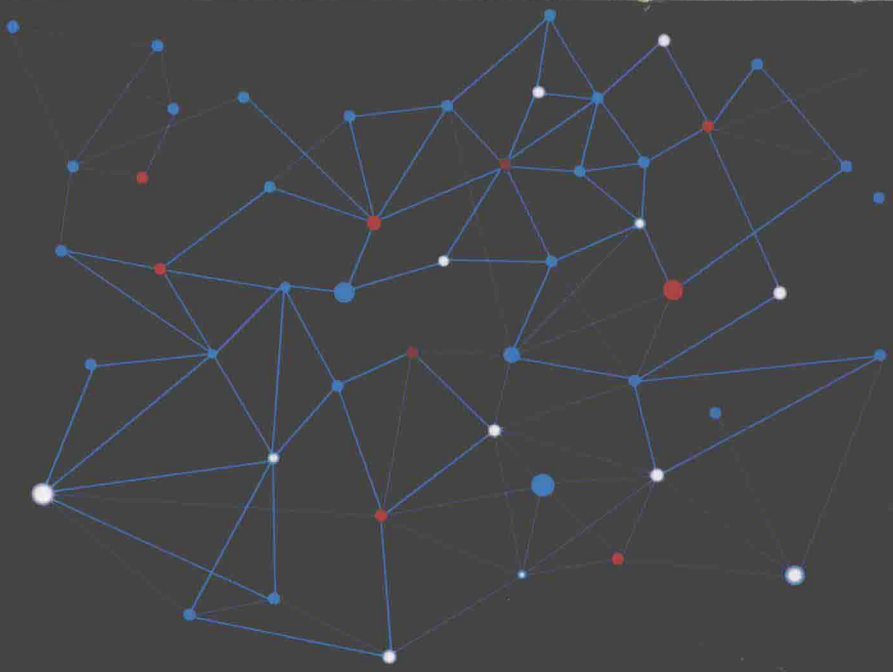


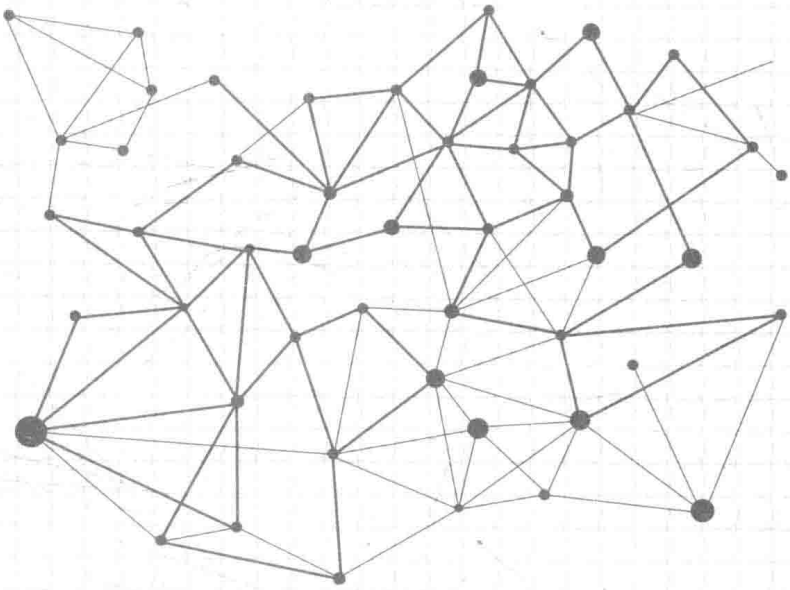
区块链

解密

「构建基于信用的」
「下一代互联网」

黄步添　蔡亮／编著

清華大學出版社



区块链解密

「构建基于信用的」「下一代互联网」

黄步添　蔡亮／编著

清華大學出版社
北京

内 容 简 介

这是一本全面深入阐述区块链技术的书籍，书中重点阐述了区块链的实现原理、共识机制、应用场景以及未来发展方向。

本书共5章，主要内容为：从比特币以及区块链的发展历程与原理等方面介绍区块链的起源与成功应用；从区块链与传统行业、人工智能、金融、大数据等方面的结合，描述了区块链能为人们带来的巨大技术变革；介绍了区块链技术的主要应用场景及相应案例，包括存在性证明、智能合约、供应链、身份验证、资产交易、预测市场、电子商务、物流、文件存储、医疗等；从原理、技术创新、发展等方面介绍了当下成功的区块链技术实践项目，包括以太坊、公证通、比特股、瑞波以及超级账本；从区块链网络自身的演化、物联网、互联网等方面描绘了区块链技术的未来蓝图——构建基于信用的下一代互联网。

本书适合希望全面了解区块链技术全貌及具体应用场景的读者。

图书在版编目（CIP）数据

区块链解密：构建基于信用的下一代互联网 / 黄步添，蔡亮编著. — 北京：清华大学出版社，2016

ISBN 978-7-302-45027-6

Ⅰ. ①区… Ⅱ. ①黄… ②蔡… Ⅲ. ①电子商务—电子支付—研究 Ⅳ. ①F713.361.3

中国版本图书馆 CIP 数据核字（2016）第 218979 号

责任编辑： 杨如林
封面设计： 杨玉兰　刘青露
责任校对： 徐俊伟
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 刷 者： 三河市君旺印务有限公司
装 订 者： 三河市新茂装订有限公司
经　　销： 全国新华书店
开　　本： 170mm×240mm　　**印　　张：** 15.5　　**字　　数：** 228 千字
