区块链蓝皮书

BLUE BOOK OF BLOCKCHAIN

No.3

中国区块链发展报告(2019)

主编／姚前

执行主编／朱烨东

ANNUAL REPORT ON DEVELOPMENT OF CHINA'S BLOCKCHAIN (2019)

2019版

社会科学文献出版社
SOCIAL SCIENCES ACADEMIC PRESS (CHINA)

区块链蓝皮书

BLUE BOOK OF BLOCKCHAIN

中国区块链发展报告（2019）

ANNUAL REPORT ON DEVELOPMENT OF CHINA'S BLOCKCHAIN (2019)

主　　编／姚　前
执行主编／朱烨东

社会科学文献出版社
SOCIAL SCIENCES ACADEMIC PRESS (CHINA)

图书在版编目(CIP)数据

中国区块链发展报告.2019 / 姚前主编. --北京:社会科学文献出版社,2019.8(2019.11 重印)
(区块链蓝皮书)
ISBN 978-7-5201-5313-3

Ⅰ.①中… Ⅱ.①姚… Ⅲ.①电子商务-支付方式-研究报告-中国-2019 Ⅳ.①F724.6

中国版本图书馆 CIP 数据核字(2019)第 159221 号

区块链蓝皮书
中国区块链发展报告(2019)

主　　编 / 姚　前
执行主编 / 朱烨东

出 版 人 / 谢寿光
组稿编辑 / 恽　薇
责任编辑 / 高　雁
文稿编辑 / 王春梅

出　　版 / 社会科学文献出版社·经济与管理分社(010)59367226
地址:北京市北三环中路甲 29 号院华龙大厦　邮编:100029
网址:www.ssap.com.cn
发　　行 / 市场营销中心(010)59367081　59367083
印　　装 / 三河市东方印刷有限公司

规　　格 / 开 本:787mm×1092mm　1/16
印 张:21.25　字 数:317 千字
版　　次 / 2019 年 8 月第 1 版　2019 年 11 月第 3 次印刷
书　　号 / ISBN 978-7-5201-5313-3
定　　价 / 138.00 元

本书如有印装质量问题,请与读者服务中心(010-59367028)联系

权威·前沿·原创

皮书系列为
“十二五”“十三五”国家重点图书出版规划项目

《中国区块链发展报告 2019》
编 委 会

京东数字科技控股有限公司
北京中科金财科技股份有限公司
北京网录科技有限公司
北京众享比特科技有限公司
北京猿链网络科技有限公司
广州通链计算机智能技术有限责任公司
武汉区块链产业园
福建省区块链协会
陕西省区块链产业联盟

主要编撰者简介

姚　前　工学博士，教授级高工，博士生导师，国务院参事室金融研究中心研究员，全国金融标准化技术委员会秘书长，中国证券登记结算有限责任公司党委副书记、总经理。曾任中国人民银行科技司副司长、巡视员，中国人民银行数字货币研究所所长，中国人民银行征信中心副主任。中国人民银行金融研究所博士后科研流动站、中国人民银行征信中心博士后科研工作站学术委员会委员，中国电子学会区块链分委会主任委员，清华大学区块链技术联合研究中心学术委员会委员，上海新金融研究院学术委员，发表学术文章近150篇，著作8部，100多项专利发明人，多次获得银行科技发展奖一等奖等奖项。

朱烨东　北京大学政治经济学博士，清华五道口金融学院EMBA，北京中科金财科技股份有限公司（股票代码：002657）董事长、创始人。北京区块链技术应用协会会长、中国上市公司十大创业领袖人物、中国软件和信息服务业十大领军人物、新三板企业家委员会首席区块链专家、2018中国区块链行业十大领军人物、2018中国新经济产业百人、2017年度中国金融科技最具影响力人物，《中国金融科技发展报告》《中国区块链发展报告》《中国资产证券化发展报告》执行主编，清华五道口全球创业领袖导师。

