# 上海市科学技术委员会

沪科指南〔2024〕10 号

# 关于发布上海市2024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：**聚焦零知识虚拟机的前沿技术路线，研发通用零

知识虚拟机，提升虚拟机数据处理性能，支撑应用生态建设。

**研究内容：**研发通用零知识虚拟机，支持包括 RUST 和 GO 在内的不少于 2 种编程语言，支持包括 BN254 曲线标量域在内的不少于 2 种有限域的可装配，实现以 CPU 运行单体证明者，在典型测试场景下（如哈希、验签），性能优于开源系统（如 Risc0）。设计新型区块链键-值（Key-Value）存储累加器，在 Halo2 开发框架中实现其零知识证明电路，电路支持累加器的更新操作证明与批量操作证明，电路规模小于典型开源系统（如 PSE-zkEVM），实现其电路以查找表形式接入零知识 EVM 电路中。上述通用零知识证明虚拟机和新型区块链 KV 存储累加器应开源代码、用例、文档。

**方向 2：大模型隐私保护技术研究**

**研究目标：**针对大模型参数与训练数据等资产隐私保护的需求，构建大模型关键参数识别、筛选及隐私保护算法框架。

**研究内容：**研发大模型隐私保护算法框架及实施方案，对于拥有不超过 130 亿参数量级的模型，算法工具能够在 2 小时内筛选出模型中最具保护价值的参数并给出推荐模型参数保护数量（不超过模型参数总量的 10%），实现针对千万级词元数据集 SFT 攻击还原训练数据的有效防护，并在类 SQL 语言生成应用场景进行验证。

**专题二：资源调度与管控**

**方向 1：跨链场景的隐私保护和安全技术研究**

**研究目标：**面向多场景跨链需求，持续提升跨链算法与解决方案的隐私保护和抗攻击能力。

**研究内容：**研究满足跨链交易的消息和身份隐私、链间关系隐私、跨链交易计算隐私、链间数据隔离等性质的新型隐私跨链方案，研究可抵御路由劫持攻击、交易延迟攻击、DDoS 攻击等安全攻击的新型安全跨链方案，跨链算法和解决方案需满足高可用性、原子性、一致性、隔离性、持久性等性质，且相对于原有区块链交易确认时间增加不超过 1 倍，吞吐量下降不超过 20%。跨链算法和解决方案应开源代码、用例、文档。

**方向 2：区块链关键安全性的理论证明技术研究**

**研究目标：**证明区块链设计满足关键安全性质，核实安全设计与实现之间的一致性。

**研究内容：**研发区块链关键安全性证明原型系统，支持对共识算法的安全性、交易的不可篡改性和数据的完整性、交易的隐私性（身份和信息匿名）以及二层网络协议的安全性证明，对不安全设计或实现，提出修复方案。系统应实现秒级高效检测，并在高频交易、跨链交易、批量交易等典型场景进行验证。原型系统应开源代码、用例、文档。

**专题三：信任增强**

**方向 1：高效抗恶意的安全多方计算协议研究**

**研究目标：**聚焦抗恶意的安全多方计算协议存在计算执行效率低、通信量大等问题，研究适用于隐私计算需求的高效协议，

突破现有安全多方计算协议的性能瓶颈。

**研究内容:** 基于 SPDZ 安全多方计算协议，设计新型的不经意传输等密码学原语，实现协议通讯量降低 50%，计算速率提升 50%以上。设计面向矩阵乘法、张量积等专用运算的加速方法，协议通讯量降低 90%，计算速率提升 5 倍以上。高效协议具备适配机器学习算法的能力，并进行原型验证。协议应开源代码、用例、文档。

**方向 2: 联邦学习性能提升技术研究**

**研究目标:** 针对当前纵向联邦学习计算和推理任务执行效率低、通信量大等问题，设计新型联邦学习算法。

**研究内容:** 基于 FATE 等开源联邦学习框架，研究联邦学习场景下联合建模的通信效率优化技术，支持逻辑回归（LR）、梯度提升树（XGB）等 2 种以上模型，在 MNIST、CIFAR-10 等典型的数据集上进行验证，在 10MB 带宽下，模型训练和推断过程通信量下降至少一个数量级。在保证通信量显著降低的同时，模型准确率下降不超过 5%。算法应开源代码、用例、文档。

**方向 3: 基于 GPU 加速的零知识证明算法研究**

**研究目标:** 针对传统 CPU 在处理 Halo2 算法时的性能瓶颈问题，研究基于 GPU 加速的 Halo2 算法，利用 CPU-GPU 异构计算技术，实现零知识证明在 BN254 曲线上的高效生成和验证。

**研究内容:** 研发基于 GPU 加速的快速数论变换（NTT）和多标量乘法（MSM）算子，支持蒙哥马利域下计算，在单个 GPU

上，相较于 32 核 CPU，MSM 算子计算效率提升 10 倍以上，NTT 算子提升 5 倍以上。研发基于 PCI-e 传输的 CPU 与 GPU 异构加速计算系统原型，支持 Halo2 算法的证明生成和验证，相较于 CPU 系统计算效率提升 4 倍以上，在单机 4 卡配置下，系统原型的并发任务处理吞吐量相较于 CPU 系统提升 12 倍以上。算子和系统原型在 256 比特下支持 $2^{30}$ 点数计算。

