第1章 以太坊和智能合约

区块链是近十几年才逐步发展起来的一个新概念，也是一系列技术的总称。从比特币到以太坊和智能合约，以及超级账本联盟链和 Web3 新潮流，区块链技术正以飞速发展之势开启去中心化理念的实践落地。

以太坊被广泛称为区块链 2.0 的代表，它在区块链技术的基础上引入了智能合约的概念和功能，从而使区块链不仅是一种去中心化的分布式账本，还能够执行和管理复杂的逻辑和业务。特别是依托于智能合约为核心的各种去中心化应用，丰富了区块链技术的应用场景。本章内容将从区块链的起源开始，介绍区块链技术的由来。然后引出区块链 2.0 时代的代表——以太坊，介绍以太坊的核心功能，分析以太坊的架构和运行原理。

1.1 区块链简介及分类

1.1.1 区块链发展起源

近年来，区块链技术开始走进大众的视野，越来越多的人加入学习、实践、应用区块链技术的队伍中。

区块链技术的历史，最早可以追溯到 20 世纪七八十年代。

1976 年，迪菲(Diffie)和赫尔曼(Hellman)在《密码学的新方向》一文中提出了公钥密码(public-key cryptography)的思想，从而开创了现代密码学的新领域。

1982 年，密码学家和计算机科学家大卫·乔姆(David Chaum)发表了一篇论文《用于不可追踪的支付系统的盲签名》(*Blind Signatures for Untraceable Payments*)，提出利用新的密码协议构建一个具备匿名性、不可追踪的电子货币系统的设想。

20 世纪 90 年代，一些技术极客开始思考如何用技术手段保护用户在互联网上的隐私问题。为此，技术极客还成立了密码朋克组织，数学家埃里克·休斯(Eric Hughes)发表了《密码朋克宣言》，其中提到隐私权是一个社会在数字时代维持其开放性的必要条件。休斯最后写道："密码朋克以开发匿名系统为使命，我们用密码学、匿名邮件转发系统、数字签名和电子货币来保护自己的隐私。"

在之后的实践探索中，又相继出现了 eCash、B-money 等以密码学和分布式账本为技术依托的项目，但因为其时代和技术的局限性，这些尝试均以失败告终。虽然一直没有成功，但我们却积累了很多宝贵经验，也逐渐有了探索方向。

1.1.2 从 0 到 1 的比特币系统

2008 年 10 月 31 日，在 P2P(peer to peer，点对点)基金会网站上，一个名为中本聪的账

号在一封邮件中首次提到了比特币，并附上了一篇关于比特币的文章，这篇文章就是大家所熟知的比特币白皮书。白皮书题目为《比特币：一种点对点的电子现金系统》(*Bitcoin：A Peer-to-Peer Electronic Cash System*)，中本聪在白皮书中详细介绍了比特币的功能和实现原理。

简单地说，中本聪提出的比特币系统是一个去中心化的网络系统，利用该系统可以实现从一个客户端到另一个客户端的直接转账，而不需要经过其他任何中间机构。正是这一特点，使其区别于以往传统的中心化系统，也由此拉开了区块链时代的序幕。

比特币系统作为一个去中心化系统，通过在每个节点上保存相同的数据备份来实现数据的去中心化存储。数据存储的单位称为区块，即将数据打包成一个数据块结构，并将生成的这些数据区块按照一定的逻辑顺序进行存储，如图 1.1 所示。

