中国通信学会
CHINA INSTITUTE
OF COMMUNICATIONS

区块链技术前沿报告

（2020年）

中国通信学会
2020年12月

版权声明

专家组和撰写组名单

顾问(以姓氏笔划为序)：

邬江兴 中国工程院院士

张　平 中国工程院院士

陈世卿 美国国家工程院院士、美国艺术与科学院院士

陈清泉 中国工程院院士、英国皇家工程院院士、匈牙利工程院荣誉院士、乌克兰工程科学院院士、香港工程科学院院士

郑纬民 中国工程院院士

周孝信 中国科学院院士

倪光南 中国工程院院士

董家鸿 中国工程院院士、法国国家外科科学院外籍院士

专家组：

组长：

郑志明 中国科学院院士，中国通信学会区块链委员会主任委员

成员(以姓氏笔划为序)：

姓名	单位	职务
王向东	中国通信学会区块链委员会	副主任委员
王栋	国网区块链科技公司	总经理
王焕然	深圳众联数字科技有限公司	董事长
亓峰	北京邮电大学	正教授
朱晖罡	北京航空航天大学	正教授
陈晓禾	中科院苏州医工所电子研究室	主任、正教授

邱望洁	广州大学人工智能与区块链研究院	副教授
杨斌	清华大学网络行为研究所	副所长、研究员
金键	中国信息通信研究院工业互联网与物联网研究所	所长、正高工
侯锐	中科院信息工程研究所信息安全国家重点实验室	副主任、研究员
袁昱	深圳清华大学研究院	主任研究员
黄河燕	北京理工大学计算机科学与技术学院	院长、正教授
曹源	湖南兆物信链科技集团有限公司	董事长
褚晓文	香港浸会大学区块链与金融科技实验室	主任、正教授
魏丽红	中国移动通信集团有限公司信网部	总经理、正高工

撰写组（按单位排名）：

单位	姓名
湖南兆物信链科技集团有限公司	葛力行，陈伯彬，邓辉
湖南宸瀚信息科技有限责任公司	谢超良，邓罡
苏州鸿链信息科技有限公司	章天乙
深识全球创新科技（北京）有限公司	林道庄，王奇

前　言

近年来，中国经济发展面临的内外部挑战不断增加，中国经济由高速增长向中高速增长转换，社会生活、生产方式向数字化转型。区块链技术的创新发展和广泛应用是这一转型过程中非常重要的核心。党中央、国务院高度重视数字经济发展及区块链技术的应用，习近平总书记近期针对区块链技术发展多次明确指示。国际上，将区块链与人工智能、自动驾驶等一并列入“第四次工业革命”，显示出区块链技术的重大意义和极为广阔的发展空间。机会与挑战并存，如今，区块链技术应用已延伸到疫情管控、智能健康医疗、数字金融、能源区块链、物联网、智能制造、供应链管理、数字资产交易等多个领域，区块链的分布式共享账本、密码算法、共识机制、激励层、合约层、数据层、网络层、以及可追溯、可证明性、永恒性、权威性保证等主要功能也是关键技术和挑战所在。

根据中国通信学会组织各专业委员会展开前沿报告的工作安排，区块链委员会汇集委员会专家委员近年实际科研、工作经验、成果，由部分专家执笔撰写了本“2020 年区块链技术前沿报告”。

本报告分析了区块链全球发展态势、国内发展现状，国内外区块链技术预见、工程难题、标准制定，涵盖区块链底层技术、跨链技术、交换技术、软硬协同技术、关键密码学技术以及相关监管架构、系统脆弱性分析和政策建议等。报告内容丰富、真实、深厚，有覆盖全面和关键侧重，可作为高校、研究机构以及金融、能源、政务服务、司法、医疗健康、产品溯源、智慧城市、物流等区块链应用行业发展和政府部门政策制定的参考。

中国通信学会区块链委员会

主任委员：

2020 年 12 月

目 录

一、 研究概述

区块链(Blockchain)是分布式数据存储、 点对点传输、共识机制、加密算法等计算机技术的新型应用模式。

自 2008 年区块链技术诞生以来，已走过 12 个年头。2016 年，国务院发布《“十三五”国家信息化规划》首次将区块链纳入新技术范畴并作前沿布局，标志着我国开始推动区块链技术和应用发展。2020 年，区块链技术作为新一代的信息技术，上升为中国的国家战略。中国通信学会是中国通信界学术交流的主渠道、科学普及的主力军、国际民间科学技术交流的主要代表，是全国通信科技工作者之家，站在当前时间节点，十分有必要研究区块链的发展现状，并对未来发展趋势给出建议。

二、 全球发展态势

目前，区块链技术应用已延伸到数字金融、物联网、智能制造、供应链管理、数字资产交易等多个领域，全球主要国家都在加快布局区块链技术发展，各国的政府及监管机构对区块链技术及其研发应用的态度逐渐从观望转向鼓励，并且积极进行了更多的尝试。

(一) 政策方面

2016 年 1 月 19 日，英国政府发布《分布式账本技术：超越区块链》白皮书，积极探索区块链未来在减少金融诈骗、降低交易成本的潜力；2016 年 6 月，新加坡金融管理局推出“沙盒计划”(Sandbox)，在可控范围内允许金融科技公司测试基于区块链等技术的创新金融产品；2017 年 4 月 1 日，日本正式实施《支付服务法案》，承认比特

