

比特币

一个虚幻而真实的金融世界

李钧 长铗 等◎著



中信出版社·CHINACITICPRESS

014005383

F830.46
30



比特币

一个虚幻而真实的金融世界

李钧 长铗 等◎著



F830.46
30



北航

C1693357

014902383

图书在版编目 (CIP) 数据

比特币 / 李钧, 长铗等著. —北京: 中信出版社, 2014.1

ISBN 978-7-5086-4300-7

I. 比… II. ①李… ②长… III. 电子货币-研究 IV. F830.46

中国版本图书馆CIP数据核字 (2013) 第250196号

比特币

著 者: 李 钧 长 铗 李耀东 喻 峰 蔡卓斯 宋欢平 袁 维

策划推广: 中信出版社 (China CITIC Press)

出版发行: 中信出版集团股份有限公司

(北京市朝阳区惠新东街甲4号富盛大厦2座 邮编 100029)

(CITIC Publishing Group)

承 印 者: 北京通州皇家印刷厂

开 本: 787mm×1092mm 1/16

印 张: 17 字 数: 235千字

版 次: 2014年1月第1版

印 次: 2014年1月第1次印刷

广告经营许可证: 京朝工商广字第8087号

书 号: ISBN 978-7-5086-4300-7 / F · 3047

定 价: 39.00元

版权所有·侵权必究

凡购本社图书, 如有缺页、倒页、脱页, 由发行公司负责退换。

服务热线: 010-84849555 服务传真: 010-84849000

投稿邮箱: author@citicpub.com

推荐序1

比特币：预示未来货币形态和体系的实验

在过去的三四年间，我在世界的不少地方，向不同的朋友和学生讲比特币的原理和意义，和者甚寡。后来，我在北京见到李钧，得知他和他的朋友们撰写出中国第一本关于比特币的专著，与此同时，他们还是比特币的发掘者和拥有者。同时为这本书写序的李笑来就是比特币的成功实践者。对此，我由衷高兴。但是，我对于比特币的理解和肯定主要基于书本和文字，并不是比特币的实践者，也不拥有比特币，更没有用比特币生活过。所以，我更多的是从货币理论和货币历史的视角，讨论我对比特币的认知，难免有局限性。

(一)

2008年年末，源自美国的金融危机已经演变为世界金融危机，形成全球性恐慌，很多国家做出了过激反应。同时，现存的世界货币金融体系，以及对这一体系有至关重要影响的国际货币基金组织遭受普遍质疑。很多经济学家预测此次金融危机可能超过20世纪30年代的大危机。

就在这一年的11月，一篇署名中本聪（Satoshi Nakamoto）的研究报告“Bitcoin: A Peer-to Peer Electronic Cash System”发表。不到两个月，即2009年1月3日，经中本聪对其提出的比特币理论系统的实际运行，即所谓的“挖掘”过程，第一个比特币的区块横空出世，其中包含50枚比特币。

世界金融危机和比特币诞生在时间上的巧合，并不意味着两者存在直接相关性。但是，在世界金融危机和比特币诞生这两个孤立事件背后，却有着强烈的历史逻辑关系。

2008年的世界金融危机，使得人们全面反思当代各国的货币体系，对各国的货币政策提出强烈批评，美元和美国货币政策则是众矢之的。有相当多的学者、政治家和企业家认识到：当代的世界货币体系，说到底，是各国法币的集合。只是在这个法币的集合中，美元是中心法币，扮演了法币的法币的角色。毫无疑问，美元对世界货币体系的衰变责任最大，但是，其他货币也不是没有问题。只有突破现行的世界货币体系，方可走出困境。问题是，目前为止没有更好的方案。最终，各国政府应对此次金融危机的基本手段大体是货币供给的量化宽松政策，扩大政府投资并强化对经济的影响力，其结果是推动了全球范围内新一轮的通货膨胀。恰恰是在这样的历史节点上，比特币提供了克服法币先天缺陷的一种崭新思路和选择。

(二)

