区块链：定义未来金融与经济新格局

作者：张健

区块链：定义未来金融与经济新格局

张健　著

ISBN：978-7-111-54109-7

本书纸版由机械工业出版社于2016年出版，电子版由华章分社（北京华章图文信息有限公司，北京奥维博世图书发行有限公司）全球范围内制作与发行。

客服热线：+ 86-10-68995265

客服信箱：service@bbbvip.com

官方网址：www.hzmedia.com.cn

新浪微博 @华章数媒

目录

推荐序一
推荐序二
序言
致谢
第0章　必然的出现
文字与货币
信息的演化
尝试定义信用
从互联网到区块链
区块链的诞生
第1章　区块链是什么
记账货币
天才的发明
共识机制与价值载体
当交易变得智能
将区块链连接起来
区块链的未来
本章结语
第2章　区块链带来的新机遇
数字货币产业链
互联网金融
物联网与共享经济
新一代基础设施
本章结语
第3章　区块链的应用场景
数字货币
众筹
清算、结算与审计
智能合约
版权与许可
公证与记录
更多
第4章　区块链技术原理
密码学基础
区块链组成
共识算法
侧链技术
附录1　比特币：一种点对点的电子现金系统
附录2　以太坊：下一代智能合约和去中心化应用平台（选译）
后记
对话作者：区块链离我们还有多远
大家谈之《区块链大革命》

未来已经来临，只是尚未流行。

——威廉·吉布森（William Gibson）

推荐序一

随着互联网金融向纵深发展，区块链技术及其应用成为人们日益关注的热点。区块链技术开始从概念走向实际应用，越来越多的资金流向区块链的创业企业以及相关领域的创新，随着各国的金融机构甚至一些大型传统企业加入区块链技术的探索行列，一场真正的革命正悄然到来。

2015年10月，《经济学人》发布封面文章：制造信任的机器——比特币背后的技术将如何改变世界。理解这句话的意思并不难，然而理解其背后的机理却相当不易。这不仅需要对于区块链本质有认识，更需要诸多跨学科的背景知识，远不是一两句话就能够解释明白的。这也是我们推荐这本书的原因所在。通读本书，最大的感受是，作为区块链行业的从业者，作者的视野和知识结构都没有局限于自身的职业。本书开篇通过简述人类社会信息转播方式和价值传递方式的演化路径，勾勒出一个从信息到信用、从互联网到区块链的发展轨迹，引出了区块链这种高效的价值传递方式出现的必然性。谈到区块链的本质，作者又从货币开始讲起，同时引入大量背景知识，让读者对区块链的内涵有更为深刻的理解。这种系统化的论述，对一项新兴技术甚至思想的推广普及，无疑有着非常重要的意义。

区块链的优势在于能够用非常低的成本解决网络交易的身份识别和个人征信，以及使用点对点的交易避免了传统集中式的清算结构，从而能够大大提高金融系统甚至整个经济体系的运行效率。除了区块链的诞生背景及本质，本书还围绕区块链的各个方面分别谈了区块链带来的新机遇、各种应用场景以及具体的技术原理等内容。比如谈到互联网金融，作者提出了“区块链将成为互联网金融梦想照进现实的关键技术”这样让人印象深刻的观点；提及物联网与共享经济，作者从理论的角度分析它们目前面临的问题，并引出区块链对解决这些问题的价值与意义。虽然本书涉及的领域非常宽泛，很难做到面面俱到，但书中所讲的各种观点以及独立思考的精神，是难能可贵的。

与常见的新技术布道者不同，本书体现了少见的冷静。作者坦承，现在的区块链处在它的婴儿时期，各方面的基础设施还很不完善，而这种不完善限制了区块链的大规模应用。在我看来，中国需要更多的这种不虚美、不隐恶、冷静务实的金融科技从业者，而这也是整个国家的金融体系稳步改革和发展的基本保证。

廖理

清华大学五道口金融学院教授、博士生导师

互联网金融实验室主任

推荐序二

2011年，已经连续创业多年的我无意中听到朋友介绍比特币；2013年下半年，火币网成为当时我们只有20多人的创业公司里并行的第四个项目。2013年9月，在火币网上线后不到3个月的时间，比特币涨到8000元一枚，火币网一跃成为行业的领军交易平台。截至今日，我们已经为超过30个国家和地区的150万用户提供交易服务，累计交易额突破1万亿元。

