区块链

BLOCKCHAIN

技术导论和开发指南

DEVELOPMENT TUTORIALS FOR BLOCKCHAIN

张 雷 过晓星 张春霞 吴新平 编著

科学出版社

国家重点研发计划项目资助(编号：2017YFE0100700)
上海市科学技术委员会科研计划项目资助(编号：18511101400)

区块链技术导论和开发指南

张　雷　过晓星　张春霞　吴新平　编著

科学出版社
北京

内 容 简 介

本书首先介绍了区块链的发展历程，重点阐述了区块链技术体系中相关的数学、密码学和计算机技术；其次围绕着互联网应用，介绍了区块链在金融、能源、医疗、物流、安全等方面的应用价值及其对未来发展趋势的预示。本书在实战技能上安排了在 Ubuntu 系统上软件的搭建、测试和开发指导，为读者学习和研究提供入门知识的同时，也进一步加深了对区块链技术是如何构建去中心化应用的理解。

本书适合所有关注区块链技术的热心读者阅读，在技术层面上不回避比特币，读者可以从本书中找到区块链与比特币的关联与区分，也可以为学习和从事区块链技术开发的读者进一步厘清区块链技术体系和应用发展规律、切实掌握区块链技术的演进和价值的挖掘提供指导。

图书在版编目(CIP)数据

区块链技术导论和开发指南 / 张雷等编著. —北京：科学出版社，2019.1

ISBN 978-7-03-059409-9

Ⅰ. ①区… Ⅱ. ①张… Ⅲ. ①电子商务—支付方式—程序设计—指南 Ⅳ. ①F713.361.3-62②TP311.1-62

中国版本图书馆 CIP 数据核字(2018)第 252186 号

责任编辑：徐杨峰 / 责任校对：谭宏宇
责任印制：黄晓鸣 / 封面设计：殷 靓

科学出版社 出版
北京东黄城根北街 16 号
邮政编码：100717
http://www.sciencep.com

南京展望文化发展有限公司排版
苏州市越洋印刷有限公司印刷
科学出版社发行 各地新华书店经销

*

2019 年 1 月第 一 版 开本：B5(720×1000) 1/16
2019 年 1 月第一次印刷 印张：18 1/2
字数：342 000

定价：80.00 元

(如有印装质量问题，我社负责调换)

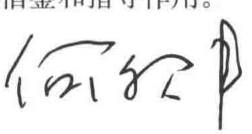
序

目前，全球新一轮产业变革持续深入，国际产业格局加速重塑，创新成为引领发展的第一动力。在此轮变革中，信息技术是全球研发投入最集中、创新最活跃、应用最活跃、辐射带动作用最大的领域，是全球技术创新的竞争高地，是引领新一轮变革的主导力量。

区块链作为分布式数据存储，点对点传输，共识机制，加密算法的集成应用，近年来已成为众多国家政府研究讨论的热点，产业界也纷纷加大投入力度。当前，区块链的应用已延伸到物联网、智能制造、供应链管理、数字资产交易等多个领域，为云计算、大数据、移动互联网等新一代信息技术发展带来新的机遇。在国内，金融企业、互联网企业、IT 企业和制造业积极投入区块链技术研发和应用推广，发展势头迅猛。

近年来，区块链技术和应用在我国引起了多个行业的广泛关注，其应用开发实践在以金融科技为代表的领域逐步开展，并已进入一个快速发展的时期。然而我们也应该认识到，此技术的发展面临机遇和风险并存的局面。近期发生的一系列安全事件，也揭示了区块链技术面临的安全风险和挑战，这要求投入新的技术研发和应用实践来推动区块链技术的成熟。

本书采用深入浅出、图文并茂的阐述方式，将区块链的技术内涵、技术体系、行业应用和开发实践融于一体，由浅入深地引导读者使用和部署区块链产品，并结合区块链在金融、物联网、能源、医疗、物流、教育、安全和公证上的应用，将当前国际上主流的区块链基础措施用于构建行业个体化的区块链。本书内容详实，分析透彻，对广大科技工作者和爱好者把握区块链发展趋势和规律，构建良好的生态圈有重要的价值。同时，本书为未来发展进行预测，并提出了完善相关技术的路线图，相信可为开展区块链研究和应用的广大科技工作者提供借鉴和指导作用。



