

马永仁◎著

区块链

技术原理及应用

一本书读懂

区块链应用蓝图

BLOCKCHAIN

深度解读区块链技术与发展前景

全景式呈现区块链全行业应用场景

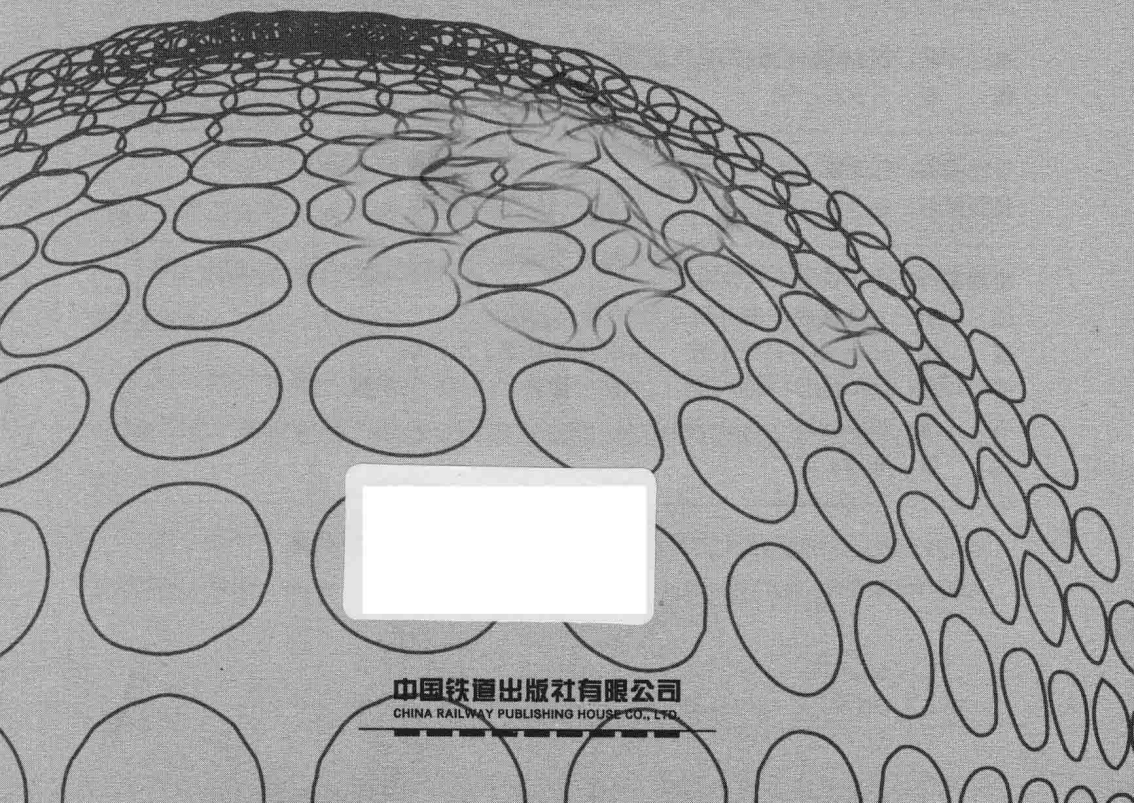
多维度阐释区块链、人工智能、加密经济学、大数据的关联与应用

中国铁道出版社有限公司
CHINA RAILWAY PUBLISHING HOUSE CO., LTD.

区块链

技术原理及应用

马永仁◎著



中国铁道出版社有限公司
CHINA RAILWAY PUBLISHING HOUSE CO., LTD.

内 容 简 介

本书以全球化的视角全景式解读区块链技术的前世、今生及未来，内容涵盖区块链的技术原理、使用场景、正在开发的商业应用、发展趋势、前景展望等，重点描述区块链的商业应用、区块链技术广泛应用的风险和挑战，为读者全方位构建区块链的商业应用前景，引领读者积极拥抱区块链，赢在未来。

图书在版编目（CIP）数据

区块链技术原理及应用 / 马永仁著. —北京：中国铁道出版社，2019.6

ISBN 978-7-113-25478-0

I. ①区… II. ①马… III. ①电子商务—支付方式
IV. ①F713.361.3

中国版本图书馆CIP数据核字（2019）第020916号

书 名：区块链技术原理及应用
作 者：马永仁 著

责任编辑：张亚慧
责任印制：赵星辰

读者热线电话：010-63560056
封面设计：MXK DESIGN
STUDIO

出版发行：中国铁道出版社有限公司（100054，北京市西城区右安门西街8号）
印 刷：北京铭成印刷有限公司
版 次：2019年6月第1版 2019年6月第1次印刷
开 本：700mm×1000mm 1/16 印张：12.75
书 号：ISBN 978-7-113-25478-0
定 价：49.00元



