

揭秘前世

比特币长久不衰的理论基础

描绘今生

区块链各行各业的应用现状

探索未来

新思维勾勒数字经济新蓝图

BLOCKCHAIN

区块链

数字经济新势能

苏拓 ◎ 著



中国财经出版传媒集团
中国财政经济出版社

BLOCKCHAIN 区块链

数字经济新势能

苏拓 © 著



中国财经出版传媒集团
中国财政经济出版社

图书在版编目 (CIP) 数据

区块链: 数字经济新势能/苏拓著. —北京: 中国财政经济出版社, 2018. 7
ISBN 978 - 7 - 5095 - 8265 - 7

I. ①区… II. ①苏… III. ①电子商务 - 支付方式 - 研究 IV. ①F713. 36

中国版本图书馆 CIP 数据核字 (2018) 第 108367 号

责任编辑: 王佳欣

责任校对: 黄亚青

封面设计: 陈宇琰

中国财政经济出版社出版

URL: <http://www.cfeph.cn>

E-mail: cfeph@cfeph.cn

(版权所有 翻印必究)

社址: 北京市海淀区阜成路甲 28 号 邮政编码: 100142

营销中心电话: 010 - 88191537 北京财经书店电话: 64033436 84041336

中煤 (北京) 印务有限公司印刷 各地新华书店经销

787 × 1092 毫米 16 开 19.5 印张 363 000 字

2018 年 7 月第 1 版 2018 年 7 月北京第 1 次印刷

定价: 56.00 元

ISBN 978 - 7 - 5095 - 8265 - 7

(图书出现印装问题, 本社负责调换)

本社质量投诉电话: 010 - 88190744

打击盗版举报电话: 010 - 88191661 QQ: 2242791300



苏拓

毕业于北京邮电大学网络与交换国家重点实验室。曾就职于中央结算公司，现服务于交易商协会。承担过多个金融市场基础设施核心系统的架构设计和建设，对互联网、金融科技等数字经济领域有长期的跟踪和研究。

区块链

——数字经济新势能

封面设计：陈宇琰

序

近年来，以 ABCD（人工智能、区块链、云计算、大数据）为代表的金融科技（Fintech）浪潮汹涌。金融科技更加重视精准、高效、智慧的管理，强调“服务渠道”和“运营管理”的内外兼修，因而能有效提高金融业务的运行效率和服务水平，引导金融回归服务实体经济的本源。金融科技已经在不少领域取得突破，发展前景被广泛看好。

区块链的概念最初来自于比特币，一款在 2008 年金融危机的阴影中诞生的加密货币，其设计者中本聪最初只是将区块链定义为点对点交易的基础组件——总账系统。区块链从本质来说是一种分布式账本技术，其最大的魔力在于能够在“弱关系”中构建具备“强连接”特征的信用网络。价值交换双方可以通过区块链直接建立信任关系，这种构建在数学公理上的信任关系是值得信赖的，人们可以基于此实现任何价值交换。因此，区块链被视为价值互联网的基石，是比肩 TCP/IP 协议的一项伟大技术。

国内外诸多概念验证和创新实践证明，区块链（或分布式账本技术）作为“业务协作中间件”，能有效链接金融业务相关参与方，解决传统金融机构业务协作中存在因信用缺失、手工操作等导致的反复确认或对账等问题，显著降低各单位金融业务处理的复杂性，提高金融业务运行的效率；此外，这种方式具有极强业务持续性服务能力，能够支持各参与单位灵活开展系统建设运维，有利于建立跨多个机构的横向数据流动机制，打通数据孤岛，提高数据标准化程度。

银行间市场是我国面向合格机构投资者的重要金融市场，包括债券、同业拆借、票据、外汇、黄金、衍生品等六个子市场。银行间市场建立之初信息系统建设就与业务创新紧密结合，银行间市场 20 年业务的发展历程就是按照“凭证无纸化、发行远程化、交易线上化、支付电子化”的思路建设信息系统的过程。银行间市场已经形成了一套成熟的、相对完整的信息系统，有效地支撑了银行间市场业务的快速、创新发展，在信息安全、灾备恢复、防范系统性灾难等方面均有保障措施。

银行间市场具有多机构、多环节、低频次等特点，是非常适合于区块链技术应用的场景。作为银行间市场的自律组织，交易商协会非常重视和关注包括区块链技术在内的金融

科技的研究应用，2017年组织推动了非金融企业债务融资工具全环链、信用链接票据全环链等概念验证工作，概念验证的情况证明了区块链解决方案的确具有独特的优势。尽管区块链还存在性能瓶颈、安全隐私等问题，但是，区块链技术有潜力作为银行间业务运转的“加速器”，促进业务协作，降低沟通成本和业务风险，提高运行透明度和监管效能。

