信息科学与技术丛书

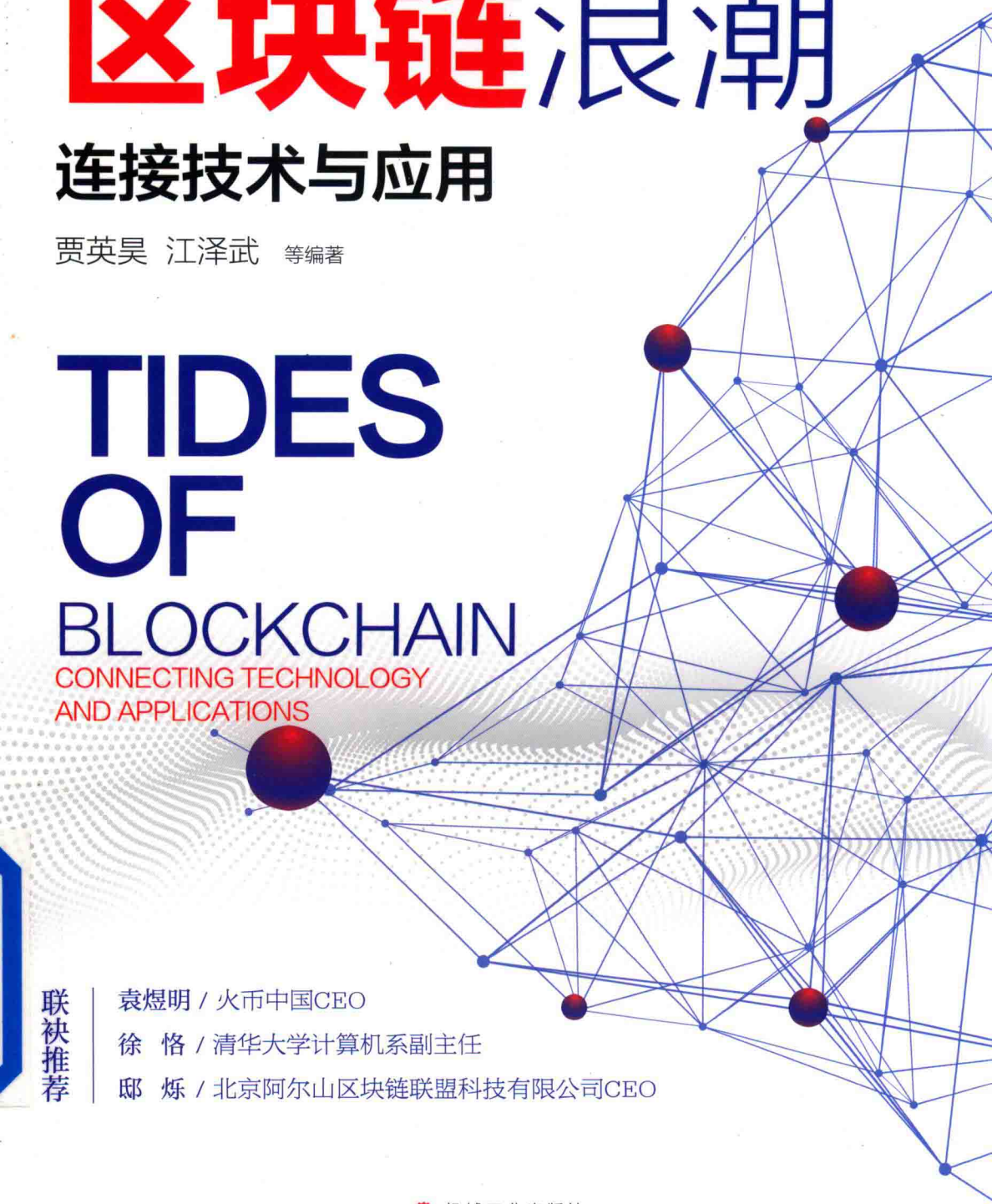
区块链浪潮

连接技术与应用

贾英昊 江泽武 等编著

TIDES OF BLOCKCHAIN

CONNECTING TECHNOLOGY AND APPLICATIONS



联袂推荐

袁煜明 / 火币中国CEO

徐 恪 / 清华大学计算机系副主任

邸 烁 / 北京阿尔山区块链联盟科技有限公司CEO

机械工业出版社
CHINA MACHINE PRESS

信息科学与技术丛书

区块链浪潮：连接技术与应用

贾英昊　江泽武　等编著

机械工业出版社

本书编写的主要目的是向读者揭示“区块链技术可以做哪些事情”“哪些行业适合应用区块链技术”“区块链技术未来将走向何方”。全书分为区块链技术篇、应用场景篇、现状与展望篇三部分。全书首先介绍区块链技术进展，再就各行业的应用进行具体分析。书中内容并未停留在浅显的技术说明上，而是通过讲解技术原理，就技术的难点、未来发展方向等给出独立见解。本书是哈希研究院多位研究者在区块链行业实践、探索、深度思考的总结和提炼。

本书面向的读者主要是已具有区块链技术基础知识，希望进一步了解技术发展脉络的业内人员，以及对区块链感兴趣、希望探索区块链技术在实际项目落脚点的从来者。

图书在版编目（CIP）数据

区块链浪潮：连接技术与应用 / 贾英昊等编著. —北京：机械工业出版社，2019.1

（信息科学与技术丛书）

ISBN 978-7-111-62296-3

Ⅰ. ①区… Ⅱ. ①贾… 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（2019）第 049404 号

机械工业出版社（北京市百万庄大街 22 号　邮政编码 100037）

策划编辑：杨　源　　责任编辑：杨　源

责任校对：张艳霞　　责任印制：张　博

北京铭成印刷有限公司印刷

2019 年 4 月第 1 版 • 第 1 次印刷

169mm×239mm • 13.5 印张 • 236 千字

标准书号：ISBN 978-7-111-62296-3

定价：59.80 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换

电话服务

服务咨询热线：（010）88361066

读者购书热线：（010）68326294

