THE QUICK GUIDE TO BLOCKCHAIN

区块链不是天使，也不是魔鬼
走近区块链，认识区块链，运用区块链

一本书读懂区块链

台海出版社

THE QUICK GUIDE TO BLOCKCHAIN

一本书读懂区块链

凌　锋◎著

台海出版社

图书在版编目（CIP）数据

一本书读懂区块链 / 凌锋著 . -- 北京 : 台海出版社，2018.6

ISBN 978-7-5168-1897-8

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

中国版本图书馆 CIP 数据核字（2018）第 084525 号

一本书读懂区块链

著　　者：凌　锋

责任编辑：高惠娟　赵旭雯

责任印制：蔡　旭

出版发行：台海出版社

地　　址：北京市东城区景山东街 20 号　　邮政编码：100009

电　　话：010 － 64041652（发行，邮购）

传　　真：010 － 84045799（总编室）

网　　址：www.taimeng.org.cn/thcbs/default.htm

E － mail：thcbs@126.com

印　　刷：玉田县昊达印刷有限公司

开　　本：710 毫米 ×1000 毫米　1/16

字　　数：115 千字

印　　张：10

版　　次：2018 年 7 月第 1 版

印　　次：2018 年 7 月第 1 次印刷

书　　号：ISBN 978-7-5168-1897-8

定　　价：39.80 元

前 言

互联网从不缺乏热词，这次的主角是“区块链”。从2016年到2018年，“区块链”概念由技术圈、加密货币投资圈等相对小众的范围逐渐扩展到整个社会各个领域。

就在今年年初，《人民日报》在2月26日刊出整版文章，三问区块链[1]：什么是区块链？区块链能做什么？区块链会成为风口吗？对区块链有关问题进行了解读。同时，有新闻报道，人民网增设了“区块链”频道[2]。在今年的全国两会上，也有政协委员对中国区块链发展献言献策。3月6日，中央纪委国家监委机关报《中国纪检监察报》刊发了题为《连接未来的“区块链”》的文章，强调“中国发展区块链，挑战和机遇并存，而最大的挑战在于‘如何让监管理解区块链并适度监管’”。

从社会上来看，更是一片火热的场景，不论是区块链概念投资、专利申请，还是区块链培训、人才招聘，甚至是借着区块链进行炒作自身产品的商家，都在一波接一波地推动着区块链的热潮。与此同时，并非所有的人都对区块链的未来乐观其成，有不少人对区块链这种具有所谓高度“去中心化”特征的技术忧心忡忡，也有人简单地把区块链等同于比特币，进而因比特币乱象甚至违法犯罪问题，产生了

1 人民网，http://capital.people.cn/n1/2018/0226/c417686-29834465.html。

2 凤凰网，http://tech.ifeng.com/a/20180305/44895533_0.shtml。

对区块链的误解。

不同观点的探讨一方面来源于新技术模式诞生初期的不确定性及代表性应用的缺乏，毕竟除比特币之外，对于社会公众而言，尚无可以明确感知到的“爆款”作品，而比特币自身也存在很多值得讨论的问题；另一方面似乎也和区块链基本知识的信息供给有关，相对于此前的技术网红“新媒体”而言，区块链的技术性更强，特别是它的原理和大众的生活逻辑存在较大差异，而弄懂这些关键技术对于理解区块链至关重要，比如区块链真的能够“去中心化”吗？加密后是否能保护隐私？是否可以彻底实现安全无虞？等等。对于这些知识点，互联网上有一些文章努力通过漫画、类比等形式加以通俗解读，但是相对来说，缺乏系统性的介绍。

与此同时，市场上销售的与区块链有关的书籍大部分是技术研究类和金融应用类，纵使有少量通俗化读物，主要还是和金融、加密货币等领域有关。笔者认为，任何革命性的技术只有在最广大的领域得到理解和实践，才能产生真正社会意义上的生产力，被视为“价值互联网”基础的区块链技术的舞台，绝不只是在金融领域，在实体经济、公益慈善、公共管理、社会治理等各方面都有很多可以想象的空间。要在更广泛的领域发挥区块链的作用，一个显而易见的前提是让人们了解和理解区块链，就这方面来说，尚没有一本以非技术和金融领域读者为主要对象梳理相关知识的区块链书籍，这也成为本书诞生的缘由之一。

本书的读者定位与目前市面的书有很大不同，并不是以技术和金融从业者为主要对象，既不是要做成区块链技术开发指南，也不是想成为区块链投资说明书。当然，这种用排除法的方式确定读者对象的做法实际上充满了“风险”，因为相对于技术类书籍或金融类书籍，

宽泛的读者定位似乎难以明确其类型和偏好，加之区块链自身的技术性很强，确实要面对不少“拦路虎”。

为了解决这些问题，笔者尝试围绕区块链的技术特点和社会价值，从其技术演进、发展历史、正反实践及与货币、金融、法律、大数据、人工智能、物联网等关系切入进行梳理，介绍基本知识、澄清误解，希望读者能在把握区块链主要特点和核心价值的基础上，以点成线、以线带面，结合各自领域进行思考。具体而言，在内容框架上分为两部分，一部分是主要从技术和历史层面介绍区块链及其特点，让读者对区块链有感性认识，可以说是“认识区块链”；另一部分则是把区块链放在整个社会中去辩证看待，并在此基础上思考如何创新运用，可以说是“运用区块链”。

