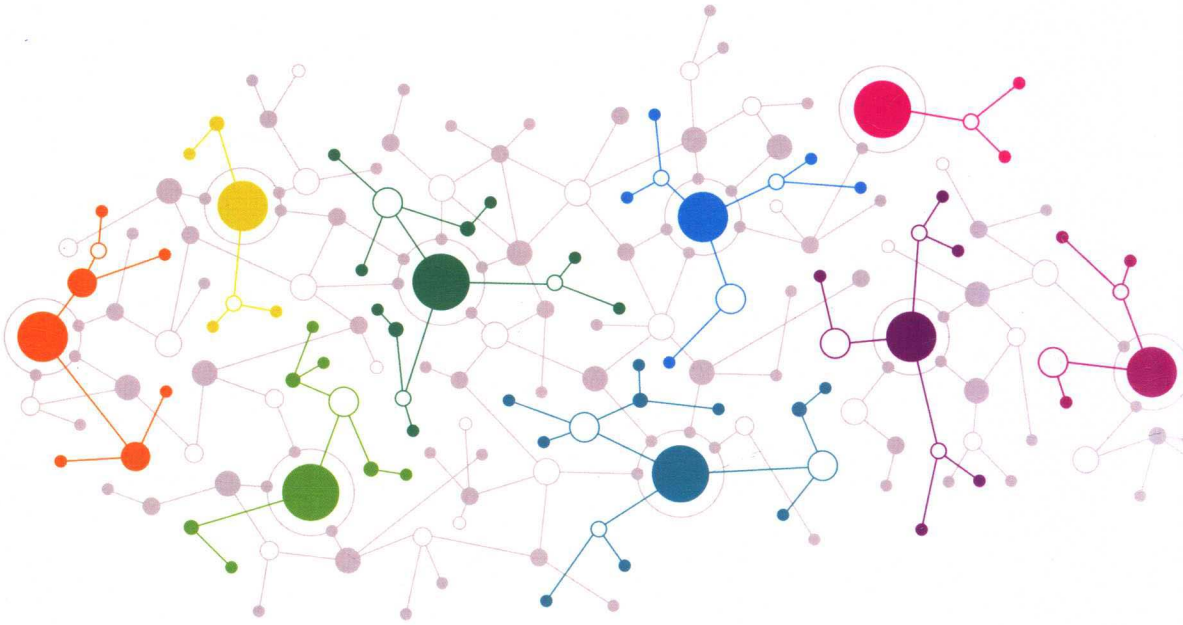
HUAWEI

本书编著团队系华为公司在国内外区块链技术和应用领域的深度实践者。

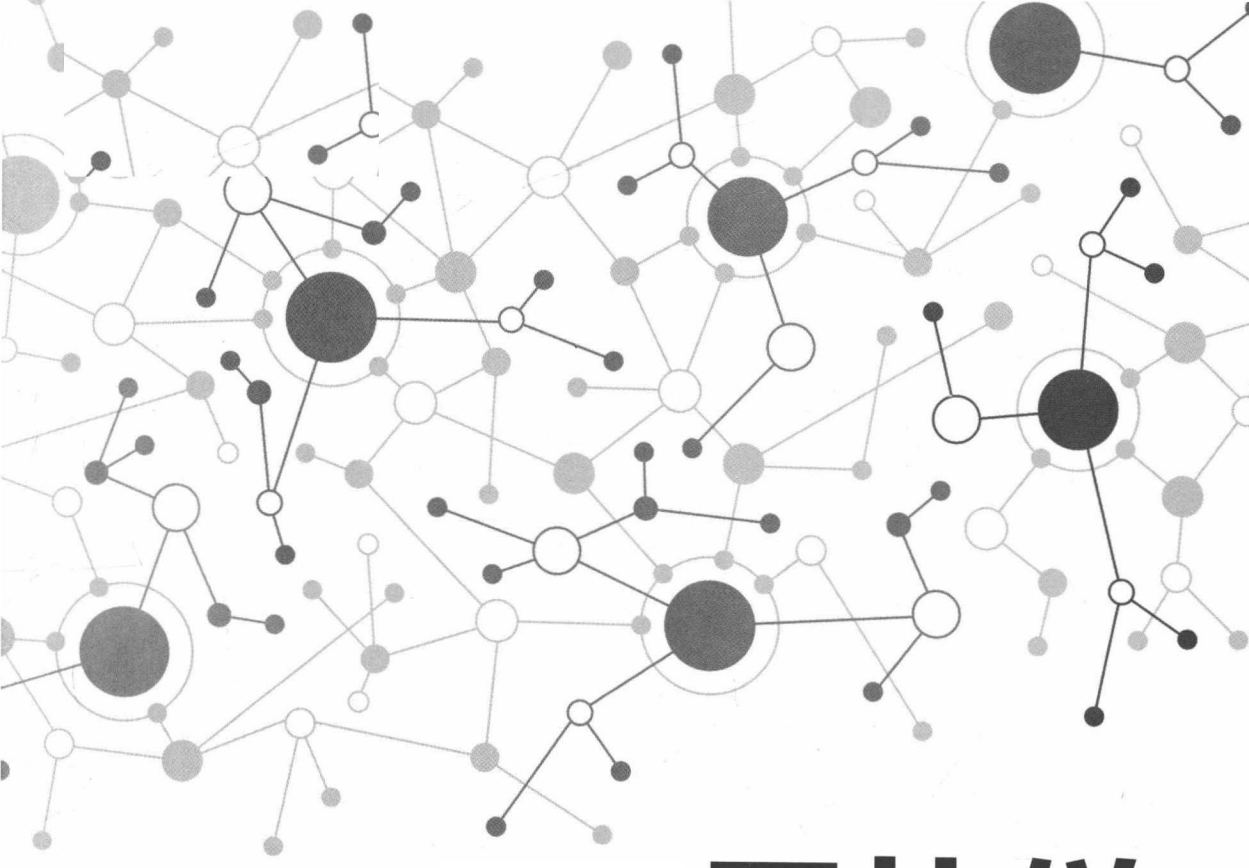


区块链
技术及应用

华为区块链技术开发团队 编著

由浅入深地介绍技术缘起、原理、演进和发展趋势，
分享剖析实际落地案例并示范应用实践过程，探究区块链价值及未来发展趋势。

清华大学出版社



区块链
技术及应用

华为区块链技术开发团队 编著

清华大学出版社
北京

图书在版编目（CIP）数据

区块链技术及应用/华为区块链技术开发团队编著. —北京：清华大学出版社，2019
ISBN 978-7-302-52383-3

Ⅰ. ①区…　Ⅱ. ①华…　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 038779 号

责任编辑：王巧珍
封面设计：傅瑞学
责任校对：王凤芝
责任印制：杨　艳

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　邮　　编：100084
社 总 机：010-62770175　　邮　　购：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质 量 反 馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 装 者：北京嘉实印刷有限公司
经　　销：全国新华书店
开　　本：185mm×240mm　　**印　　张**：15.25　　**字　　数**：329 千字
版　　次：2019 年 3 月第 1 版　　**印　　次**：2019 年 3 月第 1 次印刷
定　　价：68.00 元

