

壹比特科技/数字货币研究中心

谢平 作序 朱嘉明  
李欣贺 陆晓野 柏亮 力荐

B

比特币的魅力在哪里？比特币为什么疯狂？  
比特币的命运由谁主宰？数字货币的未来在哪里？

数字货币是财富，更是革命

# 数字货币

## 比特币数据报告与操作指南

李钧 龚明 毛世行 高航 编著

全球首部详细揭示比特币数据报告与操作指南的著作



T

C

互联网对人类所有活动的影响，当然也包括货币制度，我们要用互联网思想来想象人类可能的货币制度。特别是在十年之后，“90后”成为社会经济活动的主体，他们是“网络一代”。

——谢平

货币对历史进程的意义从来不可低估。比特币的历史意义，我们至今还难以充分认识。可惜，哈耶克和弗里德曼都已经过世，如果他们能够看到比特币，会做怎样的思考呢？

——朱嘉明

珍藏版  
随书赠送  
比特币



电子工业出版社  
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY  
<http://www.phei.com.cn>

壹比特科技/数字货币研究中心

# 数字货币

## 比特币数据报告与操作指南

李钧 龚明 毛世行 高航 编著

电子工业出版社

Publishing House of Electronics Industry

北京•BEIJING

未经许可，不得以任何方式复制或抄袭本书之部分或全部内容。  
版权所有，侵权必究。

## 图书在版编目（CIP）数据

数字货币：比特币数据报告与操作指南 / 李钧等编著. —北京：电子工业出版社，2014.1  
ISBN 978-7-121-22266-5

I. ①数… II. ①李… III. ①电子货币—研究 IV. ①F830.46

中国版本图书馆 CIP 数据核字（2013）第 318169 号

书 名：数字货币——比特币数据报告与操作指南

作 者：李 钧 龚 明 毛世行 高 航

策划编辑：刘声峰（itsbest@phei.com.cn）

责任编辑：刘声峰

文字编辑：白 涛

印 刷：三河市鑫金马印装有限公司

装 订：三河市鑫金马印装有限公司

出版发行：电子工业出版社

北京市海淀区万寿路 173 信箱 邮编 100036

开 本：720×1 000 1/16 印张：24 字数：380 千字

印 次：2014 年 1 月第 1 次印刷

定 价：50.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zltz@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

## 总 序

### “零壹财经”：互联网金融+

莱布尼茨发明的二进制计数法成为计算机程序的运行基础，引领我们进入了互联网世界。莱布尼茨说，“1 与 0，一切数字的神奇渊源。这是造物的秘密美妙的典范。”

“零壹财经”书系可以定义为“互联网金融+”系列书籍，发端于互联网金融研究，用互联网思想和互联网金融的基本逻辑搭建内容体系。在我们的计划中，它具备以下基本特点：

第一，在研究和思考问题时，回归到无的状态（0），清零先入之见，用数据、事实描述事物的基本面目；

第二，关注事物的初始状态（1），尽最大努力厘清它的来龙去脉，注重基础，探望前沿；

第三，以互联网金融为主轴线，以开放、自由、协作、分享的互联网精神，创作、编写和翻译好的内容；

第四，基于主线丰富我们的内容(+)，在比较有把握的情况下把“其他资产交易”、“其他行业”、“其他情况”接入到互联网金融的研究和思考框架之中；

第五，还有一些关于互联网和金融的思想性书籍和基础书籍；

第六，没有固定体例和口味。

至于“零壹财经”书系的动机和意义——莱布尼茨那句话里的每一个词汇都深深地吸引着我们：渊源、造物、秘密、美妙、典范。最小的粒子和最浩瀚的世界，都有无尽的趣味引诱着我们。我们选择的入口很小，也不太小。

“零壹财经”是一个专注于互联网金融研究的团队。我们希望“零壹财经”的每一本书都淳朴、大方、谦卑、有力量。

柏 亮

2013 年 12 月 25 日于北京

## 推荐序

### 互联网货币的雏形与实验

谢 平

2013 年初，我在《新世纪周刊》谈及互联网货币，提出很多信誉良好、有支付功能的网络社区将发行自己的货币，称为“互联网货币”，这类货币将广泛用于网络经济活动，使得人类社会重新回到中央银行法定货币与私人货币并存的状态。

