上海市科学技术委员会

沪科〔2023〕292 号

关于印发《上海区块链关键技术攻关专项行动方案（2023-2025 年）》的通知

各有关单位:

经市政府同意，现将《上海区块链关键技术攻关专项行动方案（2023-2025 年）》印发给你们，请认真推进落实。

特此通知。

上海市科学技术委员会

2023 年 9 月 26 日

（此件主动公开）

上海区块链关键技术攻关专项行动方案

（2023-2025 年）

区块链技术迅速发展，正在深刻改变生产关系，重构社会信用体系，成为新科技革命和产业变革的重要驱动力，推动数字信任基础设施的构建。根据《上海市建设具有全球影响力的科技创新中心“十四五”规划》，为扎实有序推进本市区块链领域关键技术突破，特制定本行动方案。

一、总体思路和主要目标

贯彻落实市委、市政府对区块链领域创新发展工作的决策部署，抢抓数字信任基础设施和 Web3.0 发展战略机遇，坚持系统布局、体系推进、市场驱动、场景牵引，统筹发展与安全，以适度超前探索建立新一代开放许可链技术体系为主线，以区块链新型体系架构、资源调度与管控、信任增强为主攻方向，以自主创新与开放协同为推进路径，建设新型研发机构，组织本市骨干型企业、高水平科研型高校和研究机构等开展有组织科研，强化产学研协同攻关，为市级区块链基础服务平台建设以及政务、跨境贸易、供应链、金融、元宇宙、数据要素流通等关键领域打造超级节点提供技术支撑。

到 2025 年，在区块链体系安全、密码算法等基础理论以及区块链专用处理器、智能合约、跨链、新型存储、隐私计算、监管等技术领域，加快实现创新突破，形成可支撑 Web3.0 创新应

用发展、可管可控、开源开放的新一代开放许可链技术体系与标准规范，为构建数字经济可信安全技术底座、培育具有全球影响力的新一代区块链创新生态奠定基础。

二、主攻方向

行动方案聚焦新型体系架构、资源调度与管控、信任增强三大主攻方向开展有组织攻关，推进区块链系统性能增强、开发运行环境优化、服务支撑能力提升，支撑新一代开放许可链技术体系构建。

（一）主攻方向一：新型体系架构

支持区块链体系安全的前沿理论研究。重点在基础软硬件技术领域，研发支持交易处理加速、密钥安全、密态计算的安全计算芯片、专用加速芯片等，达到国际先进水平；攻关广域网高鲁棒传输技术，设计面向大规模应用的高性能路由算法，实现广域网高性能、高稳定性、低延时通信，增强业务网络的通用承载能力；研究形成激励相容的经济模型，支撑区块链生态资源的合理分配和系统的稳定运行，实现原创性理论模型的突破。设计体系安全、开放、高效、可扩展、监管友好的新型区块链系统架构，构建支撑大规模应用的开放许可链网，在国际电信联盟（ITU）、电气与电子工程师协会（IEEE）等主流国际标准中实现自主技术的实质性占位。

（二）主攻方向二：资源调度与管控

重点在资源调度领域，研发异构区块链底层系统资源通用抽象模型以及存储访问、隐私保护、权限管理、合约升级、调试环境等通用中间件，实现区块链应用的模块化设计和低代码开发，

加速区块链应用生态繁荣发展。在安全监管领域，开展链上行为分析、内容管控等关键技术研究，实现区块链信息的高效分析、实时监测和有效管控，形成链上违规内容检测和管控的闭环机制，相关技术达到国际先进水平，为区块链风险预警和行为监管提供有力支撑。

（三）主攻方向三：信任增强

重点攻关隐私计算技术，研发新型协议，突破隐私计算通讯效率瓶颈，降低隐私计算开销，实现抗量子的可证明安全。推进多方安全计算与可信执行环境等技术交叉融合，开发国际先进的多技术路线融合解决方案，为区块链提供隐私保护能力，进一步提升区块链在数据流通、数字资产交易等方面的应用支撑能力，推动相关跨境应用试点。

三、重点任务

（一）基础软硬件技术突破

面向区块链系统安全高速的交易处理、广域网大规模部署的发展需求，重点攻关安全计算芯片、广域网高鲁棒传输等关键技术，推动虚拟机与执行引擎、零知识证明、同态加密、后量子密码等理论与技术创新，促进区块链基础软硬件技术达到国际领先水平。

