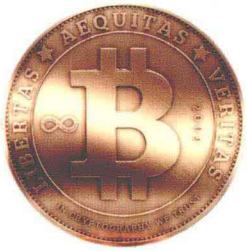
HZ BOOKS
华章科技



UNCOVERING THE SECRETS OF

BITCOIN

解密比特币

刘宁　沈大海◎著

中国比特币应用技术服务商国信深蓝
中国专业的比特币交易平台火币网
联合出品

国内资深比特币流通研究专家、比特币布道者和技术极客撰写

全面系统地阐述了比特币的基本概念、货币意义、运行原理、交易流通、世界各国对比特币的态度和政策，以及比特币投资的常识、原则、策略与技巧

机械工业出版社
China Machine Press

UNCOVERING THE SECRETS OF BITCOIN解密比特币

刘宁 沈大海◎著

机械工业出版社

图书在版编目（CIP）数据

解密比特币 / 刘宁，沈大海著 . —北京：机械工业出版社，2014.1

ISBN 978-7-111-45478-6

Ⅰ. 解… Ⅱ. ① 刘… ② 沈… Ⅲ. 电子货币 – 研究 Ⅳ. F830.46

中国版本图书馆 CIP 数据核字（2014）第 004891 号

到底什么是比特币，它的运行原理和设计逻辑是怎样的？为什么比特币成为全球关注的焦点，不同的国家对待比特币的态度和政策为何截然不同？比特币真的能成为完整意义上的世界货币，打破几千年货币由国家央行统一发行的局面吗？比特币的背后究竟蕴涵着怎样的经济思想，它会对现有的货币体系带来冲击吗？如何获得比特币并进行比特币的交易和流通？为什么比特币的价格像过山车一般大起大落，投资者们应该如何应对其中潜在的巨大风险？比特币的未来究竟会如何，只是昙花一现，还是会真正成为未来的货币之王？本书将以这些问题为脉络，多角度去揭开比特币的神秘面纱！

本书由国内比特币领域的技术极客和布道者撰写，国内最专业的比特币交易平台火币网与中国比特币应用技术服务商国信深蓝联合出品，专业性和权威性毋庸置疑。从专业的视角，用深入浅出的语言全面介绍了比特币的发展历程、基本概念、货币意义、货币特点、生成原理、运行机制、获取方法、交易方法、流通原理、世界各国政府对待比特币的态度和政策，以及比特币的投资常识、原则、策略、技巧和投资风险的规避等。此外，本书还介绍了狭义比特币的概念、原理、获取、交易和投资的相关知识。

机械工业出版社（北京市西城区百万庄大街 22 号 邮政编码 100037）

责任编辑：罗词亮

北京诚信伟业印刷有限公司印刷

2014 年 1 月第 1 版第 1 次印刷

170mm × 242 mm • 10.75 印张

标准书号：ISBN 978-7-111-45478-6

定 价：39.00 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换

客服热线：（010）88378991 88361066 投稿热线：（010）88379604

购书热线：（010）68326294 88379649 68995259 读者信箱：hzjsj@hzbook.com

前　言

2013年世界人民见证了许多大事件、大话题，其中一些在火爆之后即被淡忘，而有一些则让关注的人越来越多，甚至连国家政府都不得不参与管控，无疑，“比特币”就是其中最耀眼的明星话题。

可以说，在2013年6月以前，“比特币”这个词还不为绝大部分人所知，但自7月这个已被全球公认的“第一电子货币”的美元汇率价格猛然飙涨的那一刻开始，越来越多的人开始把目光从股市等其他投资市场中转移过来，使得不断攀升的价值红线成为许多人的聚焦点。短短几个月的时间里，以前不关注的，开始试图了解、关注直至投入；以前关注的，为之疯狂、为之高喊“全球金融革命”的口号；金融保守派们对其作出各种“深入浅出”的讲解、分析和警告……

然而，在信息爆炸的时代，百家争鸣的形式让很多人出现了瞬间的眩晕，原因在于深陷其中者观点狂热，所谓当局者迷；而旁观者们却又距之甚远，所谓雾里看花。就在这一争一驳中，比特币经历了自诞生以来价值狂飙最为疯狂的半年，这种看似疯狂的飙涨势头直到2013年年底才恢复平静。这个过程中，有人欢喜有人愁，有人连比特币是什么都没有弄清楚，就跟着大批人一起赚到了；也有人在同样懵懂的状态下跟着另外一大批人被套牢了。从这点上看，比特币的投资潮更加符合投资市场的盈亏特征。