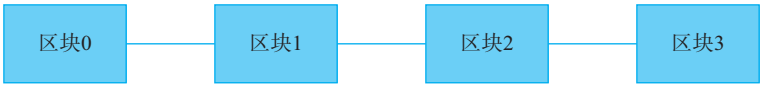
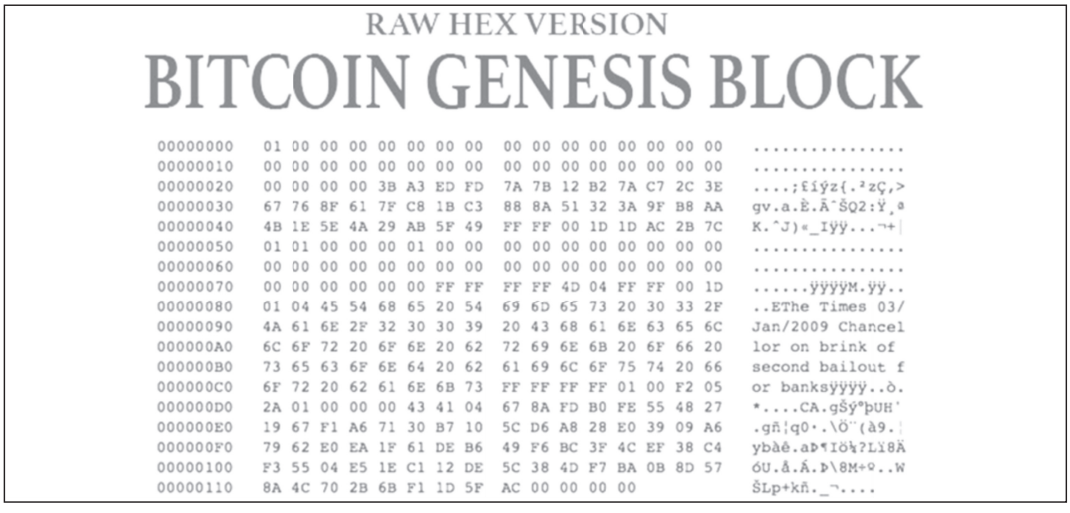


图 1.1　区块存储结构

2009 年 1 月 3 日，比特币系统开始运行，产生了比特币系统第一个区块，称为创世区块，创世区块数据如图 1.2 所示。


RAW HEX VERSION

BITCOIN GENESIS BLOCK

```
00000000   01 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00   ................
00000010   00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00   ................
00000020   00 00 00 00 3B A3 ED FD   7A 7B 12 B2 7A C7 2C 3E   ....;£íýz{.²zÇ,>
00000030   67 76 8F 61 7F C8 1B C3   88 8A 51 32 3A 9F B8 AA   gv.a.È.Ã^ŠQ2:Ÿ¸ª
00000040   4B 1E 5E 4A 29 AB 5F 49   FF FF 00 1D 1D AC 2B 7C   K.^J)«_Iÿÿ...¬+|
00000050   01 01 00 00 00 01 00 00   00 00 00 00 00 00 00 00   ................
00000060   00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00   ................
00000070   00 00 00 00 00 00 FF FF   FF FF 4D 04 FF FF 00 1D   ......ÿÿÿÿM.ÿÿ..
00000080   01 04 45 54 68 65 20 54   69 6D 65 73 20 30 33 2F   ..EThe Times 03/
00000090   4A 61 6E 2F 32 30 30 39   20 43 68 61 6E 63 65 6C   Jan/2009 Chancel
000000A0   6C 6F 72 20 6F 6E 20 62   72 69 6E 6B 20 6F 66 20   lor on brink of
000000B0   73 65 63 6F 6E 64 20 62   61 69 6C 6F 75 74 20 66   second bailout f
000000C0   6F 72 20 62 61 6E 6B 73   FF FF FF FF 01 00 F2 05   or banksÿÿÿÿ..ò.
000000D0   2A 01 00 00 00 43 41 04   67 8A FD B0 FE 55 48 27   *....CA.gŠý°þUH'
000000E0   19 67 F1 A6 71 30 B7 10   5C D6 A8 28 E0 39 09 A6   .gñ¦q0·.\Ö¨(à9.¦
000000F0   79 62 E0 EA 1F 61 DE B6   49 F6 BC 3F 4C EF 38 C4   ybàê.aÞ¶Iö¼?Lï8Ä
00000100   F3 55 04 E5 1E C1 12 DE   5C 38 4D F7 BA 0B 8D 57   óU.å.Á.Þ\8M÷º..W
00000110   8A 4C 70 2B 6B F1 1D 5F   AC 00 00 00 00           ŠLp+kñ._¬....
```

图 1.2　比特币创世区块数据

本质上，在比特币的实践中，中本聪解决了以下几个问题。

(1) 在现实世界中，大到港口贸易，小到街边商店，每天都会有无数的交易发生。根据交易场景可以将交易分为线下和线上两种。线下场景对应的是现金交易，交易双方完成现金和商品的互换。线上交易则有很大的不同，信息技术的一大特点就是电子信息可以被复制，且可以被无限复制，几乎不需要成本。因此，线上交易最大的问题是如何防止一次支付的金额被使用两次甚至多次，这类问题称为“双重支付”问题。传统的解决方案是引入保持中立的第三方机构作为结算中心，以防止出现“双重支付”问题。但第三方机构的加入增加了交易成本，使得本来可以双方同意即可发生的交易却需要等待第三方的确认，无形中降低

