# 货币的终结

未来十年全球最值得关注的科技新趋势
改变世界与经济旧有秩序的新力量

THE END OF MONEY

The Story of Bitcoin, Cryptocurrencies and the Blockchain Revolution

## 比特币、加密货币和区块链革命

比特币、加密货币和区块链技术
如何影响货币、商业和世界运作

谷歌 | 高盛 | IBM | 亚马逊 | 西门子 | 脸书
英特尔 | 沃尔玛 | 微软等
**巨头公司纷纷布局的新金融技术**

著——亚当·罗思坦 [美]
译——尚跃星

机械工业出版社
CHINA MACHINE PRESS

# 货币的终结

## 比特币、加密货币和区块链革命

THE END OF MONEY

The Story of Bitcoin, Cryptocurrencies and the Blockchain Revolution

著——亚当·罗思坦（Adam Rothstein）〔美〕
译——尚跃星

机械工业出版社
CHINA MACHINE PRESS

本书主要介绍新的数字化货币概念，描绘什么是加密货币，它是怎样形成的，以及区块链下一步将怎样发展。通过本书，我们的认知将跳出有局限性的互联网领域，走向广阔的全球金融平台。我们将具体了解密码学的数学知识，并且探索比特币社区的各种亚文化。我们将讨论是什么创造了我们口袋里的钱，是什么创造了国家的经济，是什么可能会改进这些观念。读完本书之后，你将能从一个更好的角度来预测未来的货币会是什么样子。



北京市版权局著作权合同登记　图字：01 - 2018 - 0187 号

**图书在版编目（CIP）数据**

货币的终结：比特币、加密货币和区块链革命 /
（美）亚当·罗思坦（Adam Rothstein）著；尚跃星译.
—北京：机械工业出版社，2018.10
ISBN 978 - 7 - 111 - 61233 - 9

Ⅰ.①货…　Ⅱ.①亚…②尚…　Ⅲ.①电子支付—研究
Ⅳ.①F713.361.3

中国版本图书馆 CIP 数据核字（2018）第 245795 号

机械工业出版社（北京市百万庄大街 22 号　邮政编码 100037）
责任编辑：坚喜斌　杨　洋　　责任校对：梁　静
责任印制：常天培
北京联兴盛业印刷股份有限公司印刷

2019 年 1 月第 1 版·第 1 次印刷
145mm × 210mm · 6.75 印张 · 3 插页 · 109 千字
标准书号：ISBN 978 - 7 - 111 - 61233 - 9
定价：49.00 元



凡购本书，如有缺页、倒页、脱页，由本社发行部调换

电话服务
服务咨询热线：010-88361066
读者购书热线：010-68326294
　　010-88379203
**封面无防伪标均为盗版**

网络服务
机 工 官 网：www.cmpbook.com
机 工 官 博：weibo.com/cmp1952
金　书　网：www.golden-book.com
教育服务网：www.cmpedu.com

# 前　言

我们随手从兜里或钱包里拿出一张皱皱巴巴的钞票，或许是纸质的，或者是塑料的。你可以用它来购得商品或服务，也可以存在银行以备不时之需。你知道这张钞票的价值。当你把钞票拿给别人看时，对方也同样知道这张钞票的价值，这些都是显而易见的，不是吗？

但是从2008年开始，货币形势开始变得更复杂了。有人发明了“加密货币”，而且它在短时间内席卷了全球，这种加密货币就是比特币。它将是一种全新的未来货币形式，还是对全球经济的一种威胁？相信不同的人会有不同的答案。

对于外行来说，比特币是令人困惑的，甚至是恐慌的。它到底是什么？谁在操控它？谁在使用它？出于什么目的？一系列的恐怖“标签”扣在它的头上：网络犯罪、贪污、贩毒、洗钱、腐败、谋杀甚至反政府。这些都使它变得有点臭名昭著。

但是，从另一个方面来说，加密货币也许真的会是一种全新的货币。我们也有理由相信：加密货币是对我们现在所使用的货币的改良和升级。

加密货币的发明，其核心是基于一种被称作“区块链”的技术。你将在本书中读到很多相关的知识。区块链技术是一种颠覆性的技术，它不仅体现在货币使用上，还可以应用于从法律到民主的诸多领域中。