版权所有 侵权必究

凡购买铁道版图书，如有印制质量问题，请与本社读者服务部联系调换。电话：（010）51873174
打击盗版举报电话：（010）51873659

作 / 者 / 介 / 绍



马永仁，中国人民大学经济学硕士，
纽约市大学计算机信息系统硕士，罗特格
斯商学院金融工程硕士。

曾任哥伦比亚大学数字知识风险投资
公司副总裁（该公司是由哥伦比亚大学，
斯坦福大学和密歇根大学联合创办的风险
投资公司，投资专注于数据库开发，远程
教育开发等领域的初创公司）。

曾任司班布瑞投资公司技术总监（该
公司是位于纽约的著名高科技风险投资公
司，投资专注于新型数据库，云计算等领
域的初创公司）。

世界区块链与价值互联网研究中心联合
创始人，对区块链以及即将产生的价值互
联网进行了大量研究、开发和推广工作，
是共有链和价值互联网的积极倡导者。

您@，我跑腿

随时随地为您服务



投稿合作：lampard@vip.163.com

封面设计：[www.MX DESIGN STUDIO](http://www.mxdesignstudio.com)
0076883329

试读结束：需要全本请在线购买：www.cqvip.com

PREFACE

前 言

2008年，一位只闻其名未见其人的神秘人物——中本聪，通过一篇未在任何学术期刊上公开发表的神秘论文，把比特币带到这个世界。

诞生于虚拟世界的比特币代表了人类对于数学算法的一种共识。可以说，当时的比特币获得了人们的认可，不论是最初几十个比特币能换一份比萨，还是2013年12月1日，比特币的单价超过1盎司（约等于28.35g）黄金的价格，比特币都在向世人展示其作为价值尺度的一面。

我们通过比特币，看其运行的技术和结构，即一种不需要中介却可以实现价值传递的技术，而这种技术就是区块链。

经过数年的发展，在如今这个互联网时代、数字化时代，乃至大数据时代，驱动金融发展的金融科技已经由移动互联网、大数据、云计算等应用层面，进一步转向了区块链等底层技术创新，区块链已经在成为金融科技的底层技术的同时，也正在被其他领域借鉴和引用。

为了更好地传播区块链技术，也为了使读者能够深入地理解区块链技术，在本书的写作中秉承了由浅入深、由理论到实践的思想，将全书分为三大部分：

第一部分（第1章至第3章），介绍了区块链技术的由来、核心思想及核心技术。

第二部分（第4章至第7章），重点介绍了区块链技术在大数据领域、金融领域、商业领域、社会契约等方面的应用以及已有区块链项目的落实和应用。

第三部分（第8章至第9章），对区块链技术在大数据领域、金融领域、商业领域应用的展望，以及正在开发使用的区块链项目的展望。

相信读者在阅读完本书后，在深入理解区块链核心概念和原理的同时，对于区块链的技术和典型设计实现也能了然于心，可以更加高效地开发基于区块链平台的去中心化、分布式应用。

作者
2019年3月

| 目录 |

CONTENTS

第 1 章 区块链技术：人人有本流水账 / 1

- 1.1 存放数据的集成块——区块 / 2
- 1.2 区块的延续发展——区块链 / 3
- 1.3 静态区块链技术，略有变化的数据库 / 4
 - 1.3.1 数据库的特点 / 5
 - 1.3.2 区块链数据库与传统数据库的区别 / 5
- 1.4 动态区块链技术——神奇的账本 / 8
- 1.5 区块链的分类与应用 / 9
 - 1.5.1 区块链的分类 / 9
 - 1.5.2 公有链、联盟链、私有链与侧链的区别 / 11
 - 1.5.3 区块链的应用层面 / 14

