上海市科学技术委员会

沪科指南〔2023〕20 号

关于发布上海市 2023 年度“科技创新行动计划”区块链关键技术攻关专项项目指南的通知

各有关单位:

为加快建设具有全球影响力的科技创新中心，强化本市区块链领域科技创新策源功能，根据《上海区块链关键技术攻关专项行动方案（2023-2025 年）》，上海市科学技术委员会特发布本指南。

一、征集范围

专题一：新型体系架构

方向 1：虚拟机与执行引擎技术研究

研究目标：提升区块链虚拟机并行计算性能与跨虚拟机的智能合约调用能力。

研究内容：研究虚拟机并行执行的代码静态分析冲突预测技术、基于冲突检测的并行执行结果修正技术、跨异构虚拟机的数据共享与协同执行技术，研发多种新型虚拟机并行执行算法并开源，虚拟机实现每秒执行不少于 1000 万条基础指令，实现不少于 2 种异构的虚拟机融合互通，实现具有原子性的跨虚拟机智能合约调用，搭建原型系统进行验证。

执行期限：2023 年 12 月 1 日到 2025 年 11 月 30 日。

经费额度：本研究内容为非定额资助。拟支持不超过 2 个项目，每个项目拟投入专项资助经费不超过 200 万元。企业牵头申报时，企业投入研发经费与申请资助经费之比不低于 1:1。

方向 2：后量子安全的共识机制技术研究

研究目标：应对量子计算机对区块链等公钥密码系统带来的现实威胁，突破适用于区块链系统的后量子数字签名算法，完成后量子密码算法经典安全性和量子安全性量化评估的自动化工具。

研究内容：（1）设计并开源基于哈希的后量子数字签名算法，相较于国际上 SPHINCS+等同类算法，在同等安全强度的提前下，签名大小改进不少于 10%，满足区块链通用密码算法接口规范，适配多种典型共识算法并进行原型验证。（2）设计并开源基于格的后量子数字签名算法，相较于 Dilithium 等同类算法，在同等安全强度的前提下，公钥和签名大小改进不少于 10%，计算效率提升不低于 30%，满足区块链通用密码算法接口规范，适配多种典型共识算法并进行原型验证。

执行期限：2023 年 12 月 1 日到 2025 年 11 月 30 日。

经费额度：本研究内容为非定额资助。每项研究内容拟支持

不超过1个项目，投入专项资助经费不超过200万元。企业牵头申报时，企业投入研发经费与申请资助经费之比不低于1:1。

专题二：资源调度与管控

方向1：抽象模型与中间件技术研究

研究目标：面向高效开发与部署区块链应用的需求，提出模块化区块链技术框架，研发基础组件和开发工具，实现通过统一接口管理调度底层异构区块链系统，推动区块链数据标准、系统应用接口标准和跨链互操作标准研究。

研究内容：研究区块链系统和接口抽象模型，开发可适配不少于5种典型区块链底层系统的模块化区块链技术架构并开源，研发区块链共识计算、分布式存储与访问验证、智能合约版本管理、链上资源域名解析、跨链账户管理等通用中间件，搭建原型系统进行验证。

执行期限：2023年12月1日到2025年11月30日。

经费额度：本研究内容为非定额资助。拟支持不超过2个项目，每个项目拟投入专项资助经费不超过200万元。企业牵头申报时，企业投入研发经费与申请资助经费之比不低于1:1。

方向2：内容管控技术研究

研究目标：面向区块链内容管控需求，建立多模态数据内容监管标准体系，实现多源异构时序数据敏感信息的快速识别和闭环管理，形成高效安全的区块链数据信息监管框架。

研究内容：研究区块链多模态知识库的持续更新及动态演化、未知敏感内容检测的不确定性建模以及鲁棒多模态敏感内容检测识别技术，研制并开源面向区块链数据内容的链上链下协同

监管中间件，支持不少于3种模态的数据识别，已知敏感信息识别准确率达到99%以上,未知敏感内容识别准确率达到80%以上，信息识别吞吐率不低于5万条每秒，搭建原型系统进行验证。

执行期限：2023年12月1日到2025年11月30日。

经费额度：本研究内容为非定额资助。拟支持不超过2个项目，每个项目拟投入专项资助经费不超过200万元。企业牵头申报时，企业投入研发经费与申请资助经费之比不低于1:1。

方向3：形式化验证技术研究

研究目标：提升区块链基础软件的安全可靠性与功能正确性验证能力，形成轻量级形式化验证工具，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。

研究内容：研究密码学相关代数理论的形式化，研究零知识证明编译器和零知识证明虚拟机的可靠性理论，研发并开源支持模块化验证的的程序功能正确性验证工具，搭建原型系统进行验证。

执行期限：2023年12月1日到2025年11月30日。

经费额度：本研究内容为非定额资助。拟支持不超过2个项目，每个项目拟投入专项资助经费不超过200万元。企业牵头申报时，企业投入研发经费与申请资助经费之比不低于1:1。

