这是中国乃至世界正在经历的一场重大变革

区块链革命

区块链

重塑经济的力量

韩布伟 著

区块链的三大变革：去中心化、开放性、智能合约

区块链时代来临 抢占时代红利
从反对走向热捧 从争议走向运用

中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

区块链

重塑经济的力量

韩布伟 著

中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

内 容 简 介

区块链作为一个全新的热点经济概念，具有去中心化、开放性、信息不可篡改等特点。本书将通过比特币及货币的历史来解读区块链的实质、区块链与大数据的关系及政府、投资机构的参与方式。本书对区块链来源、数字货币应用、区块链四大核心技术（分布式账本、加密授权技术、共识机制和智能合约）一一进行了理论分析与讲解。为了让读者更早地看到区块链的实际应用，我们还讲述了区块链在数字资产、公共领域、物联网方面的应用及未来区块链的发展趋势。

图书在版编目（CIP）数据

区块链：重塑经济的力量 / 韩布伟著. —北京：
中国铁道出版，2016.12
ISBN 978-7-113-22422-6

Ⅰ. ①区… Ⅱ. ①韩… Ⅲ. ①电子商务－支付方式－
研究 Ⅳ. ①F713.361.3

中国版本图书馆 CIP 数据核字（2016）第 242770 号

书　　名：区块链：重塑经济的力量
作　　者：韩布伟　著

责任编辑：吕　芠　　**读者热线**：010-63560056
责任印制：赵星辰　　**封面设计**：MX DESIGN STUDIO

出版发行：中国铁道出版社（北京市西城区右安门西街 8 号　邮政编码：100054）
印　　刷：三河市华业印务有限公司
版　　次：2016 年 12 月第 1 版　　2016 年 12 月第 1 次印刷
开　　本：700 mm×1 000 mm　1/16　**印张**：13　**字数**：189 千
书　　号：ISBN 978-7-113-22422-6
定　　价：48.00 元

前言
FOREWORD

2016年初，华尔街巨头投资银行高盛发布报告表示，区块链技术已经做好准备要颠覆这个世界。此前，高盛已经和中国IDG资本联手向区块链创业公司Circle Internet Financial投资5 000万美元。

作为数字货币比特币的底层技术，区块链彻底颠覆了传统的支付体系，重新定义了交易和各领域后勤办公的潜力。自2016年以来，不仅是是高盛，金融界其他巨头也纷纷向区块链技术抛出橄榄枝。

前摩根大通高管、信用违约互换（CDS）之母布莱斯·马斯特斯（Blythe Masters）加入数字货币公司Digital Asset Holdings，出任CEO；而包括纳斯达克、花旗、Visa在内的金融行业大咖也向区块链领域大把“砸钱”，他们联合投资了一家区块链初创公司Chain，涉及金额高达3 000万美元；花旗、摩根大通等金融机构还向一家区块链初创公司Digital Asset投资5 000万美元。

2016年1月，10多家国外大型银行对外宣称已经成功实验了区块链技术。在模拟现实（VR）环境下，区块链技术已经初步实现了银行和银行之间的即时交易，未来金融行业的操作标准很有可能就此诞生。参与区块链应用实验的10多家银行都属区块链联盟“R3 CEV”的成员，包括花旗银行、富国银行、汇丰银行、瑞士信贷银行等都是大家耳熟能详的国际著名银行。这次协作实验相当于是金融业在区块链技术应用领域的首次尝试。

金融机构纷纷关注区块链都是有原因的。俗话说先下手为强，如果反应比同行慢，最后只能被局势淘汰，因为你已经跟不上这个高速发展的科技时代了。

在当前的结算模式下，第三方清算中心管理着银行间的票据账本，而银行和银行之间的交易只能通过清算中心来完成结算。而由区块链设计出来的架构不需要经过清算中心，由银行和银行之间共同管理票据账本，交易在银行和银行之间完成。

区块链技术给金融机构带来的好处主要体现在两个方面：一方面是大幅度缩

短了结算时间。结算中心需要至少一天时间来完成结算，而区块链技术可以让结算时间缩短到分钟或秒；另一方面是提高了银行间的透明度，降低了欺诈风险。交易数据由同网络内的成员共享，任何对交易数据的修改都需要得到所有成员间的认证。