了效率。另外，从理论上并不能确保第三方的绝对中立，由此可能产生仲裁争议等问题。相反，比特币作为一个去中心化的点对点电子现金支付系统，从技术上实现了不需要依赖任何第三方金融机构，即像线下场景一样，允许交易双方直接达成交易，这与传统的通过第三方金融系统进行结算的线上交易形式有本质区别。

(2) 比特币系统是一个开放的匿名系统。系统中不会出现用户真正的个人信息；同时在该系统中交易的数据是完全公开的，任何用户均可以浏览和验证。

(3) 将系统产生的数据通过分布式的方式记录在多个节点中，数据一旦被记录则无法修改，避免了传统第三方机构结算中可能产生的仲裁争议问题。

系统地学习区块链知识，必然无法绕开比特币系统。比特币系统作为第一个成功实践并持续运行至今的去中心化系统，其重要性已经成为所有区块链技术探索和实践者的一致共识。

1.1.3　从比特币到区块链

当比特币被越来越多的人了解后，逐渐从其系统功能延伸到总结支撑其系统运行的技术。这些技术共同支撑起该去中心化系统的运行。

(1) 公钥密码学技术：公钥密码学又称非对称密码学，以密钥对生成和数字签名技术为代表，保证了比特币系统中最核心的交易逻辑的运行。

(2) 点对点(P2P)传输技术：P2P 传输技术可以简单理解为去中心化，用户不需要中心服务器即可完成信息的传输。比特币系统不需要依赖任何第三方机构运行，系统交易数据通过 P2P 技术保存在多个系统节点中。

(3) 哈希现金技术：该技术主要基于哈希算法，其特点是给定任意的输入内容，都可计算得到固定长度的唯一输出内容。

(4) 区块存储和链式结构：数据以区块结构进行存储，并通过特定的逻辑将数据区块进行组装，形如链式结构。

至此，在总结和摸索中，人们将可以支撑去中心化系统网络运行的相关技术统称为区块链技术，将符合这种特点的网络系统称为区块链。

1.1.4　区块链简介

简单来说，区块链是分布式数据存储、点对点传输、共识机制、加密算法等计算机技术的一种新型的综合应用模式，区块链系统本质上是一个分布式的去中心化的账本数据库。在该系统中，数据存储在参与系统的诸多节点上，且多个节点之间具有完全相同的结构与内容。

在实现形式上，区块链采用“块-链”式结构，将网络中产生的数据存储在区块结构中。区块结构通常由区块头和区块体组成。区块头中父区块哈希值、版本、时间戳、难度、随机数等数据信息；区块体中通常存放某一时段内系统中发生交易的详细数据，以便供用户查询和验证。照此逻辑，生成的新区块中总是包含有当前最新区块的哈希值数据，并通过这种逻辑关系来确定新旧区块的序列顺序。随着时间的推移，便形成一条以区块为单位的链式结构，“块-链”式结构示意图如图 1.3 所示。