版　　次： 2016 年 12 月第 1 版　　**印　　次：** 2016 年 12 月第 1 次印刷
印　　数： 1 ～ 3500
定　　价： 49.80 元

产品编号：070683-01

编委会

主　　编：黄步添　蔡　亮

撰　　写：王　毅　陈建海　刘振广　李启雷　龚建坤
盛远策　陈　颖　刘嘉陵　梁　然　张泽恩
少　平　曹　寅　王英健　吴思进　姜　疆
王从礼　俞之贝　毛道明　王云霄　张维赛
郑徐兵　姜集闯　李　伟　邓　旭

审　　校：王从礼　黎晓飞　杨正清

序

记得一年多以前，在和来自中国大陆的同事们讨论Blockchain的时候，这个词似乎还没有一个约定俗成的中文译名。现在，“区块链”（Blockchain）已经是技术领域中最热的词汇了。目前，中国在区块链和分布式账本（Decentralized Ledger）等领域已经处于领先地位，其主要原因在于中国拥有大量密码学和金融技术（FinTech）领域的人才。从我第一次到中国讲授有关区块链的课程以来，在短短的时间内，我就发现中国政府和企业对这一领域倾入了前所未有的关注，大量区块链加速器（Accelerator）如雨后春笋般地成长了起来。

对那些希望能更深入地了解区块链和分布式账本的读者来说，黄步添博士的这本专著来得非常及时。本书覆盖了这一领域的各类课题，能帮助读者从技术层面上进一步了解相关课题。同时，对于普通读者来说，本书的讲解又能做到深入浅出。这本专著对于中国读者来说，是原创性和综合性的，几乎对所有区块链的相关概念都进行了讨论，而且，所讨论的课题很前沿，包括以太坊（Etheruem）、分布式自治组织（DAOs），以及智能合约（Smart Contract），等等。

如果通过分布式网络（Distributed Network）进行P2P支付，在这过程中，信任就不是必需的了，这种想法在比特币的原始投资者中广为流传。实际上，非中心化（Not Centralized）的网络是最理想的。在集中化系统（Centralized System）中，每个节点都有不同的信息和支持不同的计

