

链接未来

迎接区块链与数字资产的新时代

主 编

许子敬

程剑波

魏久胜

常 浩

编 著

HCASH基金会隆重推出区块链专著
HCASH基金会名誉主席许子敬先生担任主编



机械工业出版社
China Machine Press

链接未来

迎接区块链与数字资产的新时代

主 编

许子敬

程剑波

魏久胜

常 浩

编 著



机械工业出版社
China Machine Press

图书在版编目(CIP)数据

链接未来：迎接区块链与数字资产的新时代 / 许子敬主编；程剑波，魏久胜，常浩编著.
—北京：机械工业出版社，2018.3（2018.5重印）

ISBN 978-7-111-58684-5

I. 链… II. ①许… ②程… ③魏… ④常… III. ①电子商务—支付方式—研究
②电子货币—研究 IV. ①F713.361.3 ②F830.46

中国版本图书馆CIP数据核字（2018）第032552号

链接未来：迎接区块链与数字资产的新时代

出版发行：机械工业出版社（北京市西城区百万庄大街22号 邮政编码：100037）

责任编辑：冯小妹

责任校对：殷虹

印刷：北京诚信伟业印刷有限公司

版次：2018年5月第1版第3次印刷

开本：147mm×210mm 1/32

印张：8.25

书号：ISBN 978-1-111-58684-5

定价：55.00元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换

客服热线：(010) 68995261 88361066

投稿热线：(010) 88379007

购书热线：(010) 68326294 88379649 68995259

读者信箱：hzjg@hzbook.com

版权所有·侵权必究

封底无防伪标均为盗版 本书法律顾问：北京大成律师事务所 韩光 / 邹晓东

前 言

要么拥抱颠覆，要么被颠覆

说起区块链，就不得不从比特币说起。2008年，一个化名中本聪的神秘组织发表了比特币的白皮书——《比特币：一种点对点的电子现金系统》。2014年开始，比特币的行情波动让“区块链”这个概念逐渐进入了一部分人的视野。

区块链究竟是什么？一言以蔽之，区块链是一种能够大幅降低商业社会信用成本的技术。区块链作为一个分布式的账簿，其数据一旦记录下来，就是永久保存且不可更改的。过去，当你和一个陌生人进行一个商业行为的时候，你无法百分之百地相信他，他也无法百分之百地相信你，为了解决这个问题，我们不得不需要第三方来做信用背书以证明这个交易的公平性和真实性。但是第三方信用背书就是完全没有问题的吗？有没有可能通过技术的手段，不需要信任第三方，彼此就能达成信任，从而可以直接促成交易？区块链就是为了解决这个问题而生的，通过代码和数字，

不可篡改，达成了信任的基础。通俗地说，我想和你做生意，我知道 $1+1=2$ ，你也同意 $1+1=2$ ，那我们就有了信任的基础。我们的交易会在全网广播，所有人都来作证，这样不需要第三方，我们就可以完成交易了。这是一个非常了不起的发明！商业社会发展的基石便是信用！而区块链居然大幅地降低了信用的成本。

目前，我在硅谷所认识的大多数人都把注意力集中在了人工智能上，他们认为这是最有前景的技术革命。我也被他们的热情深深感染了！人工智能将颠覆行业，并赋予我们从前只敢在超级科幻小说中想象的能力。诚然，人工智能拥有改变世界的能力，而区块链也可以。一个社会的发展，一方面是生产力的发展，另一方面是生产关系的发展，生产力和生产关系相互作用。在我的认知判断里，以人工智能为代表的新技术，代表着先进的生产力，一定有非常好的前途，可以提升很多工作的效率，而区块链则代表着先进的生产关系，把信用的成本降低到忽略不计，大幅提升了交易的效率。人工智能和区块链的结合，一定是未来最有前途的产业。

有人说，现在区块链数字货币资产涨得这么快，肯定有很多泡沫！“当主流媒体还在忙于猜测加密货币价格及其黑市阴谋时，其遗漏了这一切的本质事实。那就是，密码学家们悄然发明了一套全新的技术原型。” Haseeb Qureshi 在其文章《区块链：一场始料未及的革命（Blockchain: The Revolution We're Not Ready for）》中指出，“区块链将颠覆整个社会，它将使得仅存在于乌托邦和哲学家白日梦中的治理体系得以实现。”文中，他不仅饶有趣

