BLOCK CHAIN PRACTICE

区块链实战

吴为◎著

数字货币、金融、物联网、大数据、医疗、教育、公证等七大领域应用实例

为了不被时代淘汰，请用一周时间，读懂区块链

清華大學出版社

BLOCK CHAIN PRACTICE

区块链实战

吴为◎著

清华大学出版社
北京

内 容 简 介

本书全景式地描述了互联网前沿技术——区块链，分别从区块链的起源、区块链在全球各个国家的发展现状、区块链的四大核心技术、基于区块链底层技术的数字货币发展现状等角度进行描述。另外，为了更好地理解区块链，本书讲述了区块链在数字货币领域、金融领域、物联网领域、大数据领域、医疗领域、教育领域、公证领域等七个领域的应用。

区块链是一场技术革命。在不久的将来，我们会看到区块链与传统行业的直接较量。而且这是一场不同层面的竞争，传统行业被新技术取代已成必然趋势。所以在一切还未发生之前，关注区块链、参与区块链、应用区块链是至关重要的。

通过阅读本书，读者只需要花费一周的时间就可以理解区块链是什么以及它能干什么，并且理解区块链在各个领域的价值所在。

图书在版编目（CIP）数据

区块链实战 / 吴为著. — 北京：清华大学出版社，2017
ISBN 978-7-302-47589-7

Ⅰ. ①区… Ⅱ. ①吴… 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（2017）第 146671 号

责任编辑： 刘 洋
封面设计： 李召霞
版式设计： 方加青
责任校对： 王凤芝
责任印制： 王静怡

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： 三河市金元印装有限公司
经 销： 全国新华书店
开 本： 170mm×240mm 印 张：14.75 字 数：262 千字
版 次： 2017 年 9 月第 1 版 印 次：2017 年 9 月第 1 次印刷
定 价： 49.00 元

产品编号：075513-01

Block chain practice

前　言

2017 年 2 月，中国人民银行（简称央行）研究并测试数字票据交易平台的事件轰动了全球，该数字票据交易平台应用的基础技术就是区块链。此外，央行旗下数字货币研究所也在 2017 年上半年正式挂牌成立。这意味着中国人民银行成为全球范围内首个研究数字货币并将数字货币应用于真实生活的中央银行，并率先探索区块链技术在货币发行领域的应用。

那么，央行建立区块链数字票据交易平台对我们的现实生活会产生很大影响吗？答案是肯定的，大家可以想象一下：两三年以后，过年发红包不再是纸质钞票，而是一串串的数字密码，我们可以通过发送邮件、复制到 U 盘里或者通过手机直接将其发送给他人。

关于央行开发数字货币的原因，央行参事盛松成称：“未来的央行数字货币会从多个方面倒逼金融基础设施建设，让我国支付体系进一步完善，支付结算效率进一步提升。更值得一提的是，央行数字货币最后可以构成大数据系统，使经济交易活动的便利性和透明度进一步得到提高，这将有利于货币政策的有效运行和传导。”

在央行的积极带动下，我国各方资本纷纷在区块链行业布局。截至 2016 年年年底，平安银行、招商银行、民生银行都已经加入 R3 区块链联盟。截至 2017 年年初，我国 A 股市场上切入区块链概念的公司已经有 24 家，大部分公司是软件和信息技术提供商。

各大行业巨头公司也不甘落后。其中，万向集团建立了区块链实验室，华为加入了 Linux 基金会领导的超级账本区块链项目。另外，百度、光大投资管理公

司、中金甲子、宜信等机构向一家美国比特币初创公司投资了 6 000 万美元。

从全球范围来看，包括纳斯达克、花旗、Visa 在内的金融行业大咖也向区块链领域大把大把地砸钱，它们联合投资了一家区块链初创公司 Chain，涉及金额高达 3 000 万美元；花旗、摩根大通等金融机构还向一家区块链初创公司 Digital Asset 投资 5 000 万美元。

如今，各方都对区块链表示出极大的关注度，区块链技术正在从一片巨大的蓝海转变为一片巨大的红海。那么，区块链凭借什么魅力受到了全球关注呢？以金融业票据清算系统为例，区块链将从以下四个方面发挥作用。

