青岛“链湾”区块链系列丛书

• 描绘社会信用新蓝图

# 世界因区块链而不同

Blockchain Changes the World

陈东敏 主编
郭 峰 广 红 副主编

• 重新定义世界与经济

• 打造“区块链+”应用生态圈

• 构建全球区块链中心

北京航空航天大学出版社
BEIHANG UNIVERSITY PRESS

青岛“链湾”区块链系列丛书

# 世界因区块链而不同

陈东敏　主　编
郭　峰　广　红　副主编

北京航空航天大学出版社

**图书在版编目(CIP)数据**

世界因区块链而不同 / 陈东敏主编. -- 北京 : 北京航空航天大学出版社，2017.4

ISBN 978-7-5124-2376-3

Ⅰ. ①世… Ⅱ. ①陈… 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 063235 号



世界因区块链而不同

陈东敏　主　编

郭　峰　广　红　副主编

责任编辑　孙兴芳

*

北京航空航天大学出版社出版发行

北京市海淀区学院路 37 号(邮编 100191)　http://www.buaapress.com.cn

发行部电话：(010)82317024　传真：(010)82328026

读者信箱：emsbook@buaacm.com.cn　邮购电话：(010)82316936

北京泽宇印刷有限公司印装　各地书店经销

*

开本：710×1 000　1/16　印张：7.25　字数：100 千字

2017 年 5 月第 1 版　2017 年 5 月第 1 次印刷

ISBN 978-7-5124-2376-3　定价：39.00 元

# 编 委 会

主　　编:陈东敏

副 主 编:郭　峰　广　红

参编人员:(按汉语拼音排序)

陈海峰　陈　润　高登攀　高　炎

纪文峰　蒋　海　李　军　李少恒

廖　逸　马　刚　马　蓉　王大崑

杨　廉　杨　勇　于　潇　曾强生

翟海滨

参编单位:(按汉语拼音排序)

百灵科技

北京大学创新研究院

布比网络

点亮资本

国际大学创新联盟

金股链科技

青岛区块链研究院

数链科技

世界因区块链
而不同

物链科技

中国科学院计算所

众签科技

合作单位：中关村区块链产业联盟

万向区块链实验室

中国分布式总账基础协议联盟

赛尔网络

# 序

近年来兴起的区块链技术是继互联网、无线通信、云计算、大数据之后计算和网络技术的又一颠覆性创新，正在引起一场新的技术变革和产业变革。区块链技术是由分布式数据存储、点对点传输、共识机制、加密算法等计算机技术交汇(Convergence)而形成的一种可用于信任传递、分布和管理价值(如货币)等与诚信关联的各种交易过程和结果的信息网络应用技术。区块链去中心化的数据结构和智能合约的基本功能使得该技术具有彻底颠覆传统金融行业和价值交易体系的巨大潜力，因此受到全球金融行业和各国政府的高度关注。虽然，区块链技术起源于数字货币的诞生，但随着人们对区块链认识的不断提升和对该技术的不断拓展，区块链的应用远远超出数字货币管理的范畴，并已延伸到各类价值和商品的交易、传输中，比如供应链管理、保险业、医疗信息、工业 4.0、知识产权管理、社会福利保障、政府和社会诚信体系的维护等。可以预言，区块链技术在各个领域的成功应用，将从根本上影响和改变社会成员、企事业机构和政府的行为。

作为新兴产业，区块链在多种场景的应用中将替代多种传统服务业。这些传统行业因广泛涉及民生和社会发展，受到各种法规的管控和监督。区块链产业的发展必然会挑战现有的法规和制度。加速区块链产业的发展，一方面需要政府的积极参与，引领产业发展生态环境的建设，有序地开放市场，建立开放的监督和管理机制；另一方面需要开发区块链技术和应用的各种新创企业加强自律和社会责任感，严格把控产品和服务的可靠性、安全性和实效性，不失信于用户和市场。建立行业协会和产业标准，要坚持营造开放和公平竞争的市场环境，要对加速发展新兴行业起到积极的推动作用。

