

看得懂 学得会
用得着的
区块链入门书

一本书让你读懂区块链

一本书读懂 区块链

从未来看区块链世界

。 。 。

用技术重构金融世界，
从根本上改变我们的生活


区块链小白投资入门实操指南

张浩◎著

区块链三大变革

去中心化、开放性、智能合约

IT人士与金融界人士必读

 中国商业出版社



一本书读懂 区块链

。 。 。

张浩◎著



中国商业出版社

图书在版编目（C I P）数据

一本书读懂区块链 / 张浩 著. --北京：中国商业出版社,2018.9

ISBN 978-7-5208-0581-0

I. ①一… II. ①张… III. ①电子商务—支付方式—基本知识 IV. ①F713.361.3

中国版本图书馆 CIP 数据核字(2018)第 213342 号

责任编辑：朱丽丽

中国商业出版社出版发行
(100053 北京广安门内报国寺1号)
010-63180647 www.c-cbook.com
新华书店经销
天津中印联印务有限公司印制

*

720 毫米×1000 毫米 1/16 开 14.5 印张 190 千字
2018 年 11 月第 1 版 2018 年 11 月第 1 次印刷
定价：48.00 元

(如有印装质量问题可更换)



要说最近各个行业关注的热点，区块链技术必须算一个，最近一段时间“区块链”非常火热。火到什么程度？只要和区块链沾边的公司，股价就一飞冲天。数据显示，到现在为止，2016 年全球最大的投资项目都与区块链有关，投资金额已经分别达到 5500 万美元和 6000 万美元。

区块链是一种将分布式数据存储、点对点传输、共识机制、加密算法等计算机技术综合运用的新型应用模式。比特币就是基于区块链技术发展起来的，而区块链上智能合约的支持，使比特币以外的数字资产的点对点转移变成现实，这也是区块链引人注目的重要原因。

那么，为什么区块链有如此魅力呢？如果说今天的互联网是信息通过 TCP/IP 协议进行点对点的传递，是信息互联网，那么价值进行点对点的转移就成了由区块链技术提供技术可能。通俗地讲，区块链是去中心化的分布式记账系统。系统中的节点无需互相信任，其交易通过密码学算法连接在一起，使整个账本公开透明、可追踪、不可篡改。





如今，中国的一些行业巨头早就开始布局区块链。比如：蚂蚁金服推出的区块链喷漆技术应用到交通行业中，让碰瓷成为历史；百度布局金融+人工智能+区块链，解决了信任问题；而腾讯则对区块链技术进行重点研究，虽然还没有有相关产品，但对区块链的深度挖掘，未来多半也会推出更好的产品。

国内 BAT 三巨头的入局，给区块链行业带来了信心，不管看中的是区块链技术带来的巨大利益，还是看中区块链技术对传统行业的改变，这场革命正在影响着我们。

区块链到底是啥？有人说，比特币将成为世界通用钱银；有人说，比特币就是一个大骗子……千人千面，但区块链潜力空间不可忽视，区块链是价值互联网的柱石。究竟怎么认识区块链？为了回答这些问题，笔者特意编写了这本书。

此书从区块链的基本定义入手，介绍了区块链的发展历史、分类、特征、挖矿原理、常见误区、主要应用等，要点突出，易于理解，是一本学习区块链的入门书。相信，一定能让读者有所收益。