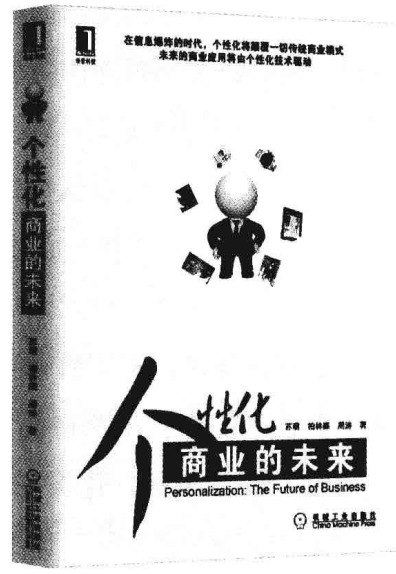
笔者之所以要写这本书，主要目的是以一个近距离观察并亲身体验者的角度，为正在关注比特币及正要进行比特币投资的读者答疑解惑。本书力求

站在中立的立场上，通过对各方言论的分析与总结，结合自身的经历，用通俗易懂的语言，从比特币的发展史、基础知识、投资解析及创业机遇等方面，结合各国政府对比特币的态度与管控，为大家揭开比特币的层层神秘面纱。

在此，笔者谨向所有比特币探索者和先驱者们致以崇高的敬意，向能够在关键时刻及时给予正确政策导向指引的国家有关部委和机构致以崇高的敬意，并向所有阅读和支持本书的读者表示衷心的感谢。希望读者可以通过阅读本书找到自己所需要的内容，理性看待比特币，理性看待新型互联网投资。如果读者可以从中得到关于理财与投资的新启发，笔者将不胜荣幸。

下面，就和笔者一起迈进神秘的比特币世界吧！

推荐阅读



O2O：移动互联网时代的商业革命

国内首部O2O著作，系统阐述和解读传统企业、电子商务企业、个人消费和与民生相关的企业如何借助O2O来重构和改善现有的商业模式，顺利在移动互联网时代实现创新与转型。

本书不仅通过大量成功案例极富洞察力地分析了O2O在营销、支付和消费体验三大方面的巨大作用，而且还经验性地总结了O2O的产品设计、O2O组织的构建与组织文化、O2O的运营。

个性化：商业的未来

超级畅销书，2012年最佳商业读本之一

在信息爆炸的时代，个性化将颠覆一切传统商业模式，未来的商业应用将由个性化技术驱动

详细解读了个性化商业模式在电子商务、移动互联网、社交网络、团购、超市、定价、新闻媒体、广告、求职招聘、婚恋交友、电影和音乐等领域的应用

目　录

第 1 章
什么是比特币

1.1 比特币的诞生

2008 年 11 月 1 日，一个自称中本聪（Satoshi Nakamoto）的人在一个隐秘的密码学邮件组里贴出了一篇研究论文，论文阐述了他对一种名为“比特币”的电子货币的新构想，于是比特币（Bitcoin，简记为 BTC）就此问世。论文如图 1-1 所示。

Bitcoin P2P e-cash paper

Satoshi Nakamoto Sat, 01 Nov 2008 16:16:33 -0700

I've been working on a new electronic cash system that's fully peer-to-peer, with no trusted third party.

The paper is available at:
http://www.bitcoin.org/bitcoin.pdf

The main properties:
Double-spending is prevented with a peer-to-peer network.
No mint or other trusted parties.
Participants can be anonymous.
New coins are made from Hashcash style proof-of-work.
The proof-of-work for new coin generation also powers the network to prevent double-spending.

Bitcoin: A Peer-to-Peer Electronic Cash System

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without the burdens of going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted 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 honest nodes control the most CPU power on the network, they can generate the longest chain and outpace any attackers. The network itself requires minimal structure. Messages are broadcasted 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.

Full paper at:
http://www.bitcoin.org/bitcoin.pdf

Satoshi Nakamoto

The Cryptography Mailing List
Unsubscribe by sending "unsubscribe cryptography" to

图 1-1 中本聪的论文原文

大意是他已经在运行一个基于 P2P 网络的现金系统，该系统有如下特点：

- 不受第三方监管；
- 该系统在 P2P 网络中防止了双重支付；
- 去中心化的生成；
- 参与者及交易是匿名的；
- 新货币的生成均通过哈希算法进行验证；
- 每一代新货币的生成验证都通过网络的力量防止出现双重支付；

……

从以上报告中，我们可以明确看出中本聪对于比特币的定义：一种 P2P 电子货币系统，无论从比特币本身的特性验证还是从尊重原创者权益的角度来讲，我们都应该为其正名，即比特币不是什么虚拟货币，而是一种完整的“电子货币”体系。

连讨论组的“老鸟”们都未曾听说过中本聪，有关他的信息也寥寥无几，而且这些信息还隐晦不明，甚至自相矛盾。网上的信息显示他在日本居住，他的电子邮箱地址来自德国的一个免费服务站点，万能的谷歌上也没有关于他的名字的任何信息，很多人推测“中本聪”是个假名，所以他至今仍是个迷。