中国在区块链的底层技术上已经形成了具有国际竞争力的自主专利技

术，应用区块链的新创技术公司更如雨后春笋般层出不穷，已经覆盖多个领域。各地政府高度重视区块链技术的落地和发展，纷纷出台扶持政策。如同互联网技术的发展，中国在区块链的核心技术和应用技术的开发上将走在世界前列。青岛“链湾”区块链系列丛书将系统地介绍区块链技术的发展史，我国自主研发的区块链的核心技术，以及区块链技术在金融服务业、医疗健康、供应链管理、食品溯源等多个领域的应用方案和案例。这套丛书的编写和出版旨在促进区块链技术产业知识的传播、人才的培养，加速区块链产业在中国的发展，提升中国在全球的竞争力。

北京大学创新研究院教授
青岛区块链研究院院长
陈东敏

2017 年 3 月

# 前　言

最近两年来，从旧金山硅谷到纽约华尔街，从北京中关村到上海陆家嘴，从各国央行到各大商业银行，从联合国、国际货币基金组织到许多国家的政府研究机构，区块链已成为讨论的热点，风险投资和产业界也纷纷加大投入力度，“区块链＋”应用创新正在成为引领发展的动力。

为什么区块链会受到如此广泛的关注呢？

我们知道，互联网是工业革命以来人类最伟大的技术发明之一，因为它解决了人与人之间近乎零成本的信息传递，短短 20 年时间就改变了我们的生活方式。然而，目前的互联网仍然存在很多问题，其中最大的痛点就是无法低成本解决信任传递问题，导致信任的传递与价值的转移方式不得不依赖于中介，不仅成本高、效率低，而且容易产生腐败与安全漏洞。而区块链技术被认为是可以低成本解决信任传递问题的有效方案。借助区块链技术，在现有的互联网上，无需第三方中介的介入，就可以使参与者以极低的成本建立信任，并在信任的基础上进行包括支付购物、提交文件、签合同、约定记录等在内的交易活动。

但区块链究竟是什么东西呢？有人说比特币是区块链，有人说区块链是个加密的分布式共享账本。2016 年 10 月由国家工业和信息化部信息化和软件服务业司指导编写的《中国区块链技术和应用发展白皮书(2016)》中说，“区块链是分布式数据存储、点对点传输、共识机制、加密算法等计算机技术在互联网时代的创新应用模式”。下面我们从一个一般的区块链网络的工作原理入手，看看区块链到底是什么。为便于非专业人士阅读，后面的叙述中我们尽量回避使用专业的密码学术语。

一个区块链网络包含多个参与者(可以是人、设备，或者其中的功能)，每个参与者都有一个经过认证的身份，并连接在同一个可直达的网络上。

参与者通过这个网络完成某种事情，下面统称为交易。任何两个或多个参与者都可以在这个网络中进行交易，包括支付购物、提交文件、签合同、约定记录等。交易完成后，交易者共同把交易记录发布到网络上，每一个参与者都可以参与审核这些交易记录的合规性，包括交易人的身份验证以及交易是否合规等，并提交审核结论。审核结论由大家投票确定，最后以大家达成共识的方式把审核结论和交易记录一起存储在一个时间有序的链条上。该链条可阅读但不可更改，被分布式地存储在整个网络上。

区块链网络的特点归纳如下：

① 所有的网络参与者都参与审核，审核人身份不可抵赖；

② 以大家达成共识的方式见证、封存交易记录；

③ 封存的交易记录按时间排序，分布式地存储共享，但不可篡改。

在上述区块链网络中，对参与者的身份认证、共识决策的达成、记录的不可篡改等，是由严格的数学算法来保证公平、公正的，是用现代密码学来保证安全的，并且在互联网上由智能设备实现一系列操作。为表述方便，我们暂且把上述特点再简单地归纳为“区块链思维”：人人审核、大家见证、身份不可抵赖、记录共享但不可篡改。

其实，上述“区块链思维”并非凭空而来，它是互联网自然演进的结果。我们知道，路由器是互联网底层的基础设施，它的基本功能就是传递信息包。每个路由器的任务就是把从上一个路由器传来的信息包传递给合适的下一个路由器，直到目的地。为此，所有的路由器必须通力合作来维持一个路由信息表。如何做到这一点呢？