味地将区块链技术与 20 世纪震惊物理学界的弦理论进行了类比，还举出 1995~2001 年互联网泡沫危机以警醒盲目跟风的投机者。

正如我所提及的，如果你也相信区块链是未来的趋势，那么这个行业还是非常早期的阶段，泡沫也许真的存在，大潮退去才知道谁在裸泳。我坚信，当尘埃清理干净以后，那些兢兢业业的真正想要改变世界的区块链创业者，一定会有所建树。

十年以后，可以预见，区块链 + 和今日互联网 + 一样寻常，所有不透明、低效的行业，都会被区块链颠覆；大部分的生活问题都可以被区块链解决，而加密数字货币作为区块链分布式的记账单位与区块链紧密结合，成为一种新型的资产，资产代币化成为一种新的趋势。

朋友们，现在有一个链接未来的机会摆在大家的面前，以往无数次的技术革新告诉我们，要么选择去拥抱颠覆，要么只能被颠覆。

魏久胜

于澳大利亚墨尔本

目 录

前言：要么拥抱颠覆，要么被颠覆

引 一个真正信任 言 时代的到来

信息的发展与区块链的出现 3

信息传播与商业发展 3

互联网实现信息互联 5

信息传播中的“拜占庭”难题 8

信用机制的发展与区块链的诞生 11

信用机制的发展与货币演进 11

账本的发展历程与区块链的出现 15

大到不能倒：中心化的缺陷和弊端 17

区块链技术创造智能信用 20

互联网技术创新	22
区块链是技术创新的产物	22
区块链让“消灭一切中介”真正成为可能	24
从信息互联到价值互联	27

1 从零开始， 认识区块链

区块链：去中心化的创举	33
区块链：从“分布式账本”到“分布式数据库”	33
区块链的优势：更安全、更透明、更民主、更可靠	36
区块链之父：中本聪	38
区块链的发展之路：从 1.0 到 3.0	40
区块链的共识机制	43
去中心化的共识难题	43
比特币的共识机制：工作量证明	45
POW 的缺陷以及其他共识机制	49
区块链的技术基础	51
哈希函数	51
密码学基础	53
数字签名	57
Merkle 树	58
侧链技术	60
区块链的几种类型	62
公有区块链	62

联合（行业）区块链 63

私有区块链 64

2 区块链的广泛应用领域

区块链在金融业的应用 69

区块链打造智能资产，将改变资产管理的方式 69

区块链让跨境支付更经济和有效率 71

区块链大大简化证券清算结算的流程 74

区块链打造更透明的众筹 78

区块链让知识产权保护更容易 81

传统知识产权保护面临的三大挑战 81

区块链可瞬间确权，让维权更容易 84

区块链与知识产权的应用实例 87

区块链让物联网真正链接万物 91

区块链技术可以作为物联网下的基础设施建设 91

区块链确保物联网信息安全，保护用户隐私 94

从万物互联到万物互信，将人工信任变成机器信任 97

通过去中心化，降低物联网的运营费用 100

区块链 + 物联网应用实例 101

区块链在人工智能领域的应用 105

区块链给人工智能提供安全保障 105

区块链解决人工智能的信任问题，且可以降低成本 108

区块链给人工智能领域带来新的机会和可能性 109

区块链 + 人工智能的应用实例	111
区块链与新零售的结合	114
区块链为新零售插上翅膀	114
用区块链追溯产品来源，杜绝假货	116
区块链助力供应链改革，根治供应链腐败	118
区块链 + 零售的应用实例	121
区块链在人力资源领域的应用	126
区块链 + 人力资源拥有无限发展空间	126
区块链 + 人力资源的应用实例	129
区块链在广告及传播领域的应用	132
区块链公司正在试图颠覆全球内容传播乱象	132
区块链让数字广告业更透明	135
应用实例：第一个基于区块链技术的“广告链”	137
区块链在公共事业领域的应用	138
区块链将构建全新的社会信用体系，打造契约社会	138
区块链与人工智能结合，构建智慧城市	140
运用区块链构建更民主、更便捷的投票系统	142
区块链创造无边界的身份验证	144
区块链在政府层面的应用实例	146

