区块链本质

陈鹏　著

清华大学出版社

区块链本质

陈鹏　著

清华大学出版社
北京

内 容 简 介

区块链是目前的一个热点科技词汇。但究竟区块链是什么，如何理解区块链的本质？区块链行业各执一词，莫衷一是，而对于普通大众而言，更是“云山雾罩”“一头雾水”。本书旨在对区块链的本质进行一个相对完整、相对系统的阐释。本书主要包括4章。第1章是对区块链的“全景鸟瞰”，将区块链从技术系统、数字基础设施以及意义空间三个不同的层次进行递进概览。第2章是对区块链的“庖丁解牛”，从区块链技术内涵的角度，将区块链中最为关键和最为核心的一些科学和技术问题进行了介绍，其中包括容错、共识机制、哈希、数字签名以及安全和形式化验证等。第3章是对区块链的“抽丝剥茧”，以技术范式的视角理解区块链，对比特币、以太坊和超级账本三个主流的区块链技术生态系统进行了相对细致的分析与比较。第4章是对区块链的“照猫画虎”，从一个原型实现的视角，参照比特币的总体模型，开发了一个小巧玲珑的Ajicoin，初步实现了P2P网络、交易、区块与区块链以及工作量证明的共识机制和币的交易等核心功能。

本书非常适合希望了解区块链相关知识和技术的读者，不仅能让读者从零开始了解什么是区块链，而且还可以引导读者动手开发自己的区块链程序，带领读者迈入区块链技术的大门。

图书在版编目(CIP)数据

区块链本质/陈鹏著. —北京：清华大学出版社，2019
ISBN 978-7-302-51118-2

Ⅰ. ①区…　Ⅱ. ①陈…　Ⅲ. ①电子商务－支付方式－研究　Ⅳ. ①F713.361.3

中国版本图书馆CIP数据核字(2018)第201342号

责任编辑：龙启铭
封面设计：何凤霞
责任校对：焦丽丽
责任印制：李红英

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦A座　　邮编：100084
社 总 机：010-62770175　　**邮　　购**：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 装 者：三河市国英印务有限公司
经　　销：全国新华书店
开　　本：170mm×230mm　　**印　张**：11.5　　**字　数**：154千字
版　　次：2019年1月第1版　　**印　次**：2019年1月第1次印刷
定　　价：39.00元

产品编号：080724-01

前言

人类究竟是何种生物？这或许是困扰人类已久并将会持续困扰人类的一个问题。对这个问题的另外一种说法是，人类的本质究竟是什么？纵观人类的发展历史，人们尝试过用宗教与语言来塑造人类的本质，甚至统一人类社会，然而最终都未能如愿。随着人类迈向21世纪，在信息与网络技术的推动下，我们强烈地感受到人类正处于一种深度技术化的状态，纳米、量子、人工智能以及基因技术正在挑战我们以往对“意识”“智能”与“情感”这些我们认为是人类最为核心概念的认知。在某种意义下，技术或许能比其他更恰当地描述人类的本质。

在21世纪的第一个20年的尾声中，人类迎来了一个极有意思的网络新概念——区块链，并在全球范围内激起了一阵不小的波澜，且这场冲击仍在继续。应该说，在信息与网络领域中，从来就不缺乏炒作的概念与题材，也仅仅是在几年前，云计算、物联网、大数据和人工智能的概念就被热炒过一番，而“智能革命”的呐喊之声也犹在耳畔。那么，区块链是步它们的后尘，还是在经过热炒之后，冷却下来，凝结为其价值宝石，成为嵌入到信息应用皇冠中的一个精美点缀？或是说，是否会成为下一代互联网络的核心，并重新打造一顶新的皇冠？

与云计算、物联网、大数据和人工智能这些技术概念有所不同，虽然这些技术的应用也遭受过伦理学的严厉批评，也被个人隐私、人类的权利等问题所困扰，然而，像区块链应用（涵盖加密数字货币、ICO等）这种受到被某些政策明令禁止的待遇尚不多见。区块链应用的拥趸与反对者之间水火不

容之势也是在其他技术中难得一见的。在区块链应用的拥趸看来，区块链是信息互联网向价值互联网转向的一个关键，它的无中心化、不可篡改以及Token机制是下一代互联网的核心。然而在区块链应用的反对者看来，区块链似乎是一个潘多拉魔盒。那么，区块链究竟是虔诚取经的“齐天大圣”，还是想投机巧取西天圣果的“六耳猕猴”？

