
“信用”机器
智能合约
去中心化
分布式治理
解读区块链
重新定义未来经济
开放共享
韦康博◎著
数字货币
当很多人还不清楚什么是PC互联网的时候，移动互联网来了。当我们还没搞清楚移动互联网的时候，大数据时代又来了。
——马 云
当我们还没有弄清楚大数据的时候，区块链又来了
中国工信出版集团
人民邮电出版社
POSTS & TELECOM PRESS

解读区块链

重新定义未来经济

韦康博◎著

人民邮电出版社

北京

图书在版编目（CIP）数据

解读区块链 ：重新定义未来经济 / 韦康博著. —
北京 ：人民邮电出版社，2017.8
ISBN 978-7-115-46213-8

Ⅰ. ①解… Ⅱ. ①韦… 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(2017)第151911号

◆ 著　　韦康博
责任编辑　李　强
责任印制　彭志环
◆ 人民邮电出版社出版发行　　北京市丰台区成寿寺路 11 号
邮编　100164　　电子邮件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
大厂聚鑫印刷有限责任公司印刷
◆ 开本：700×1000　1/16
印张：13　　2017 年 8 月第 1 版
字数：145 千字　　2017 年 8 月河北第 1 次印刷

定价：59.00 元

读者服务热线：(010)81055488　印装质量热线：(010)81055316
反盗版热线：(010)81055315

前 言

20 世纪 90 年代，互联网技术就已经成型，人类社会从工业化时代走向信息化时代，而阿里巴巴、京东和腾讯等大型网络公司借助信息化的羽翼得以成长、壮大。如今，20 多年过去了，大多数人还是相信以“BAT”（百度、腾讯、阿里巴巴）为主导的互联网巨头代表着最优越的科技和最先进的思想，然而，美国互联网领域知名的预测专家凯文·凯利却表示：“未来的世界是去中心化的。”

在商业领域，去中心化意味着将权威因素从合作中移除，它直接否定了目前势头正盛的房产中介、证券交易所、车辆交易所，甚至是银行等机构。如果去中心化真的是未来趋势，那么淘宝、京东、亚马逊、当当等一系列网络交易平台将会受到巨大冲击。

马云曾经说过一句很经典的话，当很多人还不清楚什么是 PC 互联网的时候，移动互联网来了。当我们还没搞清楚移动互联网的时候，大数据时代又来了。现在，我们完全可以再补充一句：“当我们还没有弄明白大数据的时候，区块链又来了。”有专家预言，区块链技术在未来十年，势必引领信息社会的发展方向。

区块链的去中心化也有一定的道理。我们知道，两点之间直线距离最短。人与人的交流也一样，直接交流时，双方几乎能接收到全部的信息；而如果中间有传话者，就有可能出现信息的讹传或丢失。商业交易更是如此，先进的交易平台都是由某个集团或组织控制的，它们虽然可以通过操控平台为人与人之间的交易提供便利，但也在无形之中侵犯了用户的权益。例如，目前各大交易