产品编号：082814-01

序　一

揭开区块链的神秘面纱

2009年，区块链伴随着比特币系统诞生。经过比特币类加密数字货币的“疯狂”和区块链技术在诸如金融、供应链、政务等行业的应用，人们不断感受到这种新技术的魔力，同时区块链也成为技术创新的热词。区块链是当下最受人关注的方向之一，却又让人充满了雾里看花的感觉。可以说，区块链这个名词虽然已经被大家熟悉，但人们对于区块链到底是什么却又充满了疑惑。究其原因，一方面，区块链是一种新技术，处于发展初期，而且区块链技术、生态、工具和应用正在快速发展和演进，每个人的关注点不同，导致一千个人心中有一千个“哈姆雷特”；另一方面，区块链宣传推广的不同主体，出于商业或理念的差异，从各自的角度宣扬区块链应用和所带来的价值，不同行业的从业者从不同的维度仅看到区块链的“冰山一角”，甚至很多人对区块链的理解仅止步于比特币类加密数字货币。

每个人对区块链可能都有着不同的理解，我们可以从两方面来看待这种情况：一方面，区块链技术从业者正尽力让每个人的理解趋于一致；另一方面，存在不同的理解很正常，也很有益，因为这种多样化的观点碰撞恰恰是创新灵感的源泉。但一个不争的共识就是，区块链正在从理论的探索，逐渐走向落地，并快速发展壮大。区块链作为一种新技术，具备透明可信、防篡改、可追溯、去中心化/多中心等各种应用都十分需要的特性，应用已由金融领域延伸到供应链管理、政务服务、能源、版权存证、物联网等多个领域，满足了相互不信任的多个参与者建立分布式信任的需求，实现了低成本、高效的多方协同。随着区块链从金融领域向其他各领域的渗透，区块链技术逐步步入“区块链+”的时代，可以预见“区块链+”将像“互联网+”一样为各行业注入新的活力。未来，随着各种应用对“可信”要求的增强，区块链的这些特性逐步成为各应用系统的“标配”，区块链技术也将逐步渗透到诸如操作系统、数据库、云平台等基础软件中。