在区块链的热潮下，中国也不甘落后。2016 年 1 月 20 日，中国人民银行在北京召开数字货币研讨会，宣布其数字货币研究取得了阶段性成果，并声称开始探索发行数字货币，而其背后核心就是区块链技术。在未来，区块链技术不仅会颠覆金融业，还将在众筹、证券等领域发挥巨大作用，承担“颠覆者”的角色。

区块链科学研究所创立者梅兰妮·斯万（Melanie Swan）认为，区块链技术的发展分为三个阶段：第一个阶段是数字货币领域的创新，如货币支付、转移和支付系统等；第二个阶段是智能合约创新，如证券登记、期货贷款的清算结算等；第三个阶段是人类组织形态的变革，包括科学、文化、健康以及司法、投票等领域的区块链应用。

尽管区块链已经在全球掀起热潮，但我们也应当清醒地认识到，无论在国外还是在国内，区块链技术的发展都处于早期阶段，各种区块链技术给出的解决方案都需要进一步探索和实践。

特别是在中国，“区块链”这个词对很多国人来说仍然是一个既新鲜又陌生的名词。新鲜是因为区块链好像一夜之间就成为网络上的热词，引起了社会各界人士的广泛关注；陌生是因为“区块链”这个词语让人听起来云里雾里，很难解释清楚。

作为一个新技术，人们对区块链的认知、研究和实践还远远不够。中国要想在这一领域建立起优势，引领全球，还需要更多地重视和投入。尤其是理论研究者、互联网技术派、金融从业者及政府监管部门，应当积极投入并进行良性互动。在这种形势下，《区块链：重塑经济的力量》的出版，就是为了向大家介绍区块链的技术特点以及开发应用的前景。

区块链到底是什么？区块链有什么用途？区块链具有颠覆世界的力量吗？区块链技术会重塑世界经济吗？本书会一一为你解答。接下来，让我们一起走进区块链，揭开它的神秘面纱，探寻区块链的本质吧！