中国科学院院士

二〇一八年九月五日

前言

区块链作为一种新技术，人们始终心存戒心，就怕它乱了秩序，尤其是一国的金融体系。好在不少学者和战略家讲到，区块链技术和比特币不是一回事！正如前微软（中国）公共事业部战略合作总监刘润在2018年3月的一次论坛上，把区块链技术的“父亲”笑谈为“去中心化”、“母亲”为“互联网”，区块链技术作为家族成员，自己还生出了个“比特币”。如果究其本源，区块链技术可以追溯到2009年中本聪在密码学网站上发表的《一种点对点的电子现金系统》。

有必要简单说说比特币。比特币，本质上是基于分布式记账技术的一种数字现金。在金融表现上，是模拟黄金来发行的，总体量为2 100万枚，开采量每四年减半。“去中心化”这个区块链技术的遗传基因，允许全世界不再需要任何央行就能发展比特币金融体系。显然，这与当下货币主权为核心的国家和社会的金融发展秩序有所违背。但好在区块链技术与比特币不是一回事，区块链技术属于信息技术及其应用领域，值得作为未来的发展主题进行探讨与延伸。

区块链技术世界欢迎不同的建议，哪怕是意见和争议！因为整个信息社会都将关注点放在了“数据”上，基于“数据”产生的任何技术创新体系和应用服务体系，都是一种价值再创造的胜利！与深度学习、大数据、人工智能等技术一样，区块链技术也是一种技术表现形式，并且正处于趋近热点的边缘，锐不可当！

在国内外企事业单位的研究机构中，区块链技术已成为嫁接技术和产业的桥梁。从概念、到技术体系、到产业园，区块链技术正成为创业的技术主题和未来产业结构的重要组成部分。正因如此，本书倾尽心力，将区块链的技术内涵、技术体系、行业应用和技术开发实践融于一体。在区块链技术导论上，本书将其分成技术原理和开发实践两部分。第一部分包含第1～4章。第1章阐述区块链技术发展的历程，着重介绍最早把区块链作为底层技术的比特币的运行原理，以及各种技术演进及其对应的数字代币。第2章阐述区块链技术涉及的底层支撑技术，进而全面理解区块链技术体系。第3章是区块链技术与各个行业的应

用实践，阐述区块链技术的应用价值。第4章是区块链技术及其应用带来的思辨，以及如何完善区块链技术应用体系的思考，为未来的发展进行预测。第二部分是第5章，该章是区块链技术的开发与实践指导，由浅入深地引导读者使用和部署区块链产品，以及开发和使用区块链技术生态中的其他产品；结合若干行业应用，将当前主流的区块链基础设施用于搭建个性化的区块链应用。

2018年，是中国进入新时代的开篇之年，中国作为创新型强国正在崛起，作为经济大国正在调整产业布局。在科学、技术、产业和经济上，活跃着“大数据＋人工智能＋区块链”这个组合，本书也希望借此为社会经济发展尽绵薄之力。

本书得以出版，离不开各方的支持，尤其是比特币资讯网（Bitcoin86）创始人李德福、无锡思内尔网络科技有限公司首席技术官蒋钧杰，高级开发工程师叶伟、蒋相和等的技术支持和代码贡献。整个成书过程，离不开团队与业界专家的无私支持，以及业界区块链创业公司、开源社区朋友的帮助和支持，在此一并致谢。由于作者才疏学浅，精力有限，书中难免有疏漏之处，敬请读者批评指正。在相关文献的参考和翻译区块链技术的著作时，难免存在观点的借鉴和经典论述的直接引用，在此对相关文献的作者致以热忱谢意。也欢迎广大读者针对本书中的观点与我们展开学术研讨。