或许，在我们心中的疑问远不止于上面所述，要想解开这些谜团，需要尝试解读区块链的本质，从技术的角度，深挖、再深挖，然后将它置于社会和时代的相框中，上下左右打量和深思。

目 录

第 1 章　区块链的本质追问

1.1 作为技术人造物的区块链

根据美国国家标准和技术研究所 2018 年 1 月发布的技术报告《区块链技术概览》[①]，区块链是一个分布式数字账本，其交易信息经过加密签名后以区块的形式存储。一个区块经过验证，并经过一个共识的决策，以加密的方式链接到前一个区块。随着新的区块加入，旧的区块修改起来难度就更大。新区块在网络的所有账本副本中被复制，如果出现冲突，将使用已经达成的规则进行自动消解。

在维基百科中[②]，对区块链的介绍大致如下：区块链，从词源的角度来源于“区块”与“链”两个词，它实际上是一个持续增长的记录（称为“区块”）列表，这些记录使用加密方式确保安全，并链接起来。每个区块通常包含前一个区块的加密哈希（散列）、时间戳和交易数据。区块链从设计上就抵制对数据的篡改，它是一个开放的、分布式的账本，能够有效地、以可验证和持久的方式记录两方交易。如果用作分布式账本，区块链通常由一个点对点的网络管理，并遵从节点间通信和验证新区块的协议。一旦被记录，在任何给定的区块中的数据，在没有修改后续区块的前提下都不能进行追加式修改，如果要修改，那就意味着需要破坏网络中的大多数节点。区块链在设计的时候就是安全的，它是一个具有高拜占庭容错的分布式计算机系统的实例。在一个区块链中，需要获得分布式共识。这种性质使得区块链非常适用于记录医疗数据，也非常适合记录类似于身份管理、交易处理、食品追溯和投票等管理行为。区块链是在 2008 年由中本聪发明的，用于加密数字货币（如比特币）中。比特币中的

① Dylan Yaga (NIST), Peter Mell (NIST), Nik Roby (G2), Karen Scarfone (Scarfone Cybersecurity). Draft NISTIR 8202, Blockchain Technology Overview. https://csrc.nist.gov/publications/detail/nistir/8202/draft.

② https://en.wikipedia.org/wiki/Blockchain. 于 2018 年 4 月 5 日访问.