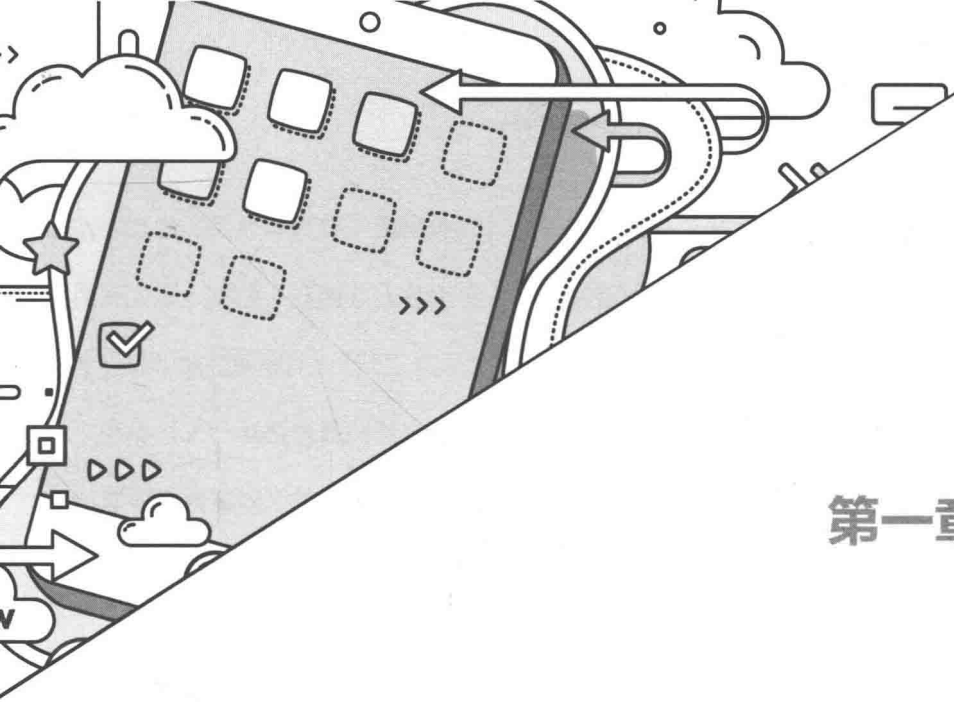
平台都可以通过记录用户的日常操作、消费习惯，甚至是个人信息来实现各种商业目的，而这部分信息本属于用户，这就相当于获取了本属于用户的利益。再如，中心化平台为了获取利润，往往要收取平台用户高额的费用，比如淘宝的商家用户每年都要向平台方支付高额的租金和扣点。另外，中心化的平台由于权力过度膨胀，必然会滋生腐败，而且各种暗箱操作也不利于资本市场的整体运营。

在互联网时代，创新就像是一道耀眼的闪电，照亮了社会发展的前进道路。纵观科技的发展之路，从互联网、移动互联网、社交网络，到当前的大数据、云计算和人工智能，凡此种种，无一不对人类社会产生了深远影响。而区块链的出现亦是如此。从发展历程来说，与区块链息息相关的去中心化理念使比特币历经了8年的发展。今天，区块链已经成为一个无法被更改的分布式账本系统，众筹保险、智能债券、跨境支付等都可以运用。自此，互联网浪潮又被区块链推向了一个新的起点。

区块链之所以倍受瞩目，不仅仅是因为它高超的技术和精密的算法，还因为它所体现的社会价值，“去中心化”“全民平等”“开放共享”“分布式”等人们以前无比向往的事物都会因为区块链的存在而一一实现。区块链通过使用不可更改的账本，真实地记录了互联网上的各种数据、历史和见证，体现了一种追求真理的精神。我们可以说，区块链是建立绝对公平公正的“信用”机器，它将重新定义这个世界。

本书从最基本的比特币系统讲起，从比特币创始人中本聪的基本思路出发，带领读者认识区块链、分析区块链，最后学会应用区块链。本书从浅显到深刻，从理论到实践，从技术到领域，从自然到社会，详细诠释了区块链的世界。全书可以分为三个部分：第一部分主要阐述区块链的起源，并介绍了区块链的基本概念和创新应用；第二部分阐述区块链的技术特征以及区块链技术的具体应用；第三部分放眼未来，以全新的世界观和价值观诠释区块链给全人类带来的巨大福音。

目 录



第一章

区块链的起源

——如何利用超时空技术破解古拜占庭的“将军困境”

依照旧有的交易模式，买卖双方往往需要寻找一个权威的“中间人”来规范操作。这个步骤解决了商业行为中的“信任”问题，但在无形中又制造了额外的损耗——“中间人”的存在，这毫无疑问会对买卖双方交易产生一定的阻碍。其实不光是商业行为，在其他任何涉及“信任”的领域，人们都需要借助权威中心的帮助。为了解决中间因素给社会生活带来的负面影响，区块链技术就应运而生了。

