，保证了区块链整体的一致性，如图 1.3 所示。

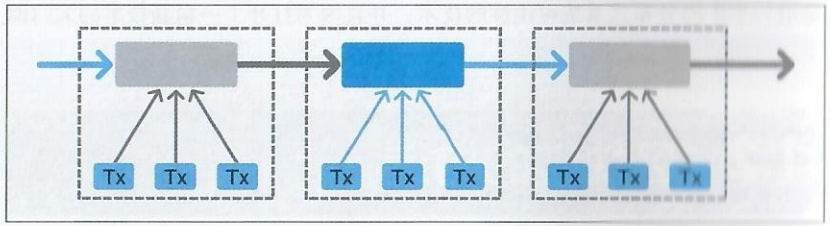

图 1.3　区块间链接

1.2.2 通过大量计算机共同管理

区块链并非通过特定服务器和计算机进行管理，而是通过大量的计算机进行分布式管理。因此，同一区块链数据是通过许多的计算机共同管理的。这种机制称为 P2P 技术，是区块链技术的重要特点之一。

1.2.3 区块链的特征

区块链技术的特征主要概括为以下 4 点。

（1）耐篡改性高。

（2）零停机时间（即使遭遇故障或者攻击也不会发生停机）。

（3）零信任。

（4）低成本。

由于区块链中各个区块之间存在相互依赖关系，在进行数据更改时，与其连接的相互关联的数据全部会发生变化。因为区块链中的数据是通过大量计算机共同管理的，所以任何能够查看区块链的人都可以查看到该区块链被更改了。

另外，由于它是以分布式系统之一的 P2P 网络为前提建立的技术，所以具有较强的抵抗故障和攻击的能力。假设有某台机器遭遇故障或者遭受攻击，通过访问周围其他的节点仍然能够恢复原本的数据，并能够获得未发生故障时的服务。

零信任是指不论利用何种系统来提高服务能力，其需要的信任风险较低。正是由于区块链有高耐篡改性的特点，即使对特定的节点没有信任却仍然可以利用系统的服务。

低成本是区块链的一大特征。以往的系统中要实现具有区块链同等程度的信息安全性，需要花费巨大的成本。另外，由于区块链在任何国家和任何地区都可以利用，使得在以往需要花费大量成本的领域，如国际汇款，其成本也大大地降低了。

1.3 区块链的类型

简单来说，区块链可以分为三种类型。由于它们各自具有不同的特点，可以根据不同的情况来区分利用。

1.3.1 公有链

公有链是指以比特币这样的虚拟货币为代表的区块链，是任何人都可以参与并且连接成网络的区块链，如图 1.4 所示。

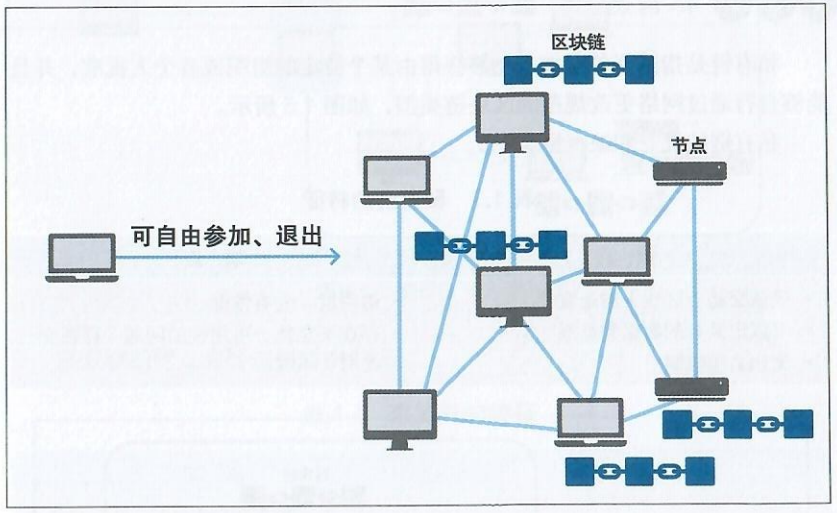

图 1.4　公有链示意图

公有链的优点和缺点见表 1.2。

表 1.2　公有链的特征

优　点	缺　点
• 无须管理员（不集中权限） • 高透明度、高公有性 • 依据合法的规则运营（变更规则必须遵守合法性）	• 交易确认速度慢 • 数据容量的问题 • 无法提供最终确定性 • 无法取消 • 不健全的法制法规