加密货币出现后，我们开始考虑把货币当作一种技术。这种技术正以势如破竹之势向前发展。同时，由于其高端的前瞻性，所带来的经济收益也不容小觑。未来，我们会遇到越来越多的创新，比如物联网产品、分权制银行，甚至自治公司。

本书将介绍这种新的数字化货币概念，具体描绘出什么是加密货币，它是怎么形成的，以及区块链下一步将怎样发展。通过本书，我们的认知将跳出有局限性的互联网领域，走向广阔的全球金融平台。我们将具体了解密码学的数学知识，并且探索比特币社区的各种亚文化。我们将讨论是什么创造了我们口袋里的钱，是什么创造了国家的经济，是什么可能会改进这些观念。

我们预测货币的未来就像是在赌马，但是读完本书之后，你将能从一个更好的角度来预测未来的货币会是什么样子。

# 目 录

# 第 1 章

# 比特币：基础知识

什么是比特币？你怎样可以获取比特币？你可以用比特币买什么？

## 什么是比特币

比特币是一种叫作加密货币的新型数字货币，它不受银行控制，也不被政府控制，它是由分布式网络计算机通过预设程序解决复杂的数学问题而生成的。比特币是基于区块链技术的加密技术，它是众多存在的加密货币中第一个出现的，也是市场上最大的加密货币。

## 怎样使用比特币

比特币不是以物理实体存在的，它没有像美元或欧元一样被制造成票据和硬币。相反，比特币存在于数字文件形态的钱包里。比特币钱包通过手机或计算机把比特币转账给其他人。

## 如何获取比特币

我们获取比特币的方式有很多种，第一种方式就是“挖矿”。你可以通过设置你的计算机执行加密运算的任务来获取比特币，通过这种方式可以获取得到少量比特币的机会。这也是最初加密货币生成的方式。然而今天，“挖矿”竞争激烈，如果没有足够大的硬件投资，通过“挖矿”的方式获取比特币是非常困难的。或者，你也可以通过购买“云挖矿”的服务雇佣他人来帮你“挖矿”。

另一种获取比特币的方式是从已经持有比特币的人那里获取。我们可以通过类似于 localbitcoins. com 这样的服务平台，与愿意用比特币来交易美元、欧元等传统货币的人来交易。

还有一种获取比特币的方式就是通过比特币交易平台来获取，这种方式可以允许你用一种货币（如美元、英镑、欧元、人民币或者比特币）来兑换成另外一种货币，就像是外币兑换一样。Mt. Gox（参照第 7 章“GOX 的艰难历程”）曾经是全球上最大的比特币交易商，直到 2014 年下线。在 2016 年年底，BitMEX 成为世界上最大的比特币交易商。

最近，一些相关的服务启动了，这些服务允许将用户的银行服务与加密货币服务关联，用户可以储蓄比特币，并且可以当作本地传统货币，如美元、英镑消费，反之亦然。Coinbase 和 Bitpay 就是两个典型的例子。

最后，获取比特币最直接的方式就是进行比特币与物品销售或服务进行交易。例如 Stripe 公司和 Paymium 公司，它们的业务就接受加密货币，同时它们也鼓励和帮助商家接受使用加密货币进行交易。