目录 CONTENTS

第 1 章　区块链即将主导这个世界 / 1

这是一场伟大的社会实验 / 2

为何采用限量限速模式 / 6

你是新一代矿工吗 / 8

知足吧，价值千万元的比萨饼你也经常吃 / 12

区块链对金融系统冲击如何 / 14

区块链与比特币是父与子的关系吗 / 16

P2P 钱包，个人资产数字化 / 20

你将是世界公民，而非一国公民 / 24

借助区块链实现家庭自动化 / 28

第 2 章　价值交换：区块链价值存在的理论基础 / 31

以价值交换为依托的人类货币进化史 / 32

由加密货币转为数字货币 / 35

虚拟币市场为什么如此火爆 / 37

价值永远不会投机，而货币会 / 41

游戏币、Q 币为什么与区块链、比特币不一样 / 44

价值主导世界，未来必定属于虚拟货币 / 47

区块链股权众筹为什么很合理 / 51

第 3 章　区块链去中心化，交易不需要第三方 / 55

节省数百亿元交易成本的新模式 / 56

被失业的金融业 / 60

去中心化、分布式核算与存储 / 61

均等的节点权利和义务，更公正 / 66

第三方维护变为共同维护 / 68

让汽车租赁与销售体验前所未有的简单 / 69

区块链改进股票交易过程 / 72

第 4 章　区块链开放性系统，自由查询数据 / 77

回顾过去，第三方系统你能看见吗 / 78

区块链数据对所有人公开 / 80

任何人都可以查询 / 83

任何人都可开发相关应用 / 86

永久存储，信息不可篡改 / 93

太可笑，有人想要造假 920 亿个比特币 / 96

你想匿名，这里可以实现 / 100

第 5 章　区块链智能合约，机器式契约信任 / 103

为第三方中介信任付出的机会成本 / 104

基于协商一致的规范和协议的区块链 / 106

数据交互是无须信任的 / 109

看涨期权的智能合约 / 113

有了区块链，选举更安全 / 116

摇滚乐队将新单曲版权编进区块链 / 119

可以用区块链保存遗嘱的 Blockchain Apparatus / 123

第 6 章　金融业先接受区块链的洗礼 / 127

为什么是金融业 / 128

支付汇款方式变革 / 131

票据清算重构 / 133

区块链让审计人员下岗 / 138

复杂的产权确认，这里很容易 / 139

轻松证明你，就是你 / 141

第 7 章　大数据时代，区块链与数据挖掘 / 147

大数据不止于大 / 148

数据让一切决定有了理论支撑 / 151

金融业离不开大数据挖掘技术 / 156

区块链系统上的大数据 / 162

区块链的仪表盘 / 165

区块链系统的数据瓶颈 / 166

区块链 + 大数据 = 医疗卫生行业的数据革命 / 168

区块链，让预测市场走得更远 / 171

第 8 章　巨头在行动，区块链的未来蓝图 / 175

各国政府态度变化，从比特币到区块链 / 176
投行高盛《区块链：将理论应用于实践》报告核心解读 / 183
区块链蕴含的投资机遇和创业机会 / 187
Bitpay 融资 3 000 万美元，下一个独角兽 / 190
智能合约平台 Symbiont 获 700 万美元融资 / 192
进入区块链领域，你需要准备什么 / 193
下一个阿里巴巴，或许在此产生 / 196

第 1 章

区块链即将主导这个世界

尽管区块链技术还处于起步阶段，但那些较早投入这一领域的创业企业已经为区块链技术的发展与崛起打好了基础。在区块链的带领下，未来比特币可能将进入实用时代，解决人们现实生活中的问题。区块链的核心是一个数据库，就像一个记录交易的账本。在未来，区块链技术将被应用在许许多多领域中，包括公证类、证券市场、支付系统等。下面，我们一起看看区块链主导下的世界是怎样的。

这是一场伟大的社会实验

区块链的应用范围很广。比特币是区块链中一个应用案例。提起虚拟货币比特币，大家都比较熟悉了。比特币是区块链技术的一种表面形式之一，区块链的应用也不仅仅局限于比特币。尽管比特币的出现带来了很大的争议。然而，由于其高的度的安全性，许多国家逐渐由反对到默认，由默认到支持。大家逐渐注意到比特币所应用的区块链技术，尽管作为虚拟货币的比特币在中国尚未被认可，但对实体货币来说，研究以区块链为基础的虚拟货币，极具探索意义。

为了便于理解，我们借助比特币来解读区块链。

人与人进行商品交易，必须以一种货币为参考。英国作为世界上最早发达的资本主义国家，于 1821 年正式启用金本位制，英镑成为英国标准货币单位。因与黄金直接挂钩，英镑很快取代黄金成为世界贸易和储备的货币，开始主导全球的金融和贸易，也使英国成为全球拥有殖民地最多、财富最雄厚、国力最强盛的“日不落帝国”。

第一次世界大战的爆发使英国的实力被严重削弱，而美国在第一次世界大战中实力大增，因此美国开始垂涎英镑的全球主导地位。美国利用第一次世界大战和战后重建获得了巨大的经济、政治利益。到 1929 年，美国工业产能占全球总量的 42.2%，相当于所有欧洲国家的产量总和。第二次世界大战时期，美国成为全世界反法西斯的战略大后方，成为第二次世界大战的主要受益国。战争几乎毁灭了德国、日本和意大利，极大地削弱了英国和法国的实力，前苏联也是满目疮痍。在

这场战争中全须全尾的美国国内生产总值占全球近一半，贸易量占全球的 40%。

世界各国为了应付战争不得不拿出大量的黄金向美国购买武器和战争物资，犹太人积累的财富也流向了华尔街。美国成为全球最大、最强盛的经济体，黄金储备占全球的 59%，美元取代了英镑的全球地位。如图 1-1 所示为基准货币的变化。

图 1-1　基准货币的变化

黄金储备之所以决定英镑、美元全球货币地位，是因为黄金具有五大核心功能，即价值尺度、流通手段、贮藏手段、支付手段和世界货币，那比特币呢?