除了写作思路外，写作内容对于笔者挑战同样不小。一则因为区块链本身还处在快速发展变化中，包括区块链的概念从严格意义上说也没有形成共识；二则区块链潜在的广泛用途，使得对其的理解和认识要参考更多领域的内容；三则就目前来看，区块链资料较少，案例缺乏，特别是非金融和非计算机领域的更是如此，且很多认识并不统一。即便在这种情况下，笔者愿意“斗胆”尝试的原因在于个人爱好和工作经历。作为评论工作者，在日常工作中接触到不少社会问题，思考过一些社会痛点；作为对计算机知识保持兴趣的业余爱好者，深信科技在社会治理领域有广阔的空间；作为曾有过机关工作经历的人，理解新技术对推动公共管理创新的重要意义。几方面原因叠加起来，使笔者对一些问题总有一种不吐不快的感觉，但总是以时间少为由，没有真正落实。幸得出版社友人鼓励和督促，才有诉之于笔头的行动，希望通过自己小小的努力，能够推动更多的人了解区块链，运

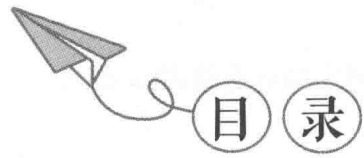
用区块链，让科技更好地服务我们的社会，造福我们的生活。

个人的能力总是有限的，对于跨领域且正在快速发展的区块链技术的跟踪和关注还远远不够，原本想要突出探讨的区块链技术在社会治理、公共管理的作用因素材料较少且自感思考尚未成熟，故相关内容在书中没有过多呈现。当然，换个角度来看，先普及基本知识，再思考深度应用及其社会意义，倒也符合事物发展的正常逻辑，希望以后能通过报刊发表或自媒体等形式与读者在这方面进行互动和交流。同时，由于个人思维的局限性，加之时间仓促，书中难免出现一些不准确、不周延或理解不到位的地方，希望大家不吝赐教，给予批评指正。可以通过电子邮件 lf_zerozone@163.com 或通过微信 readlaw 联系作者，也可以访问图书的项目页面（http://bcstime.com/lf）。

写作不是轻松的事情，离不开各方面的帮助。感谢出版社友人的策划和支持，才有清晰的结构和体系；感谢北京师范大学社会治理与公共传播研究中心主任、《社会治理》杂志社社长兼总编辑傅昌波教授在智慧治理等领域的指导和帮助；感谢中国社会科学院法学研究所研究员、国家万人计划“青年拔尖人才”支振锋教授一直以来在互联网治理等领域的启发；感谢北京法学会旅游法学研究会副秘书长王惠静女士、西门子（中国）管理研究院院长宛兵先生、中国电科华北计算所高级工程师孙宁先生等师友在区块链问题方面给予作者的支持；感谢科技博客“区势网”（http://bcstime.com）提供的项目主页；感谢家人在本书的写作过程中给予的支持和理解。

凌锋

2018 年 5 月 4 日



上篇　认识区块链

下篇　运用区块链

01 上篇
认识区块链

区块链特质：在不信任中创造信任
区块链技术：老技术成就新突破
区块链种类：分类与进化
区块链之宠：比特币风云录
区块链黑史：黑客、灰色交易……
区块链代币：ICO“神话”和无币区块链
区块链自造：开发自己的“代币”
区块链趣话：神奇的狗狗币
区块链之父：神秘的中本聪

区块链特质：在不信任中创造信任

当前，关于区块链的定义有很多。比如：

·分布在全球各地、能够协同运转的去中心化的数据库存储系统；

·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的新型应用模式等；

·防篡改的、共享的数字化账本，记录公有或私有对等网络中的交易；

·存放在非安全环境中的分布式数据库，采用密码学的方法来保证已有数据不可能被篡改，采用共识算法来对于新增数据达成共识；

……

这些定义从不同角度对区块链进行了解释，但是大都过于专业，难免枯燥，一般读者想要得到是较为明确的说法，却看到了更多不太容易理解的技术名词。我们尝试从区块链最大的特质出发，通过形象的小故事做解释，先引导大家对区块链运作的基本机制有个感性的理解，在此后的有关章节中再逐步介绍相关技术。

在山的那边、海的那边，有一个小村庄：乌特村，大概 100 余

户、500 余人居住在那里，民风淳朴，男耕女织，自给自足。

村民使用的货币是一种石头，我们就暂且称之为“石头币”。这种石头具有一种特殊的纹理，每个都不相同，石头材质来源于村西边的石山上。在老村长的主持和村民的监督下，石匠将石头打磨成两种大小的石头币，一种是大的，一种是小的，后者重量相当于前者的一半。