法币的先天缺陷，说到底就是两条：第一，法币为政府所垄断，国家

是垄断货币发行的主体。法币是通过国家权力迫使民众接受和执行的一份合同；第二，因为国家通过中央银行决定法币发行数量，其本质是不稳定的。特别是19世纪70年代之后，随着美元与黄金脱轨，各国法币都转变成没有含金量的纯粹纸币，阻碍法币发行数量持续增长的最后制度和机制不复存在，法币贬值，或者说通货膨胀成为完全不可避免的事。从这个意义上说，哈耶克认为，“历史基本上就是政府制造通货膨胀的过程。”

现行的货币制度的后果是显而易见的。一方面，通货膨胀是国家收入的基本保障：“通货膨胀一直是一种有吸引力的可供选择的收入来源，因为事实上不用任何人投票表决，政府就可以利用它征收赋税，用凯恩斯的话来说，‘它是以一种无人能弄明白的方式做到这一点的。’”^①另一方面，民众所创造的财富最终需要通过法币的形式显现，通货膨胀导致民众财富不断缩水。遗憾的是，长期以来，公众已经认定货币必须由某个最初的创造者创造，而国家就是创造者，是国家赋予货币的价值。货币天生就是政府的法币，法币就是货币的唯一存在形态。人们为国家垄断及其创造的货币付出了看不到尽头的代价，被货币奴役，逆来顺受。因为，在民众面前，并不存在可以替代政府法币的其他货币选择。

对此，哈耶克不以为然。1976年，已经77岁的哈耶克完成了《货币非国家化》一书。该书序言的开头是亚当·斯密在《国富论》里面的一段话：“我相信，世界各国的君主，都是贪婪不公的。他们欺骗臣民，把货币最初

^① 弗里德曼，货币的祸害，商务印书馆，2007年，第242页。

所含金属的真实成分，次第削减。”该书的中心思想就是，除非各国政府不再拥有对货币创造的垄断权力，否则永远无法实现价格稳定。哈耶克的理想是：在一个国家，发行具有明显差异的，并由不同货币单位构成的货币，包括让私人货币流通，并实现不同货币之间的竞争。只有这样，所有的货币发行单位才会紧缩其货币发行量，以避免因货币不断贬值而最终被淘汰的命运。为此，哈耶克提出了详尽的货币非国家化的方案。

历史常常出现严重的不公正。《货币非国家化》的出版并没有产生实质性影响。哈耶克的理念被讥笑为政治上没有可能，技术上不可行。人们的思想局限在如何改进，而不是终结政府对货币垄断的体制。即使是激烈批评通货膨胀和现代货币体系的弗里德曼也认为哈耶克的希望无法实现：能够提供购买力的私人货币，是不可能驱逐政府发行的货币的。也就是说，只能在法币不可替代的前提下，通过控制法币发行数量，抑制通货膨胀。这就是货币主义。

无疑，在思想理念方面，弗里德曼的货币主义比起哈耶克的货币思想，是一种倒退，虽然是比较温和的倒退。

(三)

尽管我们无法得知，中本聪在设计比特币的时候，是否有实现哈耶克理念的动机或者潜意识。但是，事实是在哈耶克的货币非国家化的思想早已为人们淡忘的42年之后，中本聪所开创的比特币竟然证明了哈耶克货币理念是可以实现的。

第一，比特币天生独立于任何国家、任何政府、任何央行、任何企业。

第二，比特币是开源货币，是在P2P（点对点网络）中完成解码运算后奖励给运算者（即矿工）的礼物。单个节点会向全网广播交易，矿工收集交易信息打包成新数据块。

第三，比特币的创造过程是竞争性的，需要时间、能源和其他有形成本的投入。为保持数据块匀速生成，挖矿的人越多，挖矿难度就越高，成本呈现不断上升的趋势。

第四，比特币很可能是人类自从有货币以来的第一种可以避免不断贬值的货币。基于两个原因：比特币存在终极数量，其极限是2140年的2100万枚；比特币的P2P分布式特性与去中心化的设计结构，至少在理论上排除了任何机构操控比特币供给总量的可能性。