让我们共同致力于推动区块链技术在中国新时代的发展！

张雷　教授、博士生导师
华东师范大学教育部可信软件国际合作联合实验室主任
二〇一八年七月十六日于华东师范大学丽娃河畔

目录

序 …… i

前言 …… iii

引言——区块链，不仅仅是技术 …… 001

第 1 章　区块链的前世今生 …… 016

1.1　信任机制的探寻——从信息互联网到价值互联网 …… 016

1.2　了解比特币 …… 018

1.2.1　去中心化问题的由来 …… 018

1.2.2　比特币的运行机制 …… 020

1.2.3　比特币挖矿 …… 024

1.2.4　比特币的闪电网络 …… 026

1.2.5　比特币相关的一些疑问 …… 030

1.3　从比特币到区块链 …… 034

1.3.1　下一代区块链——以太坊 …… 034

1.3.2　以太坊的工作机制 …… 036

1.3.3　以太坊中的矿工费 …… 038

1.3.4　基于以太坊的数字版权 …… 038

1.3.5　区块链 2.0——以太坊 …… 040

1.4　区块链 3.0 …… 040

1.5　其他改进的区块链加密数字代币 …… 042

1.5.1　以太坊经典 …… 042

1.5.2　莱特币 …… 044

1.5.3 瑞波币 …… 045
1.5.4 达世币 …… 047
1.5.5 狗狗币 …… 048

第 2 章 区块链的基础技术 …… 052
2.1 区块链的密码学 …… 052
2.1.1 哈希函数 …… 052
2.1.2 哈希指针链 …… 061
2.1.3 Merkle 树 …… 063
2.2 公钥密码算法 …… 065
2.2.1 对称加密 …… 065
2.2.2 非对称加密 …… 066
2.2.3 混合加密机制 …… 068
2.2.4 椭圆加密算法 …… 068
2.2.5 数字签名 …… 072
2.2.6 数字信封 …… 074
2.3 区块链共识机制 …… 074
2.3.1 分布式账本技术 …… 075
2.3.2 拜占庭将军问题 …… 076
2.3.3 共识机制 …… 077

第 3 章 区块链行业应用解析 …… 091
3.1 区块链与金融 …… 091
3.1.1 数字货币 …… 092
3.1.2 跨境支付与结算 …… 095
3.1.3 票据业务 …… 097
3.1.4 供应链金融业务 …… 099
3.1.5 证券发行与交易 …… 101
3.1.6 银行业务 …… 105
3.2 区块链与物联网 …… 107
3.2.1 物联网 …… 107
3.2.2 物联网面临的挑战 …… 109
3.2.3 物联网的好搭档——区块链 …… 111

3.2.4 区块链＋物联网的应用实例 …… 115
3.2.5 区块链＋物联网的产业现状和相关的应用场景 …… 116
3.2.6 区块链＋物联网的应用挑战和对可信标准的需求 …… 122
3.2.7 展望物联网＋区块链的未来 …… 125
3.3 区块链与能源 …… 126
3.3.1 能源行业的发展趋势 …… 126
3.3.2 能源＋区块链 …… 127
3.3.3 海外的能源区块链应用 …… 129
3.3.4 区块链在能源行业的应用前景 …… 130
3.4 区块链与医疗 …… 131
3.4.1 区块链在医疗领域的五大应用 …… 132
3.4.2 国外布局医疗的区块链公司 …… 133
3.5 区块链与物流 …… 136
3.5.1 物流与区块链完美搭配 …… 136
3.5.2 区块链在物流业的应用 …… 136
3.5.3 区块链对物流行业的变革 …… 139
3.6 区块链与教育 …… 141
3.6.1 区块链在教育领域的应用启示 …… 141
3.6.2 区块链技术在教育中的应用模式 …… 142
3.6.3 区块链技术教育应用面临的挑战 …… 148
3.7 区块链与安全 …… 151
3.7.1 区块链与信息安全 …… 151
3.7.2 区块链与大数据安全 …… 153
3.7.3 区块链与网络安全 …… 156
3.7.4 区块链与食品安全 …… 157
3.7.5 区块链安全局限 …… 159
3.8 区块链与公证 …… 161
3.8.1 公证/登记的区块链应用场景 …… 163
3.8.2 区块链公证解决方案 …… 164
3.8.3 企业级的存证解决方案 …… 165

第 4 章 区块链应用的挑战和未来 …… 168
4.1 区块链的技术争议问题 …… 169

4.2 区块链能效问题 …… 174
4.3 区块链应用的监管政策挑战 …… 175

第5章 区块链开发实践 …… 177
5.1 比特币开发 …… 177
5.1.1 比特币软件的安装(以 Ubuntu 为例)…… 177
5.1.2 比特币钱包开发 …… 179
5.2 基于 Peatio 的开源项目进行比特币交易平台搭建 …… 182
5.3 以太坊开发 …… 189
5.3.1 以太坊环境搭建(以 Ubuntu16.04 为例) …… 189
5.3.2 编译和部署智能合约 …… 191
5.3.3 基于以太坊的去中心化应用开发(+Drupal) …… 193
5.3.4 以太坊 JSON—RPC 接口开发 …… 206
5.3.5 以太坊开发实例 …… 207
5.4 基于国内公有区块链开发介绍 …… 218
5.4.1 基于小蚁链开发 …… 219
5.4.2 基于元界开发 …… 267