在火币网做出一些成绩后，经常有人来问我成功的秘诀。鸡汤也不是没有灌过，但回首往事，我清楚地知道火币网能有今天，除了全员上下的不懈努力，运气的成分必不可少。创业维艰，九死一生，不是所有的努力都能有结果，我们只是在对的时间做了一件对的事情。这件事总的来说，便是认识到了比特币乃至其背后的支撑技术——区块链的价值。

区块链可能是21世纪最让人兴奋和值得期待的技术创新之一，它创造性地使用技术的方式为交易双方建立信用，而无需第三方机构参与，从而极大地降低了交易成本。如同互联网技术革命性地降低了人类信息交互的通信成本，区块链技术的广泛应用，在未来将极大地降低价值交换的信用成本。

火币网作为行业的领军企业，因此有责任和义务向公众客观全面且深入地介绍比特币的底层技术，这也体现了我们要长期扎根数字货币产业的诚意和决心。2015年以来，随着区块链技术的蔚然成风，市场上陆续出现了一些相关书籍，但质量良莠不齐。本书作者张健力图以高屋建瓴的视角、深入浅出的文字，让普通读者也能领悟这一创新技术的价值和奥秘。本书从整个人类文明的发展讲起，从信息交换和价值传递的路径提出区块链出现的必然性，在全面地介绍这一技术突破的同时，保持研究者的冷静和客观。我作为比特币这个新兴行业的资深从业者，推荐读者阅读此书，本书可作为了解区块链技术的入门书籍，相信你在本书中可以体会到一个研究者应有的专注和专业。

2014年6月，我第一次见到本书作者张健，当时他在做国内最大的区块链查询网站（qukuai.com）。同为连续创业者的我们志同道合，相谈甚欢，很快确立了合作意向，张健也以此为契机加入了火币网团队。经过两年的共同创业，张健最为打动我的是他对区块链事业的热爱，以及对于创业的专注、坚韧和执着。2016年年初，为了更好地推进区块链业务的研发和开拓，火币网成立了区块链研究与应用中心，张健以火币网技术副总裁的身份任中心负责人。本书是该中心成立后第一项向公众展示的成果，之后我们还会有一系列的研发、教育、公众科普与商务合作项目，致力于全面推动比特币乃至区块链产业的发展。

人生的大方向很多时候是由一些微不足道的瞬间决定的。如果不是在几年前的饭桌上听到比特币的理念，我可能不会做火币网；如果不是因为火币网，我便没有机会结识张健和其他在火币网工作的同仁，也不会为了我们共同的理想而奋斗。希望对于各位读者来说，在翻开这本书的这个瞬间，也能让你们开始对区块链这个令人激动的创新技术产生兴趣，希望有越来越多的人才进入这个方兴未艾的行业，与我们共同创造一个科技引领改变的未来。

李林

火币网创始人兼董事长

序言
有幸成为新时代的亲历者

价值互联网时代

我有幸亲历的这个新时代，是价值互联网时代。而正在拉开这个时代大幕的，却是在诞生初期并不起眼，但目前越来越受到关注的区块链技术。【欢迎加入罗友书社，微信：15535237487，罗辑思维，得到APP，樊登读书会，喜马拉雅系列海量书籍与您分享】

区块链虽然以技术的面目诞生，但是其所带来的，已经远远超越技术范畴本身，正如互联网所给我们带来的一样。在我看来，区块链不仅仅是一项技术、一个工具，更是一种思想。开放、共享、去中心化，区块链的这些核心精神与互联网不谋而合。而与互联网不同的是，区块链把这样的思想从信息的传递进一步拓展到价值的传输。

互联网时代的来临，使得信息传输的成本趋于零，这已经深刻地改变了社会的经济格局及每个人的生活。这促使我思考，当未来市场交易成本趋于零的时代到来时，整个世界经济格局及社会结构将发生怎样的变化？

