中国科学院学部
科学与技术前沿论坛简报
第 103 次

学部工作局学术与文化处
《中国科学》杂志社 编报

2020 年 4 月 26 日

“区块链技术与应用”科学与技术前沿论坛综述

一、背景

2019 年 10 月 24 日，在中央政治局第十八次集体学习时，习近平总书记强调，“要把区块链作为核心技术自主创新的重要突破口”“加快推动区块链技术和产业创新发展”。随着国务院《“十三五”国家信息化规划》的稳步推进，区块链与实体经济深度融合将成为数字经济发展至关重要的一环。然而，区块链技术仍处于发展初期，尚面临技术发展路径不确定，应用场景尚缺不可替代优势，技术标准不统一等痛点，亟需通过交叉学科的发展加速行业的应用落地。

二、论坛概况

2019 年 12 月 7 日，以“区块链技术与应用”为主题的科学与技术前沿论坛在深圳开幕。论坛由中国科学院学部主办，中国科学院学部学术与出版工作委员会、中国科学院信息技术科学部、中国科学院数学物理学部承办，鹏城实验室、中国信息通信研究院、中国通信学会联合支持，北京航空航天大学、清华大学、《中国科学》杂志社、深圳中国科学院院士活动基地协办。

本次论坛的执行主席为中国科学院信息技术科学部郑志明院士和中国科学院数学物理学部王小云院士，中国科学院包为民院士、梅宏院士、尹浩院士参会。深圳市人民政府、中国科学院学部学术与出版工作委员会、鹏城实验室、中国科学院学部工作局学术与文化处的有关领导分别致辞，中国信息通信研究院金键研究员主持了会议。会上，区块链与数字身份、监管科技、金融应用、工业互联网等领域的专家作了主题报告，近 500 名来自政府、学术和企业界的代表参会。

论坛致力于对目前区块链技术与应用的发展现状进行深入讨论和全面梳理，进一步加强多个学科的交叉力度和思想碰撞，更好地推动区块链技术与应用的相互融合与共同发展。同时，为相关领域的学者搭建高层次的交流平台，鼓励学术争鸣，为在国家层面上进行相关领域跨学科发展的决策提供兼具前瞻性与可行性的规划与建议，特别是为推动区块链技术的产业落地进一步凝练目标，凝聚共识。

论坛的学术报告以视频资料的方式得以保存。

三、论坛重点关注的议题及报告

（一）Hash 函数与区块链技术

中国科学院王小云院士为本次论坛作开幕报告，从密码学角度解读区块链技术，内容涵盖了密码学的重要性、密码哈希函数、区块链技术中的密码学原理和区块链的应用领域。报告中指出，密码是保障网络与信息安全的核心技术和基础支撑，加密算法、数字签名算法和 Hash 函数是密码学三类基础算法。其中 Hash 函数是区块链的起源性技术，不仅能抵抗基于数据篡改的攻击，而且对于高效密码方案设计具有十分重要的意义。

（二）关于国际支付体系改革的一点思考

中国证券监督管理委员会科技监管局局长姚前指出，区块链是目前的研究热点，务必要深入研究。世界的命运必须由各国人民共同掌握，世界上的事情应该由各国政府和人民共同商量来办，垄断国际事

务的想法是落后于时代的，垄断国际事务的行动也肯定是不能成功的。本质上，区块链技术的分布式记账、共同验证等去中心化设计及平权理念，与国际货币体系的自发特征有着天然的吻合。因此，国际货币领域是区块链技术的绝好应用场景，可以是存量上的改进优化，亦可是增量上的全新探索，关键在于如何协调各方，凝聚共识。

（三）工业互联网中的 ID 进化与区块链“引力奇点”

中国信息通信研究院研究员金键阐述了工业互联网中的标识（Identifier，ID）进化。报告表示，ID 是资产数字化的必要基础设施，区块链技术和 ID 技术的发展助力建立可监管可治理的价值交换体系。报告强调，ID 就像人的身份证一样，在管理中 ID 为资产上链提供了机制和数据模型。ID 是未来区块链的基础组件，助力区块链构建万物互联的价值交换体系，共同提供价值流通的基础设施。

（四）从互联网到区块链，从野蛮生长到高效、有序、可信

迅雷集团首席执行官陈磊介绍了区块链技术在互联网中的应用场景。报告表示，互联网野蛮生长时代已经过去，区块链是给互联网带来秩序、规则和信任的典型技术手段，区块链技术让互联网上的数据变得真实可信，让数据可管理，有序共享。在物联网的应用中，区块链技术有助于打破“数据孤岛”。

（五）物联网安全问题

中国科学院尹浩院士在“工业互联网安全问题”主题报告中指出，区块链技术在工业互联网中可发挥重要作用，主要包括大数据、信息安全和产品交易全过程的监管三大应用，其价值和意义在于，提供一种在不可信网络中建立信息与价值交换的可信通道。当前的研究热点是跨链、隐私保护和安全监管等关键技术。但同时，区块链技术仍处于社会实验阶段，各方对区块链的概念、架构、技术特点、发展路线及治理等未完全形成共识，应用模式仍在探索阶段，还没有找到杀手级应用。需要注意的是，区块链并不适用于所有领域，在网络带宽和