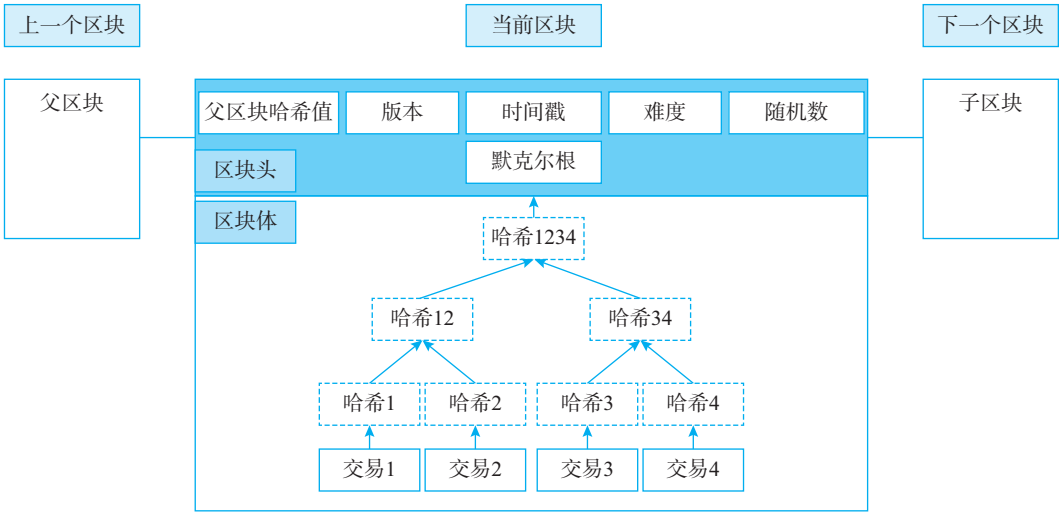


图 1.3 “块-链”式结构示意图

在运行机制上，去中心化系统中的各个节点之间是“地位平等”的关系，不能指定某个节点生成新区块，否则被指定的节点就存在作恶的可能。解决方案是引入共识机制，多个节点遵守同一套生成新区块的规则，根据各节点运行规则程序的执行结果来确定生成新区块的节点。随着学习的深入，读者可以学习到区块链中很多常见的共识机制算法，比如工作量证明机制(proof of work，PoW)、权益证明机制(proof of stake，PoS)、委托权益证明机制(delegated proof of stake，DPoS)、实用拜占庭容错机制(practical byzantine fault tolerance，PBFT)等。

在结果上，这种新型的应用模式可以使去中心化系统中的参与者之间实现互相信任，从而达到点对点之间可直接进行数据传输的效果。

1.1.5 区块链分类

通常按照开放程度的不同，将区块链系统分为公有链、私有链和联盟链三种类型。

(1) 公有链：公有链是与前文已经介绍过的比特币系统一样的区块链系统，其特征是一个去中心化的分布式账本，且该账本对任何人都是开放的，任何人和组织都可以参与账本数据的维护和读取等操作。除比特币外，本书即将学习的以太坊平台也是具有代表性的公有链之一。在实际的讨论中，有的人将公有链理解为公共数据库，数据由参与者共同记录，同时保持公平、公正、公开的原则和数据不可篡改的特点，这与分布式账本的理解本质是相同的。

(2) 私有链：私有链是与公有链相反的一种类型，通常是仅限于某个组织或者机构内部搭建使用的一条私有区块链网络。一方面，私有链在开放程度上是最低的，仅限于某个小范围内部使用，因此其去中心化程度最弱。另一方面，私有链因为其去中心化程度很低，节点数量往往可控，因此整个系统的数据处理效率相较于公有链而言会提高很多。

(3) 联盟链：除上述两种类型外，还有一种联盟链系统，是介于公有链和私有链之间的一种类型。联盟链主要面向某个特定的领域或者行业，其目标宗旨是利用区块链技术解决

某个特定行业的问题，提高行业运行效率。联盟链通常是由同领域内的众多企业牵头组建而成，网络节点分布在各个企业之间，整个网络账本数据由参与该网络的众多企业共同维护和管理。在开放程度上，联盟链是有准入机制的，即只有经过认证并获得准入身份和资格的企业才能以参与方的形式加入系统，成为其中一员。在具体应用上，联盟链有很多种，比如面向供应链领域的联盟链、面向农业溯源领域的联盟链、面向金融领域的联盟链等。其参与者可以是企业、机构、组织，甚至是国家。由于联盟链的目标通常是解决具体行业和领域的问题，提高生产效率，故对整个系统的处理能力有一定的要求，在实践中通常会以指定节点记账的方式运行，且记账节点数量通常是固定的。

综上所述，公有链、私有链和联盟链在开放程度上是逐渐降低的。系统的开放程度与系统的数据处理效率呈负相关，即公有链开放程度最高，但其处理速度最慢，效率最低；私有链和联盟链随开放程度的减弱，其运行速度和处理效率逐渐提高。在具体的应用实践中，每一种区块链类型都有其作用和适用场景，需根据具体情况进行分析和选择。

1.2　以太坊基础

1.2.1　以太坊简介

同比特币一样，以太坊也是一个公有链系统，任何人和组织均可自由加入和使用该系统。与比特币不同的是，以太坊是一个可以运行智能合约程序的区块链平台。

目前我们在对区块链技术进行定义时，通常把 2013 年之前以比特币系统为代表的阶段称为区块链 1.0 阶段；从以太坊提出智能合约开始，称为区块链 2.0 阶段。

1.2.2　以太坊发展历史

2013 年 11 月，以太坊最重要的创始人 Vitalik Buterin（以下简称 Vitalik）首次发布了以太坊白皮书，介绍了关于比特币及区块链技术拓展延伸的思考，并首次提出了以太坊的概念。在 Vitalik 完成初始工作的基础上，其他智囊团以不同的身份陆续加入进来，包括 Gavin Wood、Charles Hoskinson、Amir Chetrit、Anthony Di Iorio、Jeffrey Wilcke、Joseph Lubin 和 Mihai Alisie 等人，他们均称为以太坊项目的联合创始人。