第一，消除了票据中介角色。在应用了区块链技术之后，票据价值可以实现 P2P 无形传递，既不需要特定实物作为连接双方取得信任的证明，也不需要第三方对交易双方价值传递的信息做监督和验证。另外，票据交易双方常常需要通过票据中介来解决信息不对称问题，而借助区块链实现 P2P 交易后，票据中介的现有职能将被消除。

第二，防范票据市场风险。不透明、不规范以及高杠杆错配等潜规则使票据市场的风险频发，参与机构的多样性和逐利性也加大了这一风险。而区块链技术全网公开、数据不可篡改的特性可以防范道德风险；分布式系统无须第三方中介的特性完全避免了人为操作风险；自动控制参与者资产和负债两端平衡且数据公开透明的特性有利于控制市场风险。

第三，建立去中心分布模式的电子商业汇票系统。现有的电子商业汇票系统（Electronic Commercial Draft System，ECDS）是一个中心化系统，其中心为央行，其他银行和企业通过直连或网银代理的方式接入央行的中心化登记和数据交换系统。区块链技术将会改变现有电子商业汇票系统的存储和传输结构，建立去中心分布式模式，还能利用时间戳完整反映票据从产生到毁灭的过程，使每一张票据都可以追溯历史。区块链建立的全新连续“背书”机制将更加真实地反映票据权利的转移过程。

第四，降低了市场监管成本。多样的操作方式使得票据市场的监管变得非常繁杂。监管方式也只能是现场审核，而业务模式和流转则没有全流程的快速审查和调阅手段。

区块链的价值具有无限潜力，不仅仅是在重构票据清算系统方面，也不仅仅是在金融领域。而且区块链红海席卷全球的局势已经基本建立，各种利好也即将降临，那些提前进入区块链行业，提供建设区块链经济最原始资本的人，注定会率先品尝到区块链带来的丰厚回报。

本书特色

1. 内容全面，结构清晰

本书内容包括区块链的起源、发展、应用以及趋势预测，并重点讲述了区块链在金融领域、物联网领域、大数据领域、医疗领域、教育领域以及公证领域的应用。而且全书架构清晰，有助于读者形成框架形式的认知。

2. 案例丰富，实战性强

本书加入很多真实且具有代表性的案例，使内容更加生动有趣。而且案例的加入使理论知识不再枯燥无味，读者更容易接受其中的观点。另外，本书理论与实战相结合，非常适合没有接触过区块链的读者阅读，帮助他们快速入门，深入理解区块链的价值。

3. 语言通俗，更接地气

新概念、新技术类的图书总是被作者包装得高大上，看起来非常有范儿，但实质上却提高了读者的理解门槛。而本书倾向于采用通俗易懂的语言为读者解读深奥的理论，让读者轻松理解与区块链相关的理论、应用等知识。

本书内容及体系结构

第 1 章：讲述了区块链起源于比特币，并对比特币的发行规律、价格变化等作出详细报告，有助于读者理解区块链与比特币的关系。

第 2 章：讲述区块链在人类世界的发展现状，包括各国政府对区块链的积极态度、全国各大企业对区块链应用的投资以及 2017 年最热门的 5 家区块链初创公司。

第 3 章：介绍了区块链的四大核心技术，包括具有去中心化创新、数据高度透明、不依赖信任以及信息可回溯性四大特征的分布式账本技术，用户掌握私钥以及匿名的非对称加密和授权技术，参与者共同维护的共识机制、自动控制，以及自动执行数字承诺的智能合约。