网络服务

机 工 官 网：www.cmpbook.com

机 工 官 博：weibo.com/cmp1952

金　书　网：www.golden-book.com

教育服务网：www.cmpedu.com

序　一

毫无疑问，区块链是一个伟大的发明，它似乎有种魔力，吸引着一大批人孜孜不倦地探索它的奥秘。我拿到这份书稿时，正是全国两会期间，区块链和人工智能一起成为两会热议的话题，发展区块链等战略性新兴产业已经成为各级政府的共识。

这本书由贾英昊、江泽武以及其他几位清华大学学生区块链协会的研究者共同编写而成，汇聚了这批年轻人对于新兴技术的极大热情。作为最早关注区块链技术并率先成立高校区块链协会的清华人，他们坚持做了很多区块链理论与实践的创新尝试，看到他们即将把过去沉淀的关于区块链探索的成果整理出版，惠及广大读者，作为协会的指导老师，我由衷地祝贺他们，并为他们感到骄傲。

经历了 2018 年的非理性热潮之后，在国家的引导和市场的净化作用下，人们对区块链的认识正逐渐回归理性。但如何帮助大家正确认识区块链，还有很多工作要做。很多人仍然对区块链知之甚少，容易盲目受他人观点影响，甚至很多已经在做区块链创新工作的人，面对周遭环境变化，也常常会动摇信心。人们需要一盏指路明灯，帮助人们透过眼前的重重迷雾看清背后的本质。

本书深入浅出地阐述了区块链技术原理和发展路径，涉及了计算机系统、密码学、经济学、博弈论、计算机网络等多门复杂学科，在体现专业性的同时，兼顾了可读性。区块链在不同场景中的应用是大家最为关心的，也是本书中最有意思的部分，书中对区块链在泛金融、供应链、公益、数字身份、版权、医疗、共享经济、游戏、社交、能源等多个领域的应用进行了分析和总结，相信会对读者有所启发。

就像书中提到的一样，当前区块链的发展仍面临着诸多技术上的挑战和应用中的困难。我特别希望能有更多的人才加入探索的队伍中，也祝愿清华大学学生区块链协会未来取得更大的成绩。

清华大学计算机系副主任　徐恪

序　二

区块链是一个新兴又很综合的领域，容易让很多人望而生畏。本书分了区块链技术、应用场景、现状与展望三个部分，从技术到应用，从介绍到探讨，从现状到未来，系统阐述了区块链技术的原理，以及对经济、社会可能带来的改变。本书不仅指出了区块链技术的优势与潜力，也提出了行业目前面临的阻碍与限制，论述系统全面，行文简明清晰，是一本让人对区块链行业有较为全面认知的佳作。