第一章 揭开区块链的面纱 1

关键一：究竟什么是区块链 /3

关键二：跟区块链有关的基本原理 /9

关键三：区块链与大数据、云计算的关系 /14

关键四：区块链的共识机制，其优缺点是什么 /19

关键五：区块链小白该如何学习 /25

第二章 区块链的出现和发展 /29

要点一：区块链的产生及发展情况 /31

要点二：区块链发展的六个阶段 /37

要点三：区块链的发展历程 /40

要点四：区块链的百链竞发 /48

第三章 区块链的分类 /51

种类一：公有区块链 /53

种类二：联盟区块链 /58





种类三：私有链 /65

第四章 区块链的特征 /69

特征一：区块链的去中心化 /71

特征二：区块链的去信任 /76

特征三：区块链的开放性 /79

特征四：区块链的自治性 /82

特征五：区块链的信息不可篡改 /84

特征六：区块链的匿名性 /87

第五章 区块链挖矿原理早知道 /93

内容一：什么是“挖矿” /95

内容二：警惕挖矿的骗局 /99

内容三：比特币的挖矿机制 /101

内容四：EOS 的超级节点 /103

内容五：辨识伪“挖矿” /106

第六章 常见的区块链认识误区 /109

误区一：区块链只跟金钱有关 /111

误区二：区块链与比特币是一回事 /114

误区三：区块链能够彻底消除欺诈 /117

误区四：区块链具有成本效益，价格低廉 /121

误区五：只有大企业能够使用区块链技术 /124





误区六：智能合约等于法律合约 /128

误区七：越炒作，区块链发展越火爆 /132

第七章 区块链的多方应用 /135

应用一：最可行的应用——公证类 /137

应用二：竞争最激烈的应用——证券市场 /142

应用三：最具颠覆意义的应用——支付系统 /146

应用四：区块链技术在安全行业的应用 /149

应用五：区块链的为打车市场再添新力 /154

应用六：区块链与泛金融也能擦出火花 /156

应用七：区块链技术还能保护森林资源 /161

应用八：区块链的其他应用场景 /164

第八章 提高认识要点，积极进军区块链 /171

认识一：进军区块链的要点 /173

认识二：进军区块链需要了解军规 /176

第九章 投资区块链不要轻易入“坑” /181

第一坑：ICO /183

第二坑：梭哈 /185

第三坑：大佬 /186

第四坑：糖果 /188

第五坑：情绪投资 /189





第十章 区块链的前景展望 /191

展望一：区块链是中国经济创新的新高地 /193

展望二：区块链的赚钱经济前景 /197

展望三：国内互联网巨头的区块链布局 /202

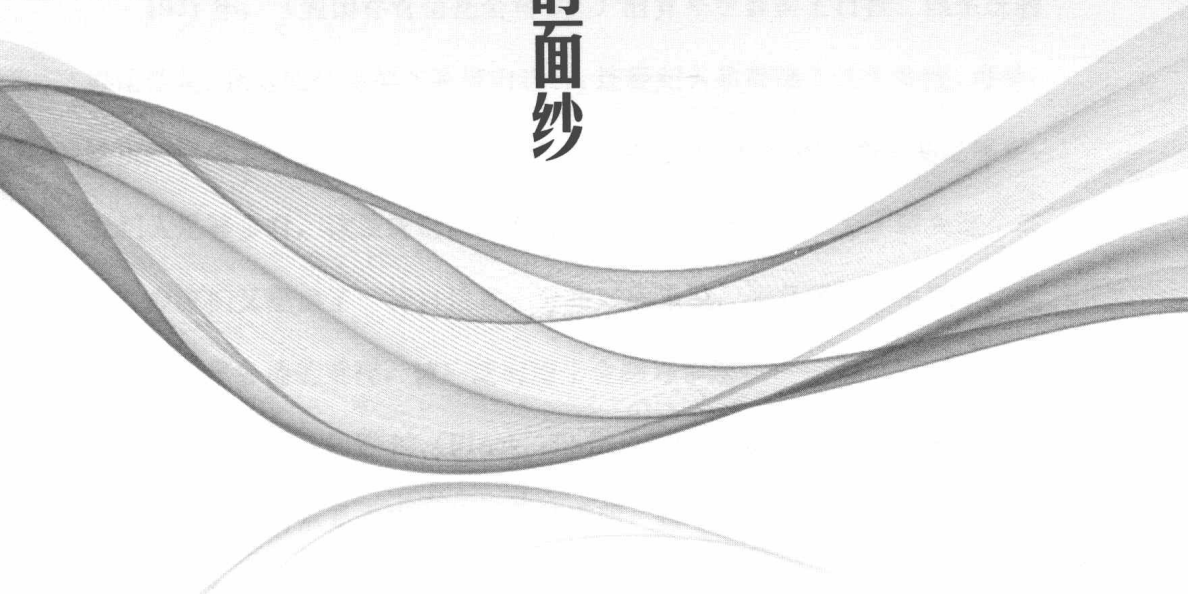
展望四：区块链的规模化产业应用 /211

后 记 /217



第一章 揭开区块链的面纱

关键一：究竟是什么是区块链





关键一：究竟什么是区块链

在纳斯达克成立之前，为了在最短的时间里完成清算，人们经常会用自行车驮着装满债券的包，在华尔街骑来骑去。可是后来，随着业务的逐渐增多，自行车似乎已经满足不了这种需要。为了让清算速度跟上交易量，20世纪60年代，华尔街每周只能交易4天，每天4个小时。时间长了，大家发现，这样不行，自行车根本就跑不过计算机。