每个路由器都有一个身份，所有的路由器连接起来组成一个可通达的网络。每个路由器不间断地接收、整理其他路由器发来的路由信息，并把自己掌握的路由信息再公告出去。一定时间后，每个路由器就都掌握了整个网络的连接状态，当然也就知道把收到的信息包送往何处了。现实的互联网路由器要更复杂一些，但原理大致如此。

小结一下路由器的特点：人人参与发送路由信息，这些信息分布式地存储在各个路由器上；所有的路由器都共享整个路由信息，并以约定的规则更新信息。这是不是与“区块链思维”有些像？不要小看这几个特点，正因为如此，才使得互联网的结构柔韧、扁平，使得规模的扩展非常容易，使得建设与运营大大简化，从而使得互联网的综合成本大大降低。

正是基于路由器的这种人人参与、大家分享的思想，才造就了互联网的高速发展，并解决了人与人之间可靠的、近乎零成本的信息传递，短短 20 年时间就改变了我们的生活方式：20 世纪 90 年代的互联网以 PC 为入口，成就了思科、雅虎、华为、谷歌、百度；2000 年以后的移动互联网以智能手机为入口，成就了移动支付和电商。毫不夸张地说，路由器的这种“人人参与、大家分享”的思想是后来“互联网思维”的根源所在，也是“区块链思维”的早期萌芽。

但是，目前互联网正在遭遇信任危机，面临发展瓶颈。看看我们周围的互联网应用，无论是即时通信、社交网络、媒体，还是银行、电商、公共服务，都是清一色的超大规模应用中心。所有这些应用中心都已经成为或正在逐步演变成为单一的庞大权利中心：每个中心都有自己独立的用户认证、账号管理、用户交易数据管理等系统，所有的这些中心之间都相互独立，甚至相互为敌；每个中心都试图把用户积累的各种记录占为己有，并依靠垄断这些“大数据”形成的“霸权”作为自己的商业模式。

即便这样一个超大的权利中心，也很难自证清白，无法有效解决互联网面临的信任危机。譬如，当甲通过某即时通信工具向乙发送信息时，甲无法证明自己发送到乙的信息在时间和内容上都是正确的，除非乙愿意配合提供准确的记录；而乙也无法证明甲发送过来的信息在时间和内容上都没有经过他人篡改。即使引入第三方监管丙的中心化系统，甲和乙也要承担丙无法如实提供准确数据的风险。

其实，信任的传递，通俗地讲就是自证清白以及如何验证清白，这是人

类社会古老的痛点。下面举个例子，看看在日常生活中，甲如何向乙自证清白，以及乙如何验证甲的清白。

① 甲提交自己对事件的详细描述，包括相关人证、物证等佐证；

② 乙首先对甲的自述进行主观分析，然后启动外调程序，就是派专人对甲所述情况及佐证进行核实；

③ 乙基于自己的分析和核实的结果，对甲的陈述给出是真或伪的结论。

这是一个相当低效费时的工作，并且有明显的系统漏洞：乙也没有办法百分之百保证参与调查的人的能力及其廉洁性。

下面我们看看在互联网上是如何进行这一工作的。举个例子，甲在一台新设备上第一次登录自己在应用中心乙（譬如支付宝或微信）注册的账号。当甲输入账号和密码后，乙通常会向甲注册的手机发送一个验证码，甲正确输入该验证码后，乙将允许甲的新设备登录。这是什么意思呢？其实，这是乙对甲做的一次身份外调，而甲的手机运营商，则是此次外调的第三方证人。当然，乙也可以采取其他的外调方法，之所以采用手机短信码验证，是因为这是目前最快捷、成本最低的方法，尽管我们已经知道这种方法也是很不安全的。

另外一个与“信任传递”关联的问题就是“价值传递”，通俗地讲就是甲向乙递交一笔费用，或支付一个“数字”。很显然，“价值传递”是“信任传递”的一个特例，我们知道，从古老的“票号”到现代银行体制，就是针对这一特例的解决方案。现代银行是如何解决价值传递问题的呢？银行本质上是一种信任中介，它通过政府或长期的商业行为建立信任，银行客户通过在银行的存款证实自己的价值，并以此为基础通过银行向第三者支付。这是一种通过一个强大的信任中介的解决方案，也是目前为止最为有效的价值传递方法。但是这种方法的代价却非常高昂：银行中介的高额运营费用，也就是价值传递的费用，必须由客户承担。