参考文献 …… 281

后记 …… 284

引言——区块链，不仅仅是技术

一

大家都认为，区块链是一种技术。

对，区块链是一种技术！

也不对，区块链所应用的领域，基本上已经脱离了技术本身的优势范畴，更多的是探讨其社会（阶级）属性。区块链是一种社会属性非常明显的技术。

两种说法的立足点不同，但都没有错，所以无须争论，就像无须拿泰迪的颜色来争论其胖瘦一样。

技术的社会属性，是很多技术人员都忽视的，也被很多使用者忽视，这是极大的损失。我们推崇备至的名词“商业模式”，究其根本是让技术发挥其社会属性罢了。

我希望帮助读者在区块链技术本身及其应用的学习和使用中，更多地用社会属性视角来审视技术，如此就会发现不一样的世界。回看互联网、物联网、P2P 等，一切技术的兴衰，都源于技术催生的社会属性的适应性变化。

区块链是一种非常有趣的技术，因为它能更容易帮助人们建立技术的社会概念，让人们把它当作打开理解所有技术的思想钥匙。或许，这可以从本书开始！

二

每当我们准备创新的时候，都觉得似乎所有的公理和公式，所有的技术和模式好像都被发明或发现了！可忽然微信圈又被各种奇迹的创造刷屏，我们又似乎觉得不断地在错过时代，被时代抛弃！如果你有这种感觉，我觉得你要看看区块链了！

我们正站在新变革来临的边缘，互联网正在经历去中心化的阶段。

密码学领域和去中心化计算网络经历了 20 年的科学研究（图 0-1），在这缓

慢的发展过程中，有过不断的尝试和失败。然而，一个偶然的尝试产生了新的进展，区块链(blockchain)技术诞生了！区块链技术一开始就有着从底层改变社会运转方式的力量的基因。这也正是区块链技术在整个发展过程中夹杂的最复杂的情感。我想，这也就是中本聪一直不愿意也不会被世人所认识的主要原因。中本聪被区块链加密了，躲过了全世界的好奇心。

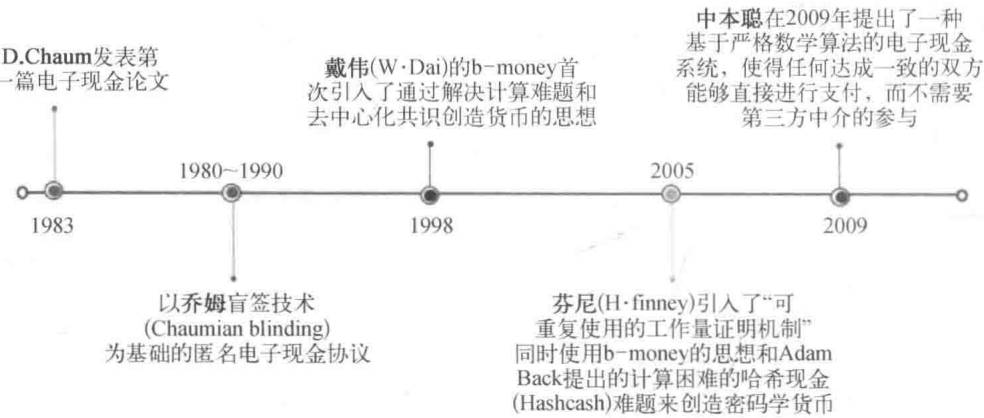


图 0-1　去中心化电子货币发展历程

互联网用长尾改变了人类和资源的组织方式，创造了一个又一个商业神话。当一个个大佬和帝国形成，看似中原已定的时候，人们开始布局下一个时代：数据技术(data technology，DT)＋人工智能(artificial intelligence，AI)。但这时区块链呱呱坠地了！有人说区块链是公共账本，有人说区块链是新的信任和信仰，有人说区块链是民主，也有人说区块链是 P2P。太神奇了，这些都是区块链！但是这些视角都无法帮助人们去思考区块链的现状和未来。如果从阶级的角度分析，从信任和安全的维度来考量，区块链具备了民间信任自治和交易安全自由的力量。这种力量，是真正民主无为而治的力量，是庶民的胜利！这种革命性的技术可能直接导致资源的重组和重新聚合。资源在不同阶级之间大规模流动，形成新的形形色色的阶层。就和商鞅变法的力量一样，会导致各种民间力量新贵的崛起，这种趋利性(就和飞蛾趋光性类似)和区块链技术两股牵引力量可能在不久的将来使区块链超过 DT＋AI，因为重组的阻力远远小于创造。

