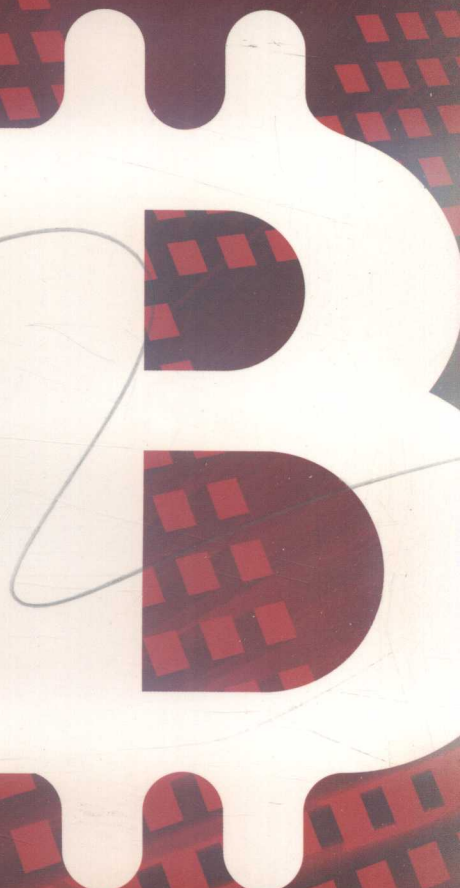


区块链 百科全书

人人都能看懂的比特币等
数字货币入门手册

孙健 / 著



中国工信出版集团



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

区块链 百科全书

人人都能看懂的比特币等
数字货币入门手册

陈健 著

藏

电子工业出版社

Publishing House of Electronics Industry

北京·BEIJING

内 容 简 介

百科全书式的内容构架,鲜活的案例和讲解,足以让每一位读者全方位、快速了解区块链和比特币等数字货币相关知识,堪称区块链和币圈完全生存手册。重剑无锋的数字货币投资思路,也是币圈掘金的指导手册。

本书以朴实生动的语言,阐述了区块链技术的“前世今生”,点明了比特币与货币的内在联系,包括数字货币发展史、区块链技术及应用解读、区块链传播圈的秘密、管好自己的数字钱包等基础知识。此外,还全方位公开了数字货币“挖矿”从原理到矿机购买与设置的整个流程,详述了数字货币交易的流程和常识,手把手演示了一个数字货币从生成到上交易所的所有过程和细节,揭露了以数字货币为名的各种套路和骗局。

本书希望让更多普通用户以最快的方式认知区块链。读完这本书,你会全方位了解区块链及比特币等数字货币相关知识,掌握基本投资理念,识别常见的套路与骗局,站在一个更高的认知起点在区块链这场技术盛宴和财富盛宴中找到自己的一席之地。

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

区块链百科全书:人人都能看懂的比特币等数字货币入门手册 / 孙健著. —北京:电子工业出版社, 2018.8
ISBN 978-7-121-34726-9

I. ①区… II. ①孙… III. ①电子货币—手册 IV. ①F830.46-62

中国版本图书馆 CIP 数据核字(2018)第 155981 号

责任编辑:董 英

印 刷:北京季蜂印刷有限公司

装 订:北京季蜂印刷有限公司

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:720×1000 1/16 印张:19.5 字数:312 千字

版 次:2018 年 8 月第 1 版

印 次:2018 年 8 月第 1 次印刷

定 价:69.00 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, 88258888。

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。

本书咨询联系方式:(010) 51260888-819, faq@phei.com.cn。

你现在一无所有的话，还会担心失去什么？

各位书友好，我是郭宏才 Chandler Guo。

众所周知，我玩比特币的出发点就是挣钱。这是一个赤裸裸的观点，赤裸到说出这种观点居然会被踢出群。

我一直相信一句话，挣钱可以解决生活中 90%的烦恼，我也相信很多草根出身的朋友都深有体会。

其实在 4 年前，2014 年我去香港开会，还舍不得一千多元钱一晚的酒店住宿费。那天晚上我和火币的高管挤在一间。我跟他说要搞矿场，内蒙古的电才三毛多一度，说得我满是憧憬，他却打起了呼噜。后来我们真的在内蒙古建起了大矿场。这是我在比特币身上挣到的第一桶金。

区块链发展到今天，已经没有人可以控制，也没有人可以阻挡。因为很多人不理解区块链，所以担心区块链的火热会引发一系列问题，但是区块链根本没有问题，恰恰相反，区块链是解决社会问题的新方法。例如现在在互联网可以自由地跨越国界，但是金融的流通却门槛重重。区块链网络就可以完全让金融像互联网那样流通起来。