**图 1.1　比特币的符号在中本聪发明加密货币不久后被创建**

2013 年 4 月，塞浦路斯银行危机导致比特币激增，从而主要的比特币交易市场容量过载，又导致比特币被突然抛售。

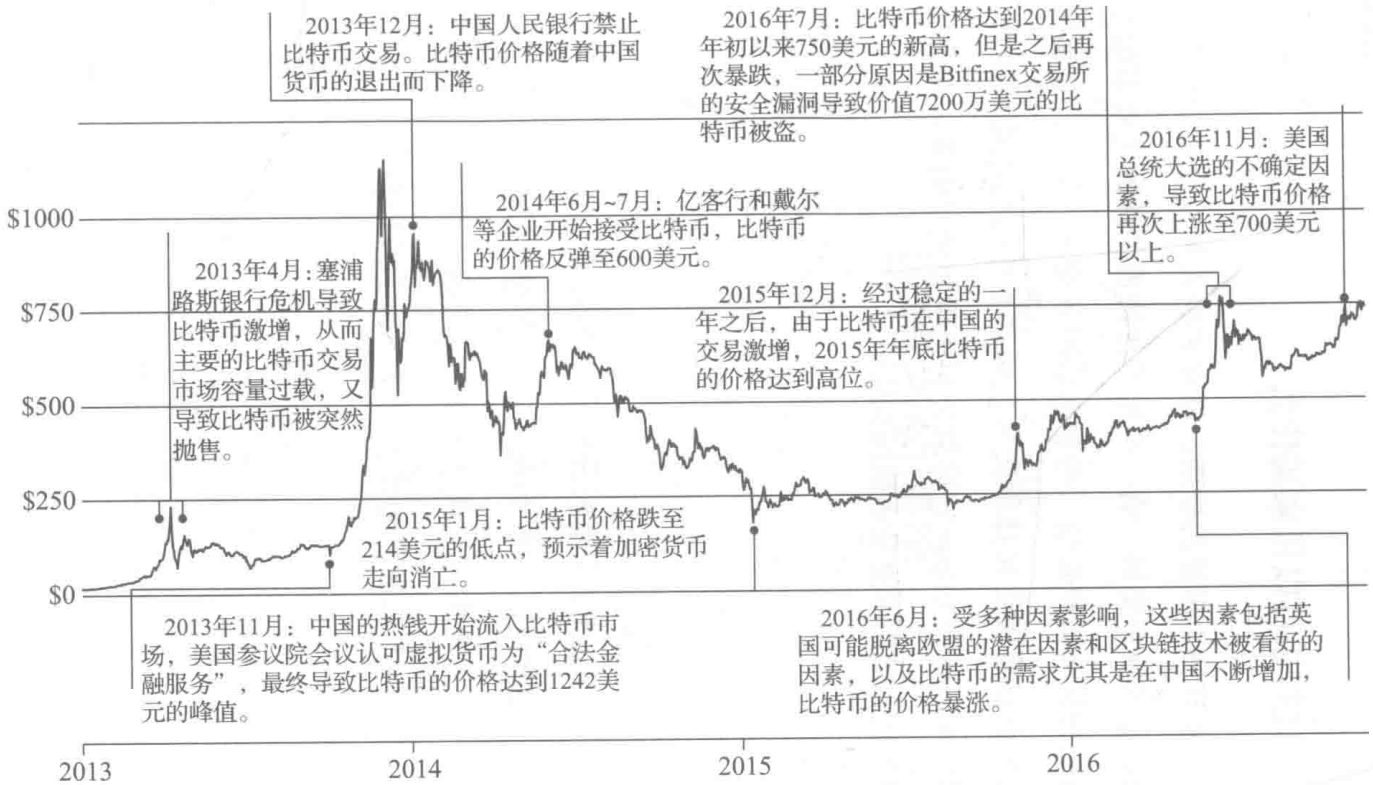


图1.2　比特币的高点和低点：比特币持有者必须准备好接受比特币价格的波动

## 比特币可以用来买什么

在比特币出现的早期，没有多少人可以使用比特币进行物品或服务交易。第一个接受比特币付款的主要市场是毒品交易市场和其他一些非法的服务交易。如今，许多主要企业直接接受比特币交易，而对于专门的比特币用户，像 Coinbase 或 Bitpay 这样的公司提供集成卡服务，允许客户在任何信用卡交易中使用比特币。

# 第 2 章

# 比特币的诞生

在 2008 年，某个不愿意透露身份的人有了个新想法。到了 2011 年，这一想法已经价值超过 5400 万美元。本章内容就是关于这种全新货币由来的故事。

改变世界的金融创见并非总是凭空出现在电子邮件的收件箱里。当密码学家亚当·巴克（Adam Back）在2008年8月收到中本聪发来的电子邮件，提出虚拟货币这个新概念时，他并没有太在意。因为自从1992年密码朋克（cypherpunk）邮件发送列表名单创建以来，跟亚当·巴克一直保持联系的名单上很多人都曾提出过这种只存在于计算机上的货币的想法，但是他都未予采纳，就更别提来自一个陌生人的想法了。

这也是人们第一次听说中本聪这个人。这个名字仿佛是某个未知的人或团体编造的一样。他所提出的这个未经测试和证实的想法，就是比特币。不到三年的时间，当中本聪从网络上消失后，时存的比特币总价值超过了5450万美元。但是这个加密货币发明者的身份从未真正被证实过。