数字货币:比特币数据报告与操作指南(珍藏版)

作者：无李钧，龚明，毛世行，高航

目录

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

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zlts@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，基于主轴线丰富我们的内容（+），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。

第一章　数字货币概况

数字货币起源

（一）早期尝试

1952年，美国加利福尼亚州富兰克林国民银行率先发行银行信用卡，标志着一种新型商品交换中介的出现。美洲银行从1958年开始发行“美洲银行信用卡”。1974年，罗兰德·莫诺（Roland Moreno）发明了IC卡作为电子货币的存储介质。1982年，美国组建了电子资金传输系统，随后英国、德国也相继研发了类似的系统。以银行信用卡为代表的电子货币迅速流行，成为当今主流的货币形式。

电子货币使得货币彻底去实体化了，虽然我们仍然会使用卡片作为电子货币的载体，但是卡片本身并不是货币，真正的货币是卡片里存储的数字。如同早期纸币对应于金库中相应价值的黄金，早期电子货币也对应于银行中相应数额的纸币。但是随着各国货币的发行转向电子化，电子货币也日益与纸币脱离，成为纯粹数字形态的货币。

电子货币是法定货币（以下简称“法币”）的电子化形式，它的发行机制与传统法币相同，资金的传输由金融机构承担和维护。许多人认为这种电子货币存在一些弊端，如无法匿名使用、无法全球流通、交易成本较高等，于是他们开始尝试设计一些新型的电子货币方案（为了与金融系统发行的电子货币相区分，我们称之为数字货币），例如20世纪90年代的DigiCash、b-money、Beez、Flooz和稍后的Bit Gold、ecash。这些尝试有的只限于纸面设计，并未实际实施；而实际实施的均以失败告终，要么根本没有流通，要么流通的范围极其有限。

失败的原因大多可归结为中心化的组织结构。这些货币由特定组织发行，他们对货币的安全使用与流通进行仲裁、监督和维护，并采用中央服务器记录货币的流通情况。在缺乏国家信用支撑的情况下，一旦发行和维护组织破产或遭受法律、道德指责，或保管总账的中央服务器被黑客攻破，该货币即面临信用破产与内部崩溃的风险。

（二）技术挑战

如果不使用中心化的组织结构，那么如何对数字货币的流通进行监管就成为一个棘手的问题。数字货币只是一串字符，复制和篡改几乎不需要成本；电子货币在网络中流通，其交易数据最终必然记录于某个“账本”之中，使用黑客技术篡改这些记录也不是难事。因此，无人维护的电子货币系统，其安全性几乎是不可能保障的，这里主要涉及两个问题：

1. 货币伪造。在中心化管理的系统中，所有用户的账户余额都会记录在中央服务器中，除非入侵中央服务器，用户无法修改自己的账户余额。如果没有这一中心化管理系统，用户的电子货币存储在自己的钱包里，那么修改余额将非常容易。

2. 双重支付。中心化管理系统通过实时修改用户的账户余额，可以有效地防止双重支付，即用户利用网络延迟等漏洞，把同一笔钱支付给两个人。无人监管的系统很难防止这一情况的发生。

早期的数字货币也曾在这两个问题上进行尝试。例如，B-money方案提出了一种协议，使用工作量证明机制进行货币发行。每笔货币的传输会广播给所有用户，每个用户都知道别人的账户，因而可以证明交易的真实性和正确性。在网络出错的情况下，用户可以申请赔偿，由第三方进行仲裁，如果仲裁无法达成一致，每个用户自行确定自己的赔偿或惩罚额。

Bit Gold方案描述了一个使用去中心化方法创建永久工作量证明链的系统，该链记录使用者的公钥、时间戳和签名。该方案认为工作量证明的价值在于稀缺、难以产生、可安全存储与传输。通过点对点的拜占庭回弹（Byzantine-resilient）方法，Bit Gold可在传输时防止双重支付。遗憾的是，拜占庭回弹方法依赖于网络地址投票而不是计算力投票，因而容易遭受女巫攻击（Sybil Attack）。

而致力于创造匿名数字货币的DigiCash方案则使用了盲签名（Blind signature）算法来切断货币提现与支付之间的联系，首次在数字货币设计中引入了密码学算法。