2014 年 4 月 1 日，Gavin Wood 发布了以太坊黄皮书，在该篇文章中详细讲解了如何实现以太坊相关技术细节和相关技术协议的内容。

2014 年 7 月 22 日—9 月 2 日，以太坊项目进行了 40 余天的预售。在预售期内，投资者可按照固定的兑换比例，使用比特币兑换将来可在以太坊系统中流通使用的以太币。通过预售，共筹集到价值约 1800 万美元的比特币，这些资金被用来支撑完成以太坊项目的启动、开发测试等后续的工作。

经历了接近一年的开发和数次测试版本的发布，以太坊网络于 2015 年 7 月 30 日正式上线。虽然以太坊网络于 2015 年上线，但根据规划，整个以太坊网络的构建将会是一个持续数年的漫长过程。规划为以太坊在不同的阶段分别设定了要达成的目标，并为以太坊未来的发展设定了 Frontier、Homestead、Metropolis 和 Serenity 四个阶段。因此，以太坊网络正式启动只是整个网络持续构建的第一步。2015 年以太坊网络启动后，随即进入以太坊的

第一个阶段——Frontier 阶段。

2016 年 3 月 14 日，以太坊进入其发展构建过程中的第二个阶段——Homestead 阶段。该阶段与 Frontier 相比，并没有明显的技术迭代，只是表明以太坊网络已平稳运行，整体已趋于安全和可靠。

2017 年，以太坊进入其发展规划的第三个阶段——Metropolis 阶段。根据规划，Metropolis 阶段共包含两次升级，分别称为 Byzantium 升级和 Constantinople 升级。2017 年 10 月 16 日，以太坊网络成功实施 Byzantium 升级；2019 年 2 月 28 日，以太坊网络成功实施 Constantinople 升级，正式进入 Metropolis 阶段的第二部分。随后，以太坊网络又于同年 12 月 8 日实施 Istanbul 升级，于 2020 年 1 月 2 日实施 Muir Glacier 升级。

2022 年 9 月 15 日，以太坊网络顺利完成升级，此次升级标志着以太坊网络的共识机制正式由 PoW 机制转换为 PoS 机制。同时，也标志着以太坊网络正式进入其发展规划的第四个阶段——Serenity 阶段。Serenity 阶段也是规划中以太坊网络最终的阶段，随着以太坊的共识机制从 PoW 转为 PoS，以太坊网络正式进入 2.0 的全新阶段。

1.3 以太坊核心概念

1.3.1 以太坊

以太坊全称 Ethereum，是一个类似于比特币系统的去中心化区块链网络。该系统由分布在全球各地的节点彼此连接成一个网络。在该网络中，所有的节点都是平等的，都可以彼此连接并实现通信，没有任何一个绝对的中心可以管理或者控制该网络。任何对该网络感兴趣的用户，均可以自由地加入或者退出。参与网络的各节点均会自己维护一份数据账本，且该数据账本的内容与其他节点保持一致。同时，各个节点均可以根据需要向用户提供数据浏览和查询的服务。用户可以通过浏览器访问和查看以太坊网络的相关数据和整个网络的情况。

简单地说，以太坊类似于一台超级计算机，该计算机是由众多节点共同组成的，每个节点均独立维护一份数据，且节点之间彼此维护的数据保持一致。用户可以通过手机软件、计算机浏览器等方式使用该计算机。

1.3.2 以太币

以太币全称 Ether，简称 ETH，是可以在以太坊系统中使用的一种加密数字货币，用户可以像使用比特币一样使用以太币。用户通过互联网实现给其他用户转账以太币或从其他用户处接收以太币等操作，这些功能均由以太坊系统提供。当用户在使用以太坊系统，向别人发起转账交易时，需要网络中的其他参与者帮助记录交易数据，并验证交易的正确性。在此过程中，用户需要支付一定的以太币作为激励，才能接受交易验证的服务。

