

刘海鹏
著

即使比特币“困局”加剧，
即使它的“安全性”受到巨大挑战，
但它曾在互联网金融中开辟出一个“新的领域”

疯狂 比特币

揭秘数字货币原理 和商业运作模式

比特币，跨越“虚拟世界”与“实体世界”的鸿沟！
掀起一场“货币革命”，颠覆我们对常规金融游戏的认识。

这是一本“老百姓们”都看得懂的“技术书”！
“平民化”趣味讲述穿插“超丑插画”让你一口气全部读完！



中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE



刘海鹏
著

疯狂

比特币

揭秘数字货币原理
和商业运作模式

中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

内 容 简 介

本书由浅入深，全面、系统地介绍了比特币的相关知识，并提供了大量例子，以供读者阅读。

本书共分 8 章。其内容包括：什么是比特币、如何获得和使用比特币、比特币挖矿指南、比特币与黄金一样吗、比特币的秘密、比特币现状及展望、令人眼花的山寨币、比特币相关网站推荐。

本书不仅适合所有想全面了解比特币知识的人员阅读，也适合各种对网络货币感兴趣的人员学习。对于想了解互联网金融的人，更是一本不可多得的案头必备参考书。

图书在版编目（CIP）数据

疯狂比特币：揭秘数字货币原理和商业运作模式 /
刘海鹏著. — 北京：中国铁道出版社，2014.8
ISBN 978-7-113-18432-2

I. ①疯… II. ①刘… III. ①电子货币—研究 IV.
①F830.46

中国版本图书馆 CIP 数据核字(2014)第 082624 号

书 名：疯狂比特币：揭秘数字货币原理和商业运作模式
作 者：刘海鹏 著

策 划：武文斌

读者热线：010-63560056

责任编辑：张 丹

封面设计：多宝格

编辑助理：刘建玮

责任印制：赵星辰

出版发行：中国铁道出版社（100054，北京市西城区右安门西街 8 号）

印 刷：北京新魏印刷厂

版 次：2014 年 8 月第 1 版

2014 年 8 月第 1 次印刷

开 本：700mm×1 000mm 1/16 印张：10.75 字数：202 千

书 号：ISBN 978-7-113-18432-2

定 价：32.00 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

疯狂比特币

2013年底的一天，一家出版社找到一个疯狂的作者去写一本疯狂书，书名为：疯狂比特币。有道是：“他人笑我太疯癫，我笑他人看不穿”。在这个科技飞速发展的时代，每一件创新都会让人觉得疯狂。当然疯狂只是相对的，相对于没有疯狂过的人来说我们都是疯狂的，但是同时相对于曾经疯狂过的人来说，没有疯狂过才是最让人觉得疯狂的。

或许大家看到这里，有些人已经被绕晕了，为了尽快说明白我到底想要说什么，在这里我采取了一种传统的方式给大家解释，那就是举个例子。这个例子怎么举呢？我觉得还是找些大家听说过的事情来举例。

比如说马云，在俺们刚开始接触互联网的1995年，马老就已经琢磨着怎么使用互联网创业了，这在当时无疑是被多数人认为是很疯狂的举动，没有人理解他在干什么。十九年后的今天，似乎当时觉得疯狂的事情现在开始变得习以为常了。

好了，切入正题，疯狂比特币，疯狂的问题已经探讨过了，现在来探讨一下比特币吧。

在2011年11月的某一天，我忽然看到了一篇刊登在《中国信用卡》杂志上的文章，文章的题目是《比特币：一种新型货币对金融体系的挑战》，作者洪蜀宁当时是人民银行南京分行的营业管理部金融票据中心研究发展科科长，并曾获得2010年江苏省五一劳动奖章。《中国信用卡》杂志则是由中国工商银行主办，人民银行、农业银行、中国银行、建设银行、保险公司、外汇管理局、交通银行、信息产业部计算机司、内贸局协办的月刊杂志。这篇文章对比特币做出了相当深刻的解析。

