BLOCK CHAIN

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

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

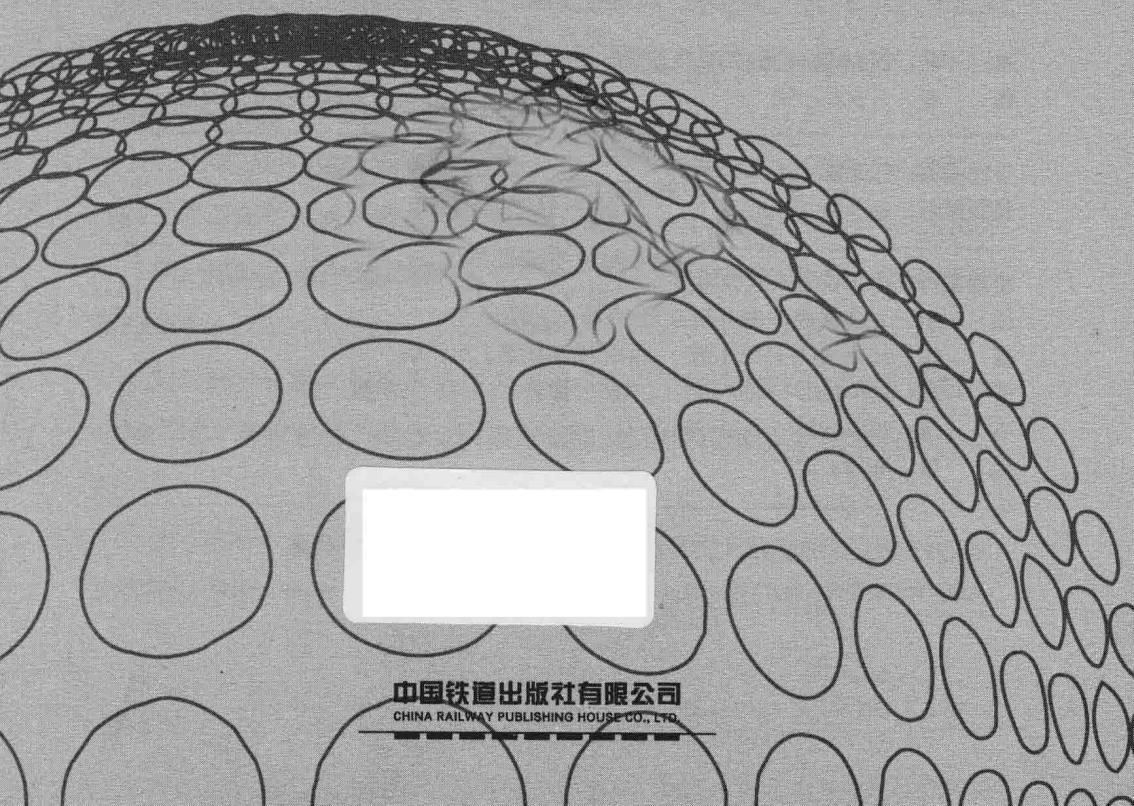
多维度阐释区块链、人工智能、加密经济学、大数据的关联与应用

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　　**读者热线电话：**010-63560056
责任印制：赵星辰　　**封面设计：**MX 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：700 mm×1 000 mm　1/16　**印张：**12.75　**字数：**196 千
书　　号：ISBN 978-7-113-25478-0
定　　价：49.00 元

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：MXX DESIGN STUDIO QQ:1766623429

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

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

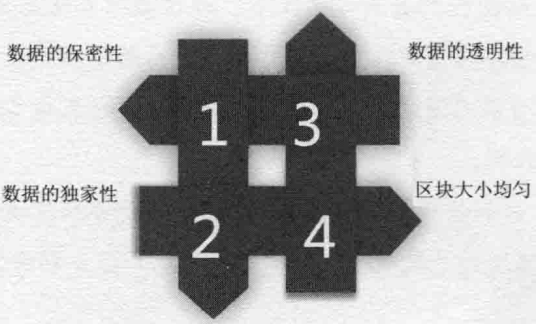
关键词： 区块、集成块、存储

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，有限定的尺寸，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

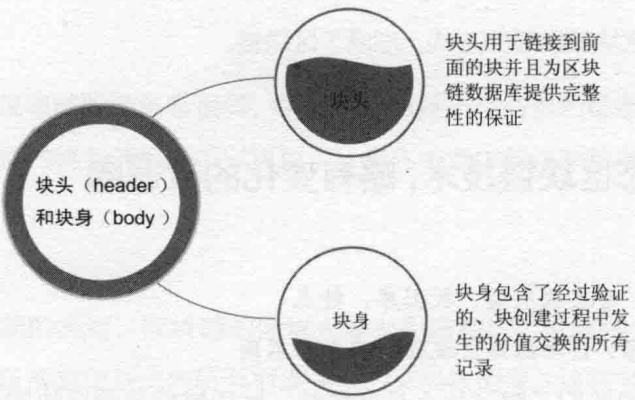
主要内容： 区块可以构成区块链

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。