由于公有链允许任何人都可以自由地加入网络，在不集中权限管理的情况下，实现了公正公平的环境。同时，由于系统是在大众的监督环境下运营的，因此能够具有高透明度和共享性。在此基础上，任何的规范变更或者交易确认等都将在合法的规则下实施。

另外，公有链也被指出具有诸如交易确认需要耗费时间，以及区块链整体数据的容量不断增加等缺点。再者，无法提供最终确定性也可以看作公有链所特有的问题。所谓最终确定性是指结算完成性，即指结算一旦确定就不能被推翻的性质。在公有链中，当有足够的区块链接的情况下，可以大大降低结算被推翻的可能性，这种时候可以看作交易具有极高的被确定的概率。以比特币的情况来说，如果有 6 个区块链接，大概率上能够获得交易的最终确定性。

1.3.2 私有链

私有链是指网络的参加者能够获得由某个特定的组织或者个人批准，并且能够自行通过网络更改规范的区块链类型，如图 1.5 所示。

私有链的优点和缺点见表 1.3。

表 1.3　私有链的特征

优　点	缺　点
• 确认交易（区块）的速度快 • 可限定共有的数据和范围 • 无须奖励机制	• 透明度、公有性低 • 存在安全性、可用性的问题（存在交易对手风险）

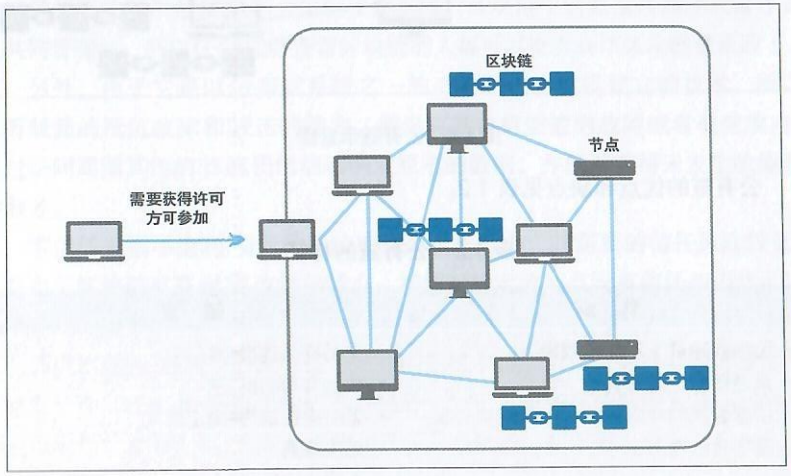

图 1.5　私有链示意图

1.3.3 联盟链

联盟链是指网络的参加者能够获得由无数个组织或者个人批准，并且通过与有限的主体建立共识的方式更改规范的区块链的类型。联盟链是介于公有链和私有链之间的一种区块链类型，如图 1.6 所示。

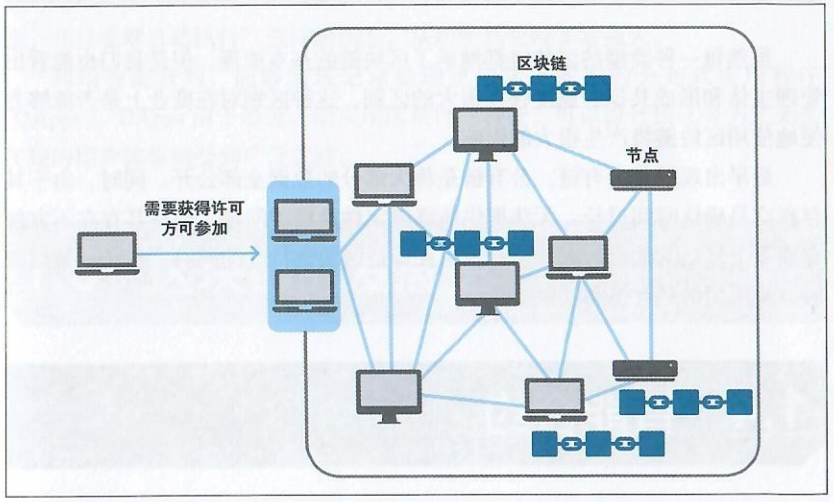

图 1.6　联盟链示意图

联盟链的优点和缺点如表 1.4 所示。

表 1.4　联盟链的特征

优　点	缺　点
• 确认交易（区块）的速度比较快 • 可限定信息的公有内容和范围 • 无需激励机制 • 抑制独断专行	• 透明度和公有性较低 • 存在安全性、可用性的问题（存在交易对手风险）