算能力，要替代它几乎是不可能的。一直以来，替代传统的集中化系统，也只能是个理想而已。比特币是由一小群人，或者说是一个人发明的。它之所以能吸引那么多人的关注，主要是因为其高度的复杂性和适应性，这使得替代集中化系统成为可能。但是，即便不从技术角度讲，中本聪（Satoshi Nakamoto）这个名字本身也很有意思，是三星（SAmsung）、东芝（TOSHIba）、中道（NAKAmichi）和摩托罗拉（MOTOrola）的起首发音的组合。如果直接以日语汉字来解释，意思是：中国人本来就聪明。这赋予了这个名字更多的神秘感，弄得绝大部分人根本不知道中本聪到底是谁。

随着人工智能领域技术的进步和计算机处理能力的提升，大家相信，有朝一日，机器会主宰人类。这可能超出了最初从事人工智能的科研人员的考虑范围，但是现在看来，在未来的某个时间点，这是有可能发生的，科幻小说已经给人们做出非常详尽的描述了。因此人们产生了这样的思想：加密技术是用来保护人类的。在20世纪90年代，在这个领域中活跃着一群自称为密码朋克（Cypherpunks）的人，他们受到黑客传统与自由主义思想（Libertarian Ideas）的影响。他们相信，在电子时代的开放社会，隐私依然是绝对必要的。他们不认为集中式系统在未来能够保障个人隐私。他们倡导的是人民应当捍卫自己的隐私权，并且通过编写具有这样功能的代码来实现这一目标。也许，他们相信当网络朋克（Cyberpunk）的小说会变成现实，在机器主导世界的情况发生时，这么做至少能在某种程度上更好地保护人类的尊严。他们相信加密与解密将是一场“魔高一尺，道高一丈”的持久战，这场斗争的结果将决定未来人类将享有多大程度的自由。对他们来说，为了人类的自由，他们是愿意承担一定的风险的。密码朋克（Cypherpunks）是密码（Ciphers）和网络朋克（Cyberpunks）两个词结合在一起产生的，从1992年9月开始就有人使用这个词了。现在密码朋克指的是一个崇尚通过加密技术来推动社会变革的社交网络群体。

2014年，我第一次在硅谷就政府在这个生态系统（Eco-system）中的重要角色做主题演讲，大家好像都听不太进去。新加坡管理大学通过网络播

客（Podcast）推送了演讲，之后新加坡沈基文金融经济研究院（SKBI）又举办了世界第一场加密货币国际学术会议，分布式账本研究社区中的很多人才开始被说服，大家认为技术可以帮助企业降低成本，提升效率。因为我们可以通过技术来保护生态系统的完全可信，而不必再去判断对方是否值得信任。后来，我又参加了一系列有关电子支付和金融技术的访谈和论坛，进一步论述了技术有推动普惠社会的效能，可以为没有充分获得银行服务的和完全得不到银行服务的群体提供低成本的基本服务，这些论述开始得到业界的重视。

黄步添博士在本书中汇总了诸多与区块链相关的课题，在其完整论述的基础上，我们可以借用上海交通大学海外教育学院周亚莉老师为我在“领航+高管前沿人才培养计划”课程的开幕演讲中所撰写的总结文稿加以概述：

（1）当前金融体系仍主要靠加强中心化来解决信任问题。为维护信任，在金融业的发展历程中，催生了大量的中介机构，包括托管机构、第三方支付平台、公证机构、银行、政府监管部门等。但中介机构处理信息仍依赖人工，且交易信息往往需要经过多道中介的传递，使得信息出错率高，且效率低下。在实践中，权威机构通过中心化的数据传输系统收集各种信息，并保存在中心服务器中，然后集中向社会公布。中心化的传输模式同样使得数据传输效率低、成本高。

（2）区块链是基于共识机制建立起来的，由集体维护的分布式共享数据库。它具有非中心化、去中介化、无须信任系统、不可篡改、加密安全、交易留痕并可追溯、透明等优点，可以有效绕过诸多中介，降低沟通成本，提高交易效率，快速确立信任关系或在交互双方未建立信任关系时即达成交易，进一步靠近了金融的本质属性和内在要求。