币的合法地位；2018 年，美国各州政府也采取措施学习与探索区块链技术，并尝试通过区块链提高政府工作的透明度和效率，美国国会、商务部国家标准和技术研究院（NIST）等部门先后发布了《2018 年联合经济报告》《区块链：背景和政策问题》《区块链和在政府应用中的适用性》《区块链技术概述》等报告，初步阐明了美国政府的监管和发展思路；2018 年 6 月，日本推出了沙盒制度，以加快推出新的商业模式和创新技术，如区块链、人工智能和物联网；2018 年 12 月，欧洲议会呼吁采取措施促进贸易和商业区块链的采用；2019 年 1 月，韩国政府将区块链技术纳入其“研究与开发税收减免的 16 个领域”之一，以促进其创新；2019 年 7 月，美国参议院商业、科学和运输委员会批准了《区块链促进法案》；2020 年以来，新加坡出台新法案允许全球加密公司在新加坡当地扩展业务；2020 年 3 月，日本金融监管机构宣布启动其全球区块链治理倡议网络，旨在促进“区块链社区的可持续发展”。

(二) 实际应用开展方面

在面向货币的区块链应用场景中，数字货币三强格局初具雏形。Facebook 2019 年 5 月发布 Libra 白皮书以来，全球数字货币出现加速发展趋势。目前逐渐形成 1）美国企业 Facebook 主导的 Libra，2）中国人民银行牵头的 DC/EP(Digital Currency Electronic Payment)，3）瑞典、法国等欧洲各国央行推动的 CBDC 的三强格局。

纵观全球应用趋势，区块链已经从金融应用全面迈向了全行业应用。2019 年 9 月 18 日，德国经济与能源部和财政部联合发布了《德

国国家区块链战略》（Blockchain-Strategie der Bundesregierung），全面推进区块链在能源、物流和供应链、医疗保健、教育/培训证书的验证等场景的应用。2019 年 10 月 8 日，欧盟委员会联合研究中心（Joint Research Centre, JRC）发布报告——《区块链的当下和未来：评估分布式账本技术的多维影响》，深入分析了分布式账本技术对多个应用领域所带来的机会和挑战。美国国土安全部（Department of Homeland Security，DHS）一直在探索区块链和分布式账本技术的应用，DHS 科学技术局设立了区块链项目，资助区块链安全性、隐私、互操作性和标准等方面的研发工作。DHS 科学技术局也在致力于将区块链整合到 DHS 下属的美国海关边境保护局、公民移民服务局以及运输安全管理局等机构的任务中。例如，2019 年 11 月，DHS 科学技术局资助 Mavennet 公司 182,700 美元，用于在海关边境保护局中使用区块链进行跨境石油进口跟踪。美国能源部（Department of Energy，DOE）通过支持的区块链研发项目促进区块链在能源行业的应用。2019 年，DOE 主要支持的项目有：1）资助佛罗里达国际大学集成区块链和机器学习技术研发新型平台，用于化石燃料发电网络中的安全数据记录和处理（40 万美元）；2）资助欧道明大学开发基于区块链的平台，用于保护化石燃料发电网络传感器身份管理和数据流安全（40 万美元）；3）资助北达科他大学建立基于区块链的化石燃料发电网络安全保护系统（39.9778 万美元）；4）资助小企业开展“用于基础设施保护的区块链安全结构”项目。DOE 的基础能源科学办公室、地热技术办公室、化石能源办公室和电力办公室均已经开展了区块链的研发部署，

研发支持领域主要集中于利用区块链保护基础设施安全等。美国国家科学基金会（National Science Foundation，NSF）在制造、环保、医疗、交通、能源等领域通过项目资助推进区块链在各行业的广泛应用。

(三) 标准和体系建设方面

在标准体系的建设上，为确保区块链生态系统不会因为标准的不同而产生分裂，很多国际标准开发组织都在积极布局和开发区块链相关的国际标准。国际标准化组织（International Organization for Standardization，ISO）于 2016 年设立了 TC307 技术委员会，开始定义区块链参考架构、分类和本体。制定标准的过程最初由澳大利亚发起。截至目前为止，TC307 技术委员会已经有 35 个成员国（P 成员）、13 个观察成员国（O 成员），公开发布了 1 个区块链领域标准，另有 10 个标准正在制定中。电气电子工程师学会（Institute of Electrical and Electronics Engineers，IEEE）作为在 160 多个国家拥有 42 万多名会员的全球最大的专业组织，于 2018 年启动了 IEEE 区块链计划（IEEE Blockchain Initiative）和设立了 IEEE 消费电子协会区块链标准委员会（IEEE Consumer Electronics Society Blockchain Standards Committee）。截至目前为止，在区块链领域，IEEE 共公开发布了 3 个正式标准，1 个标准草案，另有 52 个标准正在制定中。与此同时，美国的一些政府部门和行业协会也致力于解决行业内的操作和标准问题，DHS 正在探索在海关与边境保护等业内实施区块链的最佳实践以及全球可用的规范；认证标准委员会 X9 区块链研究小组正在开发美国区块链技术的通用术语；区块链货运联盟 BiTA 正在促进区块链在运输和物

流行业的应用，并希望在这些领域建立全行业的区块链使用标准。全球金融区块链联盟 R3 意在通过行业内标准的确立，打造良好的生态系统。

(四) 全球区块链技术应用发展主要趋势

归纳目前全球的区块链技术应用发展主要呈现以下三个趋势：

（1）区块链技术融合正在持续推进

区块链技术在落地过程中通过与应用的不断碰撞，其核心技术共识算法、智能合约设计及分析、可监管匿名隐私保护等也在不断地发展和完善，以便在进一步赋能应用的同时，降低应用研发成本，加快区块链与应用融合速度。与此同时，人工智能与区块链技术的结合可实现区块链智能合约业务的自动验证，大数据与区块链技术的结合可实现区块链数据的有效利用和可视化呈现，物联网技术与区块链技术的结合可实现区块链虚实世界的有效结合，区块链技术与多种前沿技术的深度融合，共同推进着集成创新和应用融合。