在货币理论历史中，有一个经过美国天文学家兼经济学家西蒙·纽科姆在19世纪末提出，再经欧文·费雪完善的著名方程式： $MV=PT$ 。其中，M是名义货币量，V是流通速度，P是价格指数，T是交易总量指数。但这个恒等式对于分析货币和价格的关系只具有理论和逻辑意义。在实际经济生活中，M的主要形式是政府发行的法币，其数量从来不可控制，而P必然是非稳定的。但是，如果M不再是不可控制的政府法币，而是比特币这样不会不断贬值的货币，那么，通货膨胀似乎是可以避免的。这个恒等式就具备了现实意义。

比特币价值的稳定和上升，意味着比特币的购买力的稳定和上升。比特币越来越值钱，用于购买物品和服务所需的比特币数量越来越少。也就

是说，比特币很可能有造成通货紧缩的能力，在一定程度上抵消全球通货膨胀的大势。

(四)

如果说，比特币的创造思想和方法是人类智慧的精妙显现，那么在过去短短的四五年内，比特币在全球范围被迅速传播，被人们接受和交易，规模膨胀，则无疑是货币金融领域的具有革命意义的事件，相信中本聪本人对此也是始料未及。

原因何在？答案是：比特币是财富创造和交换的创新。比特币的每笔交易既透明又匿名，每一个拥有网络客户端的人都可以查到全世界所有即时产生的比特币交易，却无须也无法得知这笔交易来自哪里，去向哪里，用作什么用途。比特币第一次从技术上提供了每一个个体自己创造的私有财产处于不可侵犯、不可冻结和不可追踪的状态。比特币的拥有者可以在完全以信任为基础的自由体系中，拥有和享用货币财富。或者说，比特币创造的是一个自己对自己负责、依靠信用运转的世界。货币主权要回归给个人，每个人有选择货币的权力，成为货币财富的主人。尤其值得注意的是，比特币生在互联网，用在互联网，加之个人间的匿名支付，使得任何政府至今无法对其交易实行征税。从根本上说，比特币是一种自由主义的生活方式。

比特币正在创建一个以比特币作为交换媒介的现实世界。比特币实现了虚拟世界和现实世界的结合，超越地域和产业部门的比特币“场”迅速形

成。不久前，各种媒体已经报道过：美国一对夫妇曾经尝试只依靠比特币生活。那似乎需要很大的勇气。而如今，比特币的应用范围从公益组织的捐款到日常应用，已经走进人们的生活。继德国宣布承认比特币的合法地位，会有更多国家加入，同时，全球接受比特币的商家也快速增加。

如果以为比特币代表的货币财富和交换体系仅仅存在于虚拟世界，将比特币简单归结于传统电子货币的一种，那是一种误解。比特币不同于传统的电子货币，因为任何传统的电子货币都要与政府的法币挂钩，至少依赖中心服务商，并没有自身的价值。而比特币与生俱有的就是其独立性，与任何政府发行的法币或中心服务商没有任何依存关系。所以，电子货币的本质必然是发散的，加剧传统货币供给总量的膨胀，而比特币的本性是收敛的，具有吸纳传统货币流通总量的能力，减少传统货币供给总量。此外，在物理意义上，比特币与一般电子货币也不同，其向周围扩散的过程不是无序的，而是有序的；流通密度不断扩展；不可能按时间顺序重复呈现比特币流通状态，交易不可逆。最值得注意的是，依附于政府和公司的传统电子货币是不可分割的，而比特币是可以分割的。当下，比特币的最小单位是小数点之后的8位数，如果需要，比特币可以分割为更小的单位。

相较于其他任何存在过和正在流通的货币，货币功能通过比特币得以充分实现。特别集中于以下3个方面：

第一，比特币更能实现货币作为交换媒介的功能，具有超越时空和超越主权的优势，应用版图遍布世界。

第二，比特币具有高度流动性的资产的功能，并成为当前全球升值最快的资产。

第三，比特币突破了传统资产负债表只能反映一个企业在某一特定时期全部资产、负债和所有者权益情况的局限，而比特币的账本不仅包括全部历史记录，而且是动态的，可以称得上是全息图像账本。

(五)