区块链用安全创造了信任，区块链将是庶民的魔戒，一定会被戴上！

三

比特币！

对，就是比特币！也叫数字货币！

它太显眼了，让人们把它与区块链等同！更多的人则是对比特币耳熟能详，对区块链却未曾听闻！

有人说，它是荷兰的郁金香，不值钱，但很贵！

但它目前的确已经成为区块链社区的硬通货！

为什么会这么矛盾着，又强劲地存在着？

区块链技术将对社会资源起到部分重组和重新聚合的作用，而且在区块链技术社会属性充分发挥作用之前，这种强劲将持续保持！逐鹿中原时期的马匹和刀剑就是重要资源。比特币的崛起，佐证了安全带来的信任的可靠性！区块链就是逐鹿中原的利器！

比特币是基于第一代区块链技术，但区块链却没有停留在比特币的光环里，它在飞速发展，很快就会和比特币分手，在不同的领域如金融、安全、能源、医疗、供应链、大数据等里面找到自己的佛像。区块链的时代，将终结比特币时代！或者说，区块链将亲手将自己的第一尊佛像终结！

区块链和比特币，从一个概念而来，终将分道扬镳！

— 四 —

任何时代的浪潮，都会有一批粉丝参与，但是参与者都带着不同的目的，而利益永远是最基础的目的。马克思曾经说过："……为了100%的利润，资本就敢践踏一切人间法律；有300%的利润，资本就敢犯任何罪行，甚至冒绞首的危险。"

2015年年底的时候，中国数字货币首次币发行(ICO)市场逐渐兴起，2016年年底到2017年则开始出现井喷现象。图0-2为数字代币ICO募资金额数据。

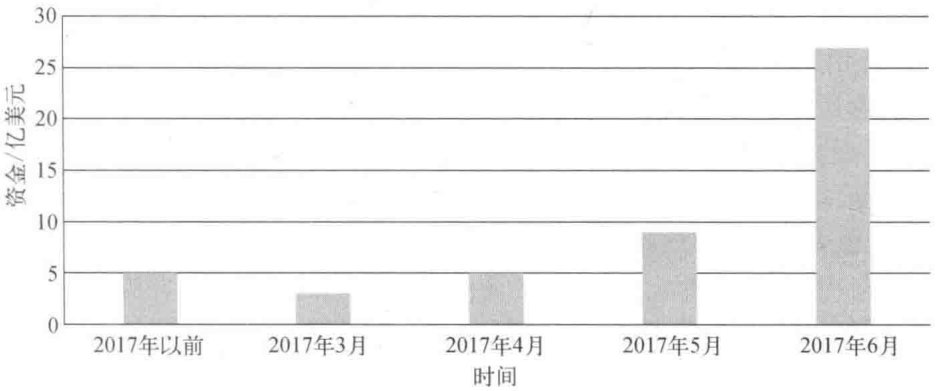


图0-2　数字代币ICO募资金额

然而，ICO 存在诸多潜在风险，包括项目失败或募资团队跑路导致的资金损失风险、价格剧烈波动引起的金融风险、借 ICO 进行的诈骗、非法集资等违法犯罪风险等。出现这样的风险，根本原因是门槛低、缺乏监管，所以在以 ICO 为服务的相关组织的影响下引发了财富效应。

中国人民银行、中央网信办、工业和信息化部、工商总局、银监会、证监会和保监会六部委于 2017 年 9 月 4 日联合发文《关于防范代币发行融资风险的公告》，终止了 ICO 的疯狂。

这个过程对行业的发展造成了非常大的负面影响，不仅对从业的技术人员，而且对关注这个行业的真正的价值投资者也带来了极其悲观的预期。

我觉得我们应该理性地对待数字货币 ICO 事件。通过 ICO 进行诈骗和非法集资与 ICO 和区块链技术的合理性本身没有必然的逻辑。就好像化妆品和养生内容同样可以被诈骗和非法集资活动所利用，但不能因此就全面否定化妆品和养生内容本身的合理性。可惜的是区块链到目前为止，还没有一个非常成功的应用让大众所熟识，所以 ICO 事件造成了一些坏的影响。ICO 的疯狂已经像癌症一样发展得超出控制，而国家的一剂猛药就像化疗一样，终结了癌细胞，也把正常的细胞变得非常孱弱。但两害相权取其轻者，这是国家目前能做的最好的决定。