当前飞速发展的数字经济依托的仍是数百年前的股份制、复式记账法等，其无法适应日新月异的产业特征的弊端正在显现出来。区块链本质是互利共赢，实现对生产关系的重要重构，凭借公开透明、不可篡改的技术保障，通过价值传输、通证经济将各方市场参与者的利益统一起来，解决了传统经济模式下市场参与者潜在利益冲突对立的问题，是一种更加灵活有效的市场机制。读完本书，您对此也许会有更多的理解。

区块链带来的生产关系重构正在应用场景落地中显现出价值来。本书梳理的泛金融、供应链、公益慈善、数字身份、版权保护、医疗健康、共享经济、游戏、社交、能源等领域也正在不断有应用项目落地。火币区块链研究院曾根据区块链应用的泛化与深入程度，提出 4 层应用层级模型（分布式账本、价值传输网络、通证激励体系、资产数字化），与书里所提的信息区块链化、价值区块链化、场景区块链化也可大致对应起来。

区块链技术作为一项新兴技术有着旺盛的生命力，而且分层、跨链、分片等各种新技术的探索与应用正层出不穷，以提升区块链系统的性能与易用性。同时也要看到，区块链行业发展是一个全面的系统性工程，包括技术进步、民众认知、监管配套等多个方面，行业发展将是一个循序渐进的过程，正如过去几十年互联网在低认知与不确定中发端到如今全面融入人们的日常生活。在人们仰望星空的同时，应该脚踏实地去认知并推动区块链行业的发展，迎接终将到来的区块链浪潮。

火币中国 CEO　袁煜明

序　三

科技与互联网的结合带来了生产力的极大解放，但同时也引发了许多混乱。区块链开启了一个新时代，它不仅仅是一项新技术，更是一种新的思维方式，它让互联网真正有可能变得可信且有秩序。这是数字科技和信息社会高度发展后所引发的必然结果。有了区块链技术，过去只有通过各种传统方式，以及烦琐的制度、工作流程和人工投入才能够有效解决的身份认定、权属确认、可信交易、信用流转、隐私保护、遵守协议约定等问题，现在通过技术手段就能够平滑地迁移到互联网上，并且做得更好、更高效，从而使互联网变成一个可以承载业务（不仅仅是信息）的场所。

不得不承认，区块链概念的提出者中本聪非常有远见，他深刻理解人类信用体系的本质，也看到了互联网的弱点。他围绕着数字货币场景，创造了一个堪称“完美”的比特币技术体系，运用密码学、分布式计算、博弈论等本就存在的技术，构建了一个去中心化、分布式存储、不可篡改、可追溯的账户和交易系统，并发明了“挖矿”这种既能够产生货币激励，同时又能维持整个生态系统良好运转的高明机制。后来者以太坊更是发明了智能合约，使得更复杂的任务可以用“代码”来保证自动和“正确”执行。

比特币早期成功地吸引了一批技术极客的认同和跟随，进而在几年后，随着资本的大规模介入，数字货币奇迹般崛起，整个世界都开始关注和追捧，特别是技术本身的迭代演进，以及各种新应用场景的开发，开始得到普遍重视。前些年，由于人性的投机和贪婪，打着区块链技术名义的数字货币泡沫爆发而来，又快速消退。初衷本是建立信任的区块链技术，一度被一些人神圣化，人们认为它无所不能，后来滥发币的欺诈本质被揭穿，又被一些人妖魔化，这些人认为它不过是一场骗局或者技术极客的“乌托邦”。

一项革命性的技术，其生命力必然是强大的，泡沫破裂后，人们开始沉思。互联网上的“信任机器”如何建立，已经悄然地有了方法论和实践基础；对技术本身的局限性和面临的挑战也有了清晰的认识，并开始了积极探索。互联网的混乱、传统信任体系的低效、诸多的痛点和巨大的应用前景、政府和商业企业的高度重视，期待务实的区块链技术和有识之士再度创造奇迹。

本书是清华大学的几位杰出学子历经一年时间，结合自身对区块链的理解

和创业经历，精心编写的一部不可多得的好作品。本书深入浅出地介绍了区块链技术的要点、流派和各种主流应用场景，特别难得的是，对一些概念理解和常见误区，都提出了自己独特的见解，并结合实例给予分析和探讨。