（2）区块链信任基础设施建设正在规划起步

区块链技术的发展重在建立可信的区块链基础设施，用以承载不同的区块链应用，对上层业务系统提供重要决策、可信验证和关键数据不可篡改存储服务。目前，各行业联盟和地方政府正在积极规划筹建行业或者地区联盟链基础设施，通过各个核心机构搭建区块链节点，共同组建区块链信任网络，继而各节点通过运行智能合约实现对上层业务的可信决策，通过管理和维护链式账本实现数据的不可篡改存证。

（3）区块链应用试点正在蓬勃发展

区块链技术在促进数据共享、优化业务流程、降低运营成本、提升协同效率、建设可信体系等方面具有重要作用。目前，区块链技术在金融管理、工业制造、食品溯源、医疗健康、社会公益等方面已经落地相关应用案例，基于区块链技术的新型数字经济模式正在持续推进构建，并将区块链底层技术服务和新型智慧城市建设结合，探索区块链技术在信息基础设施、智慧交通、能源电力等领域的应用示范，提升城市管理的智能化、精准化水平。

三、 我国发展现状

我国政府从2013年开始出台对于虚拟货币的监管政策，2013年12月，中国人民银行、工业和信息化部、中国银行业监督管理委员会等发布的《关于防范比特币风险的通知》表示，要加强比特币互联网站的管理，防范比特币可能产生的洗钱风险等。同时，基于区块链技术的研究逐渐开展，其底层价值逐渐释放。2016年10月，工业和信息化部发布《中国区块链技术和应用发展白皮书（2016）》。白皮书总结了国内外区块链发展现状和典型应用场景，介绍了中国区块链技术发展路线图以及未来区块链技术标准化方向和进程。2016年12月，国务院印发《“十三五”国家信息化规划》，首次将区块链技术列入国家级信息化规划内容。2019年10月24日，习近平在中央政治局第十八次集体学习时强调，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，探索“区块链+”在民生领域的运用，积极推动区块链技术在教育、就业、养老、精准脱贫、

医疗健康、商品防伪、食品安全、公益、社会救助等领域的应用，为人民群众提供更加智能、更加便捷、更加优质的公共服务。

国家各部委也在积极推进区块链的应用。2020 年上半年，国家各部委发布与区块链相关的政策共 26 项。从政策内容上看，工业和信息化部主推发展大数据、人工智能、云计算、物联网、区块链技术的融合及特色发展。农业农村部积极部署加快推进农业区块链大规模组网、链上链下数据协同等核心技术突破，加强农业区块链标准化研究，推动区块链技术在农业资源监测、质量安全溯源、农村金融保险、透明供应链等方面的创新应用。住建部、交通运输部、国家邮政局、国家能源局、商务部等部委结合自身行业特点，探索“区块链+”发展体系，推动各行业信息化和数字化发展。其中，住房和城乡建设部鼓励使用房屋交易电子合同，利用大数据、人脸识别、电子签名、区块链等技术，加快移动服务端建设，实现房屋网签备案掌上办理、不见面办理。交通运输部提出，在实现货运平台相关信息基本统计分析功能的基础上，应用大数据、云计算、区块链、人工智能等现代信息技术，通过与全国道路运输市场信用信息管理系统、部省两级网络货运信息监测系统等其他信息系统的对接和数据闭合分析，为交通运输主管部门业务办理、科学决策和研究分析提供数据支撑。国家邮政局提出要加快推动 5G、大数据、云计算、人工智能、区块链和物联网与制造业供应链的深度融合，提升基础设施、装备和作业系统的信息化、自动化和智能化水平；以及与医药行业的深度融合，加快区块链、射频识别 (RFID)、冷链空调、冷藏车辆、温湿度传感器等技术装备研发

和应用，鼓励快递企业依法取得医药仓储和医药流通资质，加速构建覆盖全国的全流程、可追溯、高时效的冷链医药物流网络。

在区块链的应用上，区块链在金融、能源、政务服务、司法、医疗健康、产品溯源、社区服务、公益、智慧城市、物流等行业全面落地实施。**金融领域**，2020 年 4 月 3 日，中国人民银行召开了 2020 年全国货币金银和安全保卫工作电视电话会议，会议强调“加强顶层设计，坚定不移推进法定数字货币研发工作”，显示出我国央行对 CBDC 投入的决心。2020 年 1 月 10 日，中国央行官方公众号表示，已经基本完成法定数字货币顶层设计、标准制定、功能研发、联调测试等工作。2020 年 4 月起，我国 DC/EP 已陆续在深圳、苏州、雄安、成都及未来的冬奥场景进行内部封闭试点测试，并且苏州尝试将部分交通补贴通过 DC/EP 的形式发放。区块链技术已在供应链金融、信贷融资、跨境支付、资产证券化、电子签章等金融细分领域得到广泛的应用。在技术方面，区块链分布式账本、块链式结构、共识机制、时间戳等技术的应用，有效提升链上信息的篡改难度和可追溯性、缓解信息不对称现象；与加密技术的结合有助于提升隐私保护力度、降低数据泄露风险；点对点网络的运用有助于实现信息并行传递、提升业务处理效率；智能合约的引入则有助于实现业务流程的自动化执行，并可用于融资、支付结算、信息存证及流通、资产证券化等场景，以增加信息可信度，缓解重复交易，提高相关参与方信息交流积极性和业务处理效率。**能源领域**，2020 年 2 月，国家能源局开展能源技术创新“十四五”规划支撑课题“‘区块链’技术在能源领域应用研究”，

