◆ IT人士与金融界人士必读
◆ 区块链小白投资入门实操指南

看得懂
学得会
用得着
的区块链入门书

区块链108问

一本书让你读懂区块链

荆　涛◎著

数字货币、智能合约、分布式账本……
用技术重构金融世界，从根本上改变我们的生活。

苹果、谷歌、脸书等各类巨头趋之若鹜

民主与建设出版社

区块链108问

一本书让你读懂区块链

荆　涛◎著

民主与建设出版社

·北京·

图书在版编目(CIP)数据

区块链 108 问 / 荆涛著 . -- 北京 : 民主与建设出版社, 2019.1

ISBN 978-7-5139-2004-9

Ⅰ . ①区… Ⅱ . ①荆… Ⅲ . ①电子商务－支付方式－问题解答 Ⅳ . ①F713.361.3-44

中国版本图书馆 CIP 数据核字 (2018) 第 295361 号

区块链108问

QUKUAILIAN108WEN

出 版 人	李声笑
著　　者	荆　涛
责任编辑	周佩芳
封面设计	李尘工作室
出版发行	民主与建设出版社有限责任公司
电　　话	（010）59417747　59419778
社　　址	北京市海淀区西三环中路10号望海楼E座7层
邮　　编	100142
印　　刷	天津中印联印务有限公司
版　　次	2019年3月第1版
印　　次	2019年3月第1次印刷
开　　本	710 × 1000mm　1/16
印　　张	13
字　　数	220千字
书　　号	ISBN 978-7-5139-2004-9
定　　价	48.00元

注：如有印、装质量问题，请与出版社联系。

前言

区块链和比特币是2018年的热门话题。比特币方面，甚至连其发明人中本聪也成了2018年美国《时代》周刊年度人物的有力竞争者；在2018年1月召开的达沃斯世界经济论坛上，各国首脑和商界领袖讨论最多的就是区块链。

对于普通大众来说，在没分清比特币和区块链的时候，很容易被冲昏头脑：要么一股脑儿杀进币圈，高价抢购各种虚拟数字货币；要么冲进资本市场，一看到区块链概念的股票，就掏钱购买；要么待在各种论坛、峰会上，一头雾水地听台上一群自己也没怎么搞清楚的嘉宾在大谈特谈区块链……

那么，究竟什么是区块链呢？有人认为区块链是一种数据结构，能够用数字方式进行识别和跟踪交易，还能通过计算机的分布式网络共享这些信息，创建分布式信任网络；有人认为区块链提供的分布式账本技术，为追踪资产的所有权和资产转移提供了透明和安全的手段……但这些解释并不能满足我们对区块链的好奇心。

区块链是个相当晦涩难懂的概念，而多数“区块链科普教程”都充斥着大量的技术术语和底层原理介绍，不适合没有技术背景的人阅读。作为一本轻松有趣的区块链科普读物《区块链108问》很好地解决了这个问题。

《区块链 108 问》全面解答了区块链的众多问题，比如区块链和比特币的发展历史、比特币的特点与运行原理、区块链转账原理、区块链产业链上中下游的运作、区块链资产的特点、区块链的技术原理、区块链扩容和分叉、区块链项目分类及应用等。该书不仅将晦涩难懂的抽象概念转化为 108 个问题并做了解答，还延展出许多与各问题密切相关的知识点，让区块链的形象更全面。通过这 108 个问题，读者能轻松了解区块链和比特币。

通常，一个没有技术背景的人，如果想自学这些知识，想大致搞清楚区块链的技术基础、运行原理、过往历史和生态系统，往往需要花一两个月的时间。《区块链 108 问》的目的，就是将这一两个月缩短为一两周，让读者在阅读本书的过程中就能形成对区块链的基本认识框架。