取消自由协议中的过渡环节，可以说是人类社会发展的终极趋势之一。点对点的直线对话节省了大量的社会资源，同时也更能反映沟通的本质。可以确信的是，区块链技术的出现帮助人类社会解决了一个重大难题。在生活节奏加快、各领域交流更加频繁的时代，区块链理念的诞生也因此显得更加熠熠生辉。

1. 拜占庭将军如何破解人类未解之谜

步入信息化时代之后，“万物联网”的新生活模式进入千家万户。与过去相对低效、闭塞的世界有所不同的是，互联网时代缩短了人与人之间的相对距离，提高了我们的生活质量。但是过于发达的信息技术，又在一定程度上对网络参与者的个人隐私与人身财产安全造成隐患。在前沿科技最为发达的美国，网络信息犯罪率一直居高不下，每年都有1500万居民的身份证被他人冒用，由此引发的经济损失多达千亿美元。那么，在电子交易逐渐占据主导的大时代背景下，如何保障虚拟货币的安全，就成了经济学界分外关注的话题。而正是在这样一种时代需求的推动下，区块链技术诞生了。

用学术化的技术分析来阐述区块链的理念内核未免会让人感到晦涩难懂，业内更习惯用“拜占庭将军”的故事来帮助人们快速理解区块链的技术原理。“拜占庭将军”的故事是这样的：一座坚固的城堡遭到了外来军队的攻击，城墙内

部有一万名士兵严阵以待，而城外的入侵者则是由拜占庭将军和他的副官统领的两万大军。不过，这两万人分别由 4 名副官指挥，拜占庭将军只是在大后方对军队进行统一调度。

这样一来，问题也就突显出来了：一方面，由于城堡中守军实力强大，将军必须调用两名以上的副官参与进攻；另一方面，副官中也可能有叛徒，假如他们抗拒、篡改军令，那么这次作战计划就会失败。

所以说，城外的进攻方虽然看起来兵力更强，但实际上，他们面临诸多隐患。假如，某一副官得到了干扰信息而贸然出击，那么他和属下将会面临全军覆没的危险；同样，假如有指挥官没有按照将军的指示联合进攻，那么本次军事行动也可能遭到失败。很显然，信息的准确传递就成了取胜的关键因素。

在拜占庭时期，将军并不能利用现代化科技设备来达到精准指挥的目的，书面信函才是联络各处的通用“文件”。而要确保军事命令的准确传达，一个比较可靠的办法就是在信件上附加将军和接收指令的副官的签名，同时禁止副官之间互相发信。这样一来，唯一的有效文件将在各个营地传递，最后再返回到将军手中。

在这样一套规则下，整个作战计划才会被明确下来，4 名副官也不会被间谍们的流言误导。这样一个抑制了干扰选项、确保信息唯一性的过程，就与“区块链”技术有着极高的相似度。

从本质上说，区块链技术实际上是一个去中心化的分布式账本数据库。说得更加宽泛一些，区块链就是一个包罗万象的记账本，而在这个记账本中，所有信息都是透明化且不可修改的。如此，各个节点正在传输或者已经传输的信

息，就都被赋予了唯一性的特征。更进一步说，对于区块链中发生的交易，所有节点都会“记上一笔”。这样做的好处就是，假如有人想要修改某项交易记录，那么，除非他控制了一半以上的相关节点，否则他很难成功。

在“拜占庭将军”的例子中，将军与 4 名副官就像是分散的节点，他们需要通过信号的传递来达成默契。但是这个小队伍中很可能有敌方卧底，会蓄意篡改将军的信函，所以，一封附有所有人的签名的公文，才能够保证信息的准确传达。更加重要的是，各名副官将会同时起到传信与监督的作用，他们除了在作战指令上加盖印鉴，同时还要确认这道公文的合法性，所以，改变战时情报实际上是不可能完成的事。在这个类似区块链结构的环境中，所有信息都是透明流通的，个体力量并不能改变公众账本上的既定信息。