区块链的应用不限于支付、结算、托管等金融领域，也不限于公证、溯源防伪、知识产权、共享经济、身份认证等领域，实际上区块链有潜力应用于各行各业。然而，必须清楚认识到，区块链技术尚处于高速的迭代发展的过程中，区块链的定义还在不断地完善，还有许多需要进一步解决的问题……

本书作者作为交易商协会区块链工作组的重要参与者，致力于推广区块链的知识，推动区块链的应用。衷心希望有更多专业人才潜心深入研究区块链底层技术，勇于创新，争做金融科技前沿领域的弄潮儿，共同推动区块链技术和商业世界的深度融合，推动我国金融科技的发展繁荣。

包香明

2018年6月

前言

作为一名供职于金融行业十余年的信息技术人员，笔者深刻感受到以人工智能、区块链（Blockchain）、云计算和大数据为代表的金融科技对于金融行业理念的冲击，尤其是区块链的概念非常火热。而编写此书最大的动力则来自于个人对区块链的责任感和使命感。区块链是一个具有划时代意义的技术创新，这是一项具有改变（颠覆）诸多行业运行体制的潜力技术。然而，区块链的概念相对复杂、抽象，难以理解和领会，人们对区块链的认识普遍过于概念化，并且经常出现过于哲学化甚至神化的解读，仿佛革命的磅礴之势已跃然，颠覆之势已无法逆转，这给了心机叵测者可乘之机，这既说明了区块链的商业模式和技术还需要进一步的探索，又说明了区块链从业者还有大量宣传、教育工作要做。

很多人将现阶段的区块链看作世纪之交的互联网，那段时间互联网概念的火爆一点儿不亚于今天的区块链，人们坚信互联网商业模式的想象空间，投资者对新技术充满信心。然而，当时绝大多数商业概念并不具备可实施的计划，普遍缺乏可行的盈利模式，以概念炒作代替商业经营。2000年3月10日，互联网经济泡沫开始破裂，超过5万亿美元的市值蒸发，许多互联网公司损失重大，超过一半的公司或直接退市或通过并购谋求出路，甚至破产而销声匿迹。然而，泡沫的破裂并不等于发展的停滞，互联网技术还在不断地创新，商业模式还在被探索。互联网的冬天确实没有持续太久，经过短暂的休养生息之后，互联网经济开始了新一轮商业模式的探索，很快就在第三产业生活服务领域取得了商业上的成功和技术上的突破，并逐步开始向第一和第二产业渗透，云计算、大数据、人工智能、物联网等互联网新技术又推动了工业互联网和智慧农业等产业互联网的发展，互联网早期坎坷和发展历史值得区块链从业者温故。

如今关于区块链有太多的误解或者偏见，典型如“区块链就是加密货币”“区块链无法满足高吞吐量业务需求”“挖矿是一种资源浪费”“区块链是去中心的，无须监管”“比特币没有价值，但是它背后的区块链很有价值”“区块链还没有可行的盈利模式”。本书努力从一个相对全面的角度对区块链进行分析，帮助读者更好地理解区块链技术。本书第一章主要从发展历程、概念定义、内在特征、技术架构等多个维度对区块链技术进行全面

解读,简要介绍了区块链新经济蓝图和区块链生态图谱;第二章详细剖析了比特币、以太坊、瑞波币、莱特币、暗黑系列币等加密货币的运行机制,简单介绍了法定数字货币的研究情况,本书没有涉及加密货币交易的内容,侧重于从账户、钱包、挖矿、共识等各种运行机制的维度进行阐述,区块链技术源于加密货币,加密货币又促进了区块链技术的发展完善,理解区块链技术加密货币不可不察;第三章讲述了P2P、智能合约、共识机制、加解密算法、签名算法等区块链各种关键技术,力图通过基本技术的解读理清区块链技术的概念框架,把握区块链发展的趋势;第四章详细分析了区块链在金融市场、银行业、保险业务、证券业、互联网金融等金融领域的创新案例,这些案例有来自于区块链初创公司的,也有传统金融机构推动的;第五章介绍并分析了区块链在知识产权、溯源认证、身份、传媒、物联网、电子商务、基础设施等10多个行业的创新实践;第六章从多个维度畅想了未来的数字经济,区块链将在未来的数字经济中扮演重要角色。第七章介绍了我国北京、上海、深圳、杭州等数字经济重镇区块链行业发展情况,分析了中国企业在区块链技术知识产权、技术标准、监管思路、治理实践的探索情况。笔者衷心希望能让读者感受到区块链的潜力,更希望有读者可以受此启发推动区块链技术的落地、发展和创新,数字经济的未来将更加强大,而且未来不会太遥远。