除说明比特币的特点外，他还说明了比特币当时的状况以及对金融体系可能带来的挑战。

第一，比特币固定了基础货币的投放总量，不可能发生人为的通货膨胀。实际上比特币将会一直保持紧缩，即比特币将会长期升值。



第二，由于比特币的交易没有中间机构来管理，而其匿名性也很难被追踪到终端用户，因此，比特币很可能被用来从事非法交易，如倒卖盗版印刷品、毒品和军火等。

第三，比特币交易几乎是实时的且没有手续费的，银行等中间机构无法从中获取中间收入。

第四，作为一种可能挑战主权货币的币种，它给予民众更多的选择。在各国政府为了刺激经济而滥发货币的时候，民众可以选择通缩货币而抛售主权货币，这种来自市场的有力反馈可以迅速传达到中央银行，使之重新审视其货币政策。

正是这篇文章引起了我对比特币的极大兴趣，此文让我意识到事情并没有那么简单，虚拟货币——比特币势必会对现实经济产生巨大的影响。在此后的时间里，我开始学习研究关于比特币的相关知识，并开始参与挖矿。

随着比特币的一路发展，很多当时觉得疯狂的想法开始变得理所当然。比特币也逐渐从一个默默无闻的实验品慢慢地发展到人尽皆知的新货币。虽然我并没有在这场伟大的实验当中获取很多财富，但是我认为学习和接受一个新鲜事物的过程才是最大的收获。

有收获自然希望分享，感谢出版社提供了这样一个机会能让我与大家一起分享收获。当然，如同比特币是以去中心化为核心理念一样，本书也基本是去中心化的，所有的资料的来源均有据可查。本书本着客观中立的原则，尽可能真实准确地记录一个普通比特币爱好者所掌握的关于比特币的相关知识。

最后再说说关于去中心化，其实去中心化的理念很早就有人在用了，比如说孔子的《论语》亦非孔子所著，而是其弟子录入的。

比特币也有其相似的特点，比特币相关的所有内容，包括比特币本身，几乎是比特币拥护者所提供的。这一切的一切都只是巧合吗？还是由此说明群体智慧才是最强大的？历史会证明一切的。

刘海鹏

2014年5月

比特币大事记

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshi@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

2008 年 11 月 1 日

中本聪在互联网上一个讨论信息加密的邮件组中发表论文《比特币：一种点对点电子现金系统（Bitcoin: A Peer-to-Peer Electronic Cash System）》。

2009 年 1 月 3 日

中本聪在位于芬兰赫尔辛基的一个小型服务器上挖出第一批比特币，一共 50 个，创造比特币世界的第一个区块，这天被誉为比特币的生日。





2010年5月22日

程序员拉斯洛·豪涅茨(Laszlo Hanyecz)用1万BTC购买了价值25美元的披萨，现在这两个披萨价值1000万美元，这是第一笔用比特币购买实物的交易。

2010年11月6日

比特币总市值突破100万美元，MTGOX交易所内每个比特币价值摸高到0.5美元。



2011年2月9日

MTGOX交易所的比特币价格突破了1美元。

2011年4月16日

《时代杂志》刊登 Jerry Brito 的文章，声称比特币将挑战政府和银行。



[- 3 -]



2011年7月6日

比特币进入移动支付时代，首款用于安卓系统的比特币应用上线。

2012年9月27日

比特币基金会成立，这是一个规范，保护和促进比特币发展的组织。比特币基金会声称他们的使命是帮助人们更自由地交换资源和想法。

 Bitcoin Foundation

[About](#)
[Members](#)
[Join Us](#)
[Donate](#)
[Blog](#)
[Forum](#)

[Contact](#)
[Login](#)

Freeing People to
Transact on
Their Own Terms.



