HZ BOOKS
华章IT

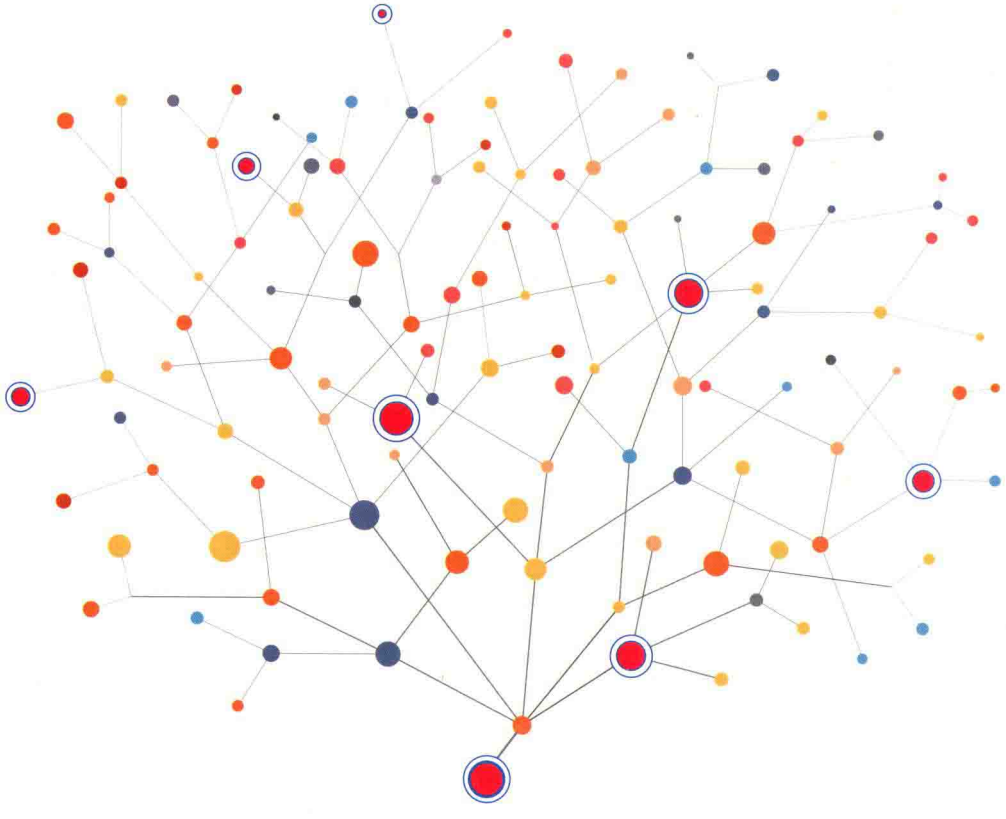
知名专家联袂推荐，实力专家联合撰写，全面性、透彻性毋庸置疑

深度讲解区块链核心技术、平台与应用开发，涵盖架构、共识、加密、P2P、比特币、以太坊、Hyperledger、EOS、潜力框架、问题与测评等

区块链技术丛书

区块链
核心技术与应用

邹均 于斌 庄鹏 邢春晓 ◎等著

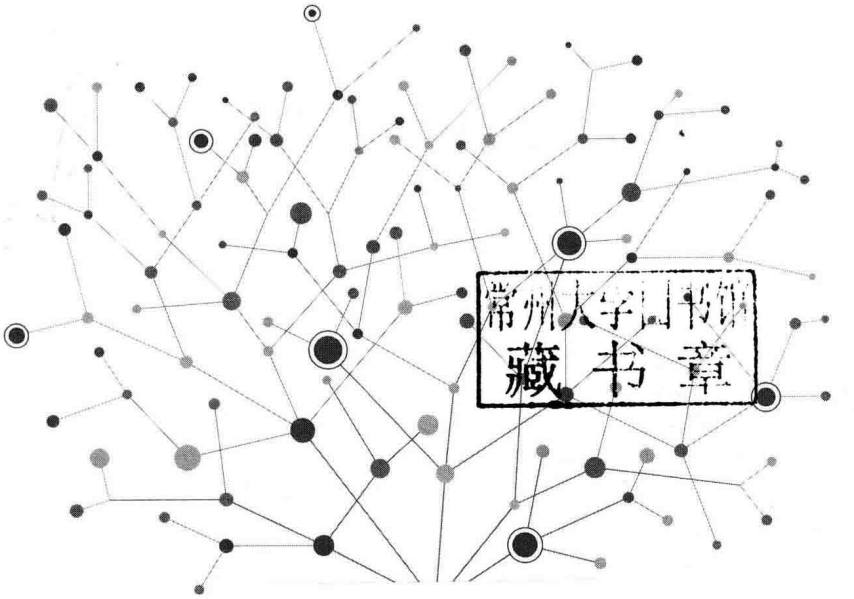


机械工业出版社
China Machine Press

区块链
技术丛书

区块链
核心技术与应用

邹均 于斌 庄鹏 邢春晓 ◎等著



机械工业出版社
China Machine Press

图书在版编目（CIP）数据

区块链核心技术与应用 / 邹均等著 . —北京：机械工业出版社，2018.8
（区块链技术丛书）

ISBN 978-7-111-60614-7

I. 区… II. 邹… III. 电子商务 - 支付方式 - 研究 IV. F713.361.3

中国版本图书馆 CIP 数据核字（2018）第 172264 号

区块链核心技术与应用

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：高婧雅 责任校对：李秋荣
印 刷：北京诚信伟业印刷有限公司 版 次：2018 年 8 月第 1 版第 1 次印刷
开 本：186mm × 240mm 1/16 印 张：24.25
书 号：ISBN 978-7-111-60614-7 定 价：99.00 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）88379426 88361066 投稿热线：（010）88379604
购书热线：（010）68326294 88379649 68995259 读者信箱：hzit@hzbook.com

作者简介

邹均 广电运通区块链科技有限公司 CEO、中关村区块链联盟副秘书长。主编技术畅销书《区块链技术指南》，在领先的国际会议和期刊上发表论文 20 余篇，其中区块链论文获 IEEE ICWS 最佳论文奖，共识算法论文由国际期刊《Transaction on Service Computing》收录并刊登。曾荣获澳中校友会“杰出校友奖”、麦考瑞大学“校长奖”。

于斌 北邮在线教育投资集团总裁、中国电子学会区块链专委会委员、中关村区块链产业联盟专家，是上海财经大学，亚洲财经商学院特聘教授。北京邮电大学通信与信息系统专业博士，主编《金融科技概论》等专著 4 本，曾获得国家科技进步二等奖，教育部一等奖。网络教育、金融科技、区块链等领域专家。

庄鹏 IBM 全球服务金融服务部高级顾问经理、资深架构师。14 年金融行业架构设计与战略咨询规划经验。拥有服务转型、大型企业级分布式系统架构设计、大数据分析、金融支付方面的丰富实施经验。最近三年专注于区块链和分布式账本架构研究，区块链相关应用和数字货币咨询研究，多次作为区块链峰会的讲师、培训专家。