区块链与 数字货币

传统货币与数字货币	153
货币发展的历程及数字货币出现的必然性	153

数字货币的优势和发展瓶颈	157
数字货币的发展回顾及现状	161
常见的数字货币简介	163
ICO 的现状：国内全面禁止 ICO	167
数字货币的常见骗局及鉴定方法	172
 比特币	175
比特币的发展历程	175
比特币的历史价格波动情况	180
比特币的硬分叉现象	183
 新兴竞争币代表：超级现金	187
超级现金：打破数字货币之间的隔阂	187
超级现金的七大目标	190
超级现金的开发路线图	201
超级现金项目的风险	203
 数字货币产业链	205
矿机产业的发展及现状	206
层出不穷的各类钱包	208
数字货币的交易方式	209
 政府对加密数字货币的态度	213
国内对数字货币的态度变化情况	213
对比特币及其他数字货币持谨慎及限制态度的国家	215
对比特币及其他数字货币中立及相对友好的国家	217



区块链的技术 发展与未来展望

区块链技术存在的难题 225

资源消耗的问题 225

处理数据速度和规模的问题 226

51% 攻击的问题 227

区块内部的博弈和冲突 231

区块链最新技术成果 232

闪电网络 232

超级账本 234

分片技术 234

区块链与数字资产的未来展望 236

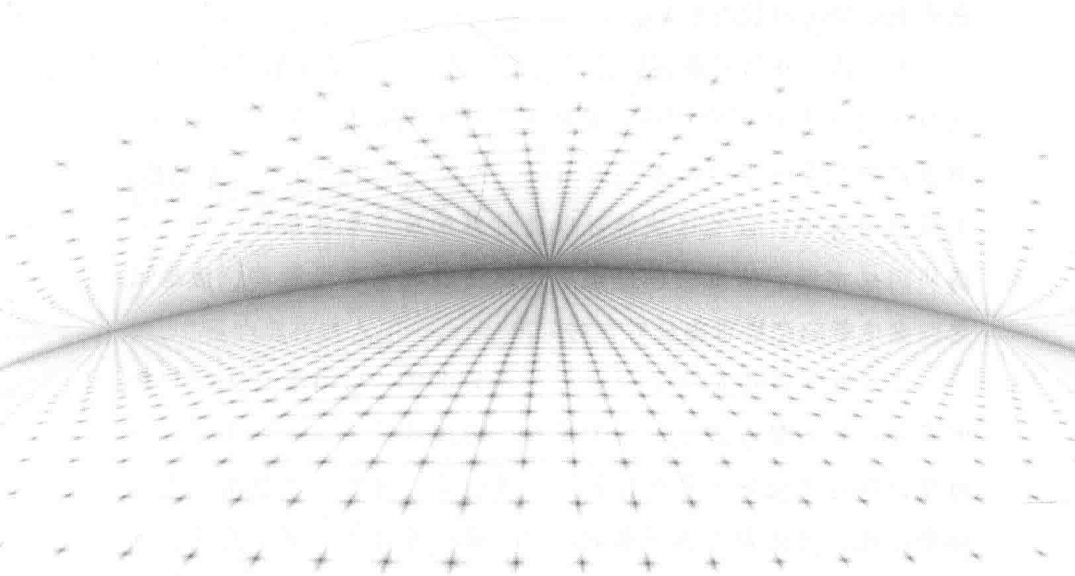
区块链瓦解数据孤岛，让大数据真正名副其实 236

区块链将共享经济转化为共生生态 240

区块链的热门应用方向 242

引 言

一个真正信任时代的到来



人类社会的进步与信息的发展息息相关，在大众传播时代，信息传播是中心化的，信息掌握在少数人手中。而在“点对点”的信息传播中，人类一直无法解决“共识”的问题，互联网实现了信息互联，却无法解决互信的问题——直到区块链出现，这些问题才有了完美的解决方案。

人类的一切活动都离不开“信用”两个字。数学家邓巴认为，人与人之间点对点的信任，其极限也就是150人。因此，当前人类活动中凡是涉及“信用”的问题，都由一个中心（第三方机构）来做信用背书。但是区块链可以通过算法建立智能信任，它公开透明、成本低、速度快、分布广泛，没有权威可以篡改、伪造记录，意味着一个真正信任时代的到来。