欢迎读者就区块链相关热点问题与本书作者探讨,作者邮箱 E-mail: sutuo. bupt@gmail. com。

(本书为作者个人观点,不代表供职单位意见)

苏 拓

2018年6月

目 录

Chapter 1	揭开区块链的神秘面纱	1
01	区块链的前世今生	3
	从幕后走向台前	3
	从极客圈子走向商业领域	5
	从区块链走向分布式账本	6
	区块链的发展历程	6
02	区块链的科普解读	7
	分布式账本说	7
	分布式网络说	8
	价值互联网说	8
	信用系统说	9
	多重功能说	9
03	互联网：从财富集中走向财富分享	10
	什么是价值	10
	信息互联网：财富集中	11
	价值互联网：财富分享	12
	传统模式与区块链模式下数据交互方案的比较	13
04	多视角解读区块链	14
	区块链强大的内在特征	14
	纵向视角下的区块链	15
	横向视角下的区块链	16
	技术维度视角下的区块链	18
05	区块链勾勒新经济蓝图	21

	助力健康的金融生态	22
	提高公证工作的效率	22
	精准知识产权的确权	22
	构建真正的分享经济	23
	重构分工合作的方式	23
	发挥溯源防伪的效能	23
	建立专属的数字身份	24
	释放物联网的内在潜力	24
	匹配大数据相得益彰	24
	激活分布式计算功能	25
06	区块链生态图谱初具雏形	26
	区块链面临的生态问题	26
	互联网生态完善前史可鉴	27
	区块链生态图谱解读	29
Chapter 2	加密货币浪潮波澜壮阔	33
01	初识虚拟货币	35
	被颠覆的权威定义	35
	虚拟货币的分类	36
02	揭秘加密货币	43
	比特币——加密货币的领跑者	43
	以太坊——全球通用的区块链平台	84
	瑞波——最成功的商业解决方案	98
	“暗黑币”系列——隐匿交易行为的典范	103
	其他加密货币——加密货币发展新态势	106
03	探析法定数字货币	110
	法定数字货币意义重大	110
	各国法定数字货币研究动态	111
	我国法定数字货币构建思路	112
Chapter 3	高速迭代发展的区块链技术	121
01	解密核心技术	123

P2P 技术	123
密码学原理	126
块链式数据结构	140
时间戳	141
共识机制	141
智能合约	148
02 联盟链平台 Hyperledger Fabric	152
Hyperledger 项目概况	152
Fabric 技术框架	154
适用于商业场景的主要原因	156
03 “非链之链”的 R3 Corda	157
R3 联盟	157
Corda 的设计理念	158
主要技术概念	160
04 区块链即服务	162
05 跨链协议	163
公证人机制	163
侧链/中继	164
哈希锁定	166
分布式私钥控制	166
行业联盟	167

Chapter 4	区块链引领金融变革新风尚	169
01	品味金融科技	171
02	重塑金融市场	172
	区块链提升金融市场运行效率的技术分析	172
	DTCC——区块链技术应用的研究先锋	173
	LINQ——运行在区块链上的私人股权市场	174
	澳交所——世界首家采用区块链技术的交易所	174
	区块链黄金平台——欧洲金融市场区块链创新实践	176
	信用卡组织 VISA ——打造支付新通道	176
	NAFMII——重视金融科技创新应用	177

上交所——高性能区块链解决方案的探索者	179
中国银联——构建区块链平台评价框架	179
上海保交所——行业联盟链的领头羊	180
颠覆还是重塑?	181
03 驱动传统银行	183
传统银行面临新挑战	183
品味“区块链+银行”的魅力	184
落地的主要障碍	187
04 重新定义证券	188
重构“区块链+证券”新视角	188
ICO——证券融资方式的创新	190
ABS 业务场景	199
05 契合保险理念	203
“区块链+保险”的六大优势	203
安永关于“区块链+保险”的机遇分析	205
打通“区块链+保险”创新的最后一公里	205
06 深植互联网金融	209
Swarm——基于区块链的分布式众筹平台	210
小蚁——新时代智能经济的支持平台	210
Circle——数字货币在线支付领域的独角兽	212
07 重构征信体系	213
现有解决方案的主要痛点	213
“区块链+征信”的优点	214
主要实践案例	214
08 助力信托行业创新	216