大家日常交易的过程，如同我们使用纸币一样，用石头币来买小到针头线脑、大到鸡鸭牛羊的生活物品和生产资料，一手交币、一手交货。交易场景是这样的：

李铁匠：张屠户，牛肉多少钱 1 斤？

张屠户：2.5 个石头币。

李铁匠：好的，成交。

李铁匠给了张屠户 5 个石头币，买了两斤牛肉。

石头币虽然是石头，但在使用过程中也会有损耗，需要不断以旧换新进行补充。这项工作是由村里的石匠来完成。村里只有一户石匠，手艺是祖传的，现在石匠年事已高，膝下的孩子不愿意做这项单调乏味的工作，都想翻过山、渡过海，看看世界有多大。

于是，乌特村遇到了一个难题，石匠手艺的后继无人导致石头币没有办法正常使用了。如果更换其他物品作为货币，不是难于携带、就是更容易损耗；虽说民风淳朴，但也没有到了每个人都是道德完人的地步，所以，在没有技术防伪的情况下，用纸币代替也不太可行。

老村长苦思冥想，头发都全白了，却一直无计可施，村民也没有

良策。一日酒酣入梦，老村长遇到一自称“仲本村”的老者，耳语数言，醒后，老村长醍醐灌顶地找到了解决方案：

1. 废除石头币，为每个村民发一个账本，用直接记账的方式代替石头币购买物品，采用一定的机制保证账本的安全和有效。

2. 考虑到记账也需要一个单位，就虚拟地提出了“乌特币”，请记住：乌特币没有任何物质载体。

3. 将村民每个人的现有财产，按照 1 个石头币等于 1 个乌特币记录在每个人的账本上。每个村民的账本上都记载了所有村民现有的财产额度。

4. 每个人保管自己的账本。

5. 在村中心最大的大树上安装一个大喇叭，每家每户发一个小喇叭。

以后村民交易的场景变成了如下这样：

李铁匠：张屠户，来斤牛肉，多少钱?

张屠户：2.5 个乌特币。

李铁匠：好的，我准备买 2 斤。

（两人跑到了村中心最大的大树旁）

李铁匠用大喇叭向全村广播：“我准备买张屠户牛肉，花费 5 个乌特币。”

接着张屠户用大喇叭向全村广播：“李铁匠买了我的牛肉，我收到了 5 个乌特币。”

接着，张三、李四、王五、周六等村民都听到了这个交易，于是

在自己的账本记上了：“某年某月某日李铁匠和张屠户有交易”，同时将李铁匠的账户减少 5 个乌特币，将张屠户的账户增加 5 个乌特币。

所有村民记载后，都拿出小喇叭，向李铁匠和张屠户反馈：“收到，已记载，确认。”

到此为止，李铁匠和张屠户的这次交易完成了，村民的账户上关于两人的乌特币金额都有了变化。如果此次交易后，李铁匠已经没有乌特币了，那么下一次，李铁匠就无法购买物品了，因为所有村民的账户上关于他的金额是 0，如果想要作弊，就得设法修改所有村民的账本，成本是相当高的。

目前，大家只需看到并理解乌特村的这些变化就可以：废除了石头币，没有一个中心化的乌特币制作机构，村民实现了新交易形式，账本是不可篡改的，或者说篡改成本大到等于不可篡改。

通过上述变化，可以发现，在一个并不是人人都是道德完人的环境下，通过制度设计实现了村民之间的信任，进而保障了交易的正常进行。或许大家通过乌特村的例子能够或多或少地理解了一些诸如分布式账本（每个村民都有账本）、共识机制（所有村民都同意交易）、非中心化的货币（乌特币并不存在，如同此前的有石匠制作的环节），等等。

不少人看到这里也许有一些疑问，比如环节太多、过程太麻烦、村民的隐私没有保障，等等。故事化解读是为了更通俗地让大家理解主要的、基础的概念，介绍区块链运行的基本原理，其他一些复杂的问题，我们会在后续的内容中逐步谈到。

区块链技术：老技术成就新突破

在前面的章节中，我们用“乌特村”的例子形象地对比了传统货币和加密货币，并模拟了乌特币交易的过程。从本章开始，将介绍区块链核心技术的有关知识。由于比特币是区块链技术目前最有代表性的应用，在以下的介绍中，相关具体实例还将以比特币为主进行说明。

区块链并非一项创新技术，而是将许多跨领域技术集成在一起，从某种角度来看是一种架构的创新。其中涉及密码学、数学、经济模型、点对点网络等。为便于理解，我们不采取从底层到应用层的技术性的介绍方式，而是假设我们都是“中本聪”，以问题为导向，在寻找解决方案的过程中逐步深入地来理解。

在“乌特村”的例子中，我们看到，记账的形式代替了货币，村民每家每户都有账本来维持彼此之间的信任关系。区块链技术核心也是如此，通过让每个用户都掌握所有数据来创造信任。从信息技术的角度来看，这个“账本”本质上是一个数据库，而且是分散到每个用户的数据库，在计算机领域，通常称之为“分布式数据库”。