第 2 章 区块链结构原理——老树开新花 / 17

- 2.1 诞生自中本聪的比特币 / 18
- 2.2 区块链与比特币 / 21
- 2.3 颠覆世界的动因之一：去中心机制 / 23
 - 2.3.1 沙丁鱼抵御鲨鱼 / 23
 - 2.3.2 拜占庭将军问题 / 24
 - 2.3.3 去中心化问题的解决 / 27
- 2.4 颠覆世界的动因之二：共识机制 / 28
- 2.5 颠覆世界的动因之三：分布式结构 / 33
 - 2.5.1 分布式的三个步骤 / 33
 - 2.5.2 分布式账本，既分布又去中心化 / 34
 - 2.5.3 时间戳与密码签名共建的分布式账本 / 37

2.6 区块链的架构模型与典型特征 / 38

2.6.1 区块链的架构 / 38

2.6.2 区块链技术结构模型 / 42

2.6.3 智能合约的特性与运行原理 / 45

第3章 区块链的密码学技术 / 47

3.1 密码学技术: Hash 算法 / 48

3.2 密码学技术: 加密算法 / 51

3.2.1 非对称加密算法 / 51

3.2.2 对称加密算法 / 52

3.3 密码学技术: 数字签名 / 54

3.4 密码学技术: 数字证书 / 57

3.4.1 数字证书: 证明信息合法性 / 57

3.4.2 数字证书修补数字签名 / 58

3.5 密码学技术: Merkle 树 / 60

第4章 基本的发展方向——全球化的大数据体系 / 63

4.1 当下的大数据时代 / 64

4.1.1 数据的来源 / 64

4.1.2 数据催生出大数据 / 66

4.2 大数据的应用价值与困境 / 68

4.2.1 大数据的应用价值 / 68

4.2.2 大数据的困境 / 71

4.3 大数据与区块链之异同 / 74

4.4 互联互通, 区块链重建大数据产业 / 76

4.4.1 区块链 + 大数据: 在区块链中使用大数据技术 / 76

4.4.2 大数据 + 区块链: 在大数据中使用区块链技术 / 77

第5章 区块链率先踏入金融领域 / 79

- 5.1 传统金融业、互联网金融与新金融 / 80
 - 5.1.1 传统金融业 / 80
 - 5.1.2 互联网金融业 / 81
 - 5.1.3 新金融业 / 82
- 5.2 互信共识与数字货币 / 85
 - 5.2.1 货币阶段史的发展 / 85
 - 5.2.2 基于区块链的数字货币 / 86
 - 5.2.3 数字货币的弊端 / 88
- 5.3 泛中心化的网络支付 / 89
 - 5.3.1 区块链的支付功能 / 90
 - 5.3.2 泛中心化的支付案例 / 91
- 5.4 区块链实现股权众筹 / 94
 - 5.4.1 众筹与股权众筹 / 95
 - 5.4.2 基于区块链技术的股权众筹模式 / 98
 - 5.4.3 基于区块链技术的股权众筹优势 / 101
- 5.5 互联网征信新模式 / 104
 - 5.5.1 征信的起源与发展 / 104
 - 5.5.2 互联网征信的模式与特点 / 106
- 5.6 基于区块链与大数据的互联网征信 / 108
 - 5.6.1 区块链征信的数据管理 / 108
 - 5.6.2 区块链征信的网络 / 111

第6章 基于区块链架构的商业应用前景 / 113

- 6.1 热点技术: 数字资产管理 / 114
 - 6.1.1 实物资产、权益资产以及数字资产 / 114
 - 6.1.2 数字资产的属性与资产数字化的原因 / 116
 - 6.1.3 区块链数字资产时代 / 117
- 6.2 虚拟变现实之物联网 / 117

- 6.2.1 互联网的延伸——物联网 / 118
- 6.2.2 物联网的局限与不足 / 119
- 6.2.3 区块链技术中的物联网 / 121
- 6.2.4 区块链技术中的物联网案例 / 122
- 6.3 区块链助力共享经济, 新经济的 DNA / 124
 - 6.3.1 共享经济存在的问题 / 124
 - 6.3.2 区块链技术与共享经济 / 125
- 6.4 理性的繁荣: 全球智能经济的兴起 / 127
 - 6.4.1 区块链与人工智能的共生 / 128
 - 6.4.2 人工智能将改变区块链 / 129
 - 6.4.3 区块链将改变人工智能 / 130
 - 6.4.4 自动驾驶与区块链技术的碰撞 / 131
- 6.5 立体供应链结构 / 132
 - 6.5.1 供应链的局限性 / 133
 - 6.5.2 区块链弥补供应链 / 135