1.3.4 区块链的应用方式

比较公有链，私有链和联盟链，总结得出各种类型区块链的特点，如图 1.5 所示。

表 1.5　各种区块链的比较

链的类型	公有链	联盟链	私有链
管理主体	无	无数个	单个
确认速度	慢	快	快
透明性、公有性	高	比较低	低

虽然每一种类型的区块链都继承了区块链的基本原理，但是我们也能看出管理主体和形成共识的速度存在很大的区别，这种区别对在商业上是否能够方便地使用区块链将产生很大的影响。

最早出现的是公有链，公有链是将大部分的数据全部公开。同时，由于其存在交易确认时间过长，无法提供最终确定性这样的问题，使得其存在不方便在商业上使用的缺点。因此，开发了在保持区块链特性的同时，在商业领域能够方便应用的私有链和联盟链。

1.4　智能合约

区块链技术具有一些独特的性质，平台型区块链和智能合约都是为了使这些特性能够更广泛地应用而开发的。

1.4.1　区块链 2.0 和平台型区块链

区块链最初是作为实现虚拟货币的技术而诞生的。但是，在虚拟货币之外的领域也萌生了利用区块链的想法，而进行了各种各样的研究开发，这被称为区块链 2.0。

平台型区块链的典型例子包括 Ethereum（以太坊）、EOS（巴比特）等。在这些区块链上可以进行编程，可以描述和执行比虚拟货币汇款难度更大的处理。

2013 年，以太坊的开发者之一的维塔利克·布特林（Vitalik Buterin），在他 19 岁时就开发出以太坊的原型，目前这一技术也正处于蓬勃发展的态势。他在谈到关于以太坊的创意时说："如果说比特币是计算器的话，那么以太坊就是智能手机。"以太坊就是一个通过支持编程语言，使任何人都可以自由地发挥想象力来构建程序、可以简单方便地使用的平台。其关键的技术就是智能合约。

1.4.2　智能合约及分布式应用程序

智能合约是指针对合约的当事人之间交换的共识内容，当满足条件时，即使当事人不在场仍然能够自动执行的一种机制。智能合约概念是 1997 年由美国的法学家、密码学家尼克·萨博（Nick Szabo）提出的，在区块链诞生之前就已经存在了。区块链上的智能合约，由于具有"被记录的合同内容不易被篡改，并且能够自动执行"这样的优点，从而使其变得非常强大。

利用智能合约，能够实现记录处理更加复杂内容的分布式应用程序（DApps）。DApps 由于通过灵活应用区块链的特征，可以设计出迄今为止无法实现的用户体验而受到广泛关注。

1.5　区块链的发展史

截至 2019 年 9 月，诞生了多种多样的区块链以及周边技术，回顾历史我们可以追溯到比特币的区块链。

1.5.1　区块链初期

20 世纪 90 年代前期～21 世纪前期，电子商务被视作一种商业模式，之后出现了被称为互联网泡沫的风潮。由于 IT 在商业上存在巨大的潜力，所以吸引了大量的投资。

在这种情况下，电子货币的开发也开始盛行起来。1996 年，索尼开发了被称为 FeliCa 的 IC 芯片，出现了使用各种各样非接触式 IC 卡的电子货币。

各种信用卡公司也开始致力于在线支付等方面的应用，电子支付的普及逐渐得到了推广。但是，从无论哪一种方式都是需要从特定企业做担保的角度上来看的，它们仍然是集中化管理的组织结构，即集中式系统。

随着时间的推移，P2P 技术的开发也变得兴盛起来，并且开始开发以 Winny 为代表的 P2P 应用程序。但是，由于时常出现诸如违反版权的数据共享，以及由于病毒传播而无法清除病毒等事件的报道，P2P 技术必须解决的问题也由此凸显出来。