邢春晓 清华大学信息技术研究院和互联网产业研究院副院长，主要研究领域：计算机软件与理论、数据库和数据仓库、大数据管理和分析、知识工程和软件工程、区块链与数字经济、智慧城市（政务、商务、文化和医疗健康）等领域。发表学术论文 350 余篇，其中 SCI 40 余篇、EI 150 余篇，发明专利 40 项。

内容简介

知名专家联袂推荐，实力专家联合撰写，全面性、透彻性毋庸置疑。深度讲解区块链核心技术、平台与应用开发，涵盖架构、共识、加密、P2P、比特币、以太坊、Hyperledger、EOS、潜力框架、问题与测评等。本书分为三篇，内容解读如下。

基础篇（第 1 ~ 6 章），着重讲解区块链技术思想、通用架构和核心技术。该部分写作时注意通俗易懂且兼顾全局，是学习基石与蓝图，涵盖区块链思想与价值、通用架构模型、基础概念与核心技术（加密、共识、P2P 网络等）。

实战篇（第 7 ~ 9 章），讲解主流区块链开发平台（比特币、以太坊、Hyperledger Fabric）的核心机制、技术细节，并给出电子现金系统、智能合约开发、完整 Fabric 网络构建与应用三个案例。

进阶篇（第 10 ~ 12 章），为进一步提升读者开发能力、眼界与研究方向，涵盖三个方面：

① 可能的发展方向，以及一些富有潜力、特色的区块链平台（EOS、Cardano、IOTA 等）；

② 区块链开发需要考虑的各种问题，包括技术局限、各种安全问题与漏洞、应对措施；

③ 区块链测评，从 6 个层面和 8 大类质量指标来设计区块链项目测评点和测试用例。

写 作 投 稿：165075460@qq.com

封面设计 · 陈潇然

About the Authors 作者简介

邹均，广电运通区块链科技有限公司 CEO、中关村区块链联盟副秘书长。主编技术畅销书《区块链技术指南》，在领先的国际会议和期刊上发表论文 20 余篇，其中区块链论文获 IEEE ICWS 最佳论文奖，共识算法论文由国际顶级期刊《 Transaction on Service Computing 》收录并刊登。澳大利亚麦考瑞大学计算机博士、商学院 MBA，曾荣获澳中校友会“杰出校友奖”、麦考瑞大学“校长奖”。

于斌，北京邮电大学通信与信息系统专业博士。主编《金融科技概论》等专著四本，曾获得国家科技进步二等奖，教育部一等奖。是网络教育、金融科技、区块链等领域专家，现任北邮在线教育投资集团总裁、中国电子学会区块链专委会委员、中关村区块链产业联盟专家，上海财经大学、亚洲财经商学院特聘教授。

庄鹏，现任 IBM 全球服务金融服务部高级顾问经理，资深架构师。拥有 14 年金融行业业务和应用架构、IT 系统集成、应用系统开发和管理、战略咨询规划经验。特别是在金融行业面向服务架构转型，企业服务总线规划和实施，分布式系统架构，大数据分析，金融支付应用方面具有深厚的技术功底及实施经验。最近三年专注于区块链和分布式账本架构研究，区块链相关应用和数字货币咨询研究，多次担任区块链峰会讲师、培训专家。