所以说，区块链技术的出现，将从规则上为相关区域的信息安全带来保障，在成熟的区块链体系中，所有被记录的数据都难以被篡改。如果我们把这一技术引入社会生活，那么很多棘手难题就都能迎刃而解，比如美国的公民证件盗用事件、世界贸易中的虚拟货币安全系数问题等。

凡此种种，都与人类生活有着密不可分的关联，而区块链技术的普及，可以极大程度地保障它们的安全性能。很显然，信息化数字生活将会是未来世界的主流形态，而人类社会对信息技术的依赖程度也会越来越高。以和人类关系最为密切的商品交易为例，未来世界的实体货币流通率将会逐渐降低，虚拟货币将会成为各类交易的核心介质。在此，区块链技术作为一个分布式账本数据库，它能够带给人类的就是高系数的安全保障。

在区块链技术原理的引导下，交易者之间会建立起一个公开透明的虚拟网

络，在这个网络中，所有交易活动都会被全体参与者记录下来。比如，该网络的节点 A 向节点 B 购买了一套茶具，那么该网络中的所有节点都会记录下本次交易的时间、地点、经过、价格、对象以及收付款情况。此后，假如 B 宣称自己没有收到货款，那么网络中的所有参与者都将会翻看自己的记账本，求证 B 说的话是否属实。

可以说，区块链技术的出现，是信息化时代的关键性产物，正是在它的帮助下，信息数据的安全性才能得到更为可靠的保障。或许在不久的将来，人类社会的信息交流与存储将会更加频繁，这对于全人类的高速发展将会起到不可磨灭的推动作用。

2. 去中心化为区块链插上“梦想的翅膀”

在庞杂的数据网络中，有一个问题是所有参与者都在全力关注的，那就是信息传递的可靠性。某次数据处理过后，当事人否认了此前的参与行为怎么办？在古代社会，我们通过道德规范来约束此类行为的发生，但是很显然，精神批判和舆论谴责并不能从根本上解决社会诚信问题，合理的规则约束才是维护公共秩序的有力手段。

实际上，要保证共生环境内既定协议的有效执行，选择一个可靠的“中心”就可以。例如，我们通过网络平台购物，正常的流程是选定商品之后，把款付给平台，然后该平台再通知卖方发货；买家收货之后，向平台发送了确认信息，平台再把货款付给卖方。

在这样一个交易流程中，买卖双方都无需担心“被骗”，因为作为促成交易的媒介，网络平台必然要承担风险把控的责任。假如卖主发出的是劣质商品或者买家要求退货，甚至是买卖双方在合同协定上出现了纠纷，那么这其中的沟通协调、规则制定等，都需要由网络平台负责。这样看来，买卖双方都得到了一个安全可靠的“中间人”，大家各司其职，似乎非常和谐。

但是，这种运作模式同样也存在不少弊病。一方面，结构流程繁复在一定程度上会给协议达成带来阻力。原本只是“买家付款→商家发货”的简单流程，现在多了个中间环节，这其中的无端消耗其实是非常糟糕的。而且在很多时候，同一个平台需要承载千万个交易，整个贸易体系本就庞杂繁复。另一方面，“中间人”的可信度又有多高呢？假如他们也“见利忘义”，那么被放了鸽子的买卖双方又该找谁追赔？

因而，协议双方一方面担心对方的诚信问题而寻求第三方公证，另一方面又希望简化流程而试图将“中间人”剔除。而这样一个矛盾的实质其实就是区块链技术中的“去中心化”。

所谓去中心化，就是将协议中的第三方权威从整体架构中移除。按照之前的理论，如果缺少了“中间人”的居中调度，单方面毁约的行为将层出不穷。区块链模式要实现“去中心化”，那就必须要拿出一个合理可行的替代方案。可以说，区块链模式是对传统的“三方认证”模式的颠覆。在它的帮助下，人类社会的网络交易、信息存储等都变得简洁、可行，而且安全系数更高。