1971年，（美国存管信托公司DTC）清算系统被提上日程。该系统的办法就是：所有的交易都在系统内进行，连经纪人也被接入这个系统。可是，这虽然提高了交易效率，但并没有改变交易的中心化结构。当交易足够多、经纪人足够多时，该系统也面临着瘫痪甚至崩盘的危险。为了解决这个问题，专家们又想出了一种自治式、分布式的系统，于是区块链出现了，之后受到世界各地的重视，被广泛应用于金融等领域。

区块链技术，简称BT（Block chain technology），是一种互联网数据库技术，其特点是去中心化、公开透明，每个人都能参与数据库记录。如果把数据库假设成一本账本，读写数据库就是一种记账行为，区块链的



基本原理是：在一段时间内找出记账最快最好的人来记账，然后将账本的该页信息发给系统里的其他人，相当于改变数据库所有的记录，发给全网的每个节点。

一、用区块链建立起来的信任

作为高冷的区块链，也许人们都不知道；作为数字货币的比特币，也许只有技术极客和资本炒家才会关心。可是，说到滴滴打车，恐怕是无人不知无人不晓，说到租房人们更会耳熟能详，说到银行服务多数人甚至还会吐槽……在这个高度中心化的社会，为了证明信用，我们付出了太多的代价，结果是互不相信对方。我们建立了银行，将金钱放在一起集中管理；建设了支付宝，做为网上交易的中介；设立了P2P平台，筹集所需的资金……之所以要做这些事，都是因为我们不相信陌生人，只有通过中介才能建立起脆弱的信任。

区块链技术是什么？什么能够真正建立起人与人之间的信任？基于对滴滴打车平台的信任，可以将车上的空位出租出去，让陌生人乘坐你的车，这就是发展共享经济的第一步。但是，我们却不能像美国人一样用爱彼迎（Airbnb）将多余的房间出租出去。能够将自己的床位、车库、厨房、乐器、电脑等私人闲置物品出租出去吗？恐怕更是难上加难。为什么？因为我们不信任他人，不知道这样做的后果。但是，区块链却可以做到。

设想这样一个场景：个人的所作所为一旦被大数据记录，被存储在



区块链的多个节点上，无法篡改，不能修饰，任何人都能够用区块链来描绘你的数字画像，都能通过区块链的评分来确定你是否可信。一旦确立了这样的体系，中介也就失去了存在价值，我们便能轻易地信任他人。

修改一个基于区块链的信用记录，修改世界上每个人的手机、电脑甚至智能设备，是不可想象的。例如，微信每天能产生多少数据？每天产生的社交、交易数据本应完全属于产生者个人，按互联网共享、平等、透明的精神，这种大数据产生的是一种“全球性的信用资源”，基于这些数据的信用体系，每个人都会变成一个被信用描述的人。一旦违反了信用，认识的人都会看到，这个人也就无法在社会上立足了。

二、到底什么是区块链

工信部指导发布的《中国区块链技术和应用发展白皮书 2016》是这样解释的：广义来讲，区块链技术是利用块链式数据结构来验证与存储数据、利用分布式节点共识算法来生成和更新数据、利用密码学的方式保证数据传输和访问的安全、利用由自动化脚本代码组成的智能合约来编程和操作数据的一种全新的分布式基础架构与计算范式。简单地说，区块链就是一种去中心化的分布式账本数据库。