摘　要

区块链技术最早应用于比特币，但随着技术的不断深入发展，应用领域早已拓宽到银行、证券、保险、艺术、公益等。特别是2018年以来，随着技术的发展创新，各家机构对区块链的接受度越来越大，给予区块链落地的机遇越来越多，更加积极地尝试应用区块链的场景，使区块链应用的范围不断扩大，具体项目不断增多，涉及的群体也越来越多，区块链的落地基础越来越坚实。这不仅使区块链技术有更宽广的应用场景，也有助于区块链技术向着更为符合现实需求、更能推动经济社会发展的方向发展，并与大数据、云计算等其他技术深度融合。

与此同时，各国政府也高度重视区块链发展：一是纷纷出台若干政策支持区块链技术的发展和区块链应用的推行；二是政府也开始尝试将区块链技术应用于政务服务和社会经济监管运行方面，甚至数字货币发行等关键领域，这在区块链技术应用中起到了引领和重要的支持作用。

本书分为总报告、政策市场篇、技术创新篇、场景应用篇，从政策颁布、市场培育、技术上的创新发展、具体场景应用描述等几个方面全面研究我国区块链的政策、立法、市场比较、关键技术以及在银行、证券、保险、支付等金融领域和其他领域的应用。同时还列出了区块链技术应用发展大事记（2018），刻画了我国区块链技术应用的整体产业发展情况和典型企业。通过系统研究我国区块链2018年的发展情况，掌握行业的最新技术与应用进展，剖析其优秀特质与不足之处，并对其未来发展方向进行前瞻思考。由此，能够概览区块链全行业发展画像，掌握最新技术发展方向和细节要点，了解落地领域与具体应用案例，知晓政府政策动态与关注重点，并为区块链行业未来发展指明方向与明确目标。

关键词：区块链　场景应用　产业地图

目　录

Ⅳ 场景应用篇

Ⅴ 附录

皮书数据库阅读使用指南

总 报 告

General Report

B.1

中国区块链发展回顾与前瞻（2019）

姚 前

摘 要：本报告从现代密码学的演进脉络追溯数字货币的发展过程，回顾区块链技术的缘起，指出非对称密码算法解决了开放系统中密钥大规模分发的问题，并带来独特的认证功能；而哈希函数具有快速收敛、不可逆、无须耗费巨大计算资源等优势，两者为数字现金的加密、签名和自主开户奠定了基础。比特币则是通过分布式共享账本与工作量证明机制的创新设计，防止去中心化条件下数字现金的“双花”，开创了价值交换技术——区块链技术。本报告还从系统架构、会计学、账户、资产交易、组织行为学、经济学六个维度，对区块链技术进行解读，指出区块链技术具有难以篡改、自由开放、数据高度可信任、容错性强优秀特质，但存在性能问题、隐私保护、安全问题、治理缺失、互操作性问题的不足。本报告最后

从共识机制与性能、跨链、治理机制、身份管理、隐私保护、数字钱包、智能合约与自组织商业模式、与其他科技的融合八大方向，对区块链技术的未来发展进行前瞻思考。

关键词： 非对称加密　哈希算法　加密货币　区块链

自2009年比特币问世以来，数字货币[①]的数量不断增长，从主流币到稳定币，热点不停地切换。根据Coinmarketcap的数据统计，截至2019年5月底，全世界共有2212只数字货币，总市值为2650亿美元。其中，比特币的市值占比最高，在2017年初一度达到90%，随后由于其他数字货币爆发式增长以及比特币价格下跌，比特币的市值占比下滑，但至今基本维持在50%的水平。接着为以太币、瑞波币、比特币现金等其他数字货币。在一定程度上，数字货币总市值与比特币价格呈正相关关系。如果按照融资额来统计，数字货币融资额在2018年占全球股票首次公开发行融资额的9%以上。比特币价格与加密资产市值的走势见图1。各类加密资产的数值占比见图2。ICO融资规模见图3。基于不同货币的比特币成交额见图4。

当前，各国对数字货币的本质并未形成一致的看法，有的将其视作货币或者支付工具，有的将其界定为特殊的商品，也有一些国家倾向于将其界定为证券。但无论如何，各国对于数字货币的底层技术——区块链技术的发展潜力高度重视。有人认为，区块链技术是继大型机、个人电脑、互联网、移动互联网之后计算范式的第五次颠覆式创新，是新一代云计算的雏形，有望像互联网一样彻底重塑人类社会活动形态，实现从目前的信息互联网向价值互联网的转变[②]。