2012年11月28日

比特币每个区块的产量按照协议减半，由每个区块产出 50 个比特币下降为 25 个，比特币价格并没有受供应缩减的消息影响。

2012年1月31日

Jeff Garzik. 开始使用第一台 AvalonASIC 矿机，从此比特币挖矿进入了 ASIC 矿机时代。





2012年3月16日

人口仅110万的欧盟成员国塞浦路斯政府冻结民众银行转账交易，对银行存款账户征税，18日关闭银行和股市，此时比特币价格为47.45美元。

2012年3月18日

美国财政部金融犯罪执法系统 FinCEN 发布了虚拟货币个人管理条例，首次阐明了虚拟货币，此时比特币价格为47.8美元。



2013年4月20日

四川芦山地震当天，李笑来在 bitcoin 官网发起对灾区的比特币捐赠，中国壹基金此后宣称共计收到捐赠比特币233个，市值22万人民币。



2013年5月3日

中国中央电视台《经济半小时》节目比较客观地向中国观众第一次介绍比特币这个新生事物。



[- 5 -]

**2013年6月27日**

德国会议作出决定：持有比特币一年以上将予以免税，被业内认为此举变相认可了比特币的法律地位。

2013年10月2日

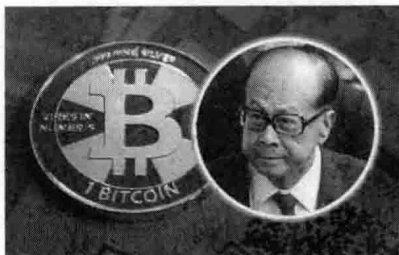
丝绸之路负责人罗斯·乌尔布莱特（Ross Ulbricht）被FBI抓获。

**2013年12月5日**

中国人民银行等5部委联合发布公告，印发《关于防范比特币风险的通知》。通知明确指出，比特币不具有与货币等同的法律地位，不能且不应作为货币在市场上流通使用。自行发债是指试点省(市)在国务院批准的发债规模限额内，自行组织发行本省(市)政府债券的发债机制。

2013年12月27日

香港《南华早报》报道，李嘉诚已通过旗下风投公司维港（Ventures）投资了一家名为BitPay的美国比特币支付公司。



第一篇 比特币入门与应用

第 1 章 什么是比特币	1
1.1 横空出世的比特币	2
1.1.1 比特币理论基础：哈耶克提的革命性建议	2
1.1.2 比特币意识萌发：米尔·弗里德曼的设想	3
1.1.3 比特币进化成长：不得不提的那些幕后科学家	3
1.1.4 比特币创造者中本聪的神秘来历	5
1.1.5 中本聪是否存在的猜想	6
1.2 比特币基本原理	8
1.2.1 常见术语解释	8
1.2.2 我的比特币在哪里	12
1.2.3 交易怎么记录的	13
1.2.4 挖矿与交易处理	14
1.3 比特币的特点	14
1.3.1 去中心化：比特币安全与自由的保证	15
1.3.2 总数恒定：比特币的发行数量是固定的	16
1.3.3 比特币交易方便	16
1.3.4 比特币交易费用低廉	17
1.3.5 专属所有权	17
1.4 疯狂的比特币	18
1.4.1 第一笔交易	18
1.4.2 疯狂过山车行情	18
1.5 比特币大事记	21
1.6 比特币常见问题解答	24
1.6.1 比特币是不是传销	24
1.6.2 比特币是一个庞氏骗局吗	24
1.6.3 早期的比特币使用者是否不公平地得到了更多的利益	24
1.6.4 挖光所有比特币需要多长时间	25
1.6.5 挖矿计算是否有实际用处？是不是浪费计算资源和能源	25