1. 安全计算芯片。研发支持区块链智能合约、交易处理以及全同态等算法硬件加速的异构融合计算芯片，研究区块链应用下的密态计算、密钥托管等标准，推动区块链数据隐私保护标准与链下安全计算规范以及全同态、零知识证明等核心算子硬件加速芯片方案的落地应用。到 2025 年，加密芯片对称加解密支持不

低于 100 千兆比特每秒（100Gbps）；非对称密码签名不低于 30 万次每秒，验签不低于 10 万次每秒；全同态基础密文计算（如同态密文加法、同态密文乘法）与现有国际最高水平的开源同态加密算法库相比加速百倍以上。

2. 广域网高鲁棒传输。针对大规模区块链节点、多方数据协作节点通信效率低、稳定性差，且难以支撑工业级生产应用的问题，推进广域低延迟通信骨干网技术研究，研发高性能、高可靠、可运维、可升级、兼容现有对等网络（P2P）系统的应用层消息路由网络，定义去中心化应用路由消息传输协议，结合传输协议优化、节点路由表和多路路由，实现高性能通信。到 2025 年，在城域网部署条件下，区块链消息传输端到端时延小于 500 毫秒；在 5000 个节点全球部署环境下，95%以上的区块链消息在 15 秒内传播至 95%的节点。

3. 虚拟机与执行引擎。面向虚拟机计算性能提升、多编程语言支持等方面的需求，研究单虚拟机合约高性能执行技术与即时编译技术，并形成开发工具。到 2025 年，区块链虚拟机具备即时编译能力，计算性能不低于 1000 万指令/秒，支持主流编程语言，支持独立于链平台的模拟执行、调试及性能采样等功能。

4. 零知识证明。面向提升零知识证明效率和易用性的需求，结合业界已有的零知识以太坊虚拟机（zk-EVM）等技术，通过设计新型协议、针对高级语言的高效编译工具，提升通用零知识证明协议的性能。到 2025 年，零知识证明算法证明生成效率较国际同类协议（Plonk 等）提升 2 倍。

5. 同态加密。面向提升同态加密算法效率和功能的需求，研

究同态计算结果的高效可验证技术，并结合硬件加速，突破计算性能瓶颈。到 2025 年，结合硬件加速，针对特定应用场景，全同态密文计算开销减少至明文计算 2 个数量级以内。

6. 后量子密码。研究区块链底层算法从经典密码向后量子密码的平稳过渡方案。到 2025 年，完成后量子密码签名算法设计，基于格的后量子数字签名算法的签名和公钥尺寸相较于 Dilithium 等算法标准缩小 10%，签名时间缩短 10-20%；基于哈希的后量子签名算法的签名尺寸和签名时间相较于 SPHINCS+等算法标准缩短 8-10%。面向量子计算机对密钥管理系统的威胁，设计量子安全的分布式密钥管理系统。形成区块链中现有公钥密码技术向后量子密码技术安全迁移的解决方案。

（二）体系架构技术创新

面向区块链体系架构创新与体系安全要求，重点攻关多链组网架构、治理与经济模型等关键技术，推动扩展分片、安全合约语言、编译器和工具、链数据存储、分布式可验证存储、密态数据库、共识机制等技术创新，促进新一代开放许可链技术体系构建。

1. 多链组网架构。研究区块提案-构建分离、数据-执行层共识解耦、模块化可插拔共识、多链协同与自适应组网等关键技术，实现不同区块链网络之间的数据和资产互操作，形成开放、高效、可扩展、监管友好的多区块链系统架构，推进相关规范与标准研究，构建可支撑大规模应用的开放许可链网。到 2025 年，形成多链组网协议以及统一的多共识层网络框架，构建开放许可链网，支持子网快速接入。

2. 治理与经济模型。研究基于博弈论的高效治理、经济激励、作恶发现、自动惩罚、自适应拍卖等关键技术，形成激励相容的经济模型，支撑区块链生态资源的合理分配和系统的稳定运行。到 2025 年，形成高效的治理工具集，包含社区构建、提案发起、治理投票、提案确认等功能，设计应用 5 种以上的标准治理方案，提高治理效率和多样性。