人们把区块链定义成一场新的革命，区块链革命的对象不是生产力，而是生产关系。毫无疑问，革命也意味着牺牲，意味着利益链条的重新洗牌。听到这些话，怂了的人就别干，干了就不要怂。不过要是你现在一无所有的话，你还会担心失去什么？

硅谷风投教父 Tim Draper 在 2014 年说比特币三年内要涨到 1 万美元，我当时就说少了，结果 2017 年底涨到了 2 万美元。他最近又说到 2022 年比特币要涨到 25 万美元，我觉得还是说少了，比特币未来经历 4 次减半之

后，在我有生之年肯定能上 100 万美元。也希望在我有生之年，能够花 100 个比特币，买一张去往月球的门票。

我最近就用比特币在美国硅谷买了一个庄园，“韭菜庄园”的招牌我已经挂在大门上。我要把这个韭菜庄园打造成全世界币圈的根据地，只要是币友都可以来。

孙健先生的这本《区块链百科全书：人人都能看懂的比特币等数字货币入门手册》写得很清晰，把区块链和数字货币的前世今生都说明白了，还揭露了不少打着区块链名号的骗局。新韭菜看完之后，快速升级成老韭菜，能少走很多弯路。

最后，建议大家一定要买一个比特币，传给自己的儿子，切记！

郭宏才 Chandler Guo

2018 年 5 月 15 日 美国纽约

区块链这个技术幽灵，对我们未来世界的意义大于人工智能

比特币和区块链，像一个技术幽灵，越来越多地进入我们的现实世界中，它们在一步一步地改变着我们原有的很多不可动摇的观念，很多人不信、不屑；很多人拥抱、投机，更有很多人谨慎观望。

在过去不到十年的时间里，比特币的崛起非常壮观，从几乎没有任何价值增长到最高点接近 2 万美元。在过去两年里，比特币的价值上涨了近 30 倍，比特币的流通价值已经接近 1700 亿美元，已高于麦当劳的市值。

究竟是什么支撑着比特币的崛起？我认为有三点：第一，比特币有一批技术的绝对信仰者；第二，总量被固定在 2100 万个的比特币，今天已经被挖过半，人们开始意识到它越来越重要的价值投资属性；第三，比特币被炒币群体高度关注并借机炒作。

然而，很多人听说过比特币，但对区块链却毫无了解。

其实，区块链技术是比特币的底层技术，比特币一直在没有任何中心化机构运营和管理的情况下运行。可以说，比特币是区块链的第一个应用，以后区块链逐步扩展到了越来越多的行业中。

我们常常把比特币比喻成 BlockChain 1.0，而把发布智能合约技术的以太坊比作 BlockChain 2.0，因为其支持了更多的区块链项目，发行自己的 Token，被译为代币或者通证。今天，越来越多的区块链公链项目，开始推动 BlockChain 3.0，即如何推动应用的成熟，如何把区块链技术应用于行业和消费市场。

区块链技术的模型自下而上由数据层、网络层、共识层、激励层、合

约层和应用层等 6 层结构组成。很多技术型创业者一看，说这没有什么新鲜技术，这是 P2P 技术的新瓶装旧酒，当年的 Napster、NetAnts，甚至快播都是做这个起家的。

但是，当我们深入研究这种新的模型，就会发现“开源共识激励”在其结构设计中的重大意义。这种新的多层级架构叠加的系统设计，融合了数据、计算、治理，构造了全新的技术文明和社会文明体系，它将给我们一个更自由、更透明、更公平的环境。

从对人类社会繁荣共生的意义上看，区块链改变价值传递的意义，一定大于人工智能对于生产力提升的意义。

有人问：区块链是对互联网的一场革命和颠覆吗？我不愿意用革命和颠覆来形容，我更愿意说，区块链和互联网，今天的两大平行世界，未来将走向逐步融合。

今后三年，每个互联网公司，都可能会有结合区块链的技术；同样，好的区块链项目，一定也要结合互联网现有的技术和用户资源，才能真正做大。

希望我们很多人能更加重视区块链，更加重视其价值，理解它发展中必然遇到的困难和机会。

《区块链百科全书：人人都能看懂的比特币等数字货币入门手册》作为区块链行业的一本百科全书，生动地展现了区块链的行业生态，让你对区块链这个技术幽灵不再畏惧和陌生，帮助你揭开区块链神秘的面纱，更好地理解区块链的价值所在。