第 2 章 如何获得和使用比特币.....	26
2.1 如何下载和使用钱包.....	27
2.1.1 下载比特币钱包.....	27
2.1.2 如何使用比特币钱包.....	28
2.2 钱包的备份与保存.....	30
2.3 其他比特币钱包概述.....	31
2.3.1 三种软件钱包（客户端）.....	31
2.3.2 四种在线钱包.....	33
2.3.3 三种手机钱包（移动钱包）.....	34
2.4 国内主流比特币交易平台.....	35
2.4.1 比特币中国（ https://vip.btcchina.com/ ）.....	35
2.4.2 OKCoin（ https://www.okcoin.com/ ）.....	36
2.4.3 火币（ http://www.huobi.com/ ）.....	37
2.4.4 中国比特币（ https://www.chbtc.com/ ）.....	37
2.4.5 比特儿.....	38
2.5 国外主流比特币交易平台.....	39
2.5.1 门头沟 MT.GOX.....	39
2.5.2 btc-e.com.....	39
2.5.3 bitstamp（ https://www.bitstamp.net/ ）.....	40
第 3 章 比特币挖矿指南.....	41
3.1 什么是挖矿.....	42
3.1.1 工作证明.....	42
3.1.2 挖矿.....	43
3.1.3 块哈希（Block Hash）算法.....	43
3.1.4 产量调节.....	44
3.1.5 块（Block）字段详解.....	45
3.1.6 新块（Block）诞生过程.....	46
3.1.7 主链分叉.....	46
3.2 用什么来挖矿.....	47
3.2.1 CPU 挖矿.....	47
3.2.2 GPU 挖矿.....	48
3.2.3 ASIC 矿机挖矿.....	49
3.2.4 云矿机挖矿.....	50
3.3 如何选择矿机.....	50

[3]

3.3.1	期货矿机	51
3.3.2	现货矿机	52
3.3.3	如何挑选购买矿机	52
3.4	矿池介绍	53
3.4.1	矿池的运营模式	53
3.4.2	主流矿池介绍	55

第二篇 比特币原理与金融模式

第4章 比特币的金融模式：比特币与黄金..... 58

4.1	比特币与美元霸权	59
4.2	关于货币的那些事儿	61
4.2.1	中国古人的货币	61
4.2.2	世界上最早的金融危机	62
4.2.3	金融危机与布雷顿森林体系	62
4.2.4	纸币信用缺失与虚拟货币的产生	63
4.2.5	网络时代的人类需要新的支付选择	65
4.2.6	横空出世的比特币	66
4.3	比特币是一种信仰和生活方式	67
4.3.1	极客与极客信仰	67
4.3.2	比特币与 P2P 思想	68
4.3.3	点对点金融与超级小钱	69
4.4	比特币与黄金的区别	70
4.4.1	比特币是“币”还是“金”	71
4.4.2	电子币的资产属性	72
4.4.3	电子币对比黄金	73
4.4.4	为什么说比特币完爆黄金	74

第5章 比特币的秘密..... 78

5.1	强大而神秘的深网	79
5.1.1	深网的运行原理	80
5.1.2	深网使用简介	81
5.1.3	深网里那些你不知道的内容	82
5.1.4	深网与比特币的渊源	84
5.1.5	“丝绸之路”兴衰史	86

5.2	神秘的中本聪.....	89
5.2.1	江湖乍现.....	89
5.2.2	时隐时现.....	90
5.2.3	神龙无首.....	91
5.2.4	中本聪都曾经说了些什么.....	93
5.3	揭秘 SHA 算法.....	96
5.3.1	SHA 算法的分类.....	96
5.3.2	已经不安全的 SHA1.....	97
5.3.3	相对安全的 SHA2.....	99
5.4	那些传说中的组织与个人.....	99
5.4.1	各种各样的机构与组织.....	100
5.4.2	与比特币有牵扯的“大神”们.....	101
第 6 章	比特币的现状 & 展望.....	104
6.1	全球比特币现状.....	105
6.1.1	全球比特币分布概况分析.....	105
6.1.2	各国政府对比特币的态度.....	112
6.1.3	国内央行对比特币的态度.....	116
6.2	跌宕起伏的比特币.....	118
6.2.1	黑客盗窃.....	118
6.2.2	携款潜逃的交易平台.....	119
6.2.3	矿机违约事件.....	121
6.2.4	MTGOX 事件与闪电崩盘.....	121
6.3	比特币应用现状.....	122
6.3.1	比特币可以买到什么.....	122
6.3.2	比特币可以去哪里消费.....	124
6.3.3	比特币线下交易网站.....	125
6.4	关于比特币的未来.....	126
6.4.1	比特币会不会消亡.....	126
6.4.2	比特币会不会成为主流.....	127
6.4.3	比特币会不会被其他虚拟货币取代.....	128
第 7 章	令人眼花的山寨币.....	129
7.1	山寨币种类.....	130
7.1.1	使用 SHA256 算法的山寨币.....	130
7.1.2	使用 scrypt 算法的山寨币.....	131