区块链技术正在快速发展，在过去10年间已经历了以加密数字货币为标志的“区块链1.0”和以智能合约为标志的“区块链2.0”，目前进入了建立跨组织互信的“区块链3.0”应用阶段，

与各种技术的结合正在加速，在各传统行业的产业价值也逐渐凸显。比如，区块链与云计算结合提供区块链云服务，极大降低了区块链的部署成本和技术门槛，让政府、企业等用户能够快速上手区块链，并通过实际落地应用感受区块链带来的价值。

近年来各国政府机构、国际货币基金组织以及标准、开源组织和产业联盟等纷纷投入区块链产业技术推动、标准拉通和应用落地推进的大潮中。随着区块链的产业价值逐渐明晰确定，区块链迅速引发了一场全球参与竞逐的“军备”大赛。同时从技术发展来看，区块链与人工智能、量子信息、移动通信、物联网等技术正在成为新一代信息技术的基石，其构建的可信机制，将有可能改变当前社会的商业模式，从而引发新一轮的技术创新和产业变革。

那么，区块链到底是什么？有什么价值？它对我们有什么影响以及如何使用这种新技术？它的未来将走向何方？这些都是值得我们思考的问题。在此之际，很欣喜能看到这样一本系统讲解区块链技术、应用场景和未来发展前景的图书出版。作者来自华为区块链技术开发团队，有丰富的技术创新和应用推广经验。本书从区块链诞生与发展的角度开篇，然后介绍了区块链的核心技术，接下来通过实际案例阐述了区块链如何与各行业相结合解决痛点问题，最后进一步展望了区块链的未来发展趋势。希望广大读者通过阅读此书，能够很好地了解区块链的本质，理解其更深层次的内在逻辑，感受区块链技术在经济与社会等各个领域的显著作用和重要影响。

区块链作为一项新技术，虽然在应用方面暂时面临一些尚待解决的问题与挑战，但这也是新技术发展过程中的正常情况。恰恰是因为这些问题与挑战的存在，才促进了技术的不断发展与成熟。另外，区块链的落地，不只是技术问题，还涉及法律、经济等多方面的因素，需要各界仁人志士共同推动，给予区块链技术更多的包容与关爱，让区块链这项新技术有更多成长的沃土与空间，使它能够孕育出更美丽的花朵。对于区块链的未来，我们充满期待。

“长风破浪会有时，直挂云帆济沧海”，相信区块链在未来能够更好地将“可信”数字世界带入每个人、每个家庭、每个组织，构建万物互联的“可信”智能世界。

华为云 BU CTO

张宇昕

序　二

用发展的眼光看待区块链技术

互联网技术的出现极大加快了信息传递的速度，降低了人类社会的信息传递成本，也深刻地改变了人们的生产方式、生活方式，并已经渗透到方方面面。当前互联网只是信息传递者，即为信息互联网，它并不关心人与人之间的协作模式和信任构建方法。而区块链在信息互联网的基础上构建了一种新的可信的大规模协作方式，以解决数字经济发展的信任问题，被誉为下一代互联网的重要特征，因此区块链被寄予众多期望。李克强总理在写给2017中国国际大数据产业博览会的贺信中表示："当前新一轮科技革命和产业变革席卷全球，大数据、云计算、物联网、人工智能、区块链等新技术不断涌现，数字经济正深刻地改变着人类的生产和生活方式，作为经济增长新动能的作用日益凸显。"

2008年底，一个化名中本聪的神秘人士（也可能是一个组织）在网络上发表了后来被称为"比特币白皮书"的论文，两个月后发布并开源了比特币系统，区块链的序幕就此拉开。近十年间涌现出数千种加密数字货币，也催生出不计其数的ICO案例。当然，最值得人们关注的还是区块链技术的发展演进。它脱胎于比特币，但却以一种独立的姿态茁壮成长。区块链作为哈希算法、数字签名、点对点传输、共识机制等多种已有技术的集成组合创新，具有抗抵赖、防篡改、可追溯、安全可信等"神奇"特性，"巧妙"地解决了多方可信协同问题，正在广泛应用于金融、供应链、政务等领域。用数据库做个对比，以数据库为核心的信息系统解决了组织内的信息管理问题，以区块链为核心的信息系统实现了组织间的可信数据管理、共享及高效协作，是对当前信息系统的有效补充。