王峰

火星财经发起人、蓝港互动创始人、极客帮创投合伙人

2018 年 5 月 24 日 中国北京

区块链是行动者的红利

2017 年，加密货币波澜壮阔的大牛市塑造了大量的财富传奇，很多人因为比特币的暴涨关注到了它背后的区块链，又有一小部分人因为开始投资加密货币正式进入了区块链的大门。在剧烈波动的市场行情中，有的人收益不菲，有的人黯然离开。但是，如果你仅仅把区块链当作“炒币”的工具，可能会以错误的姿势错过这个时代最大的浪潮之一。我相信：区块链的大红利属于行业的深度参与者和共建者，这是一个更高的认知起点。

很多新的理念和范式刚刚出现时，人们常常会谈“颠覆”，但大多数时候新技术、新范式只是帮助产业完成了进化，而没有带来摧毁。区块链也一样，我认为它并不会替代和颠覆互联网，只是为越来越中心化的互联网世界提供了另一种方案。我们可以选择目前体验更流畅、更成熟但用户缺少隐私保护和自主权的互联网，也可以选择目前尚不成熟、体验磕磕绊绊但给你高度自主权和隐私的、开放透明的区块链。

尽管相对于互联网，区块链生态的市场占有率现在可能连 0.1% 都不到，但是我们相信它在接下来的共识会越来越广泛，逐步达到 1%、10%，甚至更高。是继续在巨头林立的古典互联网血海里竞争，还是出发去仍是蓝海、疆域不断扩大的区块链世界里奔跑，这是这个时代每一个人都要思考和选择的问题。

我和公信宝的另外几位合伙人很早就开始了对区块链行业的探索、思考并付诸行动，投资过多种加密货币，做过矿池，做过区块链应用，直到 2016 年创立公信宝，在这个过程中我们遇到了很多坑，走过一些弯路，这些最终都成为了我们后来创业的宝贵财富。但不得不承认，如果在当时我

们就读过像《区块链百科全书：人人都能看懂的比特币等数字货币入门手册》这样的书，后来的我们会前进得更快。

如果你也想进入这个机会和挑战并存的世界，建议你好好读一读这本书再出发，站在一个更高的认知起点开始行动；如果你已经在路上，那么也可以在行动中实践和求证书中的观点。

我们知道，目前的区块链无论是共识、技术、应用、理念乃至监管法规和大众教育，都仍有很长的路要走。这些都要以行动来实现，希望行业中多一些实践者和思考者，少一些浮躁者和鼓吹者，推进技术发展，加快应用在切实场景中的落地，将泡沫变为现实。

黄敏强

公信宝创始人&CEO

2018年5月21日 英国伦敦

数字货币一定会从当前的投资价值， 逐渐回归到使用价值

毫无疑问，比特币是 2017 年以来最受人关注的投资品，没有之一。与此同时，伴随着首次代币发行带来的巨大暴利空间，以及坊间流传的一夜暴富的故事，区块链成为全民热议的词汇，各色人群与各类资金蜂拥而至。一时间所有的人都希望参与其中，都在为错过了比特币而悔恨。但是，因为政策的不稳定、行业极度缺乏监管及各类非法融资、操纵市场的行为，除了少数核心玩家，大量不明就里跟风而来的入门人士在不知不觉中成为了“韭菜”。

的确，区块链的发展及数字货币的繁荣是一次史诗级的浪潮。产业、技术与社会三个因素共振，必然带来超级大的投资和创业机会。然而，区块链和数字货币投资具有三个极其鲜明的特征：一是极强的技术属性，二是极强的金融属性，三是极强的社区属性。因为行业不成熟，获取暴利和血本无归同时存在。如果没有较好的技术背景、金融背景和社会理解能力，很难快速有效地切入数字货币市场。

Kcash 认为，对于大多数首次接触区块链项目和数字货币的人而言，第一重要的是学习数字资产的管理，首先确保资产的安全问题，然后才是考虑投资标的和投资回报的问题。区块链技术属性、去中心化的运行模式所带来的前所未有的资产存储状态和模式，需要新用户快速理解并熟练使用，这并不是一件容易的事情。Kcash 团队自 2013 年底开始接触比特币并开始相关领域的创业，作为国内首款跨链的数字货币钱包，在跨链技术、安全管理、用户体验等方面均处于业内一流的水平，2017 年 9 月上线至今已经