我想，接下来区块链在等待一个在国家相关立法并鼓励“沙盒”创新的时期，过了这个时期，区块链将一切坦途！

— 五 —

区块链技术中的任何一项技术，都没有划时代的进步，但神奇的是，把它们放到一起，就产生了划时代的技术。并且以此为基础的比特币运作得非常好，从实践上证明了技术的可靠性。

比特币的成功，打开了潘多拉之盒，它向人们昭示着未来。

比特币是分布式中的一致性达到业务安全的水准的奇点事件。奇点是开启新的世界的临界点！

下面三项技术是奇点的基因，它们的组合造就了神奇的区块链技术。

1. 去中介（中心化）的信任（匿名）

信息在时空上被标记，从一个区块打包传递到另一个区块，并被无限全套复制传播到网络的所有节点，从而让信息无处不在。这种去中心化的设计让单纯的互联网信息传递变得有价值，进而建构出“信任”网络。去中心化的赋权，让以权力和权威为支撑的中心体系瓦解，从而为理想主义最极致的无中心合作在网

络上完成了制度的设计。

从哲学的角度看，用“备份”中心的方式达到去中心化的效果，不能不说是概念的胜利！

那么解决去中介的信任有什么意义呢？

思考一下人类的个体关系问题。你或许马上会想起销售界的一句名言，每个人（客户）后面都有 250 个人（潜在客户）。的确是这样，不过很不幸，你所“认识”的人，不会比这个数量多多少。那么，你是如何感觉到已经融入了整个人类社会的？那就是通过中介，让人产生信任感的中介，去与陌生的第三方发生关系。除了与你“熟悉”的 250 个人建立的合作关系，以及平时的货款两讫的小额交易业务之外，你的其他社会活动都是通过中介来完成的。这样做的基本动机就是通过中介获取信任。

去中介化不是解决中介是否要存在的问题，而是在没有中介的情况下，做到和有中介一样的信任过程和良好的产出。这里首先要弄清楚的是，并不是所有事情都可以去中介。区块链给世界带来的变化是提供了以 P2P 方式产生信任的手段，或者说区块链就是两个毫无信任基础的人的中介。由此，它将改变人类活动的原有方式，更多的中介化服务将受到影响，同时，本身存在中介需求但是没有中介为之服务的长尾需求，将随着区块链应用的发展风起云涌。在转移和新创需求的过程中，随之而来的是巨大的财富。

2. 强安全的共识机制

区块链中的交易可以在没有可信第三方的情况下完全按照协议规则执行。第一代互联网的基础协议是 TCP/IP 协议，这个协议保证了传递信息时信道的可靠性，却没能解决信息是否真实的问题。而要想解决这个问题，计算机就需要克服著名的“拜占庭将军”问题，即假设一群将军需要达成在同一时间进行攻城的共识，各比特（bit）将军互不信任且存在叛徒，但只要保证叛徒不大于将军总数的 1/3，计算机就存在一个算法，能保证将军达成的共识是真实的，而区块链则通过共识算法来为这一问题提供可靠的解决方案。

共识机制是分布式领域中的一个概念。想象有一天，共识机制通过不断发展，最终像 TCP/IP 协议一样，被研发到新一代基础网络中变成基础协议，那么整个互联网既实现了通信的可靠性，又解决了信息的真实性，网络社区可以简单通过新一代网络快速构建去中心化的信任社区，那将是多美好的一天。

3. 交易公开透明且不可篡改

区块链中所有的数据记录公开透明，对所有的参与方提供设计功能，并且数据不可篡改。这种技术不仅确保了数据的正确来源，也确保了数据在中间过程

不被人拦截。

把数据从简单的传输，放到一个具有整体逻辑的框架下进行传输，能达到强容错、强自我修复的效果，规避了直接通过网络物理层和协议层寻址的网络安全隐患，是一个划时代的创举！