区块链应用，使得比特币成为第一个不需要可信权威机构或中央服务器就能解决双重支付问题(Double-spending)[①]的数字货币。

简而言之，区块链可以视为一个分布式的、用于交易的数据库(如图 1.1

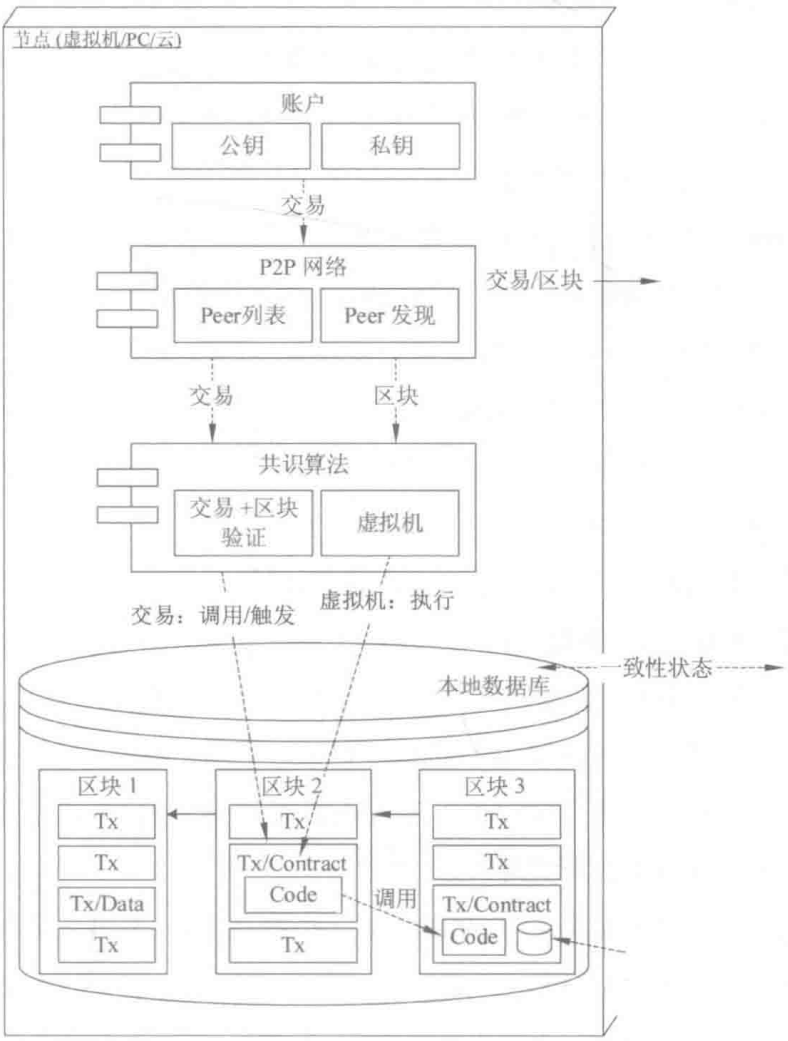

图 1.1 区块链系统的概念和关系图[②]

① 双重支付是数字货币中的一个潜在漏洞，具体是指同一个数字代币能够多次使用。

② Glaser F. *Pervasive Decentralisation of Digital Infrastructures: A Framework for Blockchain Enabled System and Use Case Analysis*[J]. Social Science Electronic Publishing, 2017.

所示)。全局分布式的节点通过点对点(P2P)的通信网络互联。其中,节点一般指的是一台物理或虚拟机器,通过 TCP/IP 和 UDP 进行通信,节点通过 IP 地址标识。用户通过其公钥来标识。用户对应的私钥用于对消息和交易进行加密签名。

节点可以保存一个所有历史的、有效交易的数据库。交易按照区块的方式组织起来。每个区块指向上一个区块,从而能够获得交易的时间顺序。一个区块内的交易顺序根据共识算法所随机选择的节点来确定。根据需要,一些轻量级的客户节点可以只收集交易区块的哈希。

区块链的核心功能是提供可验证的、不可篡改的交易,也就是说,在整个网络中,数据的更新在大多数节点中是一致的。区块链会使用复杂的数据结构(例如,Merkle 树或 Patricia Merkle 树)来高效地存储所有交易。这样,如果从所有历史交易中重新计算当前状态,单个节点对历史交易的变更会导致无效的状态。如果某个节点提出一个被其他节点视为无效的交易,提出无效交易的节点将会被其他节点所忽略,因为它与其他节点都不一致。

值得一提的是,上面提及的交易实际上有两层含义,一层含义从数据库的视角而言,数据的更新就是一次交易(在数据库术语中,也称为"事务")。另一层含义是指区块链通常用于 Token 的转移,Token 从一个用户转移到另一个用户也称为一次交易。Token 要么是系统内生的,要么是使用高层脚本语言或者编程语言所实现的。

在大多数区块链的实现中,都会内置一个脚本语言,使其能够像数据库中的存储过程那样,执行由一个交易所触发的特殊业务逻辑。在更新的技术中,如以太坊(Ethereum)和超级账本(Hyperledger),通常会扩展脚本语言,整合一个完整的编程语言,由内部的一个虚拟机来执行它。这种编程语言也能够访问复杂的数据类型和数据结构,甚至具有一个小型的、本地隔离的数据库用于存储和检索数据。代码部署在每个节点的区块链数据库上,由某个特定的交易类型所触发。这些代码通常也称为智能合约。智能合约

的执行可以类比为原子交易，即从当前的数据库状态到下一个数据库状态的转移。如果代码中的某一部分执行失败，那么整个交易便失败，不能形成下一个状态。

对信息系统的分析，我们以往都会从逻辑上划分为三个层次，一是基础设施层，二是应用层，三是展现层。从这种逻辑划分来看，我们可以将区块链从两个层次来区分，一是无中心化组织层，另一个是无中心化应用层，具体如图 1.2 所示。