根据比特币过去三四年的表现，不得不承认比特币的爆发力。比特币正处于持续的“宇宙大爆炸”状态。2010年7月17日，世界最大的比特币交易网站Mt.Gox成立，当时比特币的价格不到0.05美元。2013年11月已经超过了数百美元，逼近上千美元，比特币价值的扩张不是以十、百、千为单位，而是以万为单位。

造成比特币规模扩张和价值上升的原因主要有两点：包括美元、欧元和人民币在内的贬值，与比特币的比价不断下降，导致比特币与其他法币的汇率不断攀升；由于个人投资者、金融公司和金融资本的加入，比特币的交易数量增加，推动比特币价格上涨。

问题是，在2140年之前，比特币的“大爆炸”状态，还会持续多久？比特币所代表的财富数量，何时可以进入相对稳定的阶段？对此，现在难以预测。但是，在比特币实现终极数量之前，始终会存在上涨空间是毋庸置疑的。根本而言，比特币的升值空间取决于比特币对世界实体经济和货币经济的影响

程度，以及比特币对世界生产总值的直接和间接贡献的程度。有人估算，如果比特币价格上涨到 20 000 美元一枚，比特币的规模接近世界经济规模的 1%。

对于比特币的前途，有两种传统思维需要纠正。

第一，赋予比特币本身原本没有的意义。例如，比特币可能替代主权货币，甚至成为一种世界货币。比特币没有替代国家货币的使命，比特币的开源本质决定了它不会成为未来世界的唯一货币。

第二，将比特币的地位绝对化、神化，似乎不可替代。比特币的理念表明其一贯支持货币多元化，货币之间要竞争。近来，在比特币挖矿难度大幅提高的背景下，出现了类似比特币原理的若干新数字货币，如莱特币等，虽然各有不同的后发优势，依然无法形成挑战比特币、与比特币平等竞争的局势。比特币最值得肯定的是其开源本性、开放性和没有排他性。在理论上，不排除有一天会产生比比特币更完美的货币。

在过去的一年多时间里，中国成为比特币的重镇。自 2013 年夏季以来，比特币在中国的交易额已经超过世界交易额的 40%，中国比特币市场的参与者不再仅仅是个人和小额资本，而是更多的商业公司和更大的资本。就在近日比特币价格疯涨的同时，有中国电商网站宣布，成功达成第一笔比特币订单。不同于之前的个人之间的私下交易，这是世界首例商业零售订单。中国成为比特币最大市场。在国家严格控制传统金融机构，银行业基本为国有银行垄断的情况下，比特币在中国的发展尤其需要深入解读。

有一点很值得提及：过去几年，中国一度盛行货币阴谋论和货币战争的说法，影响广泛。但是，至今还没有人将比特币的诞生视为一种阴谋，也没有人提出比特币会加剧政权货币之间的战争。^①

(六)

在结束这篇序言的时候，我最希望表达的是：人类所经历过的货币国家化的历史，与货币非国家化的历史比较，实在是太短暂了。哈耶克主张的货币非国家化有足够的历史根据，却没有成为经济学界的主流，也不为民众所理解。在一些国家和地区，人们进行了诸如地区货币、社区货币的实验，却难以成势。比特币的出现，在唤起人们的货币非国家化的信念的同时，还提供了真实的实验。比特币证明了货币经济回归自由的可能性。

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
经济学家

^① 事实上，我过早庆幸了。就在我写这篇序言的当天，在网上看到了一种比特币阴谋论：“神秘的背后往往暗藏阴谋，比特币恐怕就是一个巨大的阴谋……美国法院、参议院以及美联储之所以对比特币接连表现出极大的兴趣，一言以蔽之，就是希望借助互联网在线交易的巨大发展潜力，将比特币创建成一个主导全球在线支付的货币，进而在美元之外创建另一个由美国主导的世界货币。”

(http://blog.sina.com.cn/s/blog_4a46559f0102e20j.html)

推荐序2 比特币的天命

所有的事物和体系都有自己的空间和时间坐标。我们的世界因哲学、政治、宗教、文化和语言之限而分隔，却因交易的愿望而合为一体。这愿望是终极的人类社会契约，赋予我们学习、合作及竞争的共同动力。这样一个包含着和谐与纷争的无尽循环，创造了超出过往世代理解范围的现代奇迹。