自互联网诞生以来，电子货币因具有方便和难以追踪的特性，并能脱离政府和银行的监管，而成为一个热门话题。20 世纪 90 年代，一个名为“密码朋克”的密码破译组织就致力于创建电子货币，但付出的努力没收到任何成效。中本聪的发明让这个困扰密码学领域数十年的难题迎刃而解。

2009 年 1 月 3 日，第一个数据块——创世区块（Genesis Block）的生成宣告比特币系统诞生。Satoshi 在创世区块中写入了图 1-2 中的信息。

这一串数字信息还原出文本为：“The Times 03/Jan/2009 Chancellor on brink of second bailout for banks”。

当时正值英国财政大臣达林被迫考虑第二次出手纾解银行危机的时刻，“Chancellor on brink of second bailout for banks”这句话上了《泰晤士报》当天的头版（见图 1-3），这既是对该区块产生时间的说明，也是对金融危机巨

大压力下，旧有的脆弱银行系统的冷嘲。

```
$ hexdump -n 255 -C blk00000.dat
00000000  f9 be b4 d9 1d 01 00 00  01 00 00 00 00 00 00 00  |................|
00000010  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
00000020  00 00 00 00 00 00 00 00  00 00 00 00 3b a3 ed fd  |............;...|
00000030  7a 7b 12 b2 7a c7 2c 3e  67 76 8f 61 7f c8 1b c3  |z{..z.,>gv.a....|
00000040  88 8a 51 32 3a 9f b8 aa  4b 1e 5e 4a 29 ab 5f 49  |..Q2:...K.^J)._I|
00000050  ff ff 00 1d 1d ac 2b 7c  01 01 00 00 00 01 00 00  |......+|........|
00000060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
00000070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 ff ff  |................|
00000080  ff ff 4d 04 ff ff 00 1d  01 04 45 54 68 65 20 54  |..M.......EThe T|
00000090  69 6d 65 73 20 30 33 2f  4a 61 6e 2f 32 30 30 39  |imes 03/Jan/2009|
000000a0  20 43 68 61 6e 63 65 6c  6c 6f 72 20 6f 6e 20 62  | Chancellor on b|
000000b0  72 69 6e 6b 20 6f 66 20  73 65 63 6f 6e 64 20 62  |rink of second b|
000000c0  61 69 6c 6f 75 74 20 66  6f 72 20 62 61 6e 6b 73  |ailout for banks|
000000d0  ff ff ff ff 01 00 f2 05  2a 01 00 00 00 43 41 04  |........*....CA.|
000000e0  67 8a fd b0 fe 55 48 27  19 67 f1 a6 71 30 b7 10  |g....UH'.g..q0..|
000000f0  5c d6 a8 28 e0 39 09 a6  79 62 e0 ea 1f 61 de     |\..(.9..yb...a.|
```

图 1-2　中本聪的创世区块

图 1-3　比特币诞生当天的英国《泰晤士报》

在 IRC（Internet Relay Chat，互联网中继聊天）里 Satoshi 这个 ID 留下了一些言论：

“Yes, [we will not find a solution to political problems in cryptography,] but we can win a major battle in the arms race and gain a new territory of freedom for several years. Governments are good at cutting off the heads of a centrally controlled networks like Napster, but pure P2P networks like Gnutella and Tor seem to be holding their own.”

“[Bitcoin is] very attractive to the libertarian viewpoint if we can explain it properly. I’m better with code than with words though”

译文如下：

“是的，我们无法找到通过密码学解决政治问题的途径，但是我们可以在军备竞赛中获取重大战役的胜利，同时夺得自由的新疆域。政府擅长击溃 Napster 那样拥有中央控制的网络，但是 Gnutella 和 Tor 这样的纯粹 P2P 网络看起来依旧安枕无忧。”

“如果我们能恰当地表述比特币系统的概念，对自由主义者来讲那会是非常有吸引力的。不过我更擅长编程而不是言辞。”

Satoshi 对密码学邮件组非常熟悉，然而这个 ID 本身却从未在 Bitcoin 项目之外的讨论中出现过。有些人认为他早在项目启动之前就做好了这个 36 岁日本男性的 ID 来掩饰自己的身份或者说保护整个项目。“Satoshi”（聪）在日文里的意思是“智慧”或“理由”。或许这就是他选择这个名字的原因。

同样在 20 世纪 90 年代早期，密码破译者大卫·乔姆（David Chaum）创建了一个匿名系统——“电子现金”（ecash），但失败了，部分原因是依赖于政府和信用卡公司的现有基础设施。之后各种电子货币尝试者不断涌现——比特金（bit gold）、RPOW、b 钱（b-money）……，但无一例外地也都失败了。

中本聪的论文于 2008 年发表，当时政府和银行管理经济的能力遭到各方质疑，信用降入谷底。美国政府向华尔街和底特律汽车巨头注入大笔资金，美联储推出“量化宽松”政策，本质上就是大量印美钞刺激经济，金价上涨。