区块链技术经常被冠以"颠覆性"技术的名号，这种名号为区块链技术的发展带来了备受关注的光环，促进了区块链技术的发展，也同时带来了一定的压力、误解甚至质疑。当前区块链技术正处于初级且快速发展阶段，回首云计算的发展历程，2010年云计算的概念和当前被大家广为接受的云计算概念已经极大不同。我们不可能直接跳到最终理想的终点，发展过程中应用驱动的中间态技术积累演进必不可少，需要业界仁人志士的共同努力，积极踏实地投

入区块链基础技术研究及服务实体经济的应用推进中。另外，区块链应用的推进较普通应用难度大，尤其是因为区块链应用涉及多个参与方，原本单个组织要构建一个信息系统就要经过内部激烈的讨论，多个参与方共同讨论构建一个新的协作机制和系统的难度可想而知。虽然推进难度不小，但是我们已经看到了很多成功的价值案例。越是颠覆性的东西推广起来阻力越大，而一旦迸发将势不可当。我们要用发展的眼光看待区块链技术，坚信基于区块链技术所构建的新的协作方式能够助力实体经济往更深层次发展。

我很高兴看到本书是基于华为公司在区块链技术应用实践方面的经验，从用户的视角，用通俗的语言介绍了区块链技术的基本原理、服务实体经济的应用场景，并以华为公有云区块链服务 BCS 为例做了翔实介绍，其中部分场景已经获得商用并取得良好收益。希望读者能够通过本书客观地理解区块链技术的价值，深入了解区块链技术本质以及区块链如何巧妙地与应用场景相结合。

用发展的眼光看待区块链技术及应用，未来已来，将至已至。

用战略的眼光看待区块链技术及应用，以变革的姿态迎接未来，决胜未来。

华为 Fellow[①]

胡子昂

① Fellow：代表华为公司专业技术人员重大成就的最高称号。

前　言

以比特币为代表的加密数字货币是区块链的应用之一。区块链不等于比特币，区块链作为一种革新的技术，已经被应用于许多领域，包括金融、政务服务、供应链、版权和专利、能源、物联网等。未来，与区块链技术接触的群体将会越来越多，对区块链技术进行更加深入的了解与探究将是很多领域的创新创业中不可或缺的一环。

区块链技术现已孕育出了大量的创业公司，而同时许多大公司也展开了对区块链技术的探究与布局。华为公司作为高新科技的领军者之一，对区块链技术已经投入了大量的研究，拥有了丰富的实践经验。我们创作本书的目的，一方面，当前提到区块链，有人会将其与比特币或各类加密数字货币画等号，我们希望借助本书消除读者的这种误解，使读者能够明白比特币或各类加密数字货币只是区块链的一种应用；另一方面，我们希望将长期以来在区块链技术的知识积累，以及对区块链在各领域应用的实践和思考，分享给广大的读者。我们希望不了解区块链的读者能够通过本书对区块链有一个系统而详尽的认识，而对区块链有所了解的读者能够通过本书获得新的启发与感悟。

关于本书

本书的目标读者是所有想充分了解区块链技术和应用的人。本书既包含区块链的基础知识，又有对区块链的应用场景以及发展趋势的探究，可以帮助非专业开发人员对区块链做系统了解。同时，本书也有对一些技术细节和算法的讨论，并以华为云区块链服务为示范平台介绍了区块链应用实践的过程，期望帮助区块链开发人员更加快速、深入地投入区块链的开发工作当中。

华为区块链技术开发团队是由教授、博士、留学归国人员、华为海外研究所科研人员和技术骨干等组成的一支高水平技术研究团队，在区块链相关的领域，如分布式系统、算法、密码

学、网络、数据管理等，都有丰富经验，平均从事相关业务经验超过 6 年；成功推动了多个政务、金融、供应链、存证等应用落地，担任可信区块链推进计划 BaaS 组组长，积极参加中国计算机学会 CCF 区块链专业委员会、ITU-T 等行业、学术和标准组织。本书是由曹朝博士主持的华为区块链技术开发团队合作完成的，作者包括（排名不分先后）：曹朝、蔡春瑜、陈黎君、丁健、郭凯、韩士泽、黄东润、金钊、雷宇宁、李保松、李继忠、厉丹阳、刘奇、刘勋、刘元章、刘再耀、罗玉龙、马新建、潘义峰、檀景辉、姚序明、王磊、张秦涛、张小军、张煜、张子怡、周萌萌。