为了方便不懂技术的朋友阅读，《区块链 108 问》尽可能少用术语，力争用通俗易懂的语言，还原区块链的幕后机制。

目录

第01章 区块链和比特币的发展历史

001. 区块链和比特币是什么关系？ / 2

002. 区块链的发展历史与未来趋势是什么？ / 3

003. 区块链 1.0、2.0、3.0 的特点是什么？ / 6

004. 区块链的五个基本特征是什么？ / 7

005. 区块链类型的划分有哪些标准？ / 9

006. 区块链的技术创新与应用有哪些？ / 12

007. 世界各国对区块链资产的态度如何？ / 15

008. 比特币产生的原因和动机是什么？ / 19

009. 比特币“白皮书”是如何诞生的？ / 20

010. 第一个比特币是如何诞生的？ / 22

011. 比特币创始人中本聪究竟是谁？ / 23

012. 中本聪的继任者是谁？ / 24

013. 密码朋克邮件组是什么？ / 25

014. 什么比萨居然能卖到 3 亿元？ / 27

015. 比特币水龙头是什么？ / 28

第02章 比特币及其特点与运行原理

016. 什么是比特币？ / 32
017. 比特币有哪些优点？ / 33
018. 比特币有哪些缺点？ / 34
019. 比特币为什么价格波动大？ / 36
020. 各国对比特币有哪些主要观点？ / 37
021. 比特币和 Q 币有哪些不同？ / 38
022. 比特币与传统货币的区别是什么？ / 40
023. 如何杜绝比特币的非法用途？ / 42
024. 如何保障比特币的安全性？ / 44
025. 比特币的交易原理是什么？ / 45
026. 新手如何试水比特币交易？ / 47
027. 比特币地址、公钥、私钥都是什么？ / 49
028. 比特币节点是什么？ / 50
029. 比特币的数字签名是什么？ / 52
030. 比特币总量为何是恒定的？ / 53
031. 交易的输出和输入是怎样的？ / 55
032. 比特币怎么记账？ / 57
033. 比特币怎么转账？ / 58
034. 比特币转账需要付手续费吗？ / 59
035. 从发出交易到矿工打包需要几步？ / 61
036. 比特币的找零机制是怎样的？ / 62

第03章 区块链转账原理

037. 区块链关键技术及运作原理是什么？ / 66
038. 建立区块链信用系统需要哪些步骤？ / 69
039. 区块链转账流程需要哪些步骤？ / 70
040. 区块链技术支付转账有哪些优势？ / 71
041. 区块链技术处理汇款有哪些优势？ / 73
042. 什么是区块链公开的分布式记账？ / 74
043. 如何保证用户有足够的余额？ / 76
044. 区块链转账为什么能按字节收费？ / 77

第04章 区块链产业链上游——挖矿

045. 区块链挖矿到底在挖什么？ / 80
046. 比特币挖矿机及其特点是什么？ / 81
047. 比特币挖矿机是如何进化的？ / 82
048. 比特币挖矿机有哪些工作步骤？ / 84
049. 如何将挖矿机接入比特币矿池挖矿？ / 85
050. 什么是比特币的矿场？ / 87
051. 比特币矿池及原理是什么？ / 88
052. 算力究竟是在计算什么？ / 90
053. 竞争记账是什么？ / 93

第05章 区块链产业链中游——交易

054. 为什么要投资区块链资产？ / 96
055. 场内交易是什么？ / 98
056. 场外交易是什么？ / 98
057. 如何理解 DEX 的安全性？ / 101
058. 币币交易是什么？ / 103
059. 量化交易是什么？ / 105

第06章 区块链产业链中游——存储

060. 比特币钱包的基本功能是什么？ / 110
061. 何为冷钱包、热钱包、全节点钱包、轻钱包、中心化钱包？ / 111
062. 各类比特币钱包的安全性特点是什么？ / 113
063. 比特币钱包的选择及使用注意事项是什么？ / 117

第07章 区块链产业链下游——支付

064. 区块链是如何变革金融支付的？ / 120
065. 区块链改变移动支付有哪些优势？ / 121
066. 区块链何以重新定义企业支付？ / 123
067. 比特币可以用于支付吗？ / 125
068. 比特币支付有哪些优势？ / 127
069. 支持比特币支付的商品有哪些？ / 128

第08章 区块链到底长什么样?

070. 区块链技术有哪些时间节点及成果? / 132
071. 为什么说区块链是制造信用的机器? / 135
072. 区块是如何连接成区块链的? / 137
073. 区块数据的相关定义有哪些? / 138
074. 为什么说最长区块链才是正确的区块链? / 140

第09章 区块链资产都有哪些特点?