探讨区块链与能源生产、交易、输送、消费、储备等领域业务的融合应用。国家电网公司建成“国网链”，探索“区块链+能源 、金融、政务”等面向社会多领域的服务新模式，已在电力交易、新能源云、安全监管、电力保险等 25 个领域落地应用。广东电网公司珠海供电局开展了基于区块链技术的绿证交易平台试点示范。南网电动汽车公司于 2020 年 1 月 31 日开出全国首份充电电费区块链电子发票。中国华能打造数字化普惠供应链金融服务平台，实现中小微供应商融资在线申请、审批、放款，解决中小企业贷款融资难等问题。中化集团完成我国首单区块链原油进口交易试点，大幅提升原油交易执行效率。2020 年 10 月 24 日，国家电网公司联合航天科技、兵器工业集团、中国石油、中国石化、华能集团等 20 余家中央企业共同发起成立了中央企业区块链合作创新平台，致力于整合中央企业技术、人才、场景等优势资源，推动关键核心技术创新，构建产业融合生态。区块链实现了从信息互联网到信任互联网的转变，将广泛应用于能源领域产业链，从而优化业务流程，降低能源运营成本，提升协同效率。**政务领域**，各地政府积极探索区块链技术与电子政务服务的场景融合，包括在行政审批、电子证照、数据共享、精准扶贫、海关贸易、城市治理、电子票据等方面的深度结合。利用区块链网络可以打破传统政务服务中的“各自为政”、“信息孤岛”等难题，深化“最多跑一次”改革，追溯数据流通过程，明晰数据权责界定，通过分布式结构降低运营成本，在信息交互过程中避免政务数据非授权访问和泄露，保障数据的安全性、真实性，协同跨部门工作、优化政务业务流程，降低跨地方、

跨部门的政务服务成本，实现政务数据的全生命周期管理，增强城市数据监督管控，提升政府管理效率。**司法领域**，2018 年 6 月，杭州互联网法院首次采纳应用区块链技术存证的电子证据，在电子存证、版权保护、立案审查等应用中，区块链技术从源头上保证上传数据的真实性，提高证据的可信度，保证区块链上电子证据的合法性和客观性。**医疗健康领域**，通过区块链技术建立互信共享机制，规范医疗行为，提升健康医疗服务效率和质量，推动健康医疗大数据应用新发展；利用匿名性、去中心化等特征保护病人隐私；推动“医联体”、“医共体”中的医疗信息互信互认，不可抵赖，患者隐私信息共享，推进医疗改革。同时，在抗“疫”过程中，区块链有助于加快公共卫生系统在紧急情况下的响应速度，防止信息造假，保持信息的透明性，保障患者隐私，结合地理位置信息快速定位感染者，加强疾病的防控效果。在药物研发过程中，利用区块链技术实现真实世界证据支持药物研发与审评的应用也在积极探索中。区块链智能合约在医疗行为的监管中也有着重大价值，出现非合规事件时，智能合约会自主跟踪合规情况、实时向相关方发送通知，有效去除检查环节，简化执行流程，降低监管成本。**产品溯源领域**，区块链技术对产品供应链的生产、运输、加工流程中的信息进行整合并写入区块链，实现了一物一码的全流程溯源，建立了对于农产品、食品、药品从生产、加工、流通到消费的全过程追溯体系。此外，利用区块链技术将乘客和司机的身份、车辆型号、行车路径、服务记录等数据记录上链，有效降低交通出行数据丢失和损坏的成本，增强参与交通管理各方之间的联系，使交通的综合

治理变得更加高效、可信。区块链技术将慈善公益活动的基础信息全部记录上链，且链上所有的信息都对全网络公开，包括每一笔款项的捐赠者、接受者、发放次数、使用方式等。任何一个环节有问题，都可以在区块链上追溯到相关责任人，消除慈善机构和捐赠人、受益人之间的信息不对称问题，从而减少纠纷，改善信任问题。

在区块链标准体系的建设上，2017 年 3 月，国家标准化管理委员会批准中国电子技术标准化研究院担任国际标准化组织（ISO） 区块链与分布式记账技术委员会（TC 307）的国内技术对口单位，加快推动我国参与区块链国际标准制定。2019 年 10 月，中国信通院、深圳税务局等联合代表中国在国际电信联盟 ITU-T SG16 Q22 会议上首次提出《基于区块链分布式账本的电子发票通用框架》标准顺利通过新标准立项。2020 年 4 月，工业部信息化和软件服务业司指导组建全国区块链和分布式记账技术标准化技术委员会。2020 年 6 月，中国通信学会区块链委员会与电气电子工程师学会（IEEE）合作，在 IEEE 消费电子协会区块链标准委员会（IEEE Consumer Technology Society (CTSoc) Blockchain Standards Committee）、IEEE 医学与生物工程协会标准委员会（IEEE Engineering in Medicine and Biology Society Standards Committee）和 IEEE 技术的社会影响协会标准委员会（IEEE Society on Social Implications of Technology Standards Committee）的联合支持下发起制定 IEEE P2677.1 等 10 项基于区块链的全方位疫情防控标准，是新冠疫情期间全球第一批立项的针对疫情防控的国际标准。也是在 2020 年 6 月，我国区块链企业“趣链科