第 7 章 区块链链接万物: 人类社会的新型契约 / 137

- 7.1 公证与认证不再是难题 / 138
 - 7.1.1 传统公证系统的弊端 / 138
 - 7.1.2 区块链能够弥补传统公证系统的不足 / 140
 - 7.1.3 身份认证不再是问题 / 141
- 7.2 知识产权的管理 / 143
 - 7.2.1 知识产权中的痛点 / 144
 - 7.2.2 区块链技术有助于保护知识产权 / 145
 - 7.2.3 区块链保护知识产权的应用案例 / 148
- 7.3 聚沙成塔式的分布式云存储 / 150
 - 7.3.1 区块链的分布式云存储 / 150
 - 7.3.2 云存储平台——Storj / 152
- 7.4 天才的设计: 区块链与能源 / 153

- 7.4.1 电力能源应用普遍现状 / 153
- 7.4.2 区块链在能源行业的应用 / 155
- 7.4.3 Transactive Grid 能源传输项目 / 157

第 8 章 可设计的蓝图：区块链有望颠覆全世界 / 159

- 8.1 区块链与大数据实现技术新融合 / 160
 - 8.1.1 区块链融入数据开发、分析与交易 / 160
 - 8.1.2 打造区块链网络平台 / 162
- 8.2 智能合约与大数据，有望促进社会共治 / 163
 - 8.2.1 小数据时代的“随机调研数据” / 163
 - 8.2.2 大数据预测，区块链变现 / 164
- 8.3 区块链领跑金融新趋势 / 166
 - 8.3.1 世界各国将区块链技术引入金融行业 / 166
 - 8.3.2 区块链新金融实验室致力研究区块链新金融项目 / 167
- 8.4 “互联网+”与“区块链”共同打造新金融 / 168
 - 8.4.1 “互联网+”双向创新新金融 / 169
 - 8.4.2 区块链与“互联网+”共同创造新金融 / 169
 - 8.4.3 新金融将完善金融生态圈 / 171

第 9 章 可预计的未来：下一个数字时代的新框架 / 173

- 9.1 区块链将引领数字经济变革 / 174
 - 9.1.1 数字经济逐渐渗入到人们的日常生活中 / 174
 - 9.1.2 区块链助力数字经济发展 / 175
 - 9.1.3 京东将在数字经济领域开展区块链技术的应用 / 177
- 9.2 区块链技术将参与与下一代物联网架构 / 179
 - 9.2.1 沃尔顿与“沃尔顿链” / 179
 - 9.2.2 “沃尔顿链”与价值物联网 / 181
- 9.3 区块链将缔造一个崭新的共享经济 / 184
 - 9.3.1 区块链拓宽共享领域 / 185

- 9.3.2 将区块链技术应用到共享经济的案例 / 186
- 9.4 区块链中的未来能源互联网 / 187
 - 9.4.1 智能合约技术与能源互联网 / 188
 - 9.4.2 美国公司 Filament 的“龙头”试验 / 190

后记 / 193

第1章

区块链技术：人人有本流水账

如今，随着互联网的快速发展，使用移动互联网开展的金融交易日益增加，人们更加关注资金使用效率和资金支付安全。区块链技术作为一项新兴的去中心化技术，通过数学算法建立共识机制，具有信息加密不可更改，分布式存储、交易效率高等优点，因此受到社会各界日益广泛的关注和重视，并吸引了越来越多的人积极探索、创新和应用。

但是，该如何理解区块链的形成呢？这就要从区块谈起，本章介绍区块和区块链的构成，以及具有数据库和账本功能的区块链。

本章导读：

- 存放数据的集成块——区块
- 区块的延续发展——区块链
- 区块链的分类与应用
- 静态区块链技术，略有变化的数据库
- 动态区块链技术，神奇的账本

1.1 存放数据的集成块——区块

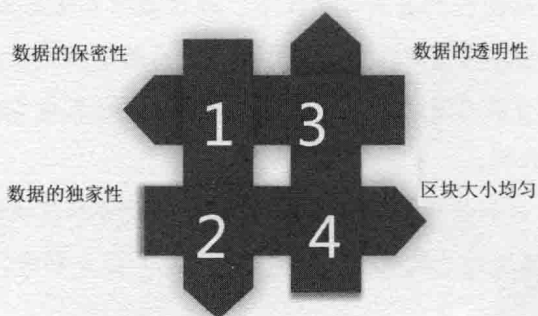
关键词：区块、集成块、存储

主要内容：区块可以用来存放数据

讲区块链技术，必然先要讲区块。

什么是区块？区块是存放交易数据的一个集成块，就像是一个虚拟的、专门用来存储交易数据的盒子，也像是数据库里的一个记录了一些交易的表，或者像是传统的记录交易的流水账里的一页。