（3）目前，区块链技术在数字货币、信贷融资、支付清算、数字票据、证券交易及登记结算、代理投票、股权众筹、跨境交易、保险经纪等方面，已从理论探讨走向实践应用。上述领域的共同特点是对信任度要求高，而传统信任机制的成本居高不下。

（4）以比特币为代表的数字货币是区块链技术最为成功的运用。比特币与传统纸币相比，发行数字货币能有效降低货币发行及流通的成本，提升经济交易活动的便利性和透明度。这种数字货币具有超币种、超国界、超主权、实时结算的特点，一旦在全球范围实现了区块链信用体系，数字货币自然会成为类黄金的全球通用支付信用。

（5）与现有的传统支付体系相比，区块链支付在交易双方之间直接进行，不涉及中间机构，即使部分网络瘫痪也不会影响到整个系统的运行。如果基于区块链技术构建一套通用的分布式金融交易协议，为用户提供跨境、任意币种实时支付清算服务，则跨境支付将会变得便捷高效和成本低廉。

（6）区块链技术被视为下一代价值互联网的主要协议之一，任何需要或者缺乏信任的生产和生活领域，区块链技术都将有用武之地。从数字货币到证券与金融合约、互助保险、教育、所有权登记、转让、博彩、防伪、物联网、智能合约，甚至旅游，还可以在公益及社会治理领域如身份认证、司法仲裁、投票、健康管理、人工智能，以及非中心化的社会组织等领域中进行广泛应用，这将会极大地改变甚至颠覆我们未来的生活。

在黄步添博士的这本专著中，您可以看到：

第1章　从区块链的起源与成功应用——比特币以及区块链的发展历程与原理等方面介绍区块链。

第2章　从区块链与传统行业、人工智能、金融、大数据等领域的结合，描述了区块链能为人们带来的巨大技术变革。

第3章　介绍区块链技术的主要应用场景及相应案例，包括存在性证明、智能合约、供应链、身份验证、预测市场、资产交易、电子商务、文件存储、物流、交易所、医疗应用等。

第4章　从原理、技术创新、发展等方面介绍了当下成功的区块链技术实践项目，包括以太坊、公证通、比特股、瑞波以及超级账本。

第5章　总结全书，从区块链网络自身的演化、物联网、互联网等方面描绘了区块链技术的未来蓝图——构建基于信用的下一代互联网。

但是，我对大家常用的“去中心化”这个词有些不同的看法。因为对于这个词的解读，很难区分到底是要“摒弃集中化授权”还是建立“分散化设置”。中文的直译似乎不能很准确地表达其内在含义。我更倾向于使用“非中心化”（Not Centralised），而不是“去中心化”（DE-Centralised）。在汉语里，与“中心化”相对的应该是“非中心化”，也就是说“不是集中式的”，而不是要摒弃中心化的“去中心化”，是“非中心化”而不是“去中心化”。“非中心化”的每个节点之间，仍然可以有“迷你中心化（Mini Centralization）”。总之，可以认为这个“去中心化”表达的是一种“分散式的”含义。最近的研究表明，如果比特币挖矿在每个节点的计算能力也都能保持一致，那么没有哪一个节点会比其他节点更有优势，“迷你中心化”也就不会发生。这样，也许我们就有了一种理想的状态：分布式系统（Distributed System）。

我希望在以后的著作和文献中，学者们应该考虑对现有词汇的翻译进行调整，不然容易混淆重要的概念。“去中心化系统”这样的提法，也会给人们带来类似于完全“无需治理”的想法，这是不正确的。即便是在一个完全分布式的系统中，仍然会由“核心开发者”“授权开发者”或者“认证开发者”来编写代码。然后，由挖矿人、股东或代币持有人（Token Holders）来决定新的治理结构或者代码是否可以被接受。虽然不需要介入软件下载，但是如果没有新的法律或者治理结构来应对这些问题，核心开发者仍然可能会面对尚不明确的法律责任。在这一领域，代码是法律，还是法律是代码？这个问题目前还没有讨论清楚。这就给可能的司法诉讼埋下了伏笔。同时，只要我们在区块链环境中还能够追踪并确认个人或者实体的身份，那么这个系统就不是真正的匿名系统而只是P2P匿名系统。讽刺的是，区块链的出现虽然是密码朋克社区的重大贡献，但是，完全的非中心化和分布式可能不会真正产生。此外，因为区块链高度透明，有可能带来和人们期望完全相反的结果，更高程度的集中化和中央控制是有可能会在分布式账本系统中出现的。但是，这一点也不会动摇密码朋克社区为此付出努力的决心，可以肯定