技”在 IEEE 数字金融与经济标准委员会（IEEE Digital Finance and Economy Standards Committee）的支持下牵头发起制定《IEEE P3801 基于区块链的电子合同标准》、《IEEE P3802 基于区块链的电子商务交易证据收集应用技术规范标准》两项区块链标准，是新成立的 IEEE 数字金融与经济标准委员会立项的第一批国际标准。2020 年 6 月 12 日，IEEE 正式发布了《IEEE 2143.1-2020 加密货币支付的通用流程标准》，该标准由我国企业牵头发起，制定过程中也有多家我国企业参与，不但是 IEEE 正式发布的第一个区块链标准，同时也是全球范围内加密货币领域的第一个正式发布的国际标准。

在行业标准上，我国的区块链底层技术框架标准化工作积极有序开展，目前已经发布的团体标准包括：《区块链和分布式账本技术参考架构》、《区块链平台基础技术要求》、《区块链隐私保护规范》、《区块链智能合约实施规范》、《区块链技术安全通用规范》、《区块链跨链实施指南》、《区块链隐私计算服务指南》、《区块链基础技术规范》。各行业也制定了具体行业的标准规范，《基于区块链技术的疫情防控信息服务平台建设指南》、《金融分布式账本技术安全规范》、《区块链防伪追溯数据格式通用要求》、《基于区块链的数据资产交易实施指南》、《基于移动互联网的防伪溯源验证通用技术条件》、《区块链电子合同平台服务规范》、《区块链电子合同平台标准》、《电子商务商品交易信息区块链存取证平台服务规范》相继发布。针对区块链底层的国家标准也在进行中，包括《信息技术 区块链和分布式记账技术 智能合约实施规范》(起草阶段)、《信息技术 区块链和分布式记账技术 存

证应用指南》（起草阶段）、《信息技术 区块链和分布式账本技术 参考架构》（征求意见阶段）。同时针对区块链的性能测试、安全测试规范也已经陆续推出。

区块链技术作为一种具备革命性和基础性的创新技术，正在与人工智能、大数据、云计算、物联网等技术融合发展，相互促进，开创新的价值空间，加快新兴技术商业落地应用。当前区块链行业产业高速发展，企业数量快速增加，从设备制造到产业应用，区块链产业链条脉络逐渐明晰。而互联网巨头的涌入，也在快速推动我国区块链产业发展。目前我国区块链产业地域分布相对集中，产业集聚效应明显；区块链应用则呈现多元化，从金融领域延伸到实体领域，在各个领域通过实现“协作环节信息化”，助力实体经济降成本提效率。

区块链产业政策体系在逐步构建，产业发展环境在持续优化。主要体现在：区块链产业发展的政策体系逐步完善，各地政府正在积极从产业高度定位区块链技术；积极加强行业监管，有力防范金融风险。

当前有一种区块链发展的阻碍是来自“量子计算将颠覆区块链技术”的焦虑，“量子计算机的强大力量将很容易破解区块链系统”。面对包括量子计算在内的诸多挑战，我国北京航空航天大学牵头的研发团队已研发出新型密码算法库 SMPQLIB，这是全球首个融合国密全体系、抗量子计算密码以及隐私保护密码工具的实用算法库，属于世界领先的第四代抗量子计算安全的公钥密码体系。而且，北京航空航天大学该合作研发团队在此基础之上首创了结合区块链软硬件协同的紧耦合可信一体化技术，并用于雄安新区区块链的整体架构。

整体来看，区块链底层平台在技术上还未有较大突破，进而限制了区块链行业解决方案的落地应用，因此，当前最迫切的问题是突破区块链底层平台的技术瓶颈，并大力发展区块链行业场景落地。

四、 技术预见

随着区块链技术应用的不断深入，结合全球区块链行业趋势，我们预见区块链技术将在以下几个方面寻求突破：

(一) 区块链底层技术

TPS 指系统每秒处理的事务数，是衡量一个区块链系统性能最重要的指标之一，TPS 决定区块链系统能够承担的业务量。影响一个区块链的性能内在因素包括共识机制、数据结构、加密算法等，以及开发时区块大小和出块时间等参数设置、系统运维中的系统优化和升级等。我们关注到，目前开源区块链的 TPS 如下：

表 1 开源区块链的 TPS

区块链	管理方	单链基础 TPS(笔数)
比特币区块链	公有链	7
以太坊	公有链	20
Hyperledge Fabric	Linux 基金会	1000
Corda	R3CEV	没有全局吞吐量
金链盟 BCOS	金链盟	1000
微软 CoCo	微软	1600
Quorum	企业以太坊联盟(包括芝交所、摩根大通等)	600

随着区块链技术与物联网，5G，大数据等技术结合，高频海量数据对于区块链自身的 TPS 要求越来越高。

Hyperledge Fabric 通过使用多链多通道技术实现在业务上对数据进行分片，在解决数据隐私的同时提高系统 TPS。即将于 11 月份发布的以太坊 2.0 将共识机制从目前 1.0 的工作量证明（PoW）转变为权益证明（PoS），并结合了分片技术。根据以太坊共同创办人布特林（Vitalik Buterin）的说法，交易速度可达每秒 10 万笔（即 100,000TPS），但以太坊 2.0 的上线日期已经多次延迟，其正式上线时间仍未确定。