[5]

7.1.3	使用其他算法的山寨币	132
7.2	不可小看的山寨币	132
7.2.1	瑞波币	133
7.2.2	莱特币	134
7.2.3	点点币	136
7.2.4	狗币	137
7.2.5	那些“坑爹”的山寨币	138
7.3	山寨币探究	140
7.3.1	如何制造山寨币	140
7.3.2	人人可造山寨币	141
7.3.3	山寨币如何作弊	142
7.3.4	珍惜投资远离山寨	143

第三篇 比特币的网络资源

第 8 章	比特币相关网站推荐	146
8.1	比特币官网	147
8.2	比特币论坛	148
8.3	块链信息	148
8.4	区块探索	149
8.5	BTC 导航	150
8.6	比巴克	151
8.7	巴比特	151
8.8	比特币实验室	152
8.9	壹比特	152
8.10	Bitell	153
8.11	币看	154
8.12	比特人	154
8.13	海峡比特币	155
8.14	比特币之家	155

第 1 章

CHAPTER 01



什么是比特币

什么是比特币？维基百科说：比特币（Bitcoin：BTC，货币符号：฿）是一种用户自治的、全球通用的加密电子货币。它与腾讯公司的 Q 币类似，你可以使用比特币购买虚拟的物品，比如网络游戏当中的衣服、帽子、装备等，只要有人接受，你也可以使用比特币购买现实生活当中的物品。但是 Q 币是中心化的，比特币是去中心化的。

1.1 横空出世的比特币

虚拟货币比特币 (Bitcoin) 的概念最初由中本聪 (Satoshi Nakamoto) 在 2009 年提出, 现在所谓的比特币是根据中本聪的论文思路设计发布的开源软件以及建构其上的 P2P (Peer to Peer, 简称 P2P) 网络。中本聪比特币论文原文可以在百度文库中查到。

比特币不是凭空突然蹦出来的, 任何事物的创新都是基于无数前人的创新理论, 更有无数前人在理论的基础上加以实践。我们可以先来看看比特币产生的历史。

提示: P2P 并不是什么新东西, 在现实生活中, 我们每天都按照 P2P 模式面对面地或者通过电话交流和沟通。实际上, P2P 就是不通过其他人传话, 直接一对一的交流的意思。

1.1.1 比特币理论基础: 哈耶克提的革命性建议

弗里德里希·奥古斯特·冯·哈耶克, 是奥地利出生的英国知名经济学家和政治哲学家, 以坚持自由市场资本主义、凯恩斯主义和反对集体主义而著称。

图 1.1 所示的这本书是哈耶克晚年最后一本经济学专著。

他在书中提出颠覆正统的货币制度的观念: 既然在一般商品、服务市场上自由竞争最有效率, 那为什么不能在货币领域引入自由竞争。

因此哈耶克提出一个革命性建议: 废除中央银行制度, 允许私人发行货币, 并自由竞争, 这个竞争过程将会发现最好的货币。

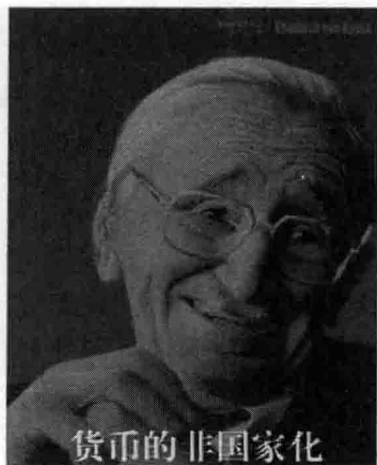


图 1.1 弗里德里希·奥古斯特·冯·哈耶