技术的发展都是为了创造更美好的生活，人类历史上一切技术革新，无不带来效率的巨大提升，例如从手工制作到蒸汽机的出现，从马车到汽车再到高铁。区块链也是这样一种技术，它的去中心化，必将影响各行各业，极大地提升效率和降低成本，便捷人们的生活。

信息的发展与区块链的出现

文字作为信息的载体，它的出现是人类文明史上的一座伟大的里程碑，它让信息可以被记录、被储存，并在更大的范围更深入地传播。没有信息的传播，就不会造就今天的文明。然而，过去的信息传播都是中心化的。在“点对点”的信息传播中，一直都有两个难解的问题：一是信息传播的一致性问题，二是信息传播中的互信性问题。在区块链出现之前，这两个难题几乎是无解的。

信息传播与商业发展

人们到处在谈论信息，我们越来越多地听到信息这个词。例如，“我们现在进入了一个信息化社会”“我们正在迈向信息高速公路”“这是一个信息爆炸的时代”。

那么，到底什么是信息呢？^①广义地说，信息就是消息。一切存在都有信息。人的五官生来就是为了感受信息的，它们是信息的接收器，五官所感受到的一切，都是信息。信息的积累和传播，是人类文明进步的基础。

人类社会赖以生存、发展的三大基础，就是物质、能量和信

① 1948年，香农发表了信息论，他对信息的定义是：“信息是用来消除不确定性的东西”。

息。世界是由物质组成的，能量是一切物质运动的动力，信息是人类了解自然及人类社会的凭据。没有信息传播，就没有交流，物质和能量就无法顺畅、和谐地流动，人类文明就不会有今天的成果。

信息看不见也摸不着，它不同于拿在手上的工具，不同于吃入嘴中的食物。但是人们却越来越意识到信息的重要性。如果把人类发展的历史看作一条轨迹，按照一定的目的向前延伸，那么就会发现它是沿着信息不断膨胀的方向前进的。信息量小、传播效率低的社会，发展速度缓慢；信息量大、传播效率高的社会，发展速度快。信息的爆炸，使人类社会加速度地向前迈进，达到了不可思议的程度。

可以说，让信息更广泛、更快速、更高效、更准确地传播，是人类社会发展的内在需求。人类对信息传播的技术探索从来都没有停止过。

整个人类的进化史，同时也是人类信息传播的发展史。在人类的整个历史发展中，经历了5次巨大的信息变革。每一次信息变革都对人类社会的发展产生巨大的推动力，带来飞跃式的进步。这5次信息革命依次为：语言的诞生、文字的诞生、印刷术的诞生、大众传播和互联网。

人类最早的信息活动，是在记号和信号时代。在这个时代，人类信息传播与动物并无多大区别，主要靠动作、表情或简单的音节来传递信息，协调狩猎活动。

直到语言出现，语言的产生是人类摆脱动物社会状态的决定性一步。语言最初是将声音与周围事物联系起来的符号，后来逐

渐提高了抽象能力，成为能够表达复杂意义的音声体系。语言的产生不仅提高了人类传播的效率，而且促进了人类思维能力的发达。

文字的发明是人类社会的一个壮举。口语的传播受到物理空间和时间的限制，不利于流传。文字的产生使人类历代的知识和智慧得到积累和传承，扩大了人类的相互交流。

文字产生后，人类经历了手抄传播阶段。手抄传播规模小，成本高，效率低，印刷术的发明大大降低了信息传播的成本，被誉为四大发明之一。

再后来，随着电磁波等技术的发明，人类进入大众传播时代，报纸、广播、电视、电影的出现，将人类的信息传播推向一个新的高度。

互联网的出现，使信息得以爆炸式传播。

人类物质文明的进步与精神文明的进步，都与信息的传播和发展密切相关。信息的交流和出现促成了商业的出现，因为交易的一个基本前提就是沟通和共识。正因为如此，秦始皇被称为“千古第一帝”，因为他统一了文字和度量衡，给不同地区的人进行经济交往和文化交流提供了便利，这是中国能成为一个统一的多民族国家不可缺少的基本条件。

互联网实现信息互联

互联网始于1969年，当时，美军担心自己的军事指挥中心遭受核攻击而陷入瘫痪，于是计划将军事指挥中心一分为四，同