同时，我们关注到基于有向无环图(Directed Acyclic Graph，简称 DAG)的拓扑结构在区块链中的应用。2015 年 9 月，Sergio Demian Lerner 发表了《DagCoin: a cryptocurrency without blocks》一文，提出了 DAG-Chain 的概念，首次把 DAG 网络从区块打包这样粗粒度提升到了交易层面。2016 年 7 月，IOTA 发布，随后 ByteBall、Nano 相继发布。国内，MT 链采用基于 DAG 的 HashNet 数据结构，对 HashGraph 共识算法做了改进和提升。HashNet 共识机制性能经泰尔实验室测试，10 分片纯性能测试 TPS 超过 240 万，10 分片运行实际交易并加上签名验证 TPS 超过 10 万。DAG 是面向未来的新一代区块链，从宏观的图论拓扑模型看，从单链进化到树状和网状、从区块粒度细化到交易粒度、从单点跃迁到并发写入，是区块链从容量到速度的一次革新。哈希图（Hashgraph）是一个 2016 年提出的基于 DAG 的协议，该共识协议使用了一个基于 Gossip 的算法，可以提供可证明的拜占庭容错共识。在理想没有故障的情况下，该协议可以做到无需领导，异步且快速地建立共识。与其他协议相比，它可以以最少的通信量达到整体的排序，Hashgraph 开创性的在公链环境下做异步 BFT 共识。传统

BFT 的一大问题是消息复杂度太高，大量消耗系统的网络带宽，无法很好地应对动态网络。Hashgraph 在传统的 Gossip Protocol 中引入了虚拟投票机制，可以在需要共识时不引起突发大规模消息传递风暴。Hashgraph 成为针对可信互联网探索的一个重要里程碑，可能突破区块链局限，从创新路径实现区块链最终理想的一个有力尝试。

(二) 区块链跨链技术

随着不同特点、不同应用场景的区块链快速发展，目前尚无成熟的标准。在建设基于区块链的应用时，采用了不同技术的底层链，现存各区块链之间的数据通信、价值转移面临着因相互独立而导致价值孤岛现象。基于此需求，跨链技术逐渐发展起来。跨链技术是区块链实现互联互通、提升可扩展性的重要技术手段。它既是区块链向外拓展和连接的桥梁，也是实现价值网络的关键。

目前有代表性的跨链技术包括：

（1）Ripple 公司主导设计发起的实现跨链交易转账的互联账目协议 Interledger Protocol(ILP)；

（2)以锚定某种原链(主要是比特币区块链)为基础的新型区块链的侧链技术；

（3）为了解决转账速度慢和网络拥堵的问题而采取的链下支付技术，包括闪电网络(Lightning Network)和雷电网络(Raiden Network)。其中，闪电网络针对比特币，而雷电网络是针对以太坊。

同构跨链和异构跨链，实现了区块链之间数据共享与业务协同。跨链技术应当满足交易效率高、用户体验好、接入门槛低、交易安全

可靠、全程可跟踪；同时，跨链还应当支持除数字货币价值以外的账户和数据的跨链，以满足诸如区块链数据在价值融通时候，实现多链价值融通。

(三) 区块链链上链下数据交换技术

随着智能合约这种新的信任模式的产生，出现了一个新的技术挑战，那就是连接性。大多数有价值的智能合约应用都需要获取来自关键数据源的链下数据，特别是实时数据和 API 数据，这些数据都不保存在区块链上。由于区块链受自身特殊的共识机制限制，无法直接获取这些关键的链下数据。

由于现有区块链的共识机制及其确定性虚拟机的固有局限，目前存在两大问题，阻碍了智能合约的广泛应用和大规模去中心化商业应用的出现。

● 智能合约既不能直接引入互联网数据，也不能自发调用外部网络 API，而任何商业应用，例如保险等，都不可避免地要与现实世界交互，特别是与互联网交互。

● 实际上，在现有的智能合约平台上，例如以太坊，链上计算资源和容量都是非常昂贵且有限的。再加上执行合约的 Gas 费用、区块 Gas 限制和验证者困境等问题，会导致合约执行的可扩展性问题，使得智能合约在链上的计算无法进行，甚至不可能实现大规模矩阵乘法、AI 模型训练、3D 渲染等商业计算目标。

链上链下数据交换技术确定的在分布式环境下的预言机软件，作为可复用的，为各链上/下行数据交互提供了具体的实现，支持的

HTTPS、基于 TLS 的自定义协议，gRPC 接口、FTPS 等功能，为现有的业务系统的数据上链以及获取链上的数据提供了具体方法。支持的现行非可信环境的增强，以及对于信创平台的支持，为构建数据协同业务提供了满足安全等级保护需求的系统平台，数据安全以及数据治理方案对于形成数据的可信可靠的多方审计提供了基础平台。

链上链下数据交换技术应当遵循 CIA 原则，即保密性(Confidentiality)、真实完整性(Integrity)、可获得性(Availability)。

五、 工程难题

(一) 如何安全使用区块链技术的工程难题

1. 基于新型数据结构的可控高性能区块链基础平台关键技术

研究基于有向无环图的支撑大规模高频次交易的共识算法、通信协议和分布式高可信存储机制等关键技术；研究区块链高扩展分片及多链技术，提升区块链可扩展性；研究账户身份、交易数据、内容数据分离及数据隐私保护技术；研究跨链技术，实现不同链之间的无缝连接和高互操作性；研究声明式和图灵完备智能合约技术，实现业务和流程的自动化处理；构建可支撑数据获取传递分析处理、数据隐蔽传输、数据隐私保护、数据高可信存储共享等多应用场景业务生态的区块链技术平台，开展典型示范应用。

2. 支持异构多链互通的新型跨链体系关键技术

针对网络空间日益显现的跨链数据（价值）流通需求，研究新型跨链体系，构建横纵贯通、覆盖网络空间的价值互联网。具体包括：研究新型区块链跨链架构，支持多条同构（异构）区块链间的数据（资