与黄金不同，比特币是虚拟货币。我们了解黄金如何成为世界货币后，就会发现比特币作为全球货币是有可能的。如图 1-2 所示为对于基准货币的变化猜想。

图 1-2　基准货币的变化猜想

众所周知，地球上的黄金总储量是有限的，但人类还没有把所有的黄金都挖出来，并且黄金的供应量也是以一个适当的年化速率在逐渐增加。当黄金的价格上升时，矿工们受到激励促使他们进行黄金的勘探和生产，因此，价格的上涨通常会伴随着产量的增长。

比特币在当下和黄金一样，“挖矿”是由价格上涨所激励的。供应量的增加及价格的上涨通过提供不容错过的好价格来鼓励那些拥有“储蓄”的人进行消费，

这在理论上有助于在商业和储蓄之间维持一个长期的平衡。但是，理论和实践经常是不一样的，我们马上就会讲到为什么，但首先让我们谈谈比特币和黄金的区别所在。在黄金的世界里，我们永远也不能想出一个时间点，在这个时间点流通中的供应量永不再增加，但在比特币的世界中，供应量增长的截止时间是已经确定了的。

2008 年，域名 bitcoin.org 被静悄悄匿名注册成功。同年 10 月 31 日，有一篇名为《比特币: P2P 电子货币系统》的论文被发表在某个网站上。10 天之后，开源社区 sourceforge.net 上出现了一个叫作 bitcoin 的项目，这就是比特币的起源。

这个项目的创造者究竟是谁没有人知道。开发者只留下了一个中本聪 (Satoshi Nakamoto) 的名字，他在搭建完比特币体系后就从互联网上彻底消失了。此后项目由两个前谷歌（Google）工程师维护，但即便是他们俩也声称从未见过中本聪。有人说中本聪是从未来坐着时间机器来到现在写了这个程序。

比特币的本质其实就是一堆复杂算法所生成的特解。特解是指方程组所能得到无限个（其实比特币是有限个）解中的一组，而每一个特解都能解开方程组并且是唯一的。

以人民币来比喻的话，比特币就是人民币的序列号，你知道了某张钞票上的序列号，你就拥有了这张钞票。 而挖矿的过程就是通过庞大的计算量不断去寻求这个方程组的特解，这个方程组被设计成只有 2 100 万个特解，所以比特币的上限就是 2 100 万。比特币区块链数量变化如图 1-3 所示。

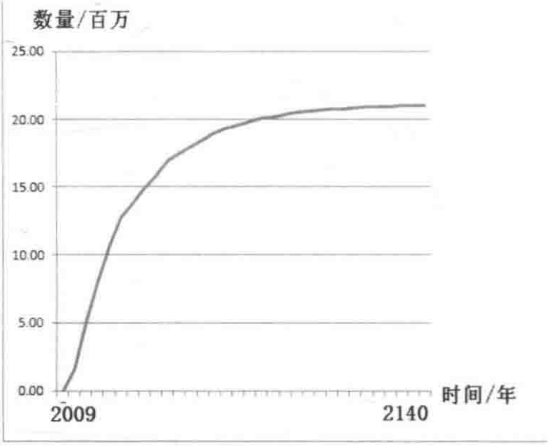

图 1-3 比特币区块链数量变化

为了控制比特币的数量，规则制定者采用 4 年减 50% 的策略。即，在第一个从 2009 年 1 月到 2012 年 1 月，约有 1 050 万个比特币被生成。随后的每 4 年这一数值减半，所以在第 5 ~ 9 年会产生 525 万个比特币，第 10 ~ 13 年生成 262.5 万个币，并以此类推。这样，比特币的总量就永远不会超过 2 100 万个。到 2140 年时，基本不会再产生新的比特币了。

由此可以看出区块链的价值。其实区块链的价值远不止于此，接下来我们看一下区块链的特点。

汇丰银行曾发表过一则研究报告，报告中建议中央银行使用区块链技术，以实现货币政策的精准投放。例如，在比特币区块链中，任何一个支付都可以被追踪，如果在一笔钱上写上一段程序，不允许投放到房地产行业，那这笔钱就永远进不了房地产公司的账户。汇丰银行之所以提出这一建议，在于区块链具有价值互联网的特点。当然，它的特点不止这一条。