第 4 章：讲述了货币的进化历史以及当前三大数字货币（比特币、以太坊和莱特币）的发展现状，还将比特币与以太坊、莱特币作对比，帮助读者了解各自优势。

第 5 ～ 10 章：分别讲述了区块链在金融领域、物联网领域、大数据领域、医疗领域、教育领域以及公证领域的应用，帮助读者对区块链的价值形成系统

认识。

第 11 章：讲述了区块链技术与物联网、大数据、人工智能等领域深度融合的发展趋势，并分析了区块链将会颠覆传统行业、改变人类世界的发展前景。

本书读者对象

- 各领域企业领导、高管
- 金融科技企业工作人员
- 数字货币相关公司工作人员
- 区块链研究以及开发者
- 对区块链以及数字货币感兴趣的其他人群

参与本书编写工作的人员还有梁萍、李改霞、赵丹丹、李恬、曾丽佳、李雪霞、李卫霞、李艳霞、李伟光、李晓青、游万梅、贾云叶、宋佳佳、龚毅、梁现丽、王逊、鲁宗保、李小菊等。

编者

2017 年 5 月

Block chain practice

目 录

第 1 章 区块链起源

1.1 区块链的发源——比特币 2

1.1.1 数字货币的龙头老大——比特币 2

1.1.2 从“币”到“链”的颠覆 4

1.1.3 区块链与比特币没有极客说得那么复杂 5

1.1.4 给你一台计算机，你也可以创造比特币 7

1.2 疯狂的区块链比特币 9

1.2.1 比特币的发行规律 9

1.2.2 比特币历史价格变化曲线 10

1.2.3 价格一个月涨六成，你见过吗？ 12

1.3 区块链比特币的价格来自价值，而非投机 13

1.3.1 区块链比特币存储于本地 13

1.3.2 网络是区块链比特币的操控者 14

1.3.3 供小于求决定区块链的超高价值 15

第 2 章 区块链——必将颠覆人类世界

2.1 区块链的春天——各国积极表态 18

2.1.1 中国央行表态支持区块链 18

2.1.2 美国政府机构加快布局区块链技术 …… 20
2.1.3 日本视区块链比特币为现金 …… 22
2.1.4 英国央行成公认最“积极”央行 …… 23
2.2 区块链应用的全球进展 …… 24
2.2.1 华尔街各顶级投行对区块链趋之若鹜 …… 25
2.2.2 区块链技术应用前景无限扩张 …… 27
2.3 2017 年最热门的 5 家区块链初创公司 …… 28
2.3.1 “隐形的比特币公司”——Blockstream …… 28
2.3.2 在线零售巨头Overstock创造的区块链交易平台——TØ …… 31
2.3.3 比特币消费类应用程序——OpenBazaar …… 32
2.3.4 搭载比特币的社会化媒体平台——Zapchain …… 34
2.3.5 资金最充裕的比特币挖矿公司——BitFury …… 36

第 3 章 区块链四大核心技术

3.1 分布式账本 …… 40
3.1.1 去中心化创新 …… 40
3.1.2 数据高度透明 …… 42
3.1.3 无须依赖信任的哈希算法 …… 45
3.1.4 银行也抵抗不了的信息可回溯性 …… 48
3.2 非对称加密和授权技术 …… 51
3.2.1 私钥掌握在用户手里 …… 51
3.2.2 匿名，这里可以实现 …… 54
3.3 共识机制 …… 57
3.3.1 工作量证明机制 …… 58
3.3.2 中心维护到参与者共同维护 …… 58
3.4 智能合约 …… 60
3.4.1 以数字形式定义的承诺 …… 60
3.4.2 全面解析智能期权合约 …… 63
3.4.3 票据理财的守护神——数字化契约 …… 65

第 4 章 区块链与数字货币

4.1 货币的终极形态——数字货币……68
4.1.1 货币自身形态进化论……68
4.1.2 数字货币的零通道费用……70
4.1.3 顺应经济全球化趋势的全球流通特性……71
4.2 比特币能买到的酷炫商品……72
4.2.1 午餐用比特币订比萨……72
4.2.2 比特币支付，戴尔、苹果都支持……73
4.2.3 用比特币全额购买特斯拉Model3……75
4.3 数字货币新前沿——以太坊……76
4.3.1 以太坊的发行模式……76
4.3.2 暴涨15倍的以太坊……78
4.3.3 比特币VS以太坊……80
4.4 比特币赚钱效应延伸——莱特币……81
4.4.1 莱特币的发行模式……81
4.4.2 比特币VS莱特币……82

