刘海鹏 著

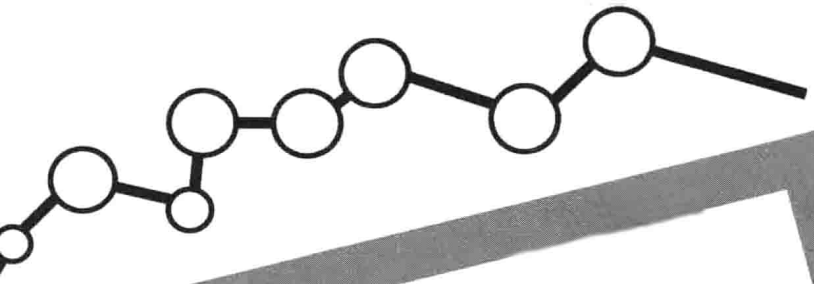
即使比特币“困局”加剧，
即使它的“安全性”受到巨大挑战，
但它曾在互联网金融中开辟出一个“新的领域”

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

前言

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
satoshin@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 1 000 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。

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。

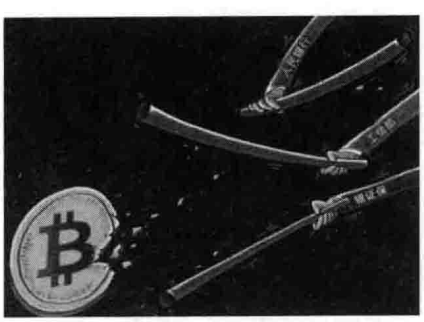
[- 5 -]

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。

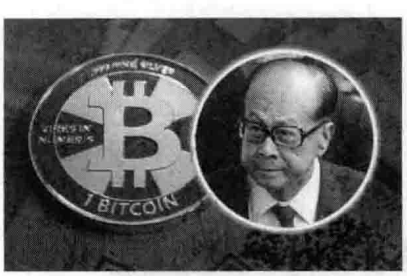


2013 年 12 月 5 日

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。



目录

第一篇　比特币入门与应用

第二篇 比特币原理与金融模式

第三篇 比特币的网络资源

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。

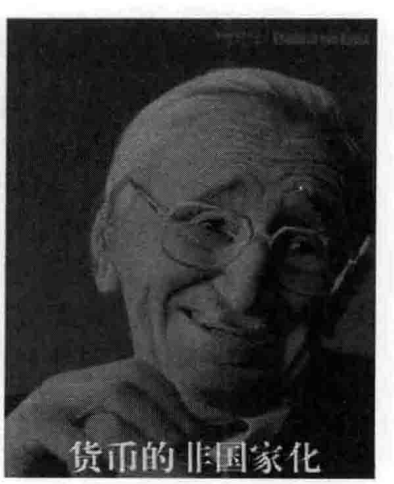


图1.1 弗里德里希·奥古斯特·冯·哈耶

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。