乘着电子商务普及的东风，电子支付开始得到普及，集中化管理的问题也逐渐被重视起来，P2P 技术也随之受到关注。然而，除非解决 P2P 技术的问题，否则无法将其应用于电子支付。各种各样的研究人员和技术人员都尝试解

决这些问题，但是仍然没有取得所需的成果。在这种状况下，打开突破口的不是别的，正是区块链技术。

1.5.2 中本聪的论文发表

区块链的原型创意是由一个名叫中本聪（Satoshi Nakamoto）的神秘人物于 2008 年 10 月在密码学邮件组列表中以共享的形式突然公开出来的。最初很多人质疑论文的内容，但是有一部分感受到该技术可行性的研究人员和技术人员开始和中本聪进行探讨，于 2009 年 1 月产生了人类历史上第一个区块。顺便说一下，区块链最初产生的区块被称为创世区块。比特币的创世区块存储了以下数据。

- 泰晤士报　2009年1月3日　“英国财政大臣正在研究第二次救助银行”
  The Times 03/Jan/2009 Chancellor on brink of second bailout for banks

由于任何人都可以看到包括比特币在内的公有链上的区块，因此创世区块及上面的数据均可以被确认，如图 1.7 所示。

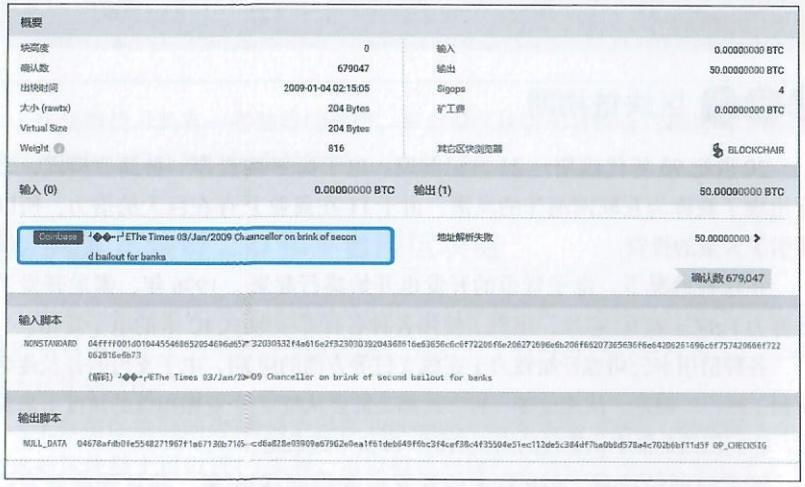

图 1.7　创世区块的内容

URL https://btc.com/4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b

在比特币的创世区块中记录这些数据有多种可能的原因，但是可以认为这是包含了对传统金融系统的批评及讽刺。人们认为，比特币的机制解决了针对因为集中化管理而导致的金融系统所投入的税收的失败这样的问题。

之后，在 2010 年 5 月 22 日，比特币的首次使用，是用 1 万 BTC（每单位比特币表示 1BTC）交换了 2 张比萨饼。就这样，比特币逐步普及起来。

1.5.3 阿尔特币的剧增

在比特币知名度逐渐提高的过程中，以比特币的区块链为基础，进一步开发出有所改进并且增加了其他附加功能的新的区块链。由此诞生了比特币之外的被称为“阿尔特币”（Altcoin）的虚拟货币。

最初的阿尔特币被称为 Namecoin（域名币）。比特币本身也分化为各种各样的阿尔特币，2017 年诞生了比特币现金、比特币金币、超级比特币等很多种类。此外，在 2018 年比特币现金分化为比特币 ABC 和比特币 SV。就这样，以比特币的区块链为起点，阿尔特币快速发展起来。

另外，随着阿尔特币的迅速增加，出现了众多的矿工。连接区块的过程称为采矿，而采矿的主体称为矿工。特别是，在采用 Proof of Work（PoW）采矿方式的区块链中，矿工所拥有的机器的运算能力是非常重要的。因此，开发了用于采矿的专用的 ASIC 芯片，加速了采矿的竞争。

1.5.4 平台型区块链的诞生

由于受比特币及其他阿尔特币激增的影响，人们开始探寻区块链的虚拟货币之外的应用方法。2015 年出现了 Ethereum（以太坊），次年发行了 Lisk。由于平台型区块链的大量发布，由此开发出各种各样的 DApps，加快了阿尔特（ALT）币的开发。