075. 如何理解区块链资产“全球流通”的特点? / 144
076. 如何理解区块链资产“匿名性”的特点? / 144
077. 如何理解区块链资产“去中心化记账”的特点? / 145
078. 如何理解区块链资产“不可复制”的特点? / 146

第10章 区块链的技术原理

079. 区块链的共识机制是什么? / 148
080. 工作量证明机制(POW)是什么? / 149
081. 权益证明机制(POS)是什么? / 151
082. 股份授权证明机制(DPOS)是什么? / 153
083. 哈希算法是什么? / 154
084. 零知识证明是什么? / 156
085. 非对称加密算法是什么? / 158

第11章 区块链扩容和分叉

086. 区块链为什么要扩容？ / 160
087. 区块链究竟该如何扩容比较合适？ / 161
088. 区块链扩容方式有哪些？ / 162
089. 区块链扩容最佳解决方案是什么？ / 164
090. 区块链分叉机制是什么？ / 166
091. 软分叉和硬分叉是什么？ / 167
092. 重放攻击是什么？ / 169
093. 如何防范重放攻击？ / 170

第12章 区块链项目的分类及应用

094. 莱特币是什么？ / 174
095. 新经币是什么？ / 175
096. 达世币是什么？ / 176
097. 门罗币是什么？ / 177
098. 大零币是什么？ / 178
099. 以太坊是什么？ / 179
100. EOS 是什么？ / 180
101. CZR 是什么？ / 181
102. Augur 是什么？ / 183
103. Golem 是什么？ / 184
104. 泰达币是什么？ / 184
105. DigixDAO 是什么？ / 186
106. 区块链生态现状如何？ / 187

107. 如何判定区块链项目的价值？ / 190

108. 如何正确地看待“区块链 +”？ / 191

后记 / 194

参考资料 / 195

第01章

区块链和比特币的发展历史

区块链是比特币的底层技术，比特币是区块链的一种应用。本章主要解答区块链和比特币的发展历史的相关问题，诸如区块链的发展历史与未来趋势、区块链的特点及基本特征、区块链的技术创新与应用、各国对区块链资产的态度，以及比特币产生的原因和动机、比特币白皮书的诞生等问题。虽然区块链和比特币现在是热门词汇，任何跟区块链沾边的概念都被渲染得极为神秘，但要估算它的真正价值，首先需要了解上述问题，然后才能把它放到历史长河里去，看看它经不经得起更长时间的考验。

001.
区块链和比特币是什么关系?

区块链技术是比特币的底层技术，火币网、清华大学五道口金融学院互联网金融实验室、新浪科技等联合发布的《2014—2016 年全球比特币发展研究报告》中提到，区块链是比特币的底层技术和基础架构。

比特币是区块链的第一个应用，其交易信息都被记录在一个去中心化的账本上面，每个账本就是一个区块。如果把区块比作一个实物账本，那么每个区块就相当于账本中的一页，比特币网络每 10 分钟就会生成一张新账页，记载这 10 分钟的交易信息。各区块之间依据密码学原理，按时间顺序依次相连，形成一个链状结构，就是所谓的“区块链”。

物理学家、日裔美国人中本聪曾经发表过一篇名为《比特币：一种点对点的电子现金系统》的论文，详细阐述了对于电子货币的新构想。从此以后，国内外各大金融机构争相对比特币底层技术区块链进行研究，同时寻求区块链技术的实际应用。因此，从某个角度来看，比特币是区块链的第一个应用，而区块链更类似于 TCP（Transmission Control Protocol，传输控制协议）、IP（Internet Protocol，网络之间互联的协议）等底层技术，二者相辅相成，没有区块链技术就不会有加密货币，反之亦然。

002.
区块链的发展历史与未来趋势是什么?