Chapter 5

区块链重构资源配置体系	219
01 “区块链+IP”——守护知识产权,挖掘 IP 价值	221
IP 重要性认知不断加强	221
重构 IP 生产消费全流程	222
主要创新实践	223
02 “区块链+传媒”——畅通传播途径,分享资讯价值	229

新微博——DECENT	229
新知乎——Steemit	230
新简书——YOYOW	232
用区块链打击假新闻——PUBLIQ	232
广告更精准——智媒链	232
新闻调查新模式——Press Coin	232
分布式新闻审核发布平台——DNN	233
重新定义新闻发布流程	234
03 公证场景——提升法律效率，助力良好秩序	234
区块链在公证场景的应用分析	234
主要创新实践	235
04 “区块链 + 共享经济”——充分利用资源，提高社会效能	239
传统共享经济方案的痛点	239
各类创新实践	241
05 “区块链 + 溯源防伪”——记录生产流通，促进质量效率	244
Everledger——为每颗钻石建立数字档案	244
唯链——领先的溯源防伪平台	245
善粮——舌尖上的工程	246
供应链类解决方案	246
公益类解决方案	246
06 “区块链 + 身份”——保护用户隐私，分享平台价值	247
ShoCard——“生物识别 + 区块链”的身份认证	247
OneName——“社交网络账号 + 区块链”的身份认证	248
Bitnation——建立世界公民身份证	248
Tradle——致力于商业领域的客户识别	248
uPort——打造永久身份信息	248
BanQu——降低金融服务门槛	249
SecureKey Technologie——保护用户隐私数据	249
Tierion——个人医疗信息数据管理	249
“身份链”——贵阳惠民利商工程	250
07 “区块链 + 物联网”——从物联网到物链网	250
ADEPT——设备自运转的首次尝试	251
Filament——设备自沟通的工业应用	251

	Tilepay——打造物联网数据交易市场	251
08	“区块链 + 基础设施”——从集中服务到分布计算	252
	新 HTTP 协议——IPFS	252
	蚁群存储方案——MaidSafe	253
	分布式云盘——Storj	254
	云存储——Sia	254
	迅雷玩客云	255
09	“区块链 + 电子商务”——降低商户成本，保护交易隐私	256

Chapter 6	未来无所不能的数字经济	259
01	价值互联网领跑未来	261
02	个人与账号完美碰撞	262
03	万物互联正在蝶化	264
04	计算技术革命未来	264
05	无处不弥漫的数据	266
	数据大爆发才刚刚开始	266
	大数据应用尚需进一步探索	267
	数据互联是深度应用的关键	267
06	“一草一木”皆有智慧	268
07	现实虚拟交相辉映	269
08	数字经济重塑世界	271
	个性在削减	271
	能力在改变	271
	全球化在推进	272
	结构在调整	272

Chapter 7	区块链中国	275
01	主要城市区块链行业分析	277
	北京——全方位领先优势明显	277
	上海——资本加持有望迎来突破	280
	杭州——精耕细作着力垂直领域	280
	深圳——行业巨头推动技术研究	281

贵阳——政府倾力打造创新新区位	282
其他城市区块链初创企业情况	283
02 中美区块链初创企业发展趋势分析	284
融资额度差距明显	284
从业人员构成不同	285
成立浪潮有先有后	286
辐射能力强弱有别	286
03 区块链专利申请情况	287
04 国内主要区块链联盟	288
Chinaledger 联盟	288
金融区块链联盟（金联盟）	289
银行间市场区块链技术研究组	289
中国区块链技术创新与应用联盟	289
05 区块链标准研究情况	289
区块链标准的意义	290
区块链标准建设情况	290
06 区块链治理模式探索	292
公有链治理模式的实践探索	293
联盟链治理模式的实践探索	293
07 区块链监管模式探索情况	294
参考文献	296
致 谢	298

Chapter 1

揭开区块链的神秘面纱

2018年2月26日,《人民日报》经济版整版刊发了《三问区块链》《抓住区块链这个机遇》《做数字经济领跑者》三篇评论文章,在加密货币行情腰斩,币圈哀鸿遍野的背景下,这三篇文章有拨乱反正之效,充分说明了国家对区块链技术的态度,稳住了区块链研究从业者的心,彰显了中国政府高瞻远瞩的眼光和领跑数字经济时代的决心。