区块链还有很多特性，但我认为上面三点是区块链比较重要的三个特性，也是最彰显社会属性的三个特性。这三个特性独立存在，且又互相依赖。

— 六 —

人是矛盾的动物，同时崇拜着远古和未来。

区块链技术一定会被过度解读，因为它是配得上被崇拜的新技术。

在阅读区块链的书籍和文章的时候，千万不要被催眠。很多概念都是值得推敲的。

(1) 安全性。产生比特币的 SHA - 256 哈希算法的一个哈希碰撞大约需要 2^{48} 年。这句话现在来讲并没有错，但是它基于两个前提：一是基于目前计算机的计算速度；二是用枚举的方法进行计算。如果前提不存在了，或者变了，那么安全性就没了，或者变弱了。

(2) 密钥安全。密码技术是区块链的核心技术之一，保证了区块链不可逆，不可伪造。因此，密码技术中密钥的存储、传输等安全风险在区块链中同样存在。区块链没有第三方，私钥由每个用户各自保管(比特币使用的是冷存储离线保存)，若用户的存储设备感染病毒，则可能会导致私钥丢失，一旦私钥丢失，则相当于用户失去了对自身数据或者资产的控制权。区块链由于去中心化，没有私钥补发与管理机制，私钥一旦丢失即无法找回。

(3) 隐私保护。区块链的隐私保护也存在安全性风险。一个区块的数据中，包含了所有交易的记录以及账户身份信息，交易信息在区块链中是公开的，账户身份信息是通过非对称加密算法加密的。所有人都可以获取到，因此如果交易信息存在一定的敏感性，那么就存在一定的风险。另外，区块链系统内各节点并非完全匿名，而是通过类似电子邮件地址的地址标识(如比特币公钥地址)来实现数据传输。虽然地址标识并未直接与真实世界的人物身份相关联，但区块链数据是完全公开透明的，随着各类反匿名身份甄别技术和大数据技术的发展，通过数据整合分析可能实现部分重点目标的定位和识别。

(4) 51%攻击。人们都说，没有一个人能拥有 51%的运算能力。这句话并不是所有人都相信。于是他们又说，即使有政府集全国之力秘密造出一台超级

计算机，用来击溃比特币来挽救自己的货币发行体系，它会发现使用该能力进行挖矿便可垄断比特币的发行权，其收益远大于击溃比特币，击溃比特币挽救自己货币发行体系动机也就不复存在了。

了解事物的边界或局限性往往比了解事物本身更重要。

技术的局限性一般也决定着技术应用的边界。

—七—

有局限性的技术，未必是坏技术。或者反过来说，没有一种技术不存在局限性。区块链的出现，将从社会组织关系开始，在数据组织关系、商业逻辑等方面改变人们的生活。在阅读本书前，读者可以先身临其境地看一下几个领域的应用，感受一下黎明的曙光。

1. 物联网

物联网龙头纷纷开始布局区块链。Forrester Wave(物联网软件平台)2016年第4季度的报告显示，IBM、PTC、GE和微软已成为占据物联网平台市场的主导企业。IBM、微软、亚马逊和SAP都在各自的云平台上提供区块链服务(blockchain-as-a-service)，为未来海量的物联网设备接入提供弹性资源池做了超前布局。其中最引人瞩目的项目莫过于IBM和三星合作研发的物联网基础设施平台Adept，它将使用三种不同的技术来解决物联网面对的技术和经济问题；而GE和Cisco更多的是关注设备的标识和存证问题。

2. 银行业

从现代银行的本质来说，银行起到了一个存储、信任的中介结构的作用，所有的金融服务都基于此延伸。除了拥有对实物货币的存储功能之外，区块链作为一种数字化的手段，利用其安全、强制信任，以及防篡改的账本的特点达到了类似的效果，同时不需要担心银行自身的信任崩塌问题。例如，埃森哲公司作为全球较大的审计和财务商务流程外包(BPO)巨头，预估全球投行若使用区块链进行银行业的清算结算业务，每年可节省至少100亿美元的成本。另外，他们认为银行未来将会绕开央行的区块链试验直接使用Swift或者Ripple的区块链技术来降低支付的成本和空间。例如，欧洲7家大型银行组成的联盟已选择与IBM携手，搭建和托管一个基于IBM区块链的全新贸易融资平台，并由Hyperledger Fabric提供支持。该平台旨在简化和促进欧洲中小企业国内和跨境贸易流程，同时帮助企业提高金融交易的整体透明度。微众银行副行长马智涛透露，微众银行与华瑞银行联合开发了一套区块链应用系统，可用于两家银行微粒贷联合贷款的结算、清算，如图0-3所示。