区块链是由一系列技术实现的全新去中心化经济组织模式，诞生于 2009 年，2017 年成为全球经济热点。为了便于理解区块链的历史与未来趋势，可以将其发展划分为六个阶段。

阶段 1：技术实验阶段（2008—2009 年）

比特币创始人中本聪 2008 年 11 月 1 日发表了一篇名为《比特币：一种点对点的电子现金系统》的论文。2009 年 1 月 3 日，比特币系统开始运行。支撑比特币体系的主要技术有哈希函数、分布式账本、区块链、非对称加密、工作量证明等，这些技术构成了区块链的最初版本。从 2008 年到 2009 年年底，比特币都处在一个极少数人参与的技术实验阶段，相关商业活动还未真正开始。

阶段 2：极客小众阶段（2010—2012 年）

2010 年 2 月 6 日诞生了第一个比特币交易所，5 月 22 日有人用 1 万个比特币购买了两个比萨。

2010 年 7 月 17 日，著名比特币交易所 Mt.Gox 成立，标志着比特币真正进入市场。可是即便如此，能了解到比特币从而进入市场参与比特币买卖的主要是狂热于互联网技术的极客们。这些极客在 Bitcointalk.org 论坛上讨论比特币技术，在个人计算机上挖矿获得比特币，在 Mt.Gox 上买卖比特币，

仅用了 4 年时间，有些人就成了亿万富翁和区块链传奇。

阶段 3 ：市场酝酿阶段（2013—2015 年）

2013 年年初，1 比特币的价格是 13 美元。

3 月 18 日，金融危机中的塞浦路斯政府关闭了银行和股市，推动了比特币价格的飙升，4 月达到最高，为 266 美元。

8 月 20 日，德国政府确认比特币的货币地位。

10 月 14 日，中国百度宣布开通比特币支付。

11 月，美国参议院听证会明确了比特币的合法性。

11 月 19 日，比特币的单价达到 1242 美元新高。可是，此时区块链还不具备进入主流社会经济的基础，价格飙升包含了过于乐观的预期。

中国银行体系的遏制、Mt.Gox 的倒闭等事件，触发了比特币大熊市，比特币价格持续下跌。

2015 年年初，比特币单价一度跌至 200 美元以下，很多企业纷纷倒闭。

阶段 4 ：进入主流阶段（2016—2018 年）

2016 年 6 月 23 日英国脱欧，9 月朝鲜进行第五次核试验，11 月 9 日特朗普当选美国总统……以这些事件为标志，世界主流经济的不确定性增强，具有避险功能、与主流经济呈现替代关系的比特币开始复苏，市场需求增大，交易规模快速扩张，开启了 2016 年至 2017 年比特币牛市。

虽然中国市场因政策管控受到遏制，但韩国、日本，以及拉美国家的市场快速升温，比特币单位价格从 2016 年年初的 400 美元最高飙升至 2017 年年底的 2 万美元，翻了 50 倍。

比特币的造富效应以及比特币网络拥堵造成的交易溢出，带动了其他虚拟货币及各种区块链应用的大爆发，出现众多百倍、千倍甚至万倍增值的区块链资产，引发全球疯狂追捧，比特币和区块链彻底进入全球视野。

阶段 5 ：产业落地阶段（2019—2021 年）

在 2017 年造富效应和区块链理想造就的众多区块链项目中，大部分会随着市场的降温而消亡，小部分会坚持下来继续推进区块链的落地。市场经历狂乱后，2018 年的虚拟货币和区块链将会在市场、监管、认知等各方面进行调整，回归理性。2019 年，坚持下来的项目会初步落地，但依然需要几年时间接受市场的检验。到 2021 年，在区块链适宜的主要行业领域，一些企业会获得稳步发展，加密货币也会得到较广泛的应用。

阶段 6：产业成熟阶段（2022—2025 年）

各种区块链项目落地见效后，区块链会进入激烈而快速的市场竞争和产业整合阶段，三五年内形成一些行业龙头，完成市场划分，区块链产业格局基本形成，相关法律法规基本健全，对社会经济各领域的推动作用快速显现。其时，加密货币将成为主流货币，经济理论会出现重大调整，社会、政治、文化也将发生相应变化，国际政治、经济关系出现重大调整，区块链在全球范围内对人们的生活产生广泛而深刻的影响。

区块链的六个发展阶段中，前两个是技术试验阶段，中间两个是主流认知阶段，后两个是产业实现阶段。目前，区块链的社会认知广度已经足够，但认知深度尚嫌不足，需要深入推进区块链知识的研究和普及，为产业发展、成熟奠定基础。

其实，区块链对于全球经济的巨大价值已经被充分认识到，对于全球社会政治生态改善的价值也在逐步显现，是一个值得各国大力投入、抢占先机的社会经济新动力。