当然这个区块也是盒子，也或者是表或者是页，总之它有一点特殊，其特殊之处如图 1-1 所示。



• 图 1-1

(1) 数据的保密性：即里面存储的数据只要是写进去了就不能改动。

(2) 数据的透明性：即里面存储的数据是谁都可以看得到，看得真切，看得完全。

(3) 数据的独家性：即里面存储的数据都是独一无二的，绝对不能重合。

(4) 区块大小均匀：即每个区块的“个头”都差不多，有限的尺寸，绝不能超标。目前，区块大小的限制是 1MB，未来有望扩容到 2MB。

区块的四个特点即为区块的本质，是区块有别于其他存储方式的根本。

1.2 区块的延续发展——区块链

关键词：区块、区块链、链接

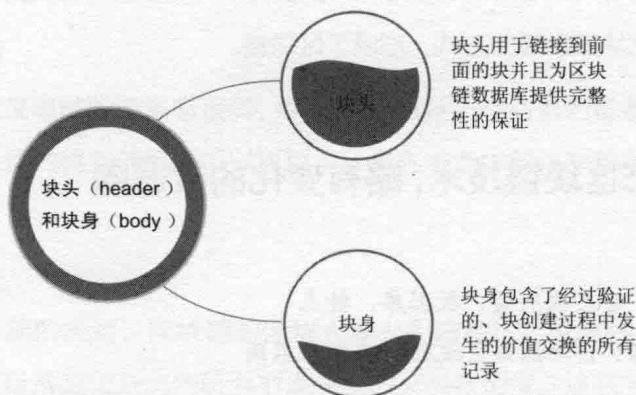
主要内容：区块可以构成区块链

若是将区块的概念放入区块链中，就是数据以电子记录的形式被永久存储下来，区块是存放这些电子记录的文件。同时，区块是按时间顺序一个一个先后生成的，每一个区块记录下它在被创建期间发生的所有价值交换活动，所有区块汇总起来形成一个记录合集。

但区块是如何构成区块链的呢？这就不得不提到区块结构。

区块结构是组成区块链的基础构造，所有区块汇总中，就包含了区块结构，区块中会记录下区块生成时间段内的交易数据，区块主体实际上就是交易信息的合集。

每一种区块链的结构设计可能不完全相同，但大结构上都可以分为块头（header）和块身（body）两部分，如图 1-2 所示。



• 图 1-2

这种区块结构有两个非常重要的特点：第一个特点，每一个区块上记录的交易是上一个区块形成之后，该区块被创建前发生的所有价值交换活动，

这个特点保证了数据库的完整性。

第二个特点，在绝大多数情况下，一旦新区块完成后被加入区块链的最后，则此区块的数据记录就再也不能改变或删除，正是这个特点保证了数据库的严谨性，即无法被篡改。

所以，区块链就是区块以链的方式组合在一起，以这种方式形成的数据库叫作区块链数据库，也就是说，区块链是系统内所有节点共享的交易数据库，这些节点基于价值交换协议参与到区块链的网络中来。

因为每一个区块的块头都包含了前一个区块的交易信息压缩值，这就使得从创世块（第一个区块）到当前区块连接在一起形成了一条长链。

但是，如果不知道前一区块的“交易缩影”值，就没有办法生成当前区块，因此每个区块必定按时间顺序跟随在前一个区块之后。

正是这种所有区块包含前一个区块引用的结构让现存的区块集合形成了一条数据长链。

“区块 + 链”的结构为我们提供了一个数据库的完整历史，从第一个区块开始，到最新产生的区块为止，区块链上存储了系统全部的历史数据。

区块链为我们提供了数据库内每一笔数据的查找功能。区块链上的每一条交易数据，都可以通过“区块链”的结构追本溯源，一笔一笔进行验证。

由此，区块就以链的方式，形成了区块链。

1.3 静态区块链技术，略有变化的数据库

关键词：静态区块链、数据库、特点

主要内容：区块链与传统数据库存在不同

上一节中我们了解了什么是区块链，区块链就是给区块加上链，利用数据短链把一个个的区块连接起来，形成一个完整的链状数据存储结构。也就像是用铁链穿起来的一串小盒子，以链的方式连起各个表构成的数据库。