邢春晓，清华大学信息技术研究院副院长，清华大学信息技术研究院 Web 与软件技术研究中心主任，清华大学智慧城市大数据研究中心主任，中国计算机学会副主任与专委委员，IEEE 和 ACM 会员。主要研究领域为数据库、区块链、数据和知识工程、海量数字媒体管理等。发表学术论文 300 余篇，其中 SCI 40 余篇、EI 150 余篇，软件著作权 23 项，发明专利 40 项，教育部科技成果 1 项。多次作为主要负责人和技术骨干参与国家重点科技项目。

张海宁（Henry Zhang），VMware 中国研发中心技术总监，加拿大西蒙弗雷泽大学计算机科学硕士，Harbor 开源企业级容器镜像仓库创始人，超级账本 Cello 项目贡献者，Cloud

Foundry 中国社区早期技术布道师之一，“亨利笔记”公众号作者。目前着重关注企业区块链应用、容器和云计算等领域的研究和开发工作。

蒋勇，技术畅销书《白话区块链》作者。专注于分布式系统设计，10 年企业信息化经历。2012 年开始接触比特币及其相关技术，熟悉区块链 1 代技术（比特币）、2 代技术（以太坊、超级账本），并进行过源码级原理研究，目前在进行智能合约安全编译以及多链架构的研发设计。

唐屹，教授，中山大学博士，广州大学数学与信息科学学院信息科学系主任。曾访问美国北卡罗来纳州立大学、香港浸会大学等高校。专注于区块链安全与应用、网络信息安全、分布式计算等领域的研究，为国外知名安全公司开发过椭圆曲线密码软件，获密码科技进步二等奖（省部级）。主持或参与完成多项国家级及省部级项目，在国内外学术期刊和会议上发表学术论文多篇。

邵周，中国计算机学会区块链专委会委员、中关村区块链联盟金融专委会专家、TOGAF 认证企业架构师、信息安全与风险管理专家，是以结果为导向的技术领导者，也是较早一批关注和实践物联网、区块链等技术的布道者和践行者。研究方向有高性能区块链、分布式存储、分布式算力、可衡量注意力、跨链协同、加密资产锚定等，著有数本科技书籍。目前就职于亚洲基础设施投资银行。

郭莹城，IBM 高级软件架构师、咨询师、敏捷开发技术教练、极客、登山爱好者。11 年电信、金融、电子政务软件研发经验，参与了新一代深圳证券交易所交易系统，以及多个外资银行的核心系统研发，对 Lisp 编译器有研究与心得，精通 Java、Scala、Go、Python、Ruby、Lisp 多种编程语言，Hyperledger 与以太坊智能合约研究者，区块链 P2P 算法专家，IBM 区块链研究小组成员。

刘胜，联动优势科技有限公司首席架构师、中国电子学会区块链专委会委员、可信区块链联盟副理事长。承担国家级区块链和数字货币等课题的研究，参与《可信区块链》《支付清算行业可信区块链》等标准编写。20 余年移动支付、数字证书认证、安全支付、区块链等领域一线研发和底层架构经验，带领团队自主研发针对行业联盟链场景的区块链底层框架 UChains（优链）。提交并公开发明专利 50 多项，其中区块链专利 8 项，已授权发明专利 5 项，曾获 2015 年北京市科学技术三等奖。

范金刚，食品区块链、金融区块链和能源区块链行业专家，太一云技术股份有限公司常务副总裁、中国区块链生态联盟副理事长、中国电子学会区块链专委会执行秘书长。曾任中关村区块链产业联盟副秘书长。主持开展过区块链基础平台测评工作，组织并策划了第一届中国区块链技术创新应用大赛等活动。2016 年在《电力信息与通信技术》杂志上发表学术论

文《区块链在能源互联网中的应用》。

张桂刚，清华大学博士后、中国科学院自动化研究所副研究员、研究生导师。主要从事人工智能、大数据及区块链研究。出版专著 1 部，发表 SCI/EI 论文 60 余篇。

陈家豪，广州大学硕士。从 2016 年开始接触区块链，在读期间主导通用加密货币钱包的开发、区块链网络安全分析等。参与 VMware 公司区块链即服务项目 BOV（Blockchain On Vsphere）开发，是 Hyperledger 社区 Cello 项目的代码贡献者之一。擅长虚拟化、区块链安全、密码学应用等技术，熟悉区块链平台比特币、以太坊、超级账本并有相关开发经验。

张权，本书特约策划人，北邮在线区块链教育与研究中心主任、信息化与数字经济研究中心（IDER）联合创始人兼 IDER 学院院长、英国 CCEG 区块链运营主管，中国移动通信联合会国际区块链创新应用联盟秘书长助理。关注区块链相关的教育与研究方向及搭建专业实践平台构建人才培养体系；擅长区块链、人工智能、物联网、制造业等项目的产品营销、市场业务拓展及平台建设与运营工作。