第 5 章 区块链在金融领域的应用

5.1 价值资产符号化……86
5.1.1 将实体世界的资产和权益迁移到网络世界……86
5.1.2 区块链上的P2P交易所……88
5.2 金融业为区块链布局主力……90
5.2.1 支付方式历史演进……91
5.2.2 支付汇款方式变革……93
5.2.3 票据清算重构……96
5.3 受影响的金融机构及案例……97
5.3.1 证券交易所……98
5.3.2 会计审计机构……100
5.3.3 银行体系……102
5.3.4 大型科技企业……104

第6章 区块链在物联网领域的应用

6.1 致力于物联网研究的三大区块链公司……108
6.1.1 最早开发区块链的公司——IBM……108
6.1.2 获500万融资的公司——Filament……110
6.1.3 开发物联网支付方案的物付宝——Tilepay……113
6.2 还未实现万物互联的物联网……115
6.2.1 物联网原理……115
6.2.2 物联网的技术架构……116
6.2.3 物联网开启爆发式增长大门……117
6.3 区块链+物联网……119
6.3.1 传统中心化模式的超高维护成本……119
6.3.2 区块链让物联网真正实现去中心化……120
6.3.3 左手比特币，右手物联网经济……121

第7章 区块链在大数据领域的应用

7.1 大数据分析价值创造模式……126
7.1.1 什么是大数据……126
7.1.2 一切都以数据为依据……130
7.1.3 以萧山警匪案为例看大数据分析的价值……133
7.2 区块链上的大数据更具有可信性……137
7.2.1 区块链与大数据共建未来信用……137
7.2.2 区块链是验证数据出处和精确性的核心工具……139
7.3 区块链可解决数据所有权问题……140
7.3.1 数据所有权本应由数据生产者享有……141
7.3.2 区块链破除大数据孤岛效应……142
7.3.3 Enigma项目助用户售卖数据……143
7.4 区块链助力大数据预测市场……144
7.4.1 Augur预测市场项目已众筹60万美元……145
7.4.2 普林斯顿大学聚焦比特币交易预测市场……147

第 8 章 区块链在医疗领域的应用

8.1 区块链电子病历……150
8.1.1 查询历史医疗数据……150
8.1.2 保存个人医疗记录……153
8.2 DNA 钱包……155
8.2.1 利用区块链进行基因存储……155
8.2.2 私人密钥唯一识别……156
8.3 药品防伪……157
8.3.1 利用区块链“监视”供应链……157
8.3.2 轻松识别假冒药品……159
8.4 蛋白质折叠……160
8.4.1 排除计算机运算的单点故障……160
8.4.2 分布式运算超过计算机……162

第 9 章 区块链在教育领域的应用

9.1 教育数据存储与分享……166
9.1.1 区块链储存教育数据……166
9.1.2 通过加密可与第三方分享……167
9.1.3 索尼全球教育借区块链实现数据加密传输……169
9.2 区块链教育证书检验系统……170
9.2.1 伪造文凭已不再有效……170
9.2.2 学信网存储数据三大弊端……171
9.3 学业成绩水平测试……173
9.3.1 比教务管理系统更智能……174
9.3.2 全球第一所接入区块链技术的学校……176

第 10 章 区块链在公证领域的应用

10.1 身份认证……180
10.1.1 “你是你”很难证明吗……180

10.1.2 区块链造就“世界公民” ····· 182
10.1.3 微软发力区块链的身份认证系统 ····· 185
10.2 产权认证 ····· 188
10.2.1 复杂的传统资产确认程序 ····· 188
10.2.2 可追踪的区块链产权变更 ····· 191
10.2.3 杜绝洪都拉斯的土地所有权纠纷 ····· 195
10.3 公证通 Factom 白皮书 ····· 197
10.3.1 Factom设计目标——真实地记录一切 ····· 197
10.3.2 解决的问题——“证明否定” ····· 200
10.3.3 公证通币430万枚价值54万美元 ····· 201