我们必须为这样的变化做好准备，因为这个时代正在朝我们走来。

我与区块链的缘分

区块链作为比特币背后的技术，于2009年年初正式诞生。而我真正关注到这项技术是在2013年。当时，随着价格的暴涨以及媒体的报道，比特币第一次走进了大众的视野。与大多数人关注点不同的是，我对比特币背后的技术产生了非常大的兴趣，于是开始一探究竟。而当我真正懂得了比特币背后的逻辑，即区块链的原理时，我被这样优雅的设计深深震撼了。这开启了我与区块链的缘分——由兴趣到事业的过程。

2014年年初，我开始着手创建一个区块查询网站。创建这个网站的初衷是，当时国内并没有这样的平台，而国外的平台对于国内用户来说，无论是速度还是体验都不尽如人意。经过一段时间的努力，2014年3月，国内首家比特币区块浏览器“区块”（Qukuai.com）正式上线。通过这个网站，任何人都可以非常方便地查询区块链的数据。网站上线以后，逐渐获得国内比特币用户的支持与青睐，这让我萌发了把这个兴趣当作事业的想法。

于是，基于区块网站，我做了一系列的功能升级，并推出了一个比特币钱包——“快钱包”。在这个过程中，我有幸结识了火币的创始人李林。怀着对这个新兴行业共同的理解与对前景的认同，我选择加入火币。作为一个年轻的品牌，火币于2013年下半年诞生并迅速成长为国内最大的比特币交易平台。通过一系列的产业链扩张，火币立志成为数字货币领域的基础服务商。如今，火币已经颇具规模，成为行业内名副其实的领军企业。这使得我们有能力也有责任来做一些基础工作，为推动整个行业的发展贡献力量。于是2016年年初，我牵头成立了火币数字货币与区块链研究中心，专注于数字货币与区块链技术的研究及行业基础设施的建设。

创作此书的初衷

最近两年，区块链从不为人知到获得越来越多人的关注，甚至正在成为一个热门的新兴领域，其实有着深刻的内在逻辑。然而，除了少数已经投入其中的公司或研究机构，大多数人对于区块链的了解还处在概念阶段，可能知道一些特征或技术术语，但并不真正知道它究竟是什么。

2016年以来，我多次参加区块链相关论坛活动，也接受了很多采访。然而没想到的是，讲得越多，似乎越觉得难讲。首先，你想把这个概念讲清楚，并不是一两句话就可以做到，因为它涉及各种各样不同领域的知识与背景。更大的挑战在于，由于听众的背景与知识结构各不相同，在短时间内通过口述让所有人理解区块链是什么以及它能干什么，简直是一件不可能完成的任务。

于是，我萌发了创作一本区块链书籍的想法。利用这本书，我可以把我对于区块链的所有理解系统且完整地呈现出来，让所有对于区块链或者对于新事物、新机会感兴趣的人，都能够在不需要太多背景知识的情况下理解区块链是什么、当前的发展如何以及可能拥有怎样的未来。最后，在火币联合创始人兼CMO杜均的提议和鼓励下，写作此书的任务正式排上日程。

时间意味着什么

不过想法虽好，要真正做到并不容易。最大的敌人是时间。由于日常工作的繁忙，想抽出大块的时间完成书稿本已非常难，加之我对于本书的内容又有着较高的要求，这对矛盾就变得愈加尖锐，在写作的过程中始终困扰着我。幸运的是，我不是一个人在战斗。若是没有团队的协助与鼓励，以及公司的大力支持，本书的完成不知道还要等上多久。

即便如此，成书的过程依然仓促，再加上我知识结构的局限，错误之处在所难免。不过我依然坚定地认为，让此书尽快面世远比把内容修订得“完美”更有意义。在一个各方面边际成本正逐步趋于零的社会，“时间”越来越成为我们最大的成本。知识可以长久存在，但机会往往转瞬即逝。我们可以学习过去的知识，却无法抓住过去的机会。我们越早一点了解到新事物，就越有可能抓住时代前行带给我们的机遇。

对于区块链这样一种协议式的、需要大规模社会协作与参与的颠覆性技术，越快让更多人了解到它的意义，就会使其越快体现出自身的价值。

让我们一起期待并拥抱价值互联网时代的到来吧！

张健

2016年5月18日于火币

致谢

本书得以面世，离不开很多人的帮助。

感谢中本聪（Satoshi Nakamoto），他开创性的工作拉开了数字货币与价值互联网的大幕。

感谢我的同事李志阔、赵海涛、张智茹、焦锋，在写作过程中我们常常进行热烈而卓有成效的讨论。李志阔协助修订了大部分章节，赵海涛参与了第4章区块链技术原理的写作，张智茹协助修订了部分章节，焦锋绘制了书中的部分插图，没有他们，本书的精彩程度将大打折扣。