**方向 4：零知识证明的 FPGA 硬件加速技术研究**

**研究目标：**针对零知识证明的速度瓶颈问题，研究 FPGA 硬件加速技术，实现 NTT 和 MSM 算子的硬件加速。

**研究内容：**研究 NTT、MSM 等零知识证明关键算子的 FPGA 硬件加速解决方案。针对 BN254 椭圆曲线，标量位宽为 256 比特，$2^{30}$ 点数的计算，采用 Xilinx Alveo U280 或相当 FPGA 卡，单卡计算时，MSM 计算时间不超过 40 秒，NTT 计算时间不超过 15 秒。不超过 10 卡集群加速时，MSM 计算时间不超过 6 秒，NTT 计算时间不超过 1.8 秒。

**专题四：支撑重点场景应用**

**方向 1：联盟链共识机制研究**

**研究目标：**面向航运贸易区块链中大规模共识和灵活仲裁集合共识的需求，研究适用于联盟链的新型拜占庭容错共识机制，助力实现航运贸易区块链大规模部署和分层共识，支撑关键业务领域共识需求。

**研究内容：**研究支持千级节点参与、支持灵活仲裁集合（如

全员 2/3 阈值、委员会 2/3 阈值、委员会全体）的新型共识机制，吞吐量不低于当前百级节点水平，并接入典型开源联盟链。上述共识算法应开源代码、用例、文档。

**方向 2：高性能交易调度技术研究**

**研究目标：**面向航运贸易等大规模区块链应用中的高频业务需求，聚焦区块内交易调度策略，提升交易调度并行度与调度性能。

**研究内容：**研究基于容器执行引擎的细粒度执行回滚技术、适用于多种合约语言（如 GO）的预测式调度等高性能并行交易调度技术，研发包括非确定性乐观并行、确定性重排序、严格按照区块内顺序等不少于 3 种交易调度算法，并实现交易调度算法链上自适应热切换，接入典型开源联盟链，实现块内交易调度时间减少 30%以上，链吞吐量提升 15%以上。调度算法应开源代码、用例、文档。

**方向 3：区块链监管技术研究**

**研究目标：**针对区块链在上海市政务、金融、航运贸易和供应链等关键场景中的应用安全与合规需求，探索和研究适用于区块链监管的技术框架，支撑相关区块链基础设施的安全运行。

**研究内容：**提出基于区块链系统的自生监管技术框架，研发完成并开源区块链监管系统的基础组件和开发工具，对区块链节点、智能合约、交易数据、系统日志等进行穿透式监管数据的采集，实现异常数据的过滤与阻断、智能合约的安全审计与漏洞探查、链上内容的智能识别决策与风险预警、系统安全性能的全流

程监控，搭建原型系统并验证，初步形成区块链系统与数据的全流程监管标准。

**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技伦理准则。拟开展的科技活动应进行科技伦理风险评估，涉及科技部《科技伦理审查办法（试行）》（国科发监〔2023〕167 号）第二条所列范围科技活动的，应按要求进行科技伦理审查并提供相应的科技伦理审查批准材料。

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. 项目执行期限为 2024 年 10 月 1 日到 2025 年 9 月 30 日。每个研究方向拟支持不超过 2 个项目，每个项目拟投入专项资助经费不超过 200 万元。

**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。

2. 项目网上填报起始时间为2024年9月2日9:00，截止时间（含申报单位网上审核提交）为2024年9月19日16:30。

**四、评审方式**

采用一轮会议评审方式。

**五、立项公示**

市科委将向社会公示拟立项项目清单，接受公众异议。

**六、实施管理要求**

1. 项目实行里程碑管理。由市科委组织形成包括重点机构

在内的项目管理团队，与项目承担单位共同制定实施计划与里程碑节点。项目管理团队定期评估项目进展情况，并及时报请市科委作出“继续实施”“暂停”“调整”“终止”等决定。

2. 项目实行统一的研发管理要求，包括进度管理、代码交付与验收等，在项目管理团队组织下在统一空间开展联合攻关，定期举行前沿技术交流活动。

3. 项目相关研发成果，应按照统一规范在ChainWeaver开源社区（www.chainweaver.org.cn）发布开源代码、用例、文档等。

**七、咨询电话**

服务热线：8008205114（座机）、4008205114（手机）

上海市科学技术委员会

2024年8月23日

（此件主动公开）

抄送：上海集成电路技术与产业促进中心

上海市科委办公室　　2024 年 8 月 23 日印发