第 11 章 区块链发展趋势分析与预测

11.1 区块链技术发展趋势 ····· 204
11.1.1 区块链与物联网、大数据、人工智能深度融合 ····· 204
11.1.2 区块链为智慧城市提供原动力 ····· 208
11.2 区块链行业发展前景 ····· 211
11.2.1 这是一场降维性经济战争，财富转移已成必然 ····· 211
11.2.2 巨额资金陆续注入，蓝海变红海 ····· 214
11.2.3 作为底层协议，注将洗牌多个传统行业 ····· 218
11.2.4 待开发应用领域多元化，互联网金融领域大有可为 ····· 219

参考文献 ····· 222

第1章
区块链起源

区块链（Blockchain）的本质是一个不依赖第三方、通过自身分布式节点进行数据存储、验证、传递和交流的网络技术方案，正如一个开放的去中心化的分布式记账本，任何人在任何时候都可以采用相同的技术标准生成信息、延伸区块链。当然，大家要想对区块链有深入了解，必须先要知道区块链的起源。

1.1 区块链的发源——比特币

说到区块链，就不得不提比特币（BitCoin）。比特币诞生于2008年，这时还没有人关注区块链。直到2013年人们才意识到比特币在没有任何中心化机构运营和管理的情况下，依然稳定地运行了将近10年，并且没有出现任何问题。于是，很多人开始注意到比特币的底层技术，即区块链。本节主要介绍区块链与比特币的关系。

1.1.1 数字货币的龙头老大——比特币

数字货币包括数字金币和密码货币，这里只讨论密码货币的范畴。密码货币是一种依靠密码技术和教研技术来创建、分发和维持的数字货币，包括比特币、莱特币、维卡币等。其中，比特币是密码货币之首。

事实上，密码货币的历史很悠久，下面来回顾一下密码货币的发展历史。

1982年，大卫·乔姆（David Chaum）最早提出了不可追踪的密码学网络支付系统，该系统允许一个人发送一串数字到另一个人，而且这个数字可被接收方修改。对加密货币的兴趣以及荷兰历史上对私密性狂热的态度在很大程度上促使大卫·乔姆迁移到荷兰。20世纪80年代末期，荷兰成了密码学和数学研究的温床，而大卫·乔姆也创立了DigiCash，并继续构建依托互联网的加密货币的研究。

尽管大卫·乔姆的研究引起了媒体前所未有的关注，但最后不幸的是，大卫·乔姆和他的公司出现了一些失误，违反了荷兰中央银行的规定。而大卫·乔姆作为妥协，不得不同意公司研发的产品卖给银行。这个调整，给DigiCash公

司带来一个好的预期——试图通过多家银行来创立一个可行的数字现金领域，但最终在 1998 年破产。

在 DigiCash 引起巨大轰动之后，越来越多的创业者试图在这个领域开创一番成就。1998 年，Wei Dai 发表文章称产生了一种匿名的、分布式的电子现金系统，命名为“b-money”。同一时期内，尼克·萨博（Nick Szabo）也发明了“Bit gold”。Bit gold 与比特币的机制非常相似，用户利用竞争解决“工作量证明问题”，然后通过加密算法将解答的结果串联在一起公开发布，从而构成了一个产权认证系统。

Bit gold 是人们公认的“比特币的前身”。随后，哈尔·芬尼（Hal Finney）在 Bit gold 的基础上开发了“可重复利用的工作量证明”。

以上发生的种种引领大家来到了 2008 年。2008 年，“bitcoin.org”域名被悄悄地匿名注册成功。同年 10 月 31 日，一个自称“中本聪”（Satoshi Nakamoto）的人在密码学网站上发表了名为《比特币：一种点对点的电子货币系统》的论文。10 天之后，开源社区 sourceforge.net 上出现了一个叫 bitcoin 的项目。而世界上首批 50 个比特币诞生于 2009 年年初。

中本聪在搭建完比特币体系后似乎就从互联网上彻底消失了，没有人见过他的真正面目。此后，比特币项目由两个前谷歌工程师维护，但即便是这两个人也声称从未见过中本聪。

2010 年，bitcointalk 论坛上用户之间的自发交易产生了比特币的第一个公允汇率。该交易是一名程序员用 10 000 个比特币购买了一个比萨饼。2011 年，维基解密、自由网、Singularity Institute、互联网档案馆、自由软件基金会以及另外一些组织都开始接受比特币的捐赠。2012 年 10 月，全球比特币付款服务提供商 BitPay 发布报告显示，超过 1 000 家商户通过他们的支付系统来接受比特币的付款。