感谢火币市场部的同事吴兴、安鑫鑫、张晓萌，没有他们的耐心督促，这本书的面世还要推迟很久。

感谢机械工业出版社的编辑老师李华君、张梦玲，感谢他们容忍我对书稿的反复修改，感谢他们专业细致认真的编校工作。

感谢火币创始人李林、联合创始人杜均，没有火币这个积极向上、充满活力的团队，这本书的完成是不可想象的；感谢火币总裁办刘月雯，她为这本书做了大量的协调工作。

感谢区块链爱好者魏然对书稿的宝贵建议及其提供的精彩文章。

要感谢的人还有很多，难以一一列举。惟愿这本书能够为区块链技术在中国的推广和发展做出尽量多的贡献。

第0章　必然的出现

这些力量并非命运，而是轨迹。它们提供的并不是我们将去往何方的预测，而是告诉我们，在不远的将来，我们会向哪些方向前行，必然而然。

文字与货币

人类在演化过程中，凭借智慧创造了无数事物，这些创造推动了人类文明的加速发展。特别是在进入信息时代以后，每天甚至每时每刻，创造都在不同领域发生着。

然而在人类文明的历史长河中，有两样东西的诞生具有极为特殊的地位，甚至其他任何创造都无法与之相提并论，它们就是文字与货币。文字的发明，使得人类能够在精神层面做到可靠的交流与传承；而货币的发明，则让人类在物质层面能够做到这一点。如果没有这两者，人类作为一个群体将无法获得知识与财富的迭代与累积，也就不会有人类辉煌的文明成果。

现今发现最早的使用文字的记录来自于公元前3000年左右，美索不达米亚平原[1]南部的苏美尔人用削成三角尖头的芦苇杆将文字刻写在泥板上，然后将泥板烘干以便于保存。这就是最早的文字形式——楔形文字。巧合的是，货币制度也同时在这一地区诞生，苏美尔人发明了已知最早的货币——大麦货币。他们将定量的大麦作为通用单位，用来衡量和交换其他各种货物和服务。更有意思的是，当年的泥板上记载的内容不是诗歌也不是哲学，而是生意。美索不达米亚文明属于城邦文明，发展出了丰富的商业行为。他们记录在泥板上的，就是经营相关的事项和账本。正如一位学者[2]所说：文字不是一种深思熟虑后的发明物，而是伴随对私有财产的强烈意识而产生的一种副产品。

图片来源：可汗学院，https://www.khanacademy.org/humanities/ancient-art-civilizations/ancient-near-east1/sumerian/a/cuneiform

而在中国，公元前210年，秦始皇统一六国之后，在全国范围内统一文字，把小篆作为全国通用的书写规范；废除各国原来的货币，统一使用圆形方孔的秦半两。统一的文字对推行法令、传播文化起了重要的作用，而统一的货币改变了过去货币的混乱状态，促进了全国各地的商品交换和经济交流。这两个举措都被作为秦始皇最重要的功绩载入史册。

《圣经·创世纪》里有一则著名的故事：起初人类有共同的语言，并且一起居住在与幼发拉底河相距不远的地方。人们利用河谷的资源在那里建筑城和塔，以聚集全体人类。上帝降临视察，认为人类过于自信和团结，一旦完成计划，人类将无所不能。上帝决定打乱人们的口音和语言，并使他们分散各地。于是高塔停工了，人们操持不同的语言，互相之间难以交流。这个塔就是巴别塔。

图片来源：维基百科，Pieter Bruegel the Elder

抛开宗教方面的意义，故事本身已经很值得玩味了。它告诉我们，如果全人类能顺畅地交流，那么所能产生的能量和带来的改变是不可估量的。而人类进行交流的载体不仅仅是语言。我们审视一下当今的世界，在全球经济一体化的背景下，人类还是被不同的货币所分割。我们不由得遐想，如果有一天建成货币的巴别塔，人类的经济生活将会面临怎样的飞跃。