但我们有这样一个问题：当今的全球金融体系拥有支配商业活动的权力。

古代世界关于饥荒、洪水和地震的恶兆，已经被金融崩溃、银行舞弊、政治对商业活动的管制和恶性通胀所替代。对于货币改革的支持者来说，中本聪的比特币仿佛一则预言，令我们振奋不已。2009年1月3日，在比特币诞生的那一天，《泰晤士报》登载了《财政部长即将发起第二次银行救市计划》。

比特币不仅仅是一种货币，更代表着一种新的金融体系。它不再需要银行，也不需要刻意讨好中间人、机构或政府。它是一个超越地域和语言的体系，赋予世界以自由。而在此之前从没有人能将财富瞬间转移至世界任何一

个地方。我们借这个体系而联通，进而实现平等。

然而，如果没有一支“队伍”大声召唤，这个世界的金融体系难以回归和谐。他们必须向世人教授关于货币本身的社会契约，比如政府和原材料并不能创造价值；一种货币的价值永远取决于其能否有效行使以下职能：贮藏价值、单位计量以及在接受此种货币以交换产品和服务的人群中充当交易的手段。

他们必须教导大众如何通过比特币王国的考试。考试科目包括密码学、编程、点对点网络、奥地利学派经济学、企业家精神和比特币宣道精神，进而在人群中寻找领袖。

这本书是你进入密码货币世界的开端。如果你希望通过考试，成为比特币世界的人才，那么你要做好准备，踏上一条危险与孤寂之路。但请相信，你不会独行。我们将会与你共渡这次旅程，抵达新的秩序与和谐。你我将成为彼此谦卑的引路人。

查尔斯·霍斯金森

比特币基金会教育委员会前主席

推荐序3

比特币：开源货币实验

比特币或许将是 21 世纪最优秀的发明之一，而在其向全球拓展的过程中，这本书将成为中国社区乃至全球比特币社区的引路人。作为中国第一本比特币领域的著作，其作者囊括了中文比特币社区里的 7 名重要成员，内容覆盖了比特币的历史、发展及未来等多个关键领域。

比特币不仅仅是一种货币，更是一项开源的去中心化运动，并且引起了更为广泛的讨论，例如货币本身所扮演的角色和所承担的使命，社会与政府之间的互动等。因此，对于个人来说，了解比特币的使命及大事年表是至关重要的。本书覆盖范围广泛，囊括了比特币发展过程中的各个里程碑事件，包括币值的大幅升跌、海盗党创始人理查德·法尔克维奇所做的工作、2013 年加州圣何塞举行的比特币大会、加利福尼亚州政府与比特币基金会之间的官司纠纷、Mt.Gox 交易所与美国政府间的沟通互动、比特币生态圈在德国的迅猛持续成长等。

而更深远的关注则落在了去中心化支付系统和交易所的未来上。比特币

是当今最优秀的加密货币，而其他的支付和交易体系，如莱特币也已崭露头角。这本书将目光投向了比特币和其他加密货币的未来，并同时将货币的历史和比特币的特有价值（这一价值远超其法币价格）纳入考量。

这本书将作为催化剂，围绕比特币这一主题，激发影响更为深远的对话。比特币及其对货币和社区的愿景使全球人民共同协作，相互分享。在一个小政府、自由市场以及如比特币生态圈这样的宣扬自由的环境里，要想成事，就必须对不同性别、不同信仰、不同文化甚至不同社会经济形态一视同仁。

比特币不仅仅是一种正在成长的电子货币，更是拥有巨大发展潜力的跨文化、无国界的货币，所有互联网用户都能使用。在全球各比特币群体正在迅速成长的今天，我期待中国比特币社区的进一步发展壮大。中国比特币社区的潜力巨大，而中国比特币社区的成功将是比特币长期成功的催化剂！我认为，这本书将进一步使中国及全球人民更深入地了解和支持比特币。让我们继续推动其在全球范围内的成长，使这一了不起的去中心化数字货币为人类所用，使其带来金融领域的进步。

伊莉莎白·浦劳熙

比特币基金会董事会成员

比特币基金会教育委员会成员

《比特币》杂志通讯主管