序一　处于“十字路口”的区块链技术及其应用[⊖] *Foreword 1*

区块链和与之相联系的加密数字货币，无疑是21世纪“横空出世”的新事物。过去数年，特别是2017年以来，区块链技术受到全球范围内的科学家、思想家、经济学家、企业家，以及政府、社会和经济组织的关注、参与和应用，全方位地影响了现存的经济结构和经济行为，一方面，迅速形成了全球性的“区块链”运动；另一方面，因为区块链技术的先天缺陷和现实困境而陷入“十字路口”境地。现在，到了以理性态度理解和认识区块链与加密数字货币真实状况，突破区块链创新瓶颈，实现区块链技术体系进化的时候。正是在这样的历史性期待下，邹均及其他几位作者撰写的《区块链核心技术与应用》，从剖析区块链的核心技术入手，对区块链的技术体系进行了理性的梳理，触及区块链的深层结构和科学基础，所以我给予相当的肯定。本书共12章，26万字。作为篇幅有限的序言，主要集中讨论处于“十字路口”的区块链及其技术体系所面临的4个基本问题。

1. 如何理解和认识区块链所存在的“先天缺陷”，以及区块链技术背后的科学层面。一般来说，任何一项新技术都可能存在“基因”和“染色体”问题，区块链也不例外，很可能反映在以下的4个“局限性”。

1.1　囿于数学工具的局限性。通常认为，区块链的核心技术是“密码学”，而区块链的密码学的重点之一则是哈希函数。也就是说，哈希函数是区块链的基石之一。哈希函数的种类很多，大多数哈希函数都是迭代性的，即使用一个哈希函数，用不同的参数进行多次迭代运算。问题是，哈希函数及其紧密联系的“素数”，甚至现代密码学，最终根源于纯粹数学分支之一的“数论”。高斯说过：“数学是科学的皇后，数论是数学的皇后”。因为数论还在发展，哈希函数尚属年轻，区块链还存在诸如算法选择不当，造成较多碰撞，导致性能下降等问题，

⊖ 在本文的撰写过程中，数学专家崔巍、齐洪胜和计算机技术专家邹均、程文彬、张洪为，特别是郑延伟，深入参与了本文的技术讨论，提供了专业意见和建议，在此表示感谢。

加之对哈希函数的有限移植，意味着区块链的底层技术建立在还处于新生阶段的“地质板块”上。至于，Merkle 树因为与哈希函数的内在联系也归结于数学问题，所谓的拜占庭将军问题的本质更是一个数学问题。在这样的意义上，可以试图用数学语言将区块链描述为：以数论为基础，通过哈希函数实现的一种“复合函数”构造。

1.2 囿于“博弈论”的局限性。区块链的本质是一种多方参与，且形成平衡关系的共识系统。这也是区块链，特别是公有链存在价值的关键所在。可以将共识系统理解为一种节点之间的“均衡”，建立在“博弈论”基础上的“纳什均衡”最接近反映区块链共识系统的状态。具体来说，纳什均衡是指这样的一种策略组合：在一个非合作博弈过程中，任一博弈方只有选择某个确定性策略，才能获得最佳收益。如果任一博弈方单独选择变换策略，悖离纳什均衡，都会损害自己的收益。问题是，当年诺伊曼和纳什研究的是有限“节点”下的小规模博弈，早已经不足以面对“由几十亿节点的庞大对象构成的社会、经济等复杂行为”[⊖]。MIT 的一个近期成果是，一位计算机科学博士在其论文中指出：“找到纳什均衡点是几乎不可能的事”[⊜]。区块链和博弈论，包括纳什均衡的现实关系是：一方面，区块链需要博弈论，包括纳什均衡工具的支持；另一方面，区块链节点的算术级数，甚至几何级数发展模式，已经突破了博弈论的框架和体系。总之，因为区块链的节点无限扩大，所以支撑区块链的博弈论和纳什均衡必然捉襟见肘，出路何在，至今并没有找到最终的科学路径。

1.3 囿于计算机语言和代码的局限性。区块链通过计算机语言和代码进行技术实现，没有软件的注入，就没有生命力和运行可行性。但是恰恰不存在完美的软件。

其一，区块链编程语言多元化，难以找到占有绝对优势的区块链编程语言，只能通过不同编程语言的互补性加以改善。在现实中，很可能发生因为任何一种编程语言自身不足，以及不同的编程语言不足的叠加，对现有区块链造成本源性的伤害。

其二，在现阶段，区块链编程语言主要依赖 C++、Java、Go 等几种“高阶语言”，但是，这些语言都需要演进，以求满足区块链技术实现的需求。可以确定的是，现有的“高阶语言”仍有很大的改进空间。逻辑上说，整个计算机语言体系仍会继续发展，新一代计算机语言势必对区块链产生冲击和影响，推动区块链的演进。