2012 年 11 月，WordPress 博客平台宣布接受比特币付款，还声称比特币可以帮助肯尼亚、海地和古巴等遭受国际支付系统封锁地区的互联网用户购买服务。2013 年 4 月，海盗湾中文网、EZTV 美剧片源网开始接受比特币捐款。同月，中国四川省遭遇雅安地震，公募基金壹基金宣布接受比特币作为地震捐款。

……

截至2017年，比特币已经在全球范围内流行开来。随后，在比特币的带领下，各种密码货币都纷纷崭露头角，走入人们的生活。

1.1.2 从“币”到“链”的颠覆

比特币自诞生之后就陆陆续续吸引了世界各个国家的注意。有了比特币之后，只要有网络就可以完成P2P（个人对个人）交易，不需要借助银行或者其他第三方中介平台。对于投资人来说，比特币就像黄金一样无惧通货膨胀，具有投资价值。

在比特币快速发展的这几年里，与比特币有关的信息一直是人们关注的焦点。比如，比特币价格的涨跌、某快餐店开始接受比特币支付、恐怖分子使用比特币交易、哪个国家政府承认比特币的合法地位，哪个国家反对比特币等。

之后，比特币的发展让其底层技术——区块链——受到了前所未有的关注。人们这才意识到，原来驱动比特币的真正有价值的核心技术是区块链。如果说，比特币对金融秩序的颠覆意义还不够，那么区块链则完全有可能颠覆这个世界。

Chain公司开发了一个以区块链技术为基础的资产交易平台，该平台可以用于市场上任意类型的资产交易，比如货币交易、股票交易、债券交易等；Counterparty、NXT和BitShares基于区块链技术打造的去中心化交易所可以在脱离传统股票交易所的情况下完成股票发行和交易；Guardtime正在研究基于区块链技术的工业级网络安全方面的应用；Holbertson利用区块链技术验证学生的学历，防止学生有学历欺诈行为；Visa和DocuSign致力于通过区块链技术构建汽车租赁市场新商业模式……

未来，如果这些区块链应用全部成为现实并且普遍运用，那么区块链一定会颠覆我们的世界。到时候，如果美国还想试图通过金融封锁的手段制裁一个国家，那么其难度之大可以想象。

区块链之所以具有颠覆意义，是因为它具有以下四个特征，如图1-1所示。

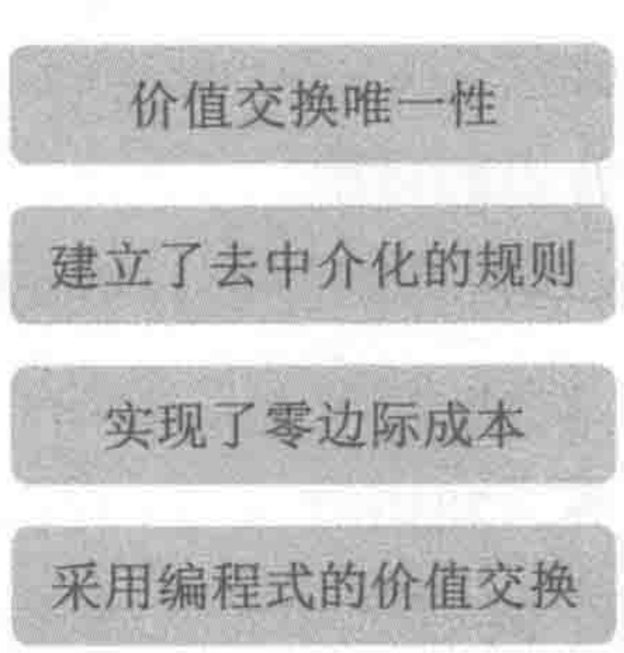

图1-1 区块链的四大特征