当时，比特币等虚拟货币尚不广为人知，人们的注意力主要落在 Q 币、亚马逊币和林登币等企业发行的机构“货币”上。这些机构货币被用于与应用程序、虚拟商品和服务有关的交易。有些与法定货币之间不存在兑换关系，只能在网络社区中获得和使用；有些可以通过法定货币来购买，但不能兑换为法定货币；还有些与法定货币之间能相互兑换。机构货币已经发展出非常复杂的市场机制，呈现出互联网货币的雏形。

到 2013 年中期，虚拟货币社区以点对点软件发行的货币引起普遍关注，发展很快，形成了形形色色的虚拟货币，例如比特币、莱特币和 Ripple 币等。2013 年底，国内出现虚拟货币投资热潮，人们对虚拟货币的了解与接受程度有所提高。根据欧洲央行的研究，2011 年美国虚拟货币交易量在 20 亿美元左右，已经超过非洲一些国家的 GDP。现在，几种典型的虚拟货币市值之和超过 100 亿美元，每日的交易量在数千万美元到数亿美



元之间。

虚拟货币在发行、维护与流通机制上与机构货币存在一定区别，具有较强的实验性质，特征包括：

第一，点对点发行，监管很少，特别是较少受到中央银行的监管；

第二，以数字形式存在；

第三，内建支付系统；

第四，被社区外成员接受和使用，作为交易媒介和价值贮存；

第五，可用来购买社区外的数据商品和实物商品；

第六，可为商品标价。

这些特性意味着虚拟货币拓展了此前互联网货币的流通范围，在法定货币体系之外建立起相对独立的、跨越国界范围的货币生态，而且接受的人越来越多，并形成独立于央行之外的全球支付系统，具有颠覆性，是互联网货币发展的一个新趋势。如何应对虚拟货币对目前的货币基础理论、货币政策理论和中央银行理论的挑战，是一个值得深入研究的课题。

这一课题遇到的一个明显障碍是相关资料的缺乏，虚拟货币社区、新闻界、监管机构乃至学术界对虚拟货币的讨论较多，系统性的资料汇集、整理和分析工作尚不充分。本书作者为此做出努力，以技术总结、事实归纳、数据统计等方式，积累了大量有价值的材料。研究界之外的普通读者，也可从这些基础材料中，获取知识，启发思考。

在互联网世界里，人们愿意把自己的“数据财富”以互联网货币为载体，这使得互联网货币的出现具有其合理性，属于“信用货币+私人货币”范畴。随着数据商品与实物商品之间的界限越来越模糊，网络经济活动和实体经济活动之间的联系越来越紧密，互联网货币会通过多种渠道影响实

物商品的价格。未来法定信用货币很可能与互联网货币并存，成为人类货币形态的第四个发展阶段。互联网对人类所有活动的影响，当然也包括货币制度，我们要用互联网思想来想象人类可能的货币制度。特别是在十年之后，“90后”成为社会经济活动的主体，他们是“网络一代”。

虚拟货币提供了一个了解、观察、规范乃至监管未来互联网货币的窗口与实验平台。这一实验仍在发展、进行之中，更加新颖的货币发行机制、支付渠道、资产管理概念和金融组织形态或将对当前的货币、金融体系带来更深刻的影响与变革。其发展状况和内外风险，同样值得关注。



# 目 录

III 总序/柏亮

V 推荐序/谢平

IX 目录

---

001 第一章 数字货币概况

003 数字货币起源

003 早期尝试

004 技术挑战

006 比特币的诞生

007 数字货币基本原理

007 防止货币伪造

008 防止重复支付

008 无须第三方监管

009 比特币的发行

010 挖矿

011 区块链

- 012 计算难度与确认次数
- 013 客户端钱包软件
- 014 比特币转账
- 015 匿名与公开
- 016 不可撤销与不可找回
- 017 数字货币技术特点
  - 017 去中心化
  - 018 基于密码学的安全通信
  - 020 公开透明
  - 021 算力民主
- 023 数字货币家族成员
  - 024 比特币 (Bitcoin)
  - 024 莱特币 (Litecoin)
  - 025 Ripple 币 (XRP)
  - 026 Mastercoin (MSC) 与 BitShares (BTS)
  - 027 Peercoin (PPC)
  - 028 Namecoin (NMC)
  - 028 其他
  - 031 部分已消失数字货币
- 033 数字货币获取与使用
  - 033 比特币获取途径