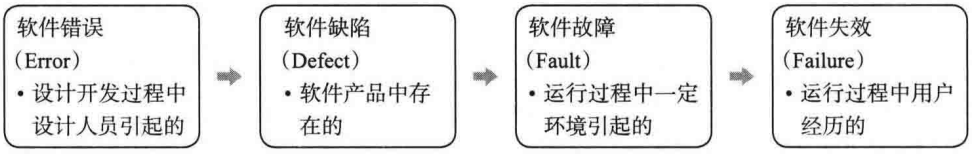
其三，现有的计算机语言正在面临与其他新技术的融合，进而影响区块链的技术体系。例如，人工智能技术和计算机语言的融合，很可能引发计算机语言系统的变革。

其四，编程人员的自觉和非自觉的错误。本书提供了区块链与软件相关的错误、缺陷、

⊖ 见本书 12.5 节。

⊜ 见本书 12.5 节。

故障和失效的关系框架图[⊖]。



1.4 囿于预期时间实验长度的局限性。至今，区块链的实验历史相当短暂，支撑比特币的区块链历史最长，应用也不足十年。但是，依据比特币系统的设计和比特币的算法，推测直到2140年最终产出2100万单位，即使从2018年起计算，仅仅挖完全部的比特币，还需要122年的时间。从理论上说，比特币技术系统的使用寿命没有上限，这个过程中，比特币系统的运行不可中断，甚至不允许进行实质性的修改。所以，本书提出了如何保证比特币系统在未来122年安然无恙地运行问题，是有相当意义的。其实，岂止比特币的区块链技术系统，绝大多数区块链的设计和应用并非是短期内可验证的，现在还没有足够的案例证明，现行支持区块链的软件和硬件系统能够支持长周期的时间目标。

进一步说，到目前为止，支撑区块链的主要底层技术的产生，早于区块链。之后，因为有了区块链理念，这些技术得以重新组合。也就是说，现阶段的区块链技术，及其数学和科学的基础，还是相当脆弱的，难以支持在商业、经济和社会的长期和大规模的应用。在人类现代科学技术发展的过程中，从基于有限科学原理的技术尝试起步，最终形成完整的学科和科学体系，不乏历史案例。例如，莱特兄弟制造飞机之时，所依据的不过是一些初步的科学原理和技术，但是伴随飞机的进化和工业化，最终形成了以飞机整体设计为目标，包括航空学、材料学、电子科学、工程制造学等众多学科的综合科学技术体系。

所以，现阶段区块链的技术很像莱特兄弟飞机的试验阶段。要想全面实现区块链的理念，就像飞行器的历史，最终不仅要实现在全天候和全方位的天空飞行，而且最终要进入宇宙空间，需要的是一个完整的科学和技术体系的支持。可以这样认为，因区块链所组合的技术，还需要一个适应区块链广泛应用的调整时期，或者进一步开发的时期，最终区块链可能演变出一个科学含量极高的综合学科体系。

2. 区块链是否存在现实的和潜在的威胁？区块链面临着为数众多的技术性困境，诸如“可扩展性”技术，“隐私保护”技术，“存储”技术，等等。但是，真正构成对区块链体系现实和潜在威胁的很可能集中在以下几个方面。

2.1 共识层结构性失衡的可能性。在区块链的架构中，或者在区块链的分布式系统中，共识层至关紧要。共识的本质是算法，一个严格共识算法需要满足4个条件：终止性、一致

⊖ 见本书图12-3。

性、合法性、诚实性。[㊀]从技术层面来讲，区块链的共识算法是基于异步通信场景。这样就要涉及 FLP 定理。该定理的研究对象覆盖异步通讯的没有时钟、不能时间同步、不能使用超时、不能探测失败、消息可任意延迟、消息可乱序等一系列特征。在异步通讯场景下，即使只有一个进程失败，也没有任何算法保证非失败进程达到一致性。[㊁]在这样的情况下，通常的共识算法会倾向选择安全性并牺牲活性，难以保证在有限时间内达成共识[㊂]。也就是说，现在的各类区块链的共识算法只有相对意义，并不存在统一的共识算法，唯有根据不同的需求，不同类型的区块链采用相对适宜的共识算法。[㊃]

诚实性	拜占庭容错	终止性 / 确定性	常见共识算法	典型场景	
1	否	否	确定性一致	Paxos、RAFT 等	企业私有链
2	是	是	确定性一致	PBFT、Q/U、Zyzzyva、RBF 等	行业联盟链
3	一定程度	是	大概率一致	PoW、PoS、DPoS 等	公有区块链

这样，就引申出两个问题：其一，已有的共识算法如何应对当下区块链数量爆炸，类型组合多样化，以及区块链类型之间差异增加的情形；其二，区块链是特定的多维动态系统，即多中心或无中心、更加分布式的网络。这个网络跨越多个子网、多个数据中心、多个机构、多个运营商，甚至多个国家，如果区块链联盟进入实质化，怎样协调不同共识算法，实现共识的共识？

不久前，一位以 maxdeath 作为笔名的作者提出：区块链的第三代技术突破，一个是零知识验证技术，另一个可能的突破点是真正无限扩展的共识算法。[㊄]这个看法，颇值得注意。

还有，区块链的功能依赖于去中心化账本，而去中心化账本取决于不同节点上的账本数据的一致性和正确性，最终取决于分布式系统中实现状态共识的算法。因为区块链的算法对一致性的制约，不可避免地影响了去中心化账本的深层基础及区块链的功能。