同样，在差不多同一时期，ICO（Initial Coin Offering）也盛行起来。ICO 是一种通过首次发行虚拟货币，然后向投资者出售，以此来筹措资金的方法。

由于在此之前的阿尔特币的激增，加上平台型区块链，使得 DApps 和 Token（代币）更加容易开发，从而使这种新的资金筹措的方式备受瞩目。2017 年 ICO 向全世界筹措了 8000 亿日元。这有助于将大量的资金注入区块链的开发。

1.5.5 私有（联盟）链的诞生

正如前文所述，为了弥补公有链的缺点，开发了私有链和联盟链。之后又陆续发布了由 Linux Foundation（Linux 基金会）主导开发的 Hyperledger、由 R3 开发的 Corda 以及由 Tech Bureau 公司开发的 mijin 等，并且出现了在商业领域也使用方便的区块链平台。

1.5.6 区块链及周边技术的多元化

到 2019 年，从基于比特币的区块链的阿尔特币开始，经历了平台型区块链、私有链以及联盟链的发布，出现了多种多样的区块链。今后将以更加快速、更具可扩展性的区块链为目标，开发出各种各样的技术。

1.6 增加的用例

截至 2019 年，为了灵活应用区块链，各种各样的项目正在进行中。为了理解区块链的应用性，下面看几个具有代表性的例子。

1.6.1 提高可追溯性

为了有效利用区块链的抗篡改性和透明度，由此产生了提高可追溯性（追踪的可能性）的项目。如食品、化工燃料、医药品等从生产到最终到达消费者的整个过程（供应链）中，能够检查是否存在不正当行为的系统。随着现代供应链的全球化的发展，在难以对所有的情况进行追踪的状况下，我们期待能够出现打破这种现状的方法。

1.6.2 分布式游戏

由于平台型区块链的诞生，出现了大量的 DApps 游戏。和传统的游戏最大的区别在于，DApps 在游戏的世界观里建立一个经济区，可以在公平透明的环境下买卖所培养的角色和获得的道具。另外，可以有少量的收费，同时期待收费方式能有更大的变化。

1.6.3 参数保险

保险是支付规定的保险费，当生病或发生事故等纠纷时获得保险赔付的一种机制，但是过去很难考虑到生活习惯以及家庭环境的影响，这样就会导致有一种不公平的感觉，因为不论生活习惯和家庭环境如何，保险费都是一样的。通过利用区块链，可以根据个人状况的不同，灵活地设定保险费，赔付也比以往任何时候更加迅捷。

1.6.4 分布式 SNS

截至 2019 年，存在各种各样的 SNS，也正在开发利用区块链的 SNS。为了使用 SNS，必须注册个人信息，但是这些数据的管理和安全性经常受到质疑。如果利用区块链，就能够提高个人信息管理方面的安全性。例如，可以在投稿和点赞等行为上设定一定的报酬，由于有奖励机制，从而可以创建更加活跃的社区。

1.6.5 与 IoT 的结合

虽然 IoT（物联网）已经开始普及，但是通过和区块链的结合，可以进一步激发出 IoT 的潜力。通过利用智能合约，当接收到来自 IoT 端的信号时，可以自动执行特定的处理，这样不需要人工干预就可以操作机器设备。另外，由于可以支付比法定货币还要细小的金额（例如像 0.01 日元这样的金额），预计会对很多商业模式产生影响。

1.7 学习区块链的意义

前面我们介绍了区块链的概要和历史，在开发基于智能合约的 DApps 时，即使不理解区块链的详细技术也能够进行开发。但是，在开发网络应用程序时，如同不理解网络以及服务器等基础设施的概念就无法进行设计和系统维护一样，在开发利用区块链的应用程序时，在理解区块链技术实质的前提下开发是非常重要的。正如我们可以追溯历史一样，区块链技术可以追溯源头至比特币区块链。本书以比特币的区块链为中心，来加深对区块链的理解。

本章习题

问题一

请选择一个有关区块链结构的不正确的描述。

（1）区块链是区块之间以连锁的形式链接而成的。
（2）在区块链的区块中，包含区块头。

（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。