产）流通与合约调用；研究应用层跨链互操作、链间跨链互操作、链下数据跨链互操作机制；设计跨链架构编程接口，屏蔽底层各条区块链的技术细节，支持开发人员快速构建跨链应用；研究安全高效的跨链数据传输与验证机制，定义跨链数据的格式规范，保证数据在区块链间的可信传递；研究跨链事务处理机制，设计无单点依赖的跨链数据（资产）流通与合约调用协议，保证在异常情况下数据（资产）流通与合约调用的原子性；研究跨链治理机制，设计跨链体系准入机制、权限机制、奖惩机制与监管审计方案；对跨链体系进行安全性分析，研究针对该体系的各类攻击及其防范措施；在网络空间对抗等场景下开展试验测试。

3. 基于区块链的国家关键基础设施人机物多域智能对抗技术

面向国家关键基础设施的社会、信息、物理融合特点，开展人机物融合的多域智能对抗技术研究，针对机器学习技术和区块链技术的脆弱性，形成人机物多域的智能对抗模型；面向国家关键基础设施各使用环节，研究工业控制系统的恶意数据注入与远程操纵方法；针对关键基础设施的智能感知、智能控制、现有安全检测系统的机器学习方法和大数据利用机理的脆弱性，研究对抗样本的生成方法和深度神经网络应用系统的操纵技术；针对基于区块链的关键基础设施智能合约应用的脆弱性，研究女巫攻击、DDoS 攻击、Eclipse 攻击等威胁模型和特定方法；面向关键基础设施控制环路的人在环口（to the loop）、人在环上（on the loop）、人在环内（in the loop）的三个脆弱性入口，研究新型的社会网络工程模型、人员辅助自动控制系统的新型威胁模

型、以人为主决策控制系统的人员操纵模型以及针对关键基础设施操作员的非理性博弈对抗机理与致胜机制。

4. 区块链软硬件协同可信一体化技术

针对区块链的快速部署和接入需求、数据隔离的安全需求以及运行环境的自主可控需求，研究基于可信环境的区块链可信一体机技术，支持以可信一体机为载体的一站式节点创建、节点组网；研究区块链技术的可信执行环境，构建融合可信硬件基础设施、可信操作系统以及可信区块链软件的可信链体系，保障执行环境的全程可信化；研究区块链软硬件一体化协同和适配技术，构建可信硬件基础设施、可信操作系统以及可信区块链软件的紧耦合架构，实现三者的一体化强绑定机制；基于身份即标识的密码系统构建区块链一体化管理平台，实现对可信硬件基础设施、可信操作系统以及可信区块链软件的统一管理。

5. 区块链底层关键密码技术

密码算法是区块链的底层技术，区块链系统中使用的密码算法决定了系统的安全强度与效率，使用的密码技术决定了区块链的安全与隐私功能。基于国密算法的密码自主可控体系：通过核心密码部件复用的模式，形成模块化、可插拔、可复用的细颗粒度密码算法可重构模型，构建融合国际密码算法标准的多模式综合密码基础库。通过基于格理论构建适配区块链公钥和签名体系需求的新型账户公钥密码与签名体系，构建应对量子计算机与量子算法的威胁的账户与交易安全防御机制；研究适用于区块链的新型公钥密码算法：随着区块链系

统的不断演化，新型公钥密码算法在区块链系统中展示了日益重要的作用。针对不同类型的区块链系统，应用和发掘新型公钥密码算法，并将其与不同场景相结合，设计并证明所得的区块链系统的安全属性。

(二) 如何感知区块链应用

1. 公有链安全监测及溯源服务关键技术研究

针对现有公有链种类多样、监测溯源复杂的问题，构建公有链通用监测及溯源服务模型，研究公有链监测分析维度；针对公有链网络拓扑复杂、网络节点探测难的问题，研究公有链网络拓扑分析技术，构建公有链网络拓扑分析方法；针对公有链自组织、分布式，网络协议加密混淆的问题，研究网络加密数据流量精细化分类技术，研究区块链网络协议、节点服务识别与监测方法；针对公有链节点动态变化难以全面有效监测的问题，研究公有链网络行为分析和异常行为监测技术；针对公有链交易匿名隐私保护强、难溯源的问题，研究公有链交易溯源及身份识别分析方法，设计匿名实体特征集关联及聚合方法；针对公有链业务种类多样、监测分析预警难的问题，研究公有链业务分析及预警方法、区块数据异常监测技术，设计多类型用户的交易模式特征提取技术。

2. 联盟链监管关键技术

面向联盟链的监管需求，以安全多方计算、零知识证明和跨链技术为基础，以隐私保护为前提，研究面向联盟链的分布式、穿透式全维度监管技术体系架构；研究智能合约的数据痕迹追踪技术，实现智能合约数据与区块链交易关联关系分析，实现智能合约内容的安全验

证；研究基于多方门限签名的分布式链上监管决策体系，实现对链上违法违规信息的取证、认定与处理；研究多方隐私交易技术，实现对监管方友好并兼顾隐私保护的区块链账本交易技术；研究新型区块结构，实现异构联盟链自适应监管技术，根据不同区块结构，自适应调整数据检测与数据屏蔽算法策略；研究新型区块结构，在区块内容不被篡改、可追溯、可复原的前提下，实现关键信息的智能屏蔽。