下面我们看看区块链是如何解决这一问题的。

再回顾一下区块链思维：人人审核、大家见证、身份不可抵赖、记录共享但不可篡改。下面通过一个简单的例子，说明在区块链网络中，甲如何向乙证明自己月收入为1万元、血型是O型这件事。假设有一个区块链网络，网络中的参与者包含诸多企业的人力资源部门、税务机构、相关银行、医院和学校。

① 甲向乙提交一个记录，表明自己月收入为1万元、血型是O型。该记录还包含3个佐证：自己工作单位丙的签字、税务部门丁的签字、医院戊的签字。

② 该记录经甲乙双方签字后提交至区块链网络审核。

③ 所有的网络参与者都对甲、乙的身份进行验证，对丙、丁、戊三方的签章进行核实。最后的审核结论由大家投票确定，并以大家达成共识的方式把审核结论和记录写入区块链中。

如果该记录通过了审核并被记入了区块链，则甲成功地向乙证明，自己月收入为1万元，血型为O型；同时，乙也验证了甲的陈述是真实的。

区块链的本质其实就是构建一个人人参与的、多中心的信任体系，并在此信任体系之上，实现可信任的数据共享。在没有区块链之前，譬如我们有10个机构在一起，也是可以共享数据的，方法就是这10个机构都把自己的接口开放出来，让另外9家去查阅。但是这个做法有个问题，就是不可信任：尽管可以让别人看我的数据，但毕竟我的数据归我管，我擅自改了别人也无法确认；对方的数据归对方管，对方改了我也无可奈何。区块链的意思是，让参与共享的10方共同拥有一个网络，对于其中的任何一个参与方，其写进的数据自己不能篡改，其写进的数据自己也不能抵赖。

那么，区块链网络的性能和成本如何呢？

与互联网中的路由器类似，区块链网络中的参与者需要参与部署区块链服务器。该服务器分布式地部署在网络中，即使部分服务器发生故障也不会影响整个网络的运行；整个网络结构柔韧、扁平，规模扩展容易，运营非

常简单。不同的是，区块链服务器可由通用 PC 构成，而互联网路由器则是专用硬件设备；路由器处理的是路由信息，而区块链服务器处理的是信任信息。可以说，部署和运营一个区块链网络的费用不会比一个通常的互联网应用网络更高。目前，投入使用的区块链网络处理的交易量可达 1 万笔每秒。随着机器处理能力的提高和算法的升级，区块链网络的处理速度还会不断提高。

2008—2013 年，有关区块链的讨论更多地局限在以比特币为首的“币圈”，人们关注的焦点是如何更快地“挖矿”以及更简便的比特币交易。2014 年，Blockchain 2.0 概念的出现是个分水岭，人们的目光从比特币本身转移到了支撑其价值转移的底层技术——区块链。中文名称“区块链”也诞生于这一年，经过多个线上微信群和线下沙龙的多次、反复争论，“区块链”这一偏重于技术属性的称谓从“价值链”“信任链”“账链”“部落链”等诸多翻译中脱颖而出，逐渐被大多数人所接受。

目前，区块链应用已延伸到金融科技、数字资产交易、物联网与互联网应用、供应链管理、政府公共管理与社会治理、能源管理及智能制造等多个领域，有可能引发新一轮的技术创新和产业变革。如果“互联网＋区块链”解决了信任的低成本传递问题，那么它将从根本上改变人类几千年来的交易模式，使得人类社会的运作更加简单、高效。

我们看到，从互联网思维到区块链思维是一脉相承的。“互联网＋区块链”是一个多中心的、去中介的、自组织的、共享数据的可信任网络，现有的互联网应用以及传统行业将逐步被重塑，无论是即时通信、社交网络、媒体，还是银行、电商、公共服务等，都将被区块链思维重构，一个崭新的“区块链＋”应用时代正在到来。

点亮资本合伙人

中关村区块链产业联盟副理事长

郭　峰

2017 年 3 月

# 目　录

# 第1章

# 区块链技术的起源