相信阅读后，读者能够对区块链到底是一种什么样的技术，它还有哪些问题和挑战，它为什么能够解决信任问题，它是否能被运用于许多真实的场景，以至于如何构建一个基于区块链的应用来解决实际问题，都会有一个比较清晰、全面的认识，进而成为区块链的“知者”。

邸烁
北京阿尔山区块链联盟科技有限公司 CEO
清华大学计算机专业博士
前 Google 技术总监

前　言

第二次世界大战结束后，人们深刻感受到科学研究转化为应用所产生的巨大力量。这种力量不仅改变大众的日常生活，并更进一步改变国家发展路径，以及全球的政治经济格局。随着电子、计算机技术在全球的迅速发展，密码学和通信技术也取得了极大的进步。

1949 年，Shannon 发表了《保密系统的通信理论》，奠定了密码学的数学基础。1976 年，Diffie 和 Hellman 发表了《密码学的新方向》，对密钥协商、数字签名等问题提出了崭新的思路，指明了整个密码学迄今的发展方向。

随后 RSA 算法、Merkle-Tree 数据结构、拜占庭将军问题、椭圆曲线加密算法等研究，标志着现代密码学基础理论和技术的确立，密码学货币的概念应运而生。随着 2008 年中本聪《比特币：点对点的电子现金系统》论文发表，综合各种技术的比特币项目于 2009 年 1 月产生第一个区块，在此后逐渐走入大众视野。其后以太坊、EOS 等项目的飞速成长，不断刺激着区块链生态的蓬勃发展。目前，区块链的应用已涵盖大部分行业，人们已能享受到便捷的快速跨境支付、购买可追根溯源的安全食品等。

从古代的结绳记事、近代的复式记账，再到互联网与线下实业的结合，每一次价值流通方式的改变，都带来人类经济体系的重大变革。区块链技术的进步，带来一种分布式、社群化、通用、实时的记账方式。这个体系允许人们对所有有益于社群的行为进行激励，使创造价值和分享价值的方式变得前所未有的流畅。人们得以想象一个开放、自由、可信任、共享共赢的价值体系，这种组织方式可以完全释放出人们的生产力和创造力，其威力将席卷目前社会上所有存在交易场景的领域。

纵观区块链行业发展的历史，技术始终起着先导和引领的作用，技术发展亦始终与经济、工业的需求紧密结合。我们专注于区块链技术的发展，探寻科技进步的路径和方向；同时对各个行业展开细致分析，指出行业痛点，让科技助力行业进一步发展。我们希望探寻科技浪潮下行业的跳动脉搏。

本书在第一部分“区块链技术篇”，将从对技术的分析开始，围绕区块链的数据结构、共识机制、密码学等内容进行研究，指出技术路径和未来方向。在第二部分“应用场景篇”，将从供应链、泛金融、共享经济等领域，对区块链与

行业的结合进行探索，叙述技术应用的可能性与解决方案。在第三部分“现状与展望篇”，将分享对区块链特定问题的思考，探寻区块链未来发展的机遇。

区块链技术在发展过程中仍存在挑战，如矿机、矿池的出现，使比特币某种程度上与集中化的银行变得类似；一些区块链项目因代码不完善而遭受黑客攻击；业内也曾出现一些不理性的声音。市场会有喧嚣的时候，也会有沉寂的时候，但无论何时，总需要有人坚定、专注地行动，用行动推动进步。

在挑战与机遇并存的未来，我们相信市场终将回归理性，回归本位价值。探求技术的进一步发展，探索行业的前进方向，正是对价值回归的支持和推动。市值的变化，不一定能完整地反映行业的情况；行业的进步，在于实实在在地提供更美好的生活，拓展人类的视野，拓宽知识的边界。

我们关心在市场背后推动行业进步的真实力量，相信那些专注于技术、专注于落地场景的项目，终会以更坚定、更强大的姿态出现在大众面前。经过沉寂、酝酿，相信区块链领域将涌现出更多应用，区块链技术也将迎来广阔的发展天地；而我们所在的此刻，或许正是不远处巨大浪潮的先声！

哈希研究院

目　录

第二部分——应用场景篇