有数十万用户，是数字货币资产存储的第一选择。

未来，随着区块链技术及市场的日益成熟，会有越来越多落地应用的场景出现。数字货币会从当前的投资价值、交易价值，逐渐回归锚定价值、使用价值，这个时候支付就会成为更加广泛的需求。Kcash 定位于区块链世界的支付宝，从数字货币钱包领域开始，已经开发出币生币理财（类似于余额宝）、数字货币质押借贷（类似于金融配资）等产品，满足用户更多、更大规模的金融需求。通过开发跨链映射的 Kchain 金融公链，实现高速便捷、无摩擦成本的支付，是 Kcash 更长远的追求。Kcash 也相信，数字货币世界的支付场景与规模将令人欣喜。

预祝所有读者都能在数字货币世界中有所斩获，而这本《区块链百科全书：人人都能看懂的比特币等数字货币入门手册》是大家入门区块链的特别好的选择。希望孙健先生能给区块链玩家带来更多优秀的作品。

余水

Kcash 联合创始人

2018 年 5 月 17 日于北京

区块链会对中介型行业进行降维打击

说到区块链，我觉得应该从《失控》这本书说起。我在 2003 年第一次读它时，被书里讲的很多概念所震撼，凯文·凯利从蜂巢这个生物组织开始讲起，引申到了民主制度、分布式管理、网络链接等。我认为区块链正是这些概念的落地实现。而比特币的诞生，在我看来更多的是一种思想、信仰的传递，中本聪和一帮技术极客们所倡导的自由主义，让比特币变成一个真正不受政府或银行控制的全球流通电子货币，这也是中本聪们对现实世界和货币体系的一个重大挑战，从目前的比特币全球流通情况来看，无疑也是一次成功的挑战。我建议所有区块链行业的人，或有兴趣加入区块链行业的人，都认真读一下《失控》和中本聪写的比特币白皮书，从思想上对区块链有个共识，区块链不仅仅是一个底层技术，更多的是一种新型的信任机制、激励模型和治理结构，通过共识、共建、共享形成了一个完善的自运行组织，区块链会对公司制度产生颠覆性的影响，同时也会对众多中介型的行业降维打击，在金融行业、游戏行业、共享经济等行业，区块链技术已经有了很多的落地应用，随着底层公链技术的不断发展，我相信会有越来越多优秀的区块链项目产生。目前我认为还处在区块链行业的 1.0 阶段，区块链领域的“腾讯”“阿里”都还没有诞生，希望读者们能抓住这个历史的机遇，拥抱区块链，拥抱未来。

对于区块链产业的投资，我们 JRR CRYPTO 主要是布局在区块链服务方面的企业，简单讲就是“卖水”型企业，比如在垂直的服务型生态链中，矿机矿池是一个生态，交易所是一个生态，公链是一个生态。在这些重要的生态中，我们都会做战略布局，掌握一些头部资源。例如交易所，我们

天使投资了币安 Binance，这是我们在区块链产业布局中的一个龙头资源。公链未来也会是一个激烈的战场，我们今年参与了 EOS 超级节点竞选，因为非常看好 EOS 的 DPOS 机制，也希望能参与和共建 EOS 这个生态。

具体到区块链的项目投资，我不太赞同所谓传统投资人、古典投资人、区块链投资人这样的区分提法。我相信商业判断的本质是不变的，最核心的还是看人、看团队、看创业者的初心。我也不认为传统、古典投资人在对项目判断上不占有优势，只是传统的投资决策流程周期比较长，在区块链“币圈一日，人间一年”的时代背景下，倒是的确需要提高效率。

目前，我既是投资人，同时也是一个创业者，在做一个数字货币的行情软件项目，这两个角色的切换，让我在面对创业者的时候能够更有同理心，在面对投资人时更知道如何切中要害地介绍项目。能够踏上区块链的浪潮，真是感到非常幸运，孙健先生的这本《区块链百科全书：人人都能看懂的比特币等数字货币入门手册》，条理清晰、内容全面，非常适合新入区块链领域的读者，帮你在区块链的历史大浪潮中，乘风破浪、一往无前。

苏兴

JRR CRYPTO 董事总经理

2018 年 5 月 25 日 中国北京

前 言

如果今天的比特币还只值 1 分钱，那么 99%的人根本不会去了解区块链、非对称加密或者主链扩容等晦涩难懂的专有名词，更不会冲破各种政策限制，无视各种风险警示，用真金白银买下各种“空气币”。而当比特币冲高到 2 万美元一“枚”的时候，不少国人重现了炒房时代的疯狂操作，“梭哈”之声不绝于耳。这场比炒房还刺激百倍的财富梦想，成为一个耀眼的黑洞，不断吞噬巨大的社会注意力。