2.2 算力的垄断倾向和趋势。区块链的运行机制可以理解成不断将“单一或多个输入值”转换为“单一或多个结果”的过程，因此区块链是一种“计算”[㊅]，一般来说，区块链天然需要算力的支持。特别是，以比特币为代表的区块链技术，使用 PoW[㊆]来确定记账权。这一机制要求节点进行大量的复杂函数计算，使得记账节点完成共识的同时，增加对区块链的攻击成本，提高了安全性。引入这一机制对区块链技术的发展产生了深远的影响：唯有通过

㊀ 见书内文 12.6 节。

㊁ 见参考资料《FLP Impossibility》，https://blog.csdn.net/chen77716/article/details/27963079。

㊂ 见书内文 5 .1.2 节。

㊃ 见书内文表 12-4。

㊄ 见参考资料 https://www.zhihu.com/question/265273597/answer/294404050。

㊅ 见参考资料 https://zh.wikipedia.org/wiki/%E8%AE%A1%E7%AE%97。

㊆ 见书内文“5. 共识算法”。

算力不断挖出区块来实现记账。如果区块链没有算力，就无法产生新的区块，就会出现交易没有人去记账的情况。这就意味着区块链的“死亡”。算力的作用也开始被狭义化为“挖矿”，其衡量标准等同于“哈希率”，即计算哈希函数输出的速度。“矿工”开始成为比特币等区块链中的重要群体，在比特币的管理范畴中不断要求更高的权利。问题在于，有可能发生区块链天然 算力遭到垄断的情况。以比特币为例，过去的十年间，其算力经历了从 CPU 到 GPU 的个体时代，短暂的 FPGA 阶段，最终进入了通过 ASIC 矿机支持的矿池垄断时代，其标志是比特币全网算力以 PBhash/s 为单位（1PB=1024T，1TB=1024GB，1GB=1024MB，1MB=1024KB）。截至本序写作时，比特币预计全网算力已经将要达到 37 000P[⊖]。

比特币全网基本信息 (自动刷新:30秒)

货币名称	比特币/Bitcoin/BTC	预计全网算力	36,397 PH/s	已开采BTC	17,070,013	未开采BTC	3,929,988
总市值	$133,789,636,971	Block总数	525,601	24h开采	171 块 2,100 BTC	平均1h开采	7.1 块 88 BTC
当前难度	4,306,949,573,981	预计下次难度	4,843,776,149,929 (+12.5%)	难度调整	574 块以后	预计需时	3天8小时

期间，基于去中心化的分布式记账的比特币，原本与之配合的分散和自由竞争的算力，迅速遭到包括芯片技术升级、能源、人力、资本大量投入的组合型冲击，造成以算力日益垄断为特征的异化。从技术角度说，在区块的挖出速度不能改变前提下，算法就会根据算力增大而提高和控制区块挖出的难度，当全网算力足够大的时候，挖矿的难度也就足够大，任何个人不太可能独自挖出完整的区块，只有加入矿池，才可能以矿池的算力挖出完整区块，个人按照其贡献算力的比例去分成。不仅如此，在矿池环境下，因为全网挖矿难度的调整不是实时的，如果发生矿池突然中止挖矿，会导致剩余矿工无法在当下的挖矿难度下准时产生区块，最终造成区块链“死亡”式的“同归于尽”。所以，建立在强大“算力”基础上的矿池实质上绑架了区块链。先是比特币，进而以太坊也面临相同的境地。

如果说中本聪是智者，却没有想到基于资本和工业能力所支持的算力垄断，早已经不仅仅是一个简单的能源、人力、资本的竞争和消耗问题，也不仅仅是个人通过挖矿获得比特币财富的权利遭到剥夺的问题，而是一旦处于垄断状态的算力失去控制的机制，很可能构成对区块链和加密数字货币生态的毁灭性破坏的问题。现在很可能只有两种可能性：①为了维持算力垄断，成本不断增大，当成本高于收益的时候，就会停止；②为了维持算力垄断“竭泽而渔”，最终同归于尽。前者可以理解为“软着陆”，后者可以理解为“硬着陆”，现在显现的主要可能性是后者。不论是“软着陆”还是“硬着陆”，都需要警惕，更需要通过技术底层创新加以防范。

需要说明的是，目前基于 PoW 所衍生出来的种种弊端，人们已经尝试了若干不同的替代

⊖ 参考图片资料来自 http://mining.btcfans.com/。

方案，例如 PoS、DPoS[⊖]等。特别是，Vitalik Buterin 针对“联合化的矿工团体出于自利目的将算力集体转移以攻击旧区块链（spawn-camp）”的可能性，提出可以加强从客户端出发的验证机制，利用均匀分布的个体用户的“协调性问题”，增加上述攻击成功的难度[⊖]。但是，以上种种方案并不意味着 PoW 的思想已经过时，也不意味着“算力”应当被摒弃。其如何演变，以及 PoW 究竟会如何发展，“算力”是否能够在区块链中发挥更重要的作用，还需要时间的验证。