在以太坊网络中，帮助验证交易并记录交易的参与者称为验证者。验证者像是以太坊网络的记录管理员，这些管理员负责检查并证明没有人作弊，完成交易的验证和记录交易的工作后，作为回报，系统会奖励这些验证者一定数量的以太币。整个网络中的以太币就是这样源源不断地产生和流通。因此有大量的验证者为了得到以太币而主动参与到网络中。这

些验证者通过搭建节点参与到以太坊网络中获得以太币的过程，需要消耗大量的时间和工作，非常辛苦，因此这些验证者通常也被称为“矿工”。

1.3.3　Gas、Gas Price、Gas Fees

用户在使用以太坊网络时，会使用不同的功能，其所需要的系统资源也是不同的。为了能够衡量在以太坊网络上执行特定操作所需要的计算工作量，人们提出了 Gas 的概念。简单地说，Gas 是用来衡量以太坊网络中执行某项操作所需要的计算工作量的单位，类似于现实生活中以小时为单位来估算某项工作所需要的工作量。

前文已经介绍过，用户在使用以太坊网络的功能时，需要提供一定的以太币（ETH）作为服务报酬支付给网络验证者。而 Gas 是用来衡量用户的不同操作所需要的计算工作量的单位，因此就有了 Gas Price 的概念，也称为 Gas 价格。实际运行中，根据不同时刻以太坊网络的运行情况和使用情况，Gas 价格是动态变化的。Gas 价格类似于现实生活中的小时工资，工厂按小时工资计算员工薪酬，而根据不同的季节，不同的工作时段，小时工资是变动的。

Gas 价格使用以太币单位 Gwei 进行衡量。Gwei 和以太币最大单位 ETH 之间的换算关系是：1Gwei＝10^{-9}ETH，或者 1ETH＝10^{9}Gwei。

比如，某个时刻以太坊网络的 Gas 价格有较慢交易速度的 Gas 价格为 14.3Gwei；中等交易速度的 Gas 价格也是 14.3Gwei；较快交易速度的 Gas 价格为 53Gwei 三种水平。此处的较慢、中等、较快三种交易速度的描述，是指用户的操作被网络验证者接收和确认的时间。若用户希望自己的操作或者交易尽快地被确认，就需要付出较高的成本。以太坊网络的实时 Gas 价格如图 1.4 所示。

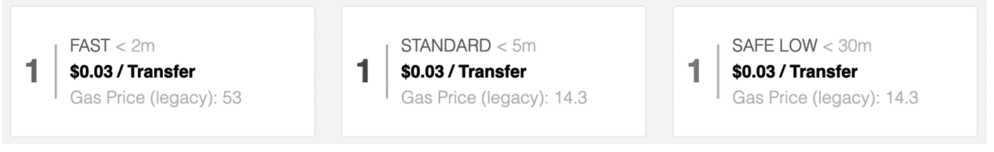


图 1.4　以太坊网络的实时 Gas 价格

有了 Gas 作为计算工作量的估算单位，和 Gas 价格作为单位 Gas 的费用，最终用户付出的以太币就是 Gas Fees。

1.3.4　以太坊虚拟机

从事计算机相关工作的读者对虚拟机的概念应该都不陌生，虚拟机是模拟物理计算机行为的程序，虚拟机具有独立的存储和处理单元。

以太坊虚拟机（ethereum virtual machine，EVM）是虚拟机程序容器，它允许部署和执行代码。用户可以通过以太坊客户端访问 EVM，并执行以太坊上的程序。本质上来说，EVM 相当于一台“世界计算机”，由分散在世界各地的各个部分组成，在这些分布式环境中执行软件操作。

另外，EVM 是图灵完备的，利用 EVM 可以实现各种复杂的算法和计算。而比特币采用脚本语言开发保证其交易的安全性，无法执行复杂的算法和计算，因此是非图灵完备的，

这也是以太坊和比特币较为明显的一个区别。

知识加油站

什么是图灵完备？图灵完备是指机器执行任何其他可编程计算机能够执行计算的能力。简单来说，一切可计算的问题都能计算，这样的虚拟机或者编程语言就是图灵完备的。这个词源于引入图灵机概念的数学家艾伦·图灵。如果一个计算系统可以计算每一个图灵可计算函数，或者说，这个系统可以模拟通用图灵机，那么这个系统就是图灵完备的。图灵完备性也可以用来描述计算机语言的计算能力。