经济学家哈耶克在《致命的自负》(*The Fatal Conceit*)一书中提出：人类文明的诞生起源于私人财产制度。价格是唯一能使经济决策者透过隐性和分散知识互相沟通的方式。

比特币的价格，就是区块链技术最好的广告。几乎所有人在得知比特币的价格走势之后，都为自己没有早两年购买比特币而后悔。在后悔之余鼓起勇气“买票上车”，却发现自己往往一不小心上了“黑车”，沦为了任人收割的“韭菜”。

在混沌未开的区块链世界中，蜂拥入场的新人往往发现自己一无所知。在一无所知的情况下进行数字货币投资，就如同买彩票一样充满希望和失望。

坦率地说，全世界大部分人不了解区块链技术，看不懂各类项目白皮书，更不关心这项技术能给人类社会带来多大进步，而只是关心自己能不能从这一次潮流中挣到钱。所以在 Telegram 群里使用中文、日文、韩文、阿拉伯文、俄文、泰文、英文交流的全世界玩家，会为争领各种糖果空投(Candy Airdrop)而疯狂转发各类项目推荐。

世界级的万众参与带来了巨额资本的投入，这更加刺激了区块链行业的发展。所以从另外一方面来看，大众对个人财产增值的欲望，最终也促进了全人类的技术进步。

然而，区块链知识在大众认知上还存在着较大的认知时间差，所以打着区块链旗号的各种骗局套路令人防不胜防，这也为整个区块链行业发展大量招黑。时至今日，依旧有人认为比特币是一场传销骗局。

与此同时，区块链技术目前依然存在大量的技术盲点和难点，而各类空气币项目层出不穷，新人入场之后往往无所适从。

有鉴于此，作为比特币新生代玩家，我希望本书用客观和理性的观察与总结，让更多普通用户以最快的方式认知和了解区块链技术，了解数字货币从发行到上市的全部过程，从而真正能从这场技术潮流和财富盛宴中找到自己的一席之地。

在本书编著期间，得到了圈内诸多专业人士的指点和提携。在此特别感谢郭宏才先生在 2018 美国比特币共识大会期间抽空为本书作序，也同样特别感谢火星财经的王峰先生、公信宝创始人黄敏强先生、Kcash 钱包联合创始人余水先生和 JRR CRYPTO 董事总经理苏兴小姐为本书作序支持！

还要特别感谢区块链圈内专家邓鹏（火星财经）、毛文（非小号）、谭晨辉（币世界）、谢小婧（币世界）、许潇鹏（公信宝）、赵进（虎尔财经）、谭金都（虎尔财经）、鲁炳铨（巴比特）、龙超（Kcash 钱包）、蒋文武（wk588.com）、高乐（区块链晴雨表）、詹蓉蓉（白话区块链）等朋友对本书的指导和支持。

我的老朋友乐媛女士、刘丽媛女士、李申伟先生、林鹏程先生、邓韵诗小姐在本书写作期间给予了宝贵的帮助，电子工业出版社董英女士为本书的出版提供了大力协助。莫小莹小姐在本书筹备期间做出了巨大贡献。在此一并致谢！

一旦逃避了学习的苦，必将面对生活的苦。与诸君共勉。

孙健

2018 年 6 月 22 日

读者服务

轻松注册成为博文视点社区用户 (www.broadview.com.cn), 扫码直达本书页面。

- **提交勘误：**您对书中内容的修改意见可在 [提交勘误](#) 处提交，若被采纳，将获赠博文视点社区积分（在您购买电子书时，积分可用来抵扣相应金额）。
- **交流互动：**在页面下方 [读者评论](#) 处留下您的疑问或观点，与其他读者一同学习交流。

页面入口：<http://www.broadview.com.cn/34726>



目 录

第 1 章 从贝壳到比特币——数字货币发展史	1
1.1 比特币折射出的时代焦虑	2
1.2 从贝壳到比特币	5
1.2.1 信任与货币	5
1.2.2 货币形式的进化	7
1.2.3 比特币与货币的 8 大特征对照	13
第 2 章 区块链技术及应用	18
2.1 区块链是什么	19
2.1.1 非对称加密及哈希算法	20
2.1.2 区块链数据结构及时间戳	22
2.1.3 分布式存储	24
2.1.4 共识机制	25
2.1.5 新的数字革命	28
2.2 区块链 6 大基本特征	29
2.2.1 去中心化	29
2.2.2 去信任化	30
2.2.3 去中介化	30
2.2.4 集体共识维护	31