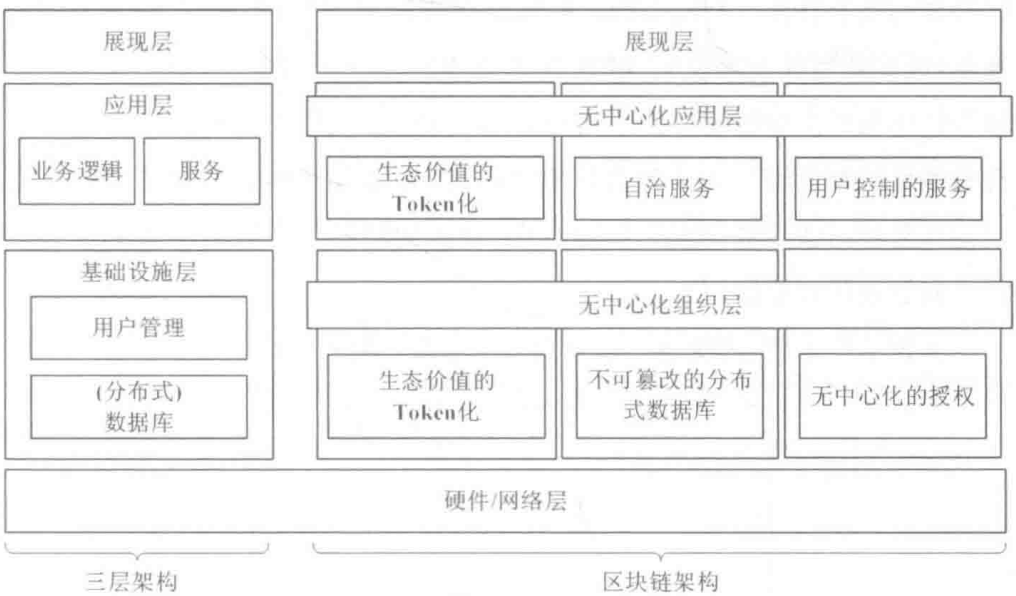

图 1.2 区块链的分层逻辑示意图

无中心化组织层包含通信层、公钥基础设施、构造和维护数据库的数据结构以及执行智能合约语言的执行环境。此外，值得一提的是，组织层具有很强的中心控制，无论是谁或哪个组织开发或维护组织层，他(他们)都能够完全地控制整个系统的运行。此外，组织层实现了基本服务，决定了哪些用户具有哪类权限。根据用户对区块链的访问权限，可以将区块链分为公链和私链。在私链中，只有那些授权的用户才可以看到并确认交易和区块。

无中心化应用层包含以智能合约形式所实现的服务的应用逻辑。与组织层不同，应用层的代码能够由任意参与者撰写并绑定到系统中。代码本身是由撰写它的参与者所控制，这样，应用层的控制是分布在部署代码的参与者手中。换而言之，应用层的控制以无中心化的方式分布在用户空间中，因此系统的控制权无中心化了。这种无中心化的控制结合所属物转移的不可篡改的表征，或者说系统状态的转换，出现了“无信任系统”(trustless system)的概念。这使得基于智能合约的业务逻辑能够以自治的方式使用区块链的所有特性。智能合约能够表示业务逻辑，即市场机制、决策并相互通信(彼此调用或者触发)。智能合约能够实现一个服务，维护一个只能由该合约访问的小型数据库。它可以计算与该交易有关的数据，并将进一步交易触发到其他用户或其他合约中。因此，智能合约能够实现复杂的市场机制和复杂的微服务交互。总而言之，自治的服务结合智能合约的无信任设置能够取代可信的中介。

从技术栈来看，区块链可以分为 4 个层次(如图 1.3 所示)。

图 1.3　区块链的技术栈

互联网是基础的技术层，其主要依赖于互联网协议 TCP/IP，由它来定义输入如何打包、寻址、传输、路由以及接收。

区块链协议层在互联网之上，通过节点所形成的 P2P 网络执行协议、基于加密共识算法完成交易，而这些交易形成分布式账本的相同副本。协议构造了一个开放、共享与可信的公共交易账本，而不受某个个体的控制。

在应用层中，比特币是最为典型的应用，在比特币网络中诞生了一个无中心化自治组织(DAO)。以太坊创新了区块链的应用形式，它通过允许智能合约的执行(DApp)而形成了可定制的公链。

用户体验层指的是在各类设备上体验区块链的应用。

无疑，无论是从组织层次体系或者从技术栈来看，区块链都是一个由许多不同部件组成的一个复杂技术人造物，它由多个部件相互通信和交互所产生。根据西蒙的观点[①]，他将复杂系统描述如下："通过非简单的方式交互的大量组成部分。在这类系统中，在实用的意义下，而非是在终极的、形而上的意义下，整体大于部分之和，通过给定部分的属性和它们交互的规律，要推断出整体的属性仍然不是一件小事情。"针对西蒙的定义，西利尔斯补充道[②]："由于相互通信与交互以及相关的信息传送，复杂系统会随着时间而变化。"诺斯罗普和他的同事认为[③]，随着自发展的亚大规模系统，包括软件系统的复杂性不断增加，为应对这种复杂性，要求一种新的、不同的观点。他们将这种观点视为一种过程转换。在以往的自顶而下的方法中，关注的是需求满足，而在复杂、无中心化的系统中，更多的是关注管控。区块链所引发的新技术现象在于在异构的、大量的系统之间的互联、互通、交互和决策。通过互联和联合行为所诉诸的整体能够被视为一个复杂技术体。这种新的、复杂的区块链整体要求一种不同于还原论的新的科学方法，它应该聚焦于这些互联和联合行为，以及随之而来的整体。

---

① Simon, H. A. 1969. *The Sciences of the Artificial*. Cambridge, Mass.: MIT Press.