如果我们进一步追本溯源，文字与货币都是人类进行更高效交流的手段。本质上，文字作为一种人际交流的手段，承载的是信息；而货币作为一种价值传输的载体，承载的是信用。自这两者诞生以来，人类信息传播和价值交换的手段也一直没有停止迭代和进化。下面将简要回顾它们发展和演变的历史。

[1] 位于今天的伊拉克境内。

[2] Cf. E. A. Speiser,“ The Beginnings of Civilization in Mesopotamia,” J. Amer.Oriental Soc., Supp. 4, 59, 17 ff., esp. 25–28（1939）.

信息的演化

在文字出现以前，人类的信息主要通过语言来传递。个人的知识来自族人的口授，集体的记忆来自祖辈的传说。文字的出现使信息不再稍纵即逝，可以更好地跨越时空。甚至有些人认为，书面文字（持久存在的文字）是我们所理解的有意识思考的前提条件。它触发了人类灵魂不可逆转的大规模变化。逻辑是书面文字的产物，是文字造就了人类的思维和历史[1]。

印刷术的发明是信息传播方式里程碑式的进步之一。印刷术使知识传播的范围和有效性得到了极大的提高。在人类走出中世纪，迎来文艺复兴、启蒙运动和科学革命的进程中，印刷术扮演了重要角色。

图片来源：http://www.gutenbergsapprentice.com Copyright ©2016 Alix Christie|Main images courtesy of the Mainz Stadtarchiv，Gutenberg Museum Mainz and University of Gottingen

时间推进到19世纪后期，随着第二次工业革命的到来，电力得到广泛使用，信息传输技术也得到了又一次跨越式的发展。人们发明了电报，文字被转换为莫尔斯码；人们发明了电话，电流承载着信息。从此以后，一个以“信息”为关键词的时代慢慢拉开了它的大幕。20世纪40年代，信息时代迎来了它最伟大的推手：香农。

香农曾向麻省理工学院的万内瓦尔·布什透露，研究传递信息的一般系统的某些基本属性是他一直的兴趣所在[2]。

图片来源：维基百科

1948年，香农发表了《通信的数学原理》，这篇具有划时代意义的论文奠定了现代信息论的基础。在文章中，香农为人类引入了一个新的单词——比特（bit）。牛顿量化了力，建立起经典物理学的大厦；香农量化了信息，打下了人类进入信息时代的基础。如今比特作为衡量信息多少的单位，已经与米、千克、分钟一样，成为人类生活中最基本的量纲之一。1949年，香农又有了重量级的发现，他公开发表的《保密系统的通信理论》一文，开辟了用信息论来研究密码学的新思路。这一发现将密码从艺术变成科学。

通信的基本问题是，在一点精确地或近似地复现从另一点所选取的信息[3]。从密码分析者的角度来看，一个保密系统几乎就是一个通信系统。待传的消息是统计事件，加密所用的密钥按概率选出，加密结果为密报，这是分析者可以利用的，类似于受扰信号[4]。在香农的理论里，信息传输、处理、检测和接收过程，与密码系统中的加密、解密、分析和破译过程都可以用信息论的观点进行分析和研究。密码系统本质上也是一种传递信息的系统。

在香农对信息的概念加以简化，并用比特（bit）作为量纲衡量后，人们发现信息几乎无处不在。比特（bit）的出现在后来引领了计算机、网络、摩尔定律以及如今发达的信息和互联网产业。

互联网的诞生标志着信息时代的真正到来。从此信息的产生与传输开始以前所未有的速度进一步突破时空限制，我们甚至正在迎来一个信息爆炸的时代。而互联网带来的信息革命，已经深刻地改变了全球的商业格局及我们每个人的生活方式。

[1] 詹姆斯·格雷克，《信息简史》，人民邮电出版社。

[2] 引用自http://ethw.org/Oral-History:Claude_E._Shannon。

[3] Claude E. Shannon, Warren Weaver. The Mathematical Theory of Communication. Univ of Illinois Press, 1949. ISBN 0-252-72548-4.

[4] 引用自http://netlab.cs.ucla.edu/wiki/files/shannon1949.pdf。