时效性可保证情况下的高价值、易实现场景下具有更高应用价值；在性能、能耗、生态、安全、监管等方面，区块链技术发展依然面临诸多挑战。

（六）区块链隐私计算框架

华南理工大学唐韶华教授在报告中鲜明地指出，区块链并不能做到“匿名”，只能做到“假名”。在智能合约隐私中，面临着用户身份、合约数据和合约代码隐私泄露的问题。报告提到了能够用来解决区块链隐私问题的密码学技术，包括零知识证明、安全多方计算、可信计算环境等。同时提出，关于区块链隐私计算仍有一些问题需要思考：一是安全和效率，现在使用复杂的密码协议可能很安全，但是效率往往不高；二是集中式和分布式的问题，传统密码学的算法往往是以集中式的计算模式来设计的，区块链是典型的分布式计算，需要进行分布式的改造；三是同步网络和异步网络的问题，密码技术的使用需要考虑区块链分布系统往往可能是异步网络；最后是隐私保护和可监管性的问题，不能过于加强隐私保护使得区块链变成犯罪分子的天堂。

（七）国内外区块链应用与产业现状及发展趋势

复旦大学斯雪明教授对国内外区块链应用与产业的现状进行了全面分析。报告指出，在中国，区块链企业集中在一线城市，金融行业和实体经济应用是主体。区块链应用呈现多样化，从金融衍生到支付领域。区块链技术应用发展迅猛，专利申请量快速增长。关于如何加速区块链产业与应用的发展，第一，要加强顶层设计，包括区块链的互联互通、监管等问题；第二，要重视基础理论与技术研究；第三，要重视自主可控技术与产品研发；第四，要加快区块链标准与规范的制订。同时要加强四个融合：一是区块链与“云大移物智”等技术的深度融合；二是与信息化建设的深度融合；三是与现有 IT 企业的深度融合，不仅要提倡“区块链+”，在这个阶段还更要提倡“+区块链”，把区块链用于现有的信息化系统建设中；四是区块链与大数据的深度

融合。

（八）区块链技术与发展

中国科学院郑志明院士作了闭幕报告。他指出，区块链行业正处于2.0到3.0的过渡阶段，到了3.0阶段，分布式价值互联网将初步形成并成为成熟的数字经济基础设施。报告指出了区块链的三元悖论以及区块链发展的关键技术、核心理论。区块链行业的生态应用将决定最后的赢家，目前公链、私链或联盟链都有一些金融等小规模行业应用，但尚未成气候，未来区块链技术发展进程中大公司未必有优势，开源力量不可小觑。当前，中国正从大国走向强国，必须重视区块链技术在数学、信息和安全等多个基础领域的原始创新，这样才有可能实现总书记对区块链提出的“理论最前沿，创新制高点”的要求。

四、论坛总结

此次论坛聚集了国内外多家研究院所和大学的区块链及相关科学领域的知名科学家，对“区块链技术”相关的各领域交流合作、交汇融通起到了很大的促进作用。与会专家高度肯定了本次论坛的重要意义，并讨论提出了今后“区块链技术”在科学和应用层面的需求，以及发展“区块链技术”的关键举措。

第一，区块链技术的核心突破。区块链技术是目前我国和欧美差距最小的技术，习近平总书记特别强调，我国要在这个新兴领域走在理论最前沿，占据创新制高点，取得产业新优势。要推动协同攻关，加快推进核心技术突破,为区块链应用发展提供安全可控的技术支撑。当前区块链技术大多数停留在概念炒作阶段，很多业务场景单纯为了“区块链”而“区块链”。然而我国目前还没有解决三元悖论等核心问题，这要通过长期的潜心研究才能取得重大突破，因此，必须回归基础理论和核心技术。事实上，习近平总书记对区块链技术的理论和后续的应用发展提出了非常高的要求，做好区块链基础理论研究，着力攻克一批关键核心技术，真正把技术研发的担子挑起来，是当前区块

链发展的关键。

第二，提升国际话语权和规则制定权。区块链技术不同于以往的信息技术，具有很强的扩张性，它的规则或话语权决定了它的影响范围，因为每一个上链开展业务的个体或机构必须服从区块链所定的规则，不论是国内还是国外。区块链规定了产业治理规则，凭借其分布式特征，影响力可迅速超越国界和地域限制。

为了实现上述两点，需要加强人才队伍建设，建立完善人才培养体系，打造多种形式的高层次人才培养平台，培育一批领军人物和高水平创新团队。区块链作为架构性创新技术，对复合型人才需求巨大，要求从事者掌握涉及密码学、信息科学、基础数学等的多学科专业技术知识。发展区块链，必须加强学科深度交叉融合的人才队伍建设，从基础研究、应用研发、产业融合等方面，前瞻性和系统性地建立人才培育体系。

（作者：郑志明，中国科学院院士，北京航空航天大学；王小云，中国科学院院士，清华大学）

联系方式：中国科学院学部工作局学术与文化处，010-59358366