- 035 比特币接受度
- 036 支付便利性
- 037 支付应用扩展
- 039 数字货币历史上的重要事件
- 045 数字货币价格变化
  - 046 第一次暴涨暴跌
  - 047 第二次暴涨暴跌
  - 051 第三次暴涨
  - 051 价格依据
- 055 数字货币风险
  - 055 价格涨跌无度
  - 056 数字货币本身的技术风险
  - 056 钱包安全问题
  - 057 区块链内容合法问题
  - 058 哈希算法被破解了怎么办
  - 059 51%攻击问题
  - 059 交易平台风险
  - 061 集成矿机风险
  - 062 政策风险

## 063 第二章 数字货币生态系统

### 065 比特币钱包

066 钱包软件（比特币客户端）

067 移动钱包

068 在线钱包

069 硬件钱包

069 脑钱包和纸钱包

### 071 比特币协议与发展

071 比特币协议概述

072 比特币协议特点

075 Bitcoin 0.8.4

076 Bitcoin 0.8.5

076 Bitcoin 0.9.0

### 081 比特币创业与风险投资

081 Buttercoin

082 比特币中国获得投资

083 中国上市公司首度掘金比特币

084 钱包公司获得投资

085 Boost Accelerator 公司

086 SatoshiDice 被收购

087 比特币信托投资

|     |           |
|-----|-----------|
| 088 | 挖矿公司      |
| 088 | 展望        |
| 089 | 交易所       |
| 089 | Mt.Gox    |
| 092 | 比特币中国     |
| 094 | Bitstamp  |
| 095 | BTC-e     |
| 096 | OKCoin    |
| 097 | 支付        |
| 097 | BitPay    |
| 099 | Coinbase  |
| 102 | eBay      |
| 103 | GlassPay  |
| 104 | BIPS      |
| 107 | 应用市场      |
| 107 | Bigpoint  |
| 109 | BitDazzle |
| 111 | 百度加速乐     |
| 112 | 盛大果壳电子    |
| 113 | 盛大天地青春里   |
| 115 | 中国电信      |

- 117 微支付
  - 118 BitWall
  - 119 BitMonet
  - 121 微交易和区块链膨胀
  - 122 未来发展
- 123 国际汇款
- 129 监管情况
  - 129 美国
  - 134 德国
  - 135 加拿大
  - 137 英国
  - 139 瑞典
  - 140 瑞士
  - 141 印度
  - 143 中国香港
  - 144 中国大陆
  - 148 其他
  - 149 展望
- 151 挖矿业
  - 151 挖矿历史回顾
  - 153 算力波动及矿池份额



|       |                          |
|-------|--------------------------|
| 156   | 矿机企业及发展                  |
| 162   | 挖矿业展望                    |
| 165   | 博彩业                      |
| 166   | SatoshiDice              |
| 167   | Just-Dice                |
| 168   | 数据统计                     |
| 171   | 全球认可趋势                   |
| 171   | 交易增长                     |
| 173   | 业内参与者                    |
| 174   | 客户端下载                    |
| 175   | 比特币发展展望                  |
| <hr/> |                          |
| 177   | <b>第三章 历史行情分析及投资风险提示</b> |
| 179   | 行情总览                     |
| 181   | 2008—2010 年行情            |
| 183   | 2011 年行情                 |
| 187   | 2012 年行情                 |
| 189   | 2013 年行情                 |
| 193   | 美元和比特币                   |
| 199   | 汇率差特点                    |
| 205   | 丝绸之路的影响                  |

206 历史

209 分析

210 警示

---

211 **第四章 数字货币入门指南**

213 比特币钱包操作指南

213 下载 Bitcoin-Qt

214 安装 Bitcoin-Qt

215 同步数据

217 接收比特币

218 发送比特币

219 查看交易行情

220 设置密码

223 数字货币挖矿指南

223 概述

224 矿机购买

228 外围设备准备

229 矿机固件更新与设置

231 矿池的选择

234 矿池设置

237 日常管理

241 兑换交易指南

241 兑换交易概述

242 比特币中国交易操作指南

250 交易平台风险分析

252 安全交易策略

255 第五章 竞争币

257 概述

259 POW 类

261 SHA 256 类

263 scrypt 类

266 科学运算

269 POS 类

273 竞争币市值统计

275 第六章 支付系统和去中心化交易所

277 中心化交易所困境

278 政府监管问题

278 网站技术架构问题

279 网站诚信问题

281 Ripple

281 Ripple 概述