3. 以链治链监管架构与关键技术研究

针对区块链目前的发展趋势和面临的监管挑战，研究区块链“以链治链”监管体系架构和关键技术；研究区块链平台的安全测评方法和介入标准，评估接入链的安全强度和准入许可；研究跨链监管体系设计，包括跨链监管的安全需求、安全机制和跨监管机构协同技术等；研究支持“以链治链”监管架构的共性关键技术，包括跨链监管技术、分布式监管机制、节点权限分级机制和智能合约自动化监管技术等；研究支持“以链治链”监管架构的核心算法，包括监管链的共识算法、密态内容审计方法、匿名可追踪方法、链上数据的受限回滚和可信擦除的证明等；研究监管链与接入链的一致性要求，包括接入链信息巡查、数据处理结果的正确性和完整性证明等。

4. 区块链系统脆弱性分析关键技术

针对关键性系统中，应用区块链技术的安全风险，从区块链本身的系统架构安全、通信协议与共识算法安全以及其上运行的应用安全等多个角度，结合密码学、网络通信和软件开发等相关技术，展开研究；针对各种区块链的核心代码程序（包括公有链和联盟链），研究

和衡量各个系统的脆弱性和安全性，并深入进行漏洞挖掘；针对多种区块链平台的周边工具（例如钱包），研究分析其中可能存在的安全漏洞，评测安全风险；研究针对区块链网络通信协议层次的攻击（例如日蚀攻击）和防护机制；研究分析多种区块链（包括公有链和联盟链）的共识算法所存在的协议漏洞和防护机制；研究分析运行于各类区块链平台（公有链的以太坊、联盟链的 Fabric 等）上的智能合约可能存在的安全漏洞，评估安全风险，总结漏洞类型和防范方法；研究目前智能合约获取链外数据的方案，分析其中所存在的安全风险，给出评价指标，并研究降低风险的方案。

5. 基于区块链的隐私保护和数据共享关键技术

针对链上数据共享和隐私保护协同问题，突破多用户的公钥密文搜索技术，搭建基于区块链的多关键字隐私保护搜索平台，实现安全的复杂逻辑组合的关键字检索，提升了密文处理下在区块链环境中的数据共享和隐私保护能力。设计支持复杂逻辑的多关键字检索方案。面向军事数据共享检索颗粒粗的问题，结合多关键字检索和公钥加密技术，实现细粒度检索；面向共享过程不可信的问题，结合零知识证明和区块链技术，实现检索结果可验证，实现多关键字可信检索和共享的可信性。

六、 政策建议

（1）培育自主可控区块链系统，确立区块链生态优势。区块链有机会成为未来的商业基础设施。我国需大力推动自主可控的区块链系统研发，进行核心技术攻关，促进区块链开源社区建设，丰富国产

区块链应用生态，占据创新制高点，取得产业新优势。

（2）平衡各方利益，推动产业改革。当前，联盟区块链虽然在各产业中均有一定应用，但距离取代原有商业模式仍有巨大距离。究其原因，很大程度上是产业中的既得利益者不愿参与，因为区块链所代表的分布式商业模式将减少寡头和中介的既得利益。可以考虑从政府的角度扶持成立产业联盟，促进新商业模式的落地，政府牵头平衡各方利益，从而推动产业改革。

（3）鼓励开源社区，促进技术发展。开放源代码是技术发展的重要手段，当前国内区块链技术产品虽然有一部分进行了开源，但是仍有较大的开放空间。大量的闭源软件限制了技术的发展及创新的速度。国家可鼓励区块链开源社区的发展，如向开源社区提供经费支持、鼓励开源社区交流活动等，促进区块链技术的开源和创新。

（4）加强监管力度，防范金融风险。区块链技术与数字货币等新兴技术需要监管力量来引导其发展。一是引入多方力量共同参与区块链监管技术的研发，改进面向区块链技术的各类监管手段与技术。二是严厉打击披着区块链“外衣”的各类骗局，虽然首次代币融资（ICO）、加密货币交易所等在中国境内已经被禁止，但在社会上仍有许多打着区块链旗号的融资项目，其中不乏庞氏骗局、蜜罐骗局等，这些骗局严重影响了人民的财产安全和区块链技术的健康发展。三是提前预防 Libra 等超主权货币对我国货币政策和支付体系的冲击，做好提前布局。

（5）协调法规标准，建设符合国情的区块链系统。区块链技术

具有永久记录的特性，这与我国现行法律中信息保护的“被遗忘权”相抵触；而现有的金融法律法规，也无法适用于区块链为基础的分布式商业上的金融行为。因此，还需从国家现有国情出发，协调各项政策法规、行业和技术标准与区块链之间的矛盾，保障民众权益的同时促进区块链技术合理发展。

（6）设立专项资金，促进区块链基础理论与核心技术研发。当前各地纷纷出台区块链扶持政策，大部分是从企业角度对各类区块链初创公司进行激励、补贴。但是我国目前区块链技术的基础理论研究及关键技术研究仍然较薄弱，需要重点突破。可考虑围绕区块链关键技术与应用，通过设立应急科学研究项目、重点项目群或重大研究计划项目等方式支持区块链基础理论和关键技术的突破，促进产学研协同健康发展。

（7）加快人才储备，加速专利布局。目前区块链人才市场存在严重的供不应求情况，国家可鼓励和支持高校设置区块链相关专业与课程，加快培养区块链专业人才。推动国内重点培训机构，加强与重点企业合作，积极培训区块链技术开发人才。我国已成为全球区块链专利数量最多的国家，可进一步引导和拓展各个行业领域的区块链专利布局。还需考虑加强区块链技术与既有产品与服务的融合创新，提升区块链专利质量，积极推动我国自主创新的区块链技术和产品走出去。

中国通信学会

地址：北京市海淀区万寿路 27 号院 8 号楼

邮政编码：100840

联系电话：010-68203021、68203019

传真：010-68203004

网址：https://www.china-cic.cn/