例如，A 向 B 借了 10 万元，约定一年后还清，C 是中间人。一年之后，A、B、C 三人来到约定地点，并完成还款事宜。这件事情看上去合理可靠，但其中

也存在不少风险：假如A和C串通一气，否认本次借贷，那么B是否会因此蒙受不白之冤？又或者C意外身亡，那么这笔借款是否就没有了公证人？但在区块链模式下，“集体认证”的方式能够很巧妙地规避上述问题，它不单单简化了协定流程，还强调了安全性。

总体而言，“去中心化”是区块链模式的重要特征，它果断移除了“中间人”在协议流程中的作用，以相关区域内部的“集体认证”取而代之。这样一种更加科学严谨的数据存储模式为区块链模式赋予了独特的权威，我们甚至可以说，“去中心化”理念的进一步推广，将会给各行各业带来深刻启发，或许在未来，世界政体也会发生颠覆性改变，比如传统的管理者消失，社会实行集体监督、自我管理的模式。这样一种生活现状，可能就是区块链理念能够带给人类的“最伟大梦想”。

3. 比特币：金融世界的“玄幻佳作”

在探讨区块链相关知识的时候，有一个概念是必须要提及的，那就是“比特币”。与传统货币有所不同的是，比特币可以看作虚拟货币，它既不属于“美国制造”，也不是“英国特产”，但是世界上很多国家都认可它的合法性，并且允许持有者用它兑换本国流通的钱币。只要饭店老板同意，我们甚至可以用比特币在饭店消费。如此看来，比特币散发着非常独特的魅力，它充当了“世界货币”的角色，但却没有任何一个政府或民族对它进行权威认证。这种世界范围内的默契，似乎也充满了令人如痴似醉的“玄幻感”。

在深入探究比特币之前，我们理应对其价值原理进行剖析。实际上，比特

币是区块链体系中的特殊产物，它没有专门的发行机构，也不能被伪造复制，而且从数额总量上说，全球比特币的存在上限是2100万个。

在区块链体系中，任何东西都是可以被交易的。无论是一个真实存在的汤锅，还是一瓶看不见摸不着的空气，又或者是抽象符号，甚至是那些闻所未闻、莫名其妙的喻指，只要有人愿意认可这件“商品”，我们都可以将其纳入“交易栏”。在区块链体系中，假如A节点喊了一句：“我有100个莫拉拉！”而其他节点也都认可了这一说法，那么A节点就真的“拥有了100个莫拉拉”，但究竟“莫拉拉”是什么、它可以做什么，都无关紧要。再进一步，假如A节点说：“我把1个莫拉拉给了B！”同时B节点也认为自己收到了1个莫拉拉，那么这个区块内部的其他节点就都会自觉地在自己的记账本上留下记录：“某年某月某时某刻，节点A将1个莫拉拉给了节点B。”

也就是说，“比特币”的诞生和“莫拉拉”如出一辙。原本我们并没有“比特币”这个概念，只不过后来人们达成了一种共识，认可了比特币在区块当中的“通货地位”，所以比特币就作为一种虚拟货币，流通于各项交易中了。

时至今日，比特币已经成了世界贸易体系中不可或缺的一环，在它的帮助下，各类贸易变得更加流畅。同时，在区块链技术支持之下的公共账本，它也为每一次交易加盖了独一无二的印章。无论是大宗商品的进出口，还是小饭馆里的一碗面，我们都可以用比特币买单。自从2009年中本聪勾画出区块链雏形并提出比特币理论，经过短短数年时间，强大的区块链技术就已经覆盖了人类生活的方方面面，比特币也红遍全球。

相比于传统货币，比特币具有强大的自我保护机制。这样说的理由是，比特