3. 扩展分片。面向区块链系统支持扩展分片的需求，研究自适应的动态分片策略、跨片交易验证、动态组网、交易分片的数据模型、网络分片协议等技术，实现高性能的链上扩容，支持动态、混合、可扩展的组网级联模式，形成大规模组网能力，提高数据存储效率和访问性能。到 2025 年，分片数量不低于 100 个，数据处理能力随分片数量线性扩展，并保证数据在分片传输、处理、存储等环节的安全性。

4. 安全合约语言。研究区块链智能合约虚拟机环境的编程语言设计理论体系。到 2025 年，设计形成一套安全、高效的新型智能合约语言并完成原型验证。

5. 编译器和工具。开发智能合约编辑、合约编译、开发环境、合约部署、合约调试等智能合约工具，推进智能合约开发者社区建设。到 2025 年，形成一套完备的智能合约开发、部署、调试工具，提升区块链智能合约开发效率，降低部署成本。

6. 链数据存储。研究链存储存储结构、数据同步机制等关键技术，提升链数据存储容量上限，提高链数据存储和查询效率及扩展性。到 2025 年，实现单节点存储容量达到拍字节（PB）级，单个区块大小达到吉字节（GB）级，单笔交易大小达到 100 兆字

节（MB）级，支持每秒不低于十万笔的交易处理。

7. 分布式可验证存储。研究数据可靠性和一致性检测、高效数据索引、动态存储调度、分布式存储激励机制等分布式可验证存储关键技术。到 2025 年，实现支持不少于 1000 个节点组网的大规模分布式可验证存储系统，支持存储规模随节点数量线性扩展，链上智能合约对分布式存储数据的读写能力达到每秒 2 万条以上。

8. 密态数据库。面向区块链系统数据安全的需求，研究高效加密算法、数据库访问控制、密文数据检索计算等技术，提高数据的多维度安全保护和访问效率。到 2025 年，密态数据库支持灵活的策略设置和用户访问权限管理，支持拍字节（PB）级别的数据存储和处理。

9. 共识机制。研究共识容错、节点动态变更、节点签名、通讯拓扑、并行处理、流水线处理、容错恢复、可验证随机数等技术，构建高效、安全、抗量子攻击的共识算法，解决区块共识性能随着节点数量增加而下降的难题。到 2025 年，基于标准密码假设，设计形成新型高性能共识机制，可保证在不超过 1/3 节点被攻击控制条件下的一致性和可用性，且共识决策达到 100%的最终性，在 1000 个广域网节点组成的区块链网络中实现 10 兆比特每秒（10Mbps）以上的吞吐率。

（三）资源调度技术攻关

面向区块链底层系统支撑应用生态发展的需求，重点攻关区块链系统抽象模型与中间件等关键技术，推动资源调度、跨链互操作、可信数据上链等技术创新，促进结构化、可扩展性强、可

靠性高的区块链资源调度平台构建。

1. 抽象模型与中间件。研究区块链底层系统资源通用抽象模型理论，研发存储访问、隐私防护、权限管理、合约升级、调试环境等通用中间件，完善区块链系统应用接口、链上域名解析等标准规范。到 2025 年，研发不少于 10 种区块链基础组件和开发工具，适配不少于 5 种异构底层区块链系统，实现区块链应用的模块化设计和低代码开发。

2. 资源调度。面向区块链应用快速适配、异构系统资源便捷调用的需求，研究异构区块链系统适配与封装、底层链计算/存储资源的动态管理调度、链上资源定位解析、跨链协同调度等关键技术，建立跨区块链系统的协作与资源调度机制。到 2025 年，适配不少于 5 种异构底层区块链系统与存储系统，实现区块链应用对底层系统资源的高效调用，并支持区块链应用的可迁移部署。

3. 跨链互操作。面向不同区块链系统间信息共享、协作互通的需求，研究跨链安全模型、跨链通信与互操作协议、基于可信执行环境的跨链网关、基于密码学方案（包括零知识证明、多方安全计算等）的跨链桥等关键技术。到 2025 年，实现异构区块链的跨链通信和互操作，支持无需信任假设的链上验证跨链模式，适配不少于 5 种异构底层区块链系统，跨链合约调用吞吐率不低于 10000 笔交易每秒（10000TPS）。