① 根据发行者的不同，数字货币可分为法定数字货币和私人加密货币。本报告中的数字货币是指以比特币为代表的私人加密货币，或称为加密资产（Crypto Assets）。

② 袁勇、王飞跃：《区块链技术发展现状与展望》，《自动化学报》2016年第4期。

图 1　比特币价格与加密资产市值的走势

资料来源：Cryptocompare，Coinmarketcap 和欧洲中央银行。

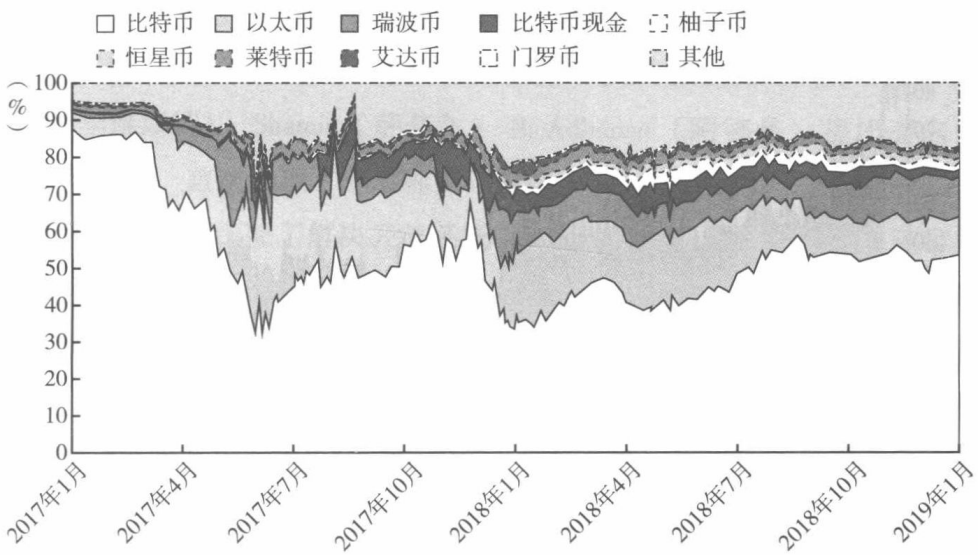

图 2　各类加密资产的数值占比

资料来源：Cryptocompare，Coinmarketcap 和欧洲中央银行。

本报告将从现代密码学的演进脉络追溯数字货币的发展过程，回顾区块链技术的缘起，提出理解区块链技术的六个维度，并剖析区块链技术的优秀特质与不足之处，最后对其未来发展方向进行前瞻思考。