2.3 传统经济模式和工具的侵蚀。面对区块链及其所支持的加密数字货币的横空出世和蓬勃发展，有一种广泛传播的乐观看法：区块链和加密数字货币诞生、传播与应用，具有强大的生命力，代表了打破传统经济生态平衡，改变传统金融和产业秩序的“新物种”。但是，现实更多展现的是相反的一面，即传统经济模式与工具对区块链和加密数字货币的生态体系影响。

其一，包括比特币在内的主要加密数字货币的价值，需要通过以美元为代表的法币加以体现。之所以发生这样的情况，主要因为在现实世界还没有形成比特币或者其他加密数字货币的自我循环和交易的市场。

其二，传统以法币作为投资手段的各种资本，全面进入区块链和加密数字货币领域，形成“资本主权”。

其三，诸如商业银行、投资银行、交易所等机构模式，正在与区块链、加密数字货币和 Token“嫁接”，甚至“融合”。

其四，部分“移植”区块链和加密数字货币原理和技术，以求强化传统经济和货币体系。一些国家开发的法定加密数字货币，就是典型案例。

要特别注意的是区块链“财富效应”幻觉，夸大以区块链为技术基础的数字资产的价值转移、定价与交易，误导人们以传统商业化的原则理解和判断区块链的价值。简言之，当下回答如何看待传统经济模式和区块链系统的相互作用，或者彼此混合的后果，是否能够重构人类信任体系，最终谁改造谁，还为时过早。但是，有一点是值得考虑的：区块链及其理念与技术原本是为了解决传统经济制度的缺陷，然而面对传统经济工具、制度和机构的全方位接触，尚处于早期的和脆弱状态的区块链生态，并不具备强大的自我保护机制，面临被传统经济模式和工具再改造的可能性。

3. 现阶段区块链存在怎样的创新路径？区块链过去、现在和未来的生命力，都取决于其创新能力。区块链的创新主要是两类：在现阶段区块链主流架构下的创新，以及从本源上突

⊖ 见书内文“5. 共识算法”。

⊖ 见参考资料《Engineering Security Through Coordination Problems》，Vitalik Buterin。

破了主流框架的创新。

3.1 基于区块主流架构和具有“路径依赖”特征的创新。现在普遍看法是，比特币是区块链的 1.0，以太坊是区块链的 2.0。在主流框架下的创新主要集中在以下几个方面。

其一，突破“可扩展性”限制。主要包括比特币通过“分叉”的扩容方案，以太坊自身的 Plasma、State Channel、Raiden、Truebit、Sharding 和 Casper 等扩容方案㊀，以及诸如侧链技术（RootStock、Polkadot、Cosmos）、区块扩容、链下计算、分区共识、分片的“内部分割”等处于试验阶段的选择方案㊁。

其二，改善存储。工程实例至少有：Swarm（以太坊的 P2P 文件共享协议）、Storj（一种“分布式存储”技术），以及 IPFS（一种 P2P 超媒体协议）㊂。

其三，EOS 代表的区块链操作系统。根据 EOS 白皮书显示，预计其可扩展至单链几千 TPS、全网并行百万 TPS 的交易吞吐量，并且主网已于 2018 年 6 月上线，是未来区块链平台强有力的竞争者。㊃

其四，开发具有隐私和法规的区块链，例如 Cardano。Cardano 是世界上第一个由研究为主导，基于科学哲学开发出来的区块链项目，也是第一个采用同行评审技术的区块链项目，可用于发送和接收数字资金，支持各种去中心化应用和智能合约。㊄

其五，提高智能合约的安全性。形式化验证技术正在逐步应用到区块链智能合约代码检查。其原理是，根据某个或某些形式规范或属性，使用数学的方法证明其正确性或非正确性。㊅

其六，满足区块链测试需求，参考“ISO/IEC 25010 标准”来完善测试模型。在这本书提供的参考测试模型中，区块链评测涉及 8 个维度，31 个分维度。㊆

3.2 突破现阶段区块链主流架构的创新。必须注意到，在区块链主流架构下的创新，只具有相对意义。例如，比特币在顶层设计阶段就没有彻底解决共识问题，只是将问题加以转换，“一方面通过区块链的序号作为虚拟时间基准，另一方面通过‘挖矿’的经济动力来促使比特币链的不断延伸”㊇。在这个意义上，中本聪用此类经济方法解决分布式系统共识问题确实相当智慧。进一步说，现阶段的区块链，难以升级。一旦区块链被部署和进入生产模式，

㊀ 见书内文 10.3.1 节。

㊁ 见书内文 10.2 节。

㊂ 见书内文 10.3.10 节。

㊃ 见书内文“10.3.2 节。

㊄ 见书内文“10.3.3 节。

㊅ 见参考资料 https://zh.wikipedia.org/wiki/%E5%BD%A2%E5%BC%8F%E9%AA%8C%E8%AF%81。

㊆ 见书内文 12.2 节。

㊇ 见参考资料《区块链正本清源：从计算机科学评看区块链的起源和发展》。https://blog.csdn.net/omnispace/article/details/80467188。