从本质上来说，区块链技术是一种数据库技术，是一种账本技术，账本记录着一个或多个账户的资产变动、交易情况，也就是一种结构最为简



单的数据库。我们平常在笔记本上记录的流水账、银行发过来的对账单，都是典型的账本。

安全是区块链技术的一大特点，主要体现在两方面：一是分布式的存储架构，节点越多，数据存储的安全性越高；二是其防篡改和去中心化的巧妙设计，任何人都很难按规则修改数据。

以网购交易为例，传统模式是：买家购买商品，将钱打到第三方支付平台，等卖方发货、买方确认收货后，再由买方通知支付机构将钱打到卖方账户。由区块链技术支撑的交易模式则不同：买家和卖家能够直接交易，不用借助任何中介平台。买卖双方交易成功后，系统会通过广播的形式将交易信息发布出去，所有收到信息的主机会在确认信息无误后将这笔交易记录下来，所有的主机都会为这次交易做好数据备份。即使今后某台机器出现问题，也不会影响数据记录。

提到区块链，很多人就把它与比特币联系在一起，有些人甚至还认为区块链就是比特币。其实，比特币是区块链的一种呈现方式，区块链并不等同于比特币。区块链是比特币的底层技术和基础架构，而比特币则是区块链的成功应用，并不是说区块链只能应用到比特币上。

三、区块链的作用

区块链能解决金融、公益、监管、打假等众多领域的痛点难点，但要满足很多适用条件。



1. 金融领域的作用

金融服务是区块链技术的第一个应用领域，区块链技术能很好地解决支付、资产管理、证券等多个痛点。比如，在支付领域，金融机构特别是跨境金融机构的对账、清算、结算等成本都很高，需要经过众多流程，不仅会在用户端和金融机构后台业务端产生高昂的费用，也会让小额支付业务无法开展。运用区块链技术，则能够降低金融机构间的对账成本及争议解决的成本，显著提高支付业务的处理效率。同时，区块链还能让支付领域独具成本和效率优势，使金融机构更好地处理小额跨境支付，实现普惠金融。比如，为解决金融机构间对账成本高的问题，2016年8月微众银行跟上海华瑞银行合作，一起推出了微粒贷机构间对账平台。之后，洛阳银行、长沙银行也相继接入机构间对账平台，通过区块链技术，优化了微粒贷业务的机构对账流程，提高了运营效率，降低了运营成本。



2. 公益领域的作用

在公益领域，区块链技术也被广泛运用。比如，蚂蚁金服涉足区块链的首个应用场景是公益，帮助听障儿童获得了一笔善款，运用区块链技术促进公益更加开放透明。区块链公益平台就像在互联网上构建了一个专门用于邮寄资金的邮局，用户捐的每一笔钱，都被打包成一个包裹，通过区块链平台传递，每经过一个节点，都会盖上一个邮戳，最后送到受捐人手上。如此，就能保证用户捐的每一笔钱都是透明的、可追溯的、无法篡改的。

3. 打假方面的作用

在商品打假方面，区块链技术更能大显身手。蚂蚁金服将区块链技术



用在正品溯源上，目前来自澳大利亚、新西兰海淘的某些商品，比如奶粉，只要用支付宝扫一扫，就能知道是不是正品。不同于过去商家自录入的商品信息，区块链能让多位“记账师”公正、独立、不可抵赖地完成记账。

4. 监督方面的作用

对于金融监管，区块链技术也发挥着重要作用。2017年金融区块链合作联盟（深圳）发布的《金融区块链底层平台 FIS CoB CoS 白皮书》认为，区块链为金融监管机构提供了一致且易于审计的数据，通过对机构间区块链的数据分析，能够更快、更精确地监管金融业务。例如，在反洗钱场景中，各账号的余额和交易记录都是可追踪的，任意一笔交易的任何一个环节都会受到监管，极大地提高了反洗钱力度。

由此可见，区块链确实能解决很多领域的痛点和难点，但区块链也不是万能的，也有很多适用条件。比如，区块链技术去中心化的特点适合多方参与的场景，只是单边或双边，参与价值就不大。同时，需要每个节点都进行核对，区块链技术也不能被运用于高频交易的活动；区块链强调的是公开透明，不适合对数据隐私要求高的场景。