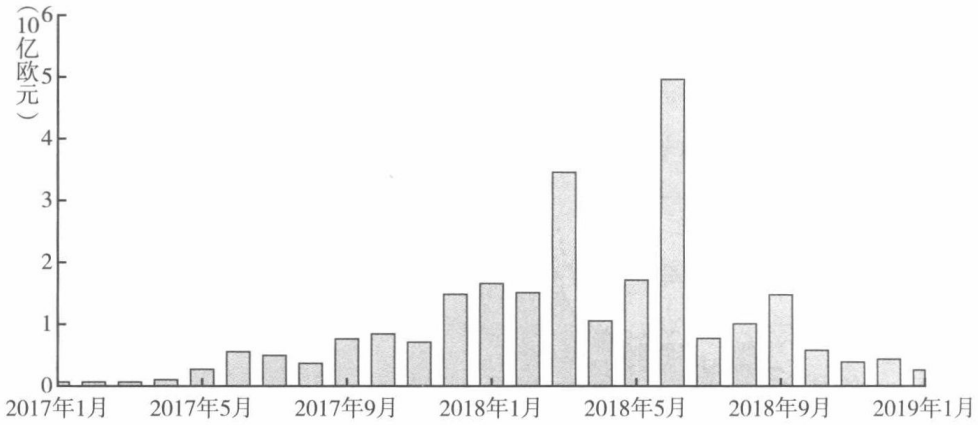

图3　ICO 融资规模

资料来源：Coinschedule。

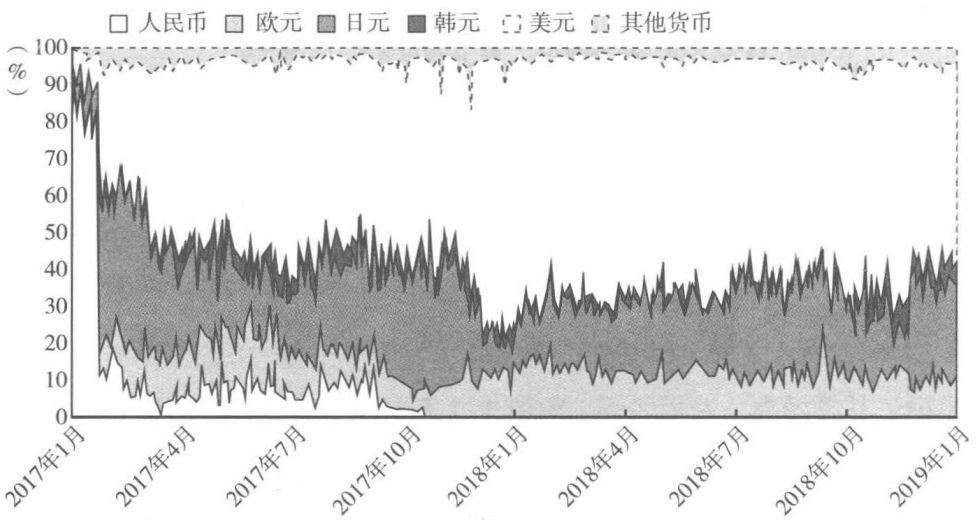

图4　基于不同货币的比特币成交额占比

资料来源：Cryptocompare 和欧洲中央银行。

一　现代密码学演进

罗马非一日建成。想准确理解区块链技术的缘起，我们需要回到40多年前以研究现代密码学的发展历史。现代密码学的一个革命性突破是解决

对称密码算法无法在大规模的信息加密传输中普及的问题。对称密码算法是指加密和解密共用一个密码，也称单钥密码算法。它的最大缺陷是，信息发送方必须和每个接收方约定好对称密钥，这样在密钥的大规模分发过程中，无法有效防止密钥被窃取或者被人攻击，也不太容易去管理那么多的密钥。

对此，1976 年，Diffie（迪菲）和 Hellman（赫尔曼）提出了新的思路，他们将原来的一个密钥分成一对密钥，一个密钥用于加密，另一个密钥用于解密。加密密钥公开，称为公钥。解密密钥不能公开，唯独本人秘密持有，不能让别人知道，称为私钥。如果张三想给李四发信息，张三要用李四的公钥对信息进行加密，那么只有李四的私钥才能解开，其他任何人都解不开。同样，李四想给张三发信息，要用张三公开的公钥进行加密，而只有张三手上有的那把私钥才能解开加密后的信息。这样的思路就很好地解决了单密钥体系下的密钥大规模分发的问题。这就是非对称密码机制的思想。1978 年，Rivest（李维斯特）、Shamir（萨莫尔）和 Adleman（阿德曼）提出著名的 RSA 密码算法，首次实现了非对称密码算法。

非对称密码算法除了解决开放系统中密钥大规模分发的问题外，还带来原来对称密码体制不具备的功能，那就是非常独特的认证功能。比如，如果张三想给别人发信息，那么张三不仅用别人的公钥对报文进行加密，同时还可用张三的私钥进行签名，这样别人就可以用张三的公钥进行验签，判定报文是不是由张三发出的。认证功能的出现使信息加密传输形式发生革命性的变化：信息既可以加密，也可以签名，就像支票一样，信息的加密传输有了抗抵赖的功能。所以说，非对称密码机制的实现是密码学的一次重大革命，密码学的应用因此从军事领域走向民用领域。

哈希算法是现代密码学的又一个飞跃。它也叫“安全散列函数”，最早的 SHA 哈希算法由美国国家安全局设计，于 1993 年发布。2010 年，中国国家密码管理局公布中国商用密码哈希算法标准：SM3 密码哈希算法。