在功能上进行添加、修改和删除，难度甚大，成本甚高。[⊖]现在，通常的区块链修改，都会造成区块链系统的软分叉或者硬分叉，造成时间、精力和经济上的浪费。

所以，区块链的真正创新必须突破主流架构，实现顶层理论设计和数学方法上的创新。这种突破主流框架的创新，已经悄然开始。到目前为止，DAG（Directed Acyclic Graph，有向无环图）为代表的技术属于突破现阶段区块链主流架构的创新。“比特币的效率一直比较低，基于 PoW 共识下的出块机制是原因之一，由于链式的存储结构，整个网络中同时只能有一条链，导致出块无法并发执行。DAG 从根本上摒弃了区块概念，交易直接进入全网中，达到所谓的无区块（Blockless）效果，网络中的交易可以容纳 N 倍。”[⊜]

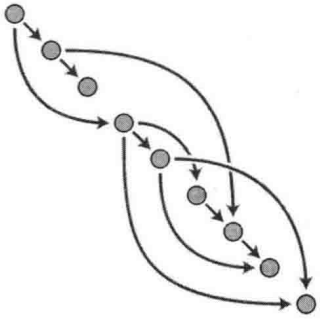
具体说，DAG 有 4 个特点。

其一，交易速度快。交易速度远远高于基于 PoW 和 PoS 的区块链交易速度。

其二，无须挖矿。DAG 把交易确认的环境直接下放给交易本身，无须由矿工打包成区块后同意交易顺序。所以 DAG 网络中没有矿工的角色。

其三，无手续费。交易发起只需要做简单的 PoW，整个网络中的 PoW 都是发起交易者自己做的，而不是交给矿工，所以发起交易无须手续费。

其四，需要见证节点。DAG 需要见证人机制的存在。超越 DPoS、PoS、PBFT，最终实现在效率与安全性上的一种平衡。[⊜]DAG 的数学基础不再是数论，而是图论，即拓扑学，即以空间、维度与变换作为研究对象的学科。图论原理显然更接近对区块链基本模式的描述。DAG 模式如下[⊛]。



第一次提出 DAG 跟区块链结合是在 NXT 社区，该社区的成员大多集中在东欧和俄罗斯，去中心化对他们更具有现实意义。现在，基于 DAG 原理和技术的 IOTA，由 4 名平均年龄不

⊖ 见参考资料《MOAC 号称“众链之母”：他们在区块链技术上有什么创新？》。

⊜ 见参考资料 https://zhuanlan.zhihu.com/p/31764777。

⊜ 同上。

⊛ 见参考资料 https://ethereum.stackexchange.com/questions/1993/what-actually-is-a-dag。

到30岁、最年轻者仅21岁的团队所创立，推出不到两年，其价格在虚拟货币中已经攀升至第8名，他们更高的目标是成为“物联网”的骨干。此外，Swirlds公司开发的Hashgraph技术也是DAG结构的一种。Hashgraph通过Gossip about Gossip协议，“让每个节点都维护着所有节点跟其他节点的通信历史，每个节点在完成拜占庭协议时，不需要经过网络多轮通信，节点本地环境就可以直接模拟拜占庭协议。Hashgraph在数学上可以证明满足异步拜占庭容错，至少跟比特币一样安全。”[㊀]不过，对于Hashgraph技术，尚有很大争议。

4. 怎样实现区块链系统维系“熵值减少”状态？区块链是典型的信息系统，其生命力取决于其内在的信息熵的大与小和高与低。

邹均在本书前言中提出：“在香农创立的信息论中，信息是确定性的一个度量，而熵也是信息量的一个度量。熵越大，越无序，信息量越少。而从这个意义上来说，区块链系统是一个熵值减少的系统，因为共识所确定的状态就是信息，而信息也就是有序和确定性”。[㊁]邹均的上述说法是否精确，可能还需要讨论。但是，邹均提出了两个有意义的问题：其一，区块链是一个熵值减少的系统；其二，共识导致熵值减少。

4.1 何谓“信息熵”？为了理解“信息熵”，首先需要理解什么是“信息”？信息没有标准定义，按照香农（C. E. Shannon，1916-2001）的“信息论”，可以理解为一串以逻辑论的01（即计算机的“二进制”）编码的数列。至于信息熵，则是基于数学，或者统计学上的抽象概念，所描述的是信息本身的一种性质，这种性质独立于信息的形式内容。具体说，信息熵的几个基本属性如下。

1）单调性。发生概率越高的事件，不确定性越低，其所携带的信息熵越低。相反，事件的可能选择越多，不确定性越大。

2）非负性，即信息熵不能为负。

3）信息熵应该是随概率连续变化的。

4）累加性，即多随机事件同时发生存在的总不确定性的量度可以表示为各事件不确定性的量度的和。[㊂]

在这里，信息熵与信息量概念发生某种重合。信息量是衡量信息消除的不确定性（Uncertainty）的度量，更准确地说，就是“变量不确定度的平均度量”，信息论中将它称之为

㊀ 见参考资料 https://www.jianshu.com/p/9f181cefba8d?from=timeline。

㊁ 见书前言。

㊂ 参考资料：https://www.zhihu.com/question/22178202。