区块链本身自带价值互联网的四大特点，如图 1-4 所示。

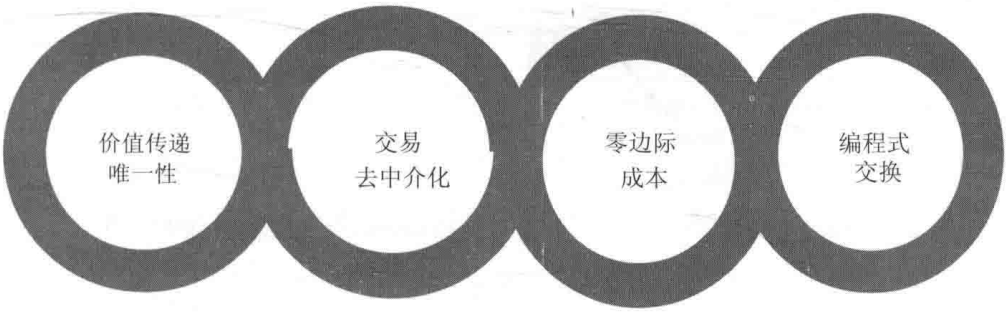

图 1-4　区块链本身自带价值互联网的四大特点

第一，通过互联网进行 P2P 或点对点价值交换时，需要解决信息传递的问题。例如，我们在网上发邮件，发给一个人与发给 100 人，不会出现明显的成本增加。而如果通过互联网付款时，就只能付给一个人。所以，信息可以无限地复制，而价值交换需要保持其唯一性。为了避免这种现象发生，我们就需要通过区块链来阻止。

第二，价值互联网需要建立一个规则。这一规则使互联网在价值交换中实现去中介化，在没有金融业做担保的情况下，也能实现让人放心的支付功能。这时就需要一个使双方都信任的算法来保证，区块链就是这个算法。

第三，零边际成本。因为没有第三方参与，只是通过一个算法使双方建立信任关系，所以这里交易的成本就特别低，基本可以实现交易零成本。

第四，价值编程式交换。例如，你通过基金会做一次捐款，用途为校园的修建。如果你使用数字货币上的区块链去支付这笔钱，可以在区块链上写一个小小的程序，把学校的账户写上去，然后一起寄给基金会。如果基金会不往指定的学校账户支付这笔钱，那么这笔钱基金会永远得不到，也汇不出去。因为你付的不仅仅是钱，还有一段代码。

这场实验已经在全球展开，美国、德国、中国、日本等国家已经在关注区块链的动态，各大投资机构也纷纷入场，大家不妨静下来，等着传奇发生。

为何采用限量限速模式

“比特疯”是流行于互联网的一个新词汇，寓意为“疯狂的比特币”。作为网络虚拟资产，每一块比特币的产生、消费记录都会记录在区块链上，不存在伪造的可能。随着比特币的流行，比特币已经可以兑现成大多数国家的货币。数量有限而且具有极强的稀缺性是比特币与其他虚拟货币最大的区别。

比特币（Bitcoin）也叫作“比特金”，首次发行于 2009 年 1 月 3 日。比特币的获得离不开计算机程序计算。如果你有一台配置还不错的计算机，并且对于计算机程序略懂一二，就可以下载一个客户端，使用特定软件，完成特定数学程序后获得一定数量的比特币。业内将获取比特币的过程称为“挖矿”。显然，“挖矿”与开心网上流行的“偷菜”不一样，它对计算机硬件要求非常高，而且所进行的数学计算也是极为复杂的。

比特币有两个明显的特征：首先，比特币是通过网络节点计算产生的，不像人民币、日元、美元一样有固定的发行方。只要具备了相应条件，任何人都可以参与制造比特币；其次，比特币的发行量是限量限速的，这是因为软件算法的特解有一定的额度，所以不会无限量发行。现有的比特币数量越多，将来挖掘新币的难度也就越大。截至 2016 年，已有的比特币约为 1 530 万个。到 2140 年左右，比特币的产量将达到其上限——2 100 万个，在上一节中已经做了说明。