4. 可信数据上链。面向链上与链下的数据互联互通需求，开展可信物联网终端、分布式预言机、数据可靠性验证模型等关键技术研究，实现区块链与链外系统、物联网设备之间的信息互联互通。到 2025 年，研发支持多类型终端设备和万级组网规模的

物联网设备区块链模组，兆字节（MB）级可信数据上链过程不超过 500 毫秒（500ms），构建验证准确率不低于 90%、验证时间小于 1 秒的数据可信性评估模型。

（四）安全管控技术研究

面向区块链系统与应用生态安全发展的需求，重点攻关区块链链上行为分析、内容监管等关键技术，推动形式化验证、漏洞挖掘等技术创新，促进区块链管控技术发展。

1. 链上行为分析。针对区块链去中心化维护和交易自动化处理的特点，研究链上公开数据采集和索引、交易关联性分析、细粒度地址聚类、真实世界数据标签采集、交易风险分析模型等关键技术，构建链上活动监管分析、区块链应用合规监管框架。到 2025 年，研发区块链交易审计系统、交易追溯分析系统、风险动态监控预警系统等新型监管工具，支持不少于 3 种异构的区块链系统，地址标签/交易关联性分析准确率达到 99%以上，实时识别不少于 10 种异常行为。

2. 内容管控。针对去中心化区块链系统无前置审核的特点，研究可监管共识与治理架构、链上关键词过滤、图片文字提取等关键技术，实现区块链多模态内容传播的管控。到 2025 年，研发区块链内容管控系统，实现对内容查阅频次的统计、对敏感内容的识别与屏蔽、对异常地址的行为与资金流向的追踪，支持不少于 3 种异构的区块链系统，不少于 3 种模态的数据识别，敏感信息识别率达到 99%以上，信息识别吞吐率不低于 5 万条每秒。

3. 形式化验证。面向区块链系统可证明安全性的需求，研究面向密码学代数理论的程序验证、基于密码学假设的编译正确性

验证、快速迭代程序的验证机制等关键技术，研发形式化验证算法库与工具。到 2025 年，形成轻量级的形式化验证工具，验证代价降低到 1:12 以下，支持对密码算法库的验证，形成安全、高效的基础算法和组件库。

4. 漏洞挖掘。面向区块链应用漏洞快速发现的需求，研究智能合约代码漏洞挖掘和自动化修复等关键技术，研发具备多种漏洞挖掘与修复功能的智能合约安全工具。到 2025 年，工具支持不少于 15 种漏洞类型的自动检测和不低于 90%的修复率，实现对智能合约应用的自动检测。

（五）信任增强技术突破

围绕数字身份安全和数据资产交易流通技术要求，重点攻关隐私计算等关键技术，推动基于区块链的可信身份、可验证计算等技术创新，进一步提升区块链作为信任基础设施在数据流通、数字资产交易等方面的应用支撑能力，推动相关跨境应用试点。

1. 分布式数字身份。面向用户对数字身份安全、隐私保护、互认互通的需求，研究分布式数字身份（DID）模型，研制集数字身份认证、使用与管理的区块链数字身份终端，开发数字身份应用系统，解决跨域身份互认互通难的问题。到 2025 年，区块链分布式数字身份终端，支持 SM4 与 AES 等对称加密算法，支持 SM2 与 ECC-secp256k1、Ed25519 等非对称加密算法，支持 SM3 与 SHA256、SHA512 等主流哈希密码算法，支持用户友好型多方密钥管理与恢复等功能。完成数字身份应用系统开发，实现分布式数字身份的自主创建与管理，支持千万级用户规模，身份验证时间不超过 500 毫秒。

2. 隐私计算。针对现有隐私计算技术效率和安全性难以适应区块链应用场景需求的问题，研究新型多方安全计算协议，突破通信效率瓶颈，提升计算效率，并实现抗量子的可证明安全。研究可信执行环境的机密计算技术。研究多方安全计算、可信执行环境、联邦学习等技术的交叉融合，形成多技术路线融合的解决方案。到 2025 年，设计出不少于 3 种恶意敌手模型下的高效率多方安全计算协议，相比国际/国内同类协议运行效率提升一倍以上；多技术路线融合的隐私计算解决方案在亿级参数规模的神经网络模型训练和推理中实现应用。