哈希算法又称信息摘要，众所周知，文章摘要是对文章内容的概括总结。通过文章摘要，我们就能理解文章的大部分意思。哈希算法也有这样的

功能，它可以把任意的信息集，用非常简单的信息予以描述。它是一个特别的数学函数：给定输入很容易得到输出，但是从输出计算输入不可行。这就像从全文得出摘要很容易，但要根据摘要把全文再重写一遍就很不容易了。此外，哈希算法还有一个有意思的特性，只要原始信息稍微发生变化，摘要就变得完全不一样，这一特性非常有用。

与对称加密算法和非对称加密算法不同，哈希函数是一种快速收敛的算法，从输入到输出的计算非常快，迅速收敛数值，无须耗费巨大的计算资源，而从输出倒推输入又几乎不可行。基于这样优秀特质，哈希函数得到广泛的应用，我们习以为常的人民币冠字号码即由哈希算法产生。在数字货币领域，哈希算法常常被当作数字货币交易挖矿、交易区块链接以及钱包地址压缩生成的工具，得到广泛的应用。

二　数字货币的中心化与去中心化：区块链技术的缘起

长期以来，密码学家有个想法，既然邮件能够加密、签名发送出去，那么手里的现金能不能像邮件一样，加个数字信封，进行加密和签名后，从一端发送到另外一端？这就是最早的数字现金思想的由来。随着现代密码学的发展，数字现金的技术实现逐渐成为可能，引起许多密码学家的广泛兴趣。

1982 年，David Chaum（大卫·乔姆）在顶级密码学术会议——美密会议上发表了一篇论文《用于不可追踪的支付系统的盲签名》。论文中提出了一种基于 RSA 算法的新型密码协议——盲签名。利用盲签名构建一个具备匿名性、不可追踪性的电子现金系统，这是最早的数字货币理论，也是最早能够落地的试验系统，得到了学术界的高度认可。

但 Chaum 当时建立的还是传统的“银行、个人、商家”中心化模式。每个使用过的 E-Cash 序列号都会被存储在银行数据库中，且每次交易系统都要验证 E-Cash 序列号的唯一性，因此系统会维持一个已交易序列号的数据库。随着交易量的上升，该数据库就会变得越来越庞大，验证过程也会越

来越困难。

面对中心化数字货币模式的缺陷，2008 年，中本聪发表了经典论文《比特币：一种点对点的电子现金系统》，提出了一种全新的去中心化的电子现金系统，其核心思想之一就是通过对等网络方式消除单个中心化依赖，实现点对点交易；同时，将已花费的数字货币序列号（UTXO）数据库转变成未花费的数字货币序列号数据库，控制数据规模，并利用哈希算法，打上时间标记，纵贯相连。这一底层支撑技术就是我们今天热议的区块链技术的来源。当然，也有人提出早在 1990 年到 1991 年，W. Scott Stornetta 和 Stuart Haber 就提出了区块链的想法。为确保数字文档的精确性，他们认为如果不去信任某个人或者机构，“那就去信任每一个人，也就是说，让世界上的每一个人都是数字文档记录的见证者”。就理念而言，这一思想确实与比特币区块链的思路相通：去中心化的本质就是多中心化——既然没有了权威中心，那么大家都成了中心，但各个中心既须自律亦须他律，彼此之间相互验证，相互制衡，以构造严丝合缝的信任机器。

所以中本聪的区块链技术不仅是“分布式”和“共享”的简单理念，它还综合采用了密码学、分布式数据库（大规模数据存储与处理）、点对点通信（P2P 网络）、共识机制（分布式一致性）等技术进行组合创新。狭义的区块链技术是一种按照时间顺序将数据区块以链表的方式组合成特定数据结构，并以密码学方式保证的不可篡改和不可伪造的去中心化共享总账，能够安全存储简单的、有先后关系的、能在系统内验证的数据。广义的区块链技术则是指利用加密技术来验证与存储数据、利用分布式共识算法来新增和更新数据、利用运行在区块链上的代码，即智能合约，来保证业务逻辑的自动强制执行的一种全新的多中心化基础架构与分布式计算范式。

三　理解区块链技术的六个维度

第一个维度，从系统架构看，区块链技术是一种全新的信息网络架构。从大型机到个人电脑，再到移动智能终端，互联网技术的进步与应用打破了