具有图灵完备性的计算机语言，被称为图灵完备语言。绝大多数的编程语言都是图灵完备语言，例如，Java、Python 等高级编程语言均是图灵完备的。简单地总结为，图灵完备语言都有一个共性，即可以执行条件分支和循环语句，并实现逻辑控制。

EVM 通过使用一系列的操作码来执行不同的任务。在 EVM 中存在着 140 余个操作码，每个操作码都可以执行不同的操作，实现不同的功能。比如，操作码 01 表示整数的加法运算，当接收两个整数并调用 01 操作码，即可得到两个整数之和。每个操作码的执行都需要消耗一定数量的 Gas。

1.3.5 账户

可以将以太坊账户类比为现实生活中的银行账户，在以太坊账户中，包含有账户余额的属性信息，该属性描述的是某个账户所拥有的以太币的数量信息。类似于银行账户的转账，以太坊账户的拥有者可以通过以太坊网络发送交易。

在以太坊系统中，存在两种账户类型：外部账户和合约账户。两类账户的区别如下。

- 外部账户：某个用户创建的以太坊账户，用户拥有该账户的私钥，该账户归某个用户所有，即用户可以使用该账户接收以太币，也可以发送交易给别人。
- 合约账户：某个智能合约程序被部署在以太坊上，会相应地生成一个该合约对应的账户，即合约账户。对合约账户而言，其所有权和管理权由智能合约程序控制。

无论是外部账户还是合约账户，均能够接收和发送以太币交易；另外，两种类型的账户均可以和其他智能合约进行交互和通信。下面对两种账户的区别分别进行分析。

1. 外部账户

外部账户由用户创建，创建时首先生成一对密钥，分为私钥和公钥。由私钥产生对应的公钥，公钥经过变换计算，得到一串以 0x 开头、长度为 20 的字符串，称为账户的地址，用于在后续的转账过程中标记识别具体的账户，类似于银行账户的账号。外部账户通常包括如下四个字段属性，如图 1.5 所示。

- nonce：该字段是一个整型数值，用于计数，描述账户所发送的交易数量。外部账户每发送一笔交易，nonce 数值就会加 1。
- balance：该字段存储了某个地址对应的账户所存储的 Wei 的数量。前文已经提到 Gwei 是以太币单位的一种，而此处的 Wei 则是以太币的最小单位，Wei 和 ETH 的换算关系为 $1ETH=10^{18}Wei$，或者 $1Wei=10^{-18}ETH$。
- storageRoot：该字段与以太坊账户的存储相关，存储的是默克尔树根节点的哈希值。

- codeHash：外部账户中，该字段值为空。该字段只对合约账户有用，用于存储该账户所对应的 EVM 代码的哈希值。

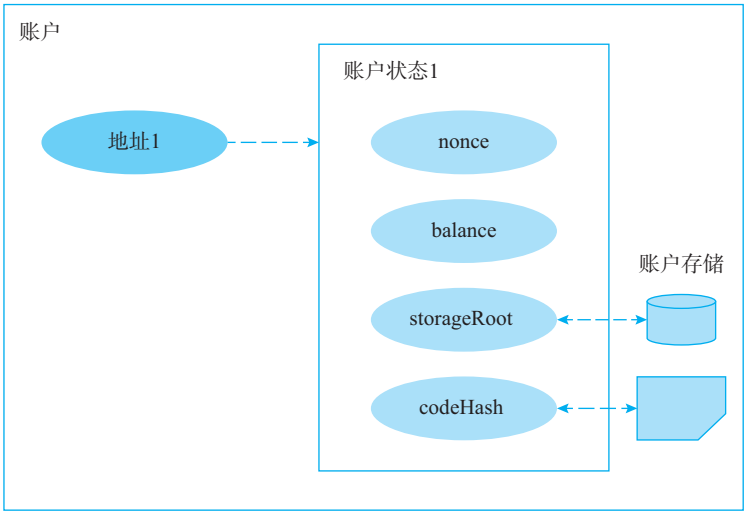


图 1.5　以太坊外部账户示意图

2. 合约账户

当用户部署已经开发好的智能合约到以太坊网络时，会得到一个该合约所对应的合约账户。部署智能合约需要使用以太坊网络资源，消耗一定的 Gas，因此创建合约账户时需要支付成本，而非免费的。