3. 可验证计算。面向区块链系统和应用高效验证计算结果正确性的需求，开展可验证计算技术研究，提升可验证计算的可靠性、数据一致性和性能。到 2025 年，提出 2 种以上可验证计算安全协议，可支持大规模数据秒级计算，在可验证全同态加密、后量子零知识证明、链下扩容、链上区块压缩等方向实现应用。

四、加快创新体系建设

围绕区块链技术创新、应用拓展和生态构建，建设技术创新支撑平台，打造一批典型应用场景，形成具有全球影响力的新一代区块链生态集群。

（一）技术创新支撑平台

建设支撑区块链原创技术试验验证的新一代开放许可链试验床，承载区块链技术创新成果的测试验证和产品工程化。鼓励区块链新型研发机构设立成果转化实体，面向跨境航运贸易场景，推动跨境贸易主链建设，面向数字人民币场景，推动数字人民币企业应用。

（二）区块链应用示范

依托本市资源优势及特色，打造一批典型应用场景和一批标杆工程。聚焦政务领域，推动政府公共数据上链，促进政务公共链服务和垂直场景应用的政务区块链平台建设。聚焦跨境贸易领域，引导各产业主体，加快航运贸易数字化平台建设，解决贸易领域“信息孤岛”问题，实现与国际主流航运贸易平台的数据传递和价值交换，探索开展跨境商品溯源、离岸贸易数据管理、跨境电子发票交换、数字贸易管理等应用示范。鼓励在数据要素流通、供应链、金融、元宇宙等领域开展区块链创新应用示范。

（三）区块链创新生态

鼓励本市企业积极参与区块链开源生态建设，加快推进区块链标准化能力建设，支持专业机构开展测试认证、安全审计等服务，提升区块链安全可信保障水平。依托本市创新基金，引导带动社会资本共同参与，为区块链产业发展营造良好融资环境。举办具有国际影响力的区块链技术峰会、创新大赛等活动，加快国内外具备潜力的区块链企业、项目、人才团队在上海的落地集聚。

五、保障措施

（一）加强组织领导

根据市委市政府的统一部署，组建区块链关键技术攻关工作小组，加强顶层设计和统筹协调。建立决策咨询机制，联动区块链领域相关专家资源，会同相关协会、学会以及智库等，研究区块链技术发展的重大问题，对区块链技术方向和发展任务提供咨询，为政府决策、行业发展及时提出意见建议。

（二）创新科研组织机制

聚焦主攻方向和重点任务，推动基础研究、关键技术攻关和

成果转化。聚焦基础前研究，探索政府长周期科研支持方式，引导鼓励社会各界捐赠或设立科学基金会，推动新型研发机构、高水平研究型高校、科研院所等各类创新主体协作融通，加快原创性突破。聚焦重大关键技术、战略产品，强化企业创新主体地位，组织行业龙头企业牵头打造创新联合体，探索“揭榜挂帅”“赛马制”等机制，加强联合攻关，适时培育市级科技重大专项，加快重大关键技术突破。推动区块链领域高质量孵化器和重点产业园区建设，加速本土企业成长和成果转化。

（三）建设新型研发机构与成果转化平台

聚焦区块链基础软硬件等关键核心技术，引进国内外高端人才在沪设立区块链新型研发机构，探索以任务为导向的“预算+负面清单”经费支持方式，建立以创新绩效为核心的中长期综合评价机制。支持各区基于本区域的资源禀赋和发展需求，通过搭建平台、优化环境、创新体制机制等方式，推进新型研发机构与成果转化平台的培育和建设，在资金、场地等方面给予配套支持。

（四）加强人才队伍建设

立足国际高端和全球视野，支持新型研发机构、龙头企业等载体用好外籍人才认定标准、引进渠道和支持措施，集聚一批引领国际科技前沿的区块链理论研究与工程化高端人才。引导高校、科研院所、企业等加大青年区块链人才培养力度，创造多学科交叉、多行业融合的交流平台和发展机会，支持青年人才挑大梁、当主角。

上海市科委办公室　　2023 年 9 月 26 日印发