② Cilliers, P. 1998. *Complexity and Postmodernism: Understanding Complex Systems*. London: Routledge.

③ Northrop, L., et al. 2006. *Ultra-Large-Scale Systems: The Software Challenge of the Future*. Pittsburgh: Software Engineering Institute, Carnegie Mellon University.

1.2 作为数字基础设施的区块链

区块链不仅仅是一个技术人造物(technical artifact),更是一项数字基础设施(digital infrastructure)。根据大卫·蒂尔森(David Tilson)等人的观点[①],数字基础设施与传统基础设施存在如下的差异:

首先,传统基础设施依赖于底层技术能力与服务交付模型的紧密功能耦合。传统基础设施与数字基础设施不同,它们并不是递归组织的,电力和水力设施不能生成式地创建新的基础设施业务来挑战上面的服务。

其次,数字基础设施具有很强的可扩展性,其组成部分(例如路由器或传输设备)能够相对容易地进行升级或替代。与传统基础设施相比,数字基础设施可以在性能上发生飞跃,规模上快速增长而成本急剧下降,这些都是传统基础设施无法实现的。

第三,数字化内在的灵活性使得数字基础设施以传统基础设施所不能企及的方式延展其范围和规模。数字基础设施具有向上灵活性(upward flexibility),因为它对使用其底层的通信和存储能力创建任何应用和服务都是开放的。另一方面,数字基础设施具有向下灵活性(downward flexibility),因为大量的数字或者物理网络潜在地都提供所需的互联性和其他功能。这种灵活性是由软件的延展性所提供的。

最后,数字基础设施所传送的是比特,这是一个承载最有丰富意义的单个质料。数据之于数字基础设施,与汽车之于交通基础设施或电子之于电力设施都有所不同。数字数据有着物理基础设施中所不能发现的、唯一的

① David Tilson, Kalle Lyytinen, Carsten Sørensen, (2010) *Research Commentary—Digital Infrastructures: The Missing IS Research Agenda*. Information Systems Research 21(4): 748-759. http://dx.doi.org/10.1287/isre.1100.0318.

特性。用户、机器或社群在使用数字基础设施的过程中，需要对在网络中所传输的比特意义进行协商和安排。对于基础设施的使用和增长而言，新的层次化互操作标准和应用服务接口的共同定义是本质的。例如，在YouTube视频中，共享的视频编码标准不仅可以实现共同观看和分享视频，还允许对原始编码进行标记、重新混排甚至修改，从而创造一个不断繁荣的空间。

无疑，区块链是一类社会技术(sociotechnical)系统，区块链的无中心化这一标志性特征使得它(将会)对社会结构产生极其深远的影响。与一些互联网平台(例如，阿里云、亚马逊AWS等)一样，许多的区块链平台(例如，以太坊、EOS、Steemit等)也扮演着一个数字基础设施的角色。这些区块链平台是一个共享的、无边界的、异构的、开放的、不断演化的社会技术系统，它包含一个各类信息能力、用户、操作和设计领域等各种装备好的基础。

大多数的区块链平台具备再生能力(generattivity)。所谓再生能力是指任何自包含的系统在没有系统发起者输入的前提下，能够创造、产生或生产出新的输出、结构或者行为[①]。正是由于这种再生能力，从某种意义上而言，区块链平台总是处于“未完成”的状态，它们具有许多可以构想的用途，公众以及组织可以在其上发明或分享许多新的、好的应用。譬如，在以太坊中，人们可以通过创建智能合约，在不同的领域来创造和分享应用。

与一般的数字基础设施一样，区块链平台也面临着变化和控制的悖论。在这种双螺旋旋转作用下，区块链平台不断地发展，如图1.4所示。

从变化的悖论而言，区块链平台也是在稳定性和灵活性之间张力的作用下不断发展。一方面，区块链平台极具可扩展性，例如，从2014年的6月到2014年的9月，比特币的用户数量从540万用户增加到650万用户，增加了21%。从P2P的网络属性而言，理论上区块链平台本身的扩展性是极其好的。另一方面，由于区块打包和全网广播，使得区块链平台在吞吐上随着

① https://en.wikipedia.org/wiki/Generativity.