据了解，中国已经超越美国和日本成为比特币投资交易最活跃的国家之一，如图 1-5 所示是 2009 ~ 2016 年比特币在中国日交易量的增长情况。

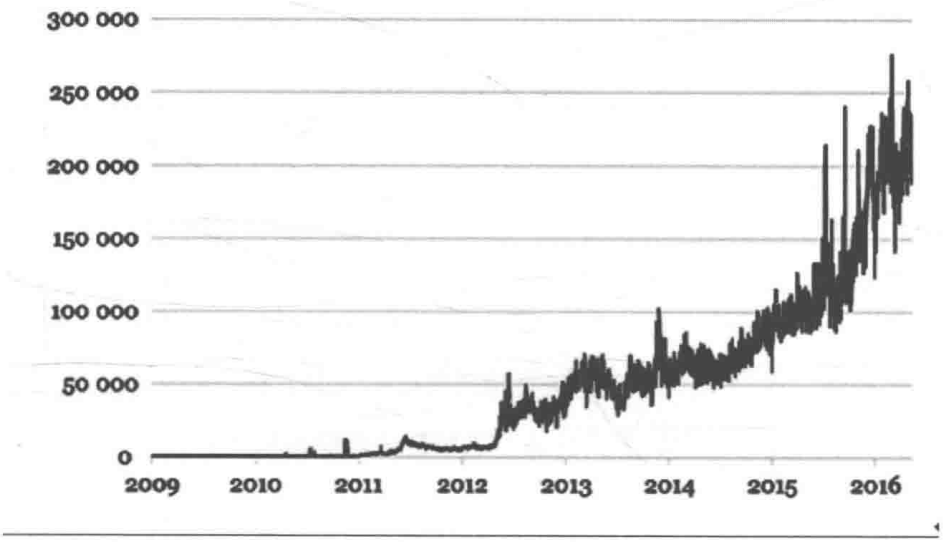

图 1-5　2009 ~ 2016 年比特币在中国日交易量的增长情况

因为比特币而一夜暴富的投资人数不胜数。有成功的投资人说：“现在的一枚比特币是一部苹果手机，以后将会成为一栋房子。”与此同时，投资人也不能忽视比特币投资的风险。

在最初诞生的几年里，比特币几乎不为大众所知，而且没有什么价值。情况发生改变是从 2013 年塞浦路斯发生金融危机开始的。某些欧洲国家的货币大幅贬值，而比特币却突然一路高涨，掀起了炒作热潮并带动了整个数字货币行业的掘金狂潮。2013 年 11 月，一枚比特币相当于 8 000 元人民币，综合涨幅超过

10 000 倍。2013 年年底，中国央行宣布比特币在中国为“非法货币”。此后，比特币市场开始冷静下来，比特币的价值持续走低。

然而，人们发现，比特币自推出以来，从未出现过资金或用户信息被盗用的记录，充分证明了其安全性。这使得人们对比特币背后的区块链技术的信息不断加强。

2016 年以来，各国纷纷采取行动关注以比特币为代表的数字货币。2016 年 1 月 20 日，中国人民银行数字货币研讨会在北京召开，央行明确表示将争取早日发行央行数字货币。与此同时，日本国会也批准有关加密数字货币的新法案，将数字货币视为一种具有货币功能的合法支付形式。另外，作为全球金融中心之一的英国也宣布发布数字货币 RSCoin 并进行测试。

作为一种投资标的，比特币为什么会得到众多投资人的喜爱呢？最主要的原因就是比特币的数量和挖掘速度都极其有限，不像股票、纸币一样可以增发。相比之下，数字货币具有天然抗通货膨胀的属性。

综上所述，比特币无论从金融层面还是社会层面，都已经从默默无闻变得万人瞩目。而因其具有限量限速的特征，越早尝试吃螃蟹的人就越能占据先机。

你是新一代矿工吗

作为一种总量只有 2 100 万的数字货币，比特币的价值高也是符合常理的。价值连城的比特币吸引着众多人士的注意力，很多人都想知道除了金钱交易以外获取比特币的渠道。由于比特币存在于数字空间中，隐藏在特定算法里，所以必须投入足够多的人力物力才能挖掘出来。通过计算机设备运算产生比特币的过程就是所谓的比特币“挖矿”，而操作这一过程的人就是新一代矿工。在这一过程中，新的区块不断产生，成为区块链。