方向4：漏洞挖掘技术研究

研究目标：面向区块链智能合约代码和底层基础设施代码的漏洞发现需求，形成面向区块链智能合约源代码、区块链底层基础设施源代码和汇编代码的漏洞挖掘框架与工具。

研究内容：研究符合区块链代码特性的漏洞挖掘技术，结合

经典程序分析技术、人工智能理解和密码语义挖掘技术，研发并开源可高效准确挖掘区块链代码漏洞的自动化框架与工具，支持区块链智能合约源代码、字节码以及区块链底层基础设施源代码（C、C++、Java、Golang、Solidity 等）和汇编代码（x86/64、ARM 等）的漏洞挖掘，对每 10 万行源代码/汇编代码进行分析的时间低于 1 小时，支持 15 种以上智能合约的自动化修复，修复成功率不低于 90%，搭建原型系统进行验证。

执行期限：2023 年 12 月 1 日到 2025 年 11 月 30 日。

经费额度：本研究内容为非定额资助。拟支持不超过 2 个项目，每个项目拟投入专项资助经费不超过 200 万元。企业牵头申报时，企业投入研发经费与申请资助经费之比不低于 1:1。

专题三：信任增强

方向 1：零知识证明与可验证计算技术研究

研究目标：设计完成支持硬件高并行加速的零知识证明协议，基于通用服务器处理能力，对 2^{30} 级别电路规模输入，零知识证明生成速度不超过秒级。

研究内容：研究新型开源密码算法以降低传统零知识证明协议中的串行密码运算操作，研发针对高并行零知识证明协议的计算优化和内存优化开发框架与基础工具，搭建原型系统进行验证。

执行期限：2023 年 12 月 1 日到 2025 年 11 月 30 日。

经费额度：本研究内容为非定额资助。拟支持不超过 2 个项目，每个项目拟投入专项资助经费不超过 200 万元。企业牵头申报时，企业投入研发经费与申请资助经费之比不低于 1:1。

方向 2：同态加密结果可验证技术研究

研究目标：针对全同态加密算法本身无法保证同态操作结果正确性的问题，突破全同态加密算法结果可验证技术。

研究内容：设计并开源可验证同态操作正确性的高效全同态加密算法框架与高性能算法库，对单次自举操作（Bootstrapping），实现分钟级的正确性证明与毫秒级验证，证明大小不超过 KB 级别，搭建原型系统进行验证。

执行期限：2023 年 12 月 1 日到 2025 年 11 月 30 日。

经费额度：本研究内容为非定额资助。拟支持不超过 2 个项目，每个项目拟投入专项资助经费不超过 200 万元。企业牵头申报时，企业投入研发经费与申请资助经费之比不低于 1:1。

二、申报要求

除满足前述相应条件外，还须遵循以下要求：

1. 项目申报单位应当是注册在本市的法人或非法人组织，具有组织项目实施的相应能力。

2. 对于申请人在以往市级财政资金或其他机构（如科技部、国家自然科学基金等）资助项目基础上提出的新项目，应明确阐述二者的异同、继承与发展关系。

3. 所有申报单位和项目参与人应遵守科研诚信管理要求，项目负责人应承诺所提交材料真实性，申报单位应当对申请人的申请资格负责，并对申请材料的真实性和完整性进行审核，不得提交有涉密内容的项目申请。

4. 申报项目若提出回避专家申请的，须在提交项目可行性方案的同时，上传由申报单位出具公函提出回避专家名单与理由。

5. 所有申报单位和项目参与人应遵守科研伦理准则。

6. 已作为项目负责人承担市科委科技计划在研项目 2 项及以上者，不得作为项目负责人申报。

7. 项目经费预算编制应当真实、合理，符合市科委科技计划项目经费管理的有关要求。

8. 各研究内容同一法人单位限报 2 项。

9. 获资助的项目负责人及其所在单位应承诺将项目所产生的研究成果和数据资料等报送市科委。

三、申报方式

1. 项目申报采用网上申报方式，无需送交纸质材料。申请人通过“中国上海”门户网站（http://www.sh.gov.cn）--政务服务--点击“上海市财政科技投入信息管理平台”进入申报页面，或者直接通过域名https://czkj.sheic.org.cn/进入申报页面:

【初次填写】使用“一网通办”登录（如尚未注册账号，请先转入“一网通办”注册账号页面完成注册），进入申报指南页面，点击相应的指南专题，进行项目申报;

【继续填写】使用“一网通办”登录后，继续该项目的填报。有关操作可参阅在线帮助。

2. 项目网上填报起始时间为2023年10月11日9:00，截止时间（含申报单位网上审核提交）为2023年10月30日16:30。

四、评审方式

采用一轮通讯评审方式。

五、立项公示

上海市科委将向社会公示拟立项项目清单，接受公众异议。

六、咨询电话

服务热线：021-12345、8008205114（座机）、4008205114（手机）

上海市科学技术委员会

2023 年 9 月 27 日

（此件主动公开）

上海市科委办公室　　2023 年 9 月 27 日印发