本书的内容

本书系统详实地讲解了区块链技术的各个方面，主体内容包括三大部分：区块链演进及技术介绍、区块链的应用、区块链未来的价值和发展趋势探究。

本书对区块链基础知识的介绍从区块链的鼻祖——比特币开始，然后介绍区块链的技术基础，比如共识算法和智能合约，并由此说明它的特性，比如透明性和不可篡改性。本书还通过介绍区块链的发展历程以及区块链的不同类型，使读者对区块链整体有基本了解。

介绍完基础知识以后，本书对区块链的价值和应用场景做了进一步的讨论，主要分析了金融、供应链、政务服务、存证与版权、能源五大行业的业务场景、现状及痛点、区块链解决方案和价值。最后总结了判断某个领域能否应用区块链技术的五个准则，这部分内容对于创业创新和投资决策都有一定的借鉴意义。书中还以华为云区块链服务为例，展示了如何使用区块链服务快速开发区块链应用，为感兴趣的开发人员提供参考。

本书还收集了业界对于区块链的不同观点，以及关于区块链的一些常见问题，并对几个常见的区块链平台做了简单的介绍，同时对区块链未来可能的应用领域、产生的价值及发展趋势进行了展望。

本书虽然系统地从各个方面阐述了区块链的各种知识，但各个章节之间相对独立，便于读者查阅参考。对某些章节已经比较了解的读者，可以直接跳到感兴趣的章节进行阅读。我们相信本书能够使读者以一种最有效率的方式充分地了解区块链。

勘误和支持

由于编写时间仓促，编写人员水平有限，书中内容出现疏漏在所难免。如果读者发现任何问题和不足，还请不吝指正。如果对本书内容有任何的疑问，也欢迎通过出版社联系我们。我们将十分感谢读者的反馈，并会及时对本书内容作出勘误和修改。

致谢

本书是由华为区块链技术开发团队完成的，大家在繁忙的开发工作中抽出时间编写书

稿，感谢大家的辛苦付出，同时感谢徐直军、李英涛、郑叶来、龚体、胡子昂、廖振钦、杜娟、黄津、金雪锋、杨开封、樊薇萱、万汉阳、陈威、饶争光、俞岳、郑文钦和宋承朝，以及华为公司其他主管对我们写作的大力支持。感谢邢紫月与出版社的大量沟通，促成了本书的快速出版。还要感谢雷宇宁和韩士泽承担了全书的审阅工作，给出大量有价值的建议。最后，感谢我们每一位家人的支持陪伴，我们的工作因为有了家人的支持和期待才变得更有意义。

华为区块链技术开发团队

2018 年 12 月

目　录

第二部分 区块链应用

第一部分
区块链技术

区块链技术来源于比特币，也因为比特币的疯狂而备受瞩目。区块链技术发展到现在，无论是在技术上的深度与广度，还是在应用场景上的宽度，均取得了较大突破。虽然比特币类加密数字货币在区块链领域依然备受关注，但是百花齐放的区块链应用，尤其是大量企业级区块链应用的出现正在催熟区块链技术，区块链技术正处于快速发展演化期，未来会拥有一个更大的可以施展拳脚的舞台。

第1章
疯狂的比特币及其原理机制

1.1 比特币的诞生

2008年11月,一位化名为中本聪(Satoshi Nakamoto)的人,在密码学论坛 metzdowd.com 发表的一篇名为 *Bitcoin: A Peer-to-Peer Electronic Cash System*(《比特币:一种点对点的电子现金系统》)的论文中首先提出了比特币。2009年1月3日,中本聪发布了比特币系统并挖掘出第一个区块,被称为"创世区块",最初的50个比特币宣告问世。同时有趣的是,中本聪在创世区块中带上了一句话以证明这个区块挖出于2009年1月3日,这句话就是图1.1中的《泰晤士报》2009年1月3日的头版新闻标题——*Chancellor on brink of second bailout for banks*(《财政大臣正处于第二次救助银行之际》)。图1.2是创世区块的原始二进制数据及其ASCII码文本表示,可以看到其中所携带的标题信息,在图中已用方框圈出。

截至2018年,比特币系统已经运行了整整十年。比特币系统软件全部开源,系统本身分布在全球各地,无中央管理服务器,无任何负责的主体,无外部信用背书。在比特币运行期间,有大量黑客无数次尝试攻克比特币系统,然而神奇的是,这样一个"三无"系统,近十年来一直都在稳定运行,没有发生过重大事故。这一点无疑展示了比特币系统背后技术的完备性和可靠性。近年来,随着比特币的风靡全球,越来越多的人对其背后的区块链技术进行探索和发展,希望将这样一个去中心化的稳定系统应用到各类企业应用之中。在本书第二部分,我们将选取代表性行业为例,讲述比特币背后区块链技术的各类相关应用。