地说，保护人类在由机器主导的世界中的尊严，是一个高尚而值得探索的目标。也就是说，最理想的完全摒弃集中化授权的分布式系统，也许只在理论中存在。

信任是个稀有的资源，上述区块链的特点补充了我们现在以技术、平台、数据为基础所建立的信任系统。书名《区块链解密：构建基于信用的下一代互联网》充分反映了很多专家对区块链的评价。黄步添博士的著作出版得非常及时，大家应该都看一看，非常高兴我能有幸为本书作序。在此向云象区块链和黄步添博士致以最美好的祝愿。

李国权
新加坡新跃大学（SIM University, Singapore）金融科技与区块链教授
美国斯坦福大学2015 Fulbright学者
新加坡经济学会副会长

前言

互联网领域最知名的“预言家”凯文·凯利在《失控》一书中指出，未来世界的趋势是去中心化的。亚当·斯密的“看不见的手”就是对市场去中心化本质的一个很好的概括。点与点之间直线距离最短，人与人之间沟通的最佳模式也应该是直接沟通，无论从哪个方面切入，去中心化的市场本质都是无可辩驳的。

我们可能正面临一场革命的晨曦，这场革命始于一种新的、边缘的互联网经济。世界经济论坛（即达沃斯论坛）创始人克劳斯·施瓦布（Klaus Schwab）说：“自蒸汽机、电和计算机发明以来，人们又迎来了第四次工业革命——数字革命，而区块链技术就是第四次工业革命的成果。”区块链作为下一代的可信互联网，必将颠覆所有在其之上的业务，让整个基于互联网的企业、生态、产业链彻底做一次变革创新。

马云曾经说过：“很多人还没搞清楚什么是PC互联网，移动互联网来了，我们还没搞清楚移动互联的时候，大数据时代又来了。”现在，我们是否可以在后面加上一句：“人们还没搞清楚大数据是什么，区块链又来了。”威廉·吉布森曾说过：“未来已经发生，只是尚未流行。”相信区块链技术能够引领未来5～10年的计算机和互联网领域的发展，我们已隐约能听见不远的未来，由区块链技术掀起的革命的滚滚风雷。

首先感谢清华大学出版社的大力支持，才会促成本书的出版。本书全面阐述了区块链的技术原理、应用场景，以及未来的发展方向。盛远策、王从

礼、毛道明、王云霄、张维赛等参与了第 1 章的编写工作；王毅、李启雷、姜集闯等参与了第 2 章的编写工作；王英健、吴思进、姜疆、龚建坤、王从礼、陈颖、俞之贝等参与了第 3 章的编写工作；刘嘉陵、梁然、张泽恩、少平等参与了第 4 章的编写工作；曹寅、郑徐兵、盛远策、李伟、王毅、邓旭等参与了第 5 章的编写工作。

特别感谢新加坡经济学会副会长李国权教授为本书作序，浙江大学何钦铭教授、教育部长江学者陈积明教授、陈文智教授、纪守领教授以及新加坡国立大学 Roger Zimmermann 教授等对云象区块链团队的大力支持，以及云象区块链的王备博士、王津航博士、石太彬、杨文龙、温琪、朱纪伟、王光瑞、候文龙等专家的参与。

希望本书的出版，能为广大区块链技术爱好者和创业者提供帮助。

编者　黄步添

目录