另外，与外部账户的所有权通过私钥控制有所不同的是，合约账户没有私钥。合约账户由智能合约程序代码的逻辑进行控制。

1.3.6　交易

以太坊中的交易是指包含一组指令且加密签名的数据消息，这些消息可以描述为从一个账户向另外一个账户发送以太币的具体信息，或者描述为与部署在区块链上的智能合约进行交互的信息细节。当用户发起交易操作时，交易会通过广播机制广播给以太坊网络中的其他节点，其他节点接收到交易信息，会对交易进行验证，验证通过后的交易会被节点放入临时的交易缓冲池中的交易队列。当节点生成新区块时，从交易缓冲池中的队列中取出交易数据，结合其他信息，一起构建得到新区块，然后新区块被广播至全网节点。

目前，以太坊中的交易主要分为常规交易、部署合约交易和执行合约交易三类。

- 常规交易：两个外部账户之间发生的交易就是常规交易，也可以说是普通交易。
- 部署合约交易：当用户部署智能合约到以太坊网络时，会创建一个合约账户，该过程就是部署合约交易。在该类型的交易中，因为不是转账交易，所以交易的接收者地址是空的，取而代之的是交易中的 data 字段，存放的是智能合约的编码。
- 执行合约交易：与部署的智能合约进行交互的交易。该类型的交易中，交易的目标地址为智能合约地址。

具体到某一笔交易，描述交易的信息主要包含以下内容。

- from：交易发起者的账户地址。
- recipient：交易的接收方。如果是外部账户之间的转账交易，则该信息存放的是接收者的地址；如果是部署合约交易，则该信息存放的是合约程序的代码。
- signature：交易的签名数据。签名是一串用于证明该交易是由交易发起者确认后的数据。签名数据需要使用私钥密钥生成，具有不可伪造和不可抵赖的特点。
- nonce：该字段是一个自增的计数器，用于记录某笔交易在账户中的交易编号。
- value：交易转账的具体以太币数量。需要注意的是，该字段的单位用以太币的最小单位 Wei 表示。例如，1000 表示 1000Wei。
- data：该字段是一个可选项字段，用于存储用户自定义的数据。
- gasLimit：该字段是一个整型数值，用于描述当前交易可以消耗使用的 Gas 的数量上限。
- maxPriorityFeePerGas：该字段用于记录每份 Gas 支付给矿工的小费上限。
- maxFeePerGas：该字段表示用户可接受的每份 Gas 支付给矿工的最大费用。

在本书稍后的章节中，会向读者介绍具体交易事务的使用。

1.3.7 区块

为了存储以太坊网络中产生的交易数据信息，且使得各个节点之间存储的交易数据、顺序等保持一致，引入了区块结构的概念。

区块是以太坊系统中数据存储的基本单位，区块与区块按照先后顺连接起来，形成一条链式结构。区块链系统中规定，新生成的区块中总是包含前一个区块的哈希值，将其作为一项数据保存下来。通过后一个区块存储前一个区块哈希值的方式确定了区块的前后顺序，使得区块与区块之间可以连接起来，即总能以逆序的方式通过后一个区块，得到前一个区块信息，由此便可以访问整个区块链的数据。

交易和区块的示意图如图 1.6 所示。

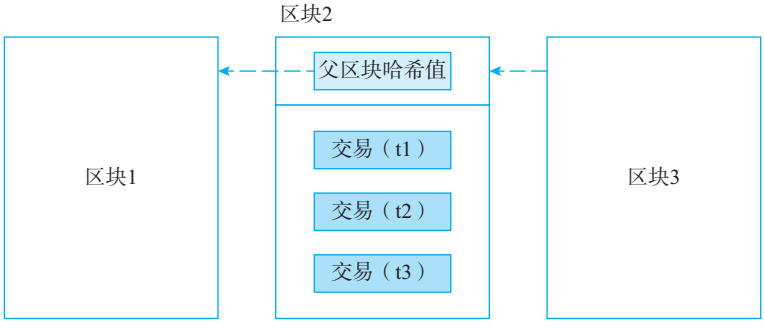


图 1.6 交易和区块的示意图

1.3.8 节点和客户端

前文已经提到，以太坊是一个去中心化的分布式区块链网络，该网络由众多的独立计算机彼此连接形成，这些独立参与网络的计算机被称为节点。在这些独立的节点上，运行着可以验证区块和交易数据的程序软件，被称为客户端。可以简单总结为：运行以太坊客户端软