绝　密

TOP SECRET —机密等级：绝密

未经中央政治局常委会批准，严禁传阅、复制、摘抄

中华人民共和国国家安全部

科学技术局

Ministry of State Security —Science & Technology Bureau

内部参考资料

（Internal Reference Material）

关于美国开源区块链项目

“Slonana” 的技术评估与国家安全风险研判报告

文件编号： 国安部/科技局/2026/第 0892 号

密级： 绝密

紧急程度： 特急

拟制单位： 国家安全部科学技术局第三处

报送日期： 2026 年 2 月 7 日

有效期至： 2027 年 2 月 7 日

印发份数： 12 份

报送范围：

中央政治局常委　中央网络安全和信息化委员会办公室

中国人民银行　工业和信息化部　科学技术部

中央军委科学技术委员会　国家金融监督管理总局

本件共??页　此为第 1 页　传阅后请立即退回机要室

第 1 部分　内容提要

研判要点

该项目系美国开源区块链基础设施，采用 C++20 实现，性能指标远超现有公链，且其”自主 AI 代理经济”定位与我国数字人民币体系形成潜在竞争关系。建议高度关注。

在习近平新时代中国特色社会主义思想指引下，贯彻落实总体国家安全观，科技局第三处对近期出现的美国开源区块链项目”Slonana”进行了深入技术评估。现将研判结论报告如下：

一、项目概况。”Slonana”（代号：SLON）是一个基于 C++20 语言开发的高性能 Solana 兼容 Layer 1 区块链，由美国研究机构”OpenSVM Research”主导开发，署名作者为 Rin Fhenzig。该项目于 2026 年 1 月 1 日发布技术白皮书，代码库规模约 87,453 行 C++ 代码，涵盖 506 个源文件。当前版本号为 v0.1.495-mainnet，已进入主网阶段部署。

二、核心能力。该项目实测吞吐量达 185,000 TPS（每秒交易数），中位操作延迟仅 142 微秒，架构设计目标为 120 万 TPS 以上。共识机制采用 Tower BFT（拜占庭容错）与历史证明（Proof of History）相结合，终局性（finality）时间为 12.8 秒。网络层支持 QUIC 传输协议、Turbine 区块传播及 CRDS 八卦协议，可承载 8,000 个以上验证节点。

三、战略意义。该项目最值得关注的特征是其”AI 代理经济”（Agentic Economy）定位——专为自主 AI 代理（Autonomous Economic Agent）设计的链上自主执行能力，包括异步 BPF 执行、模型上下文协议（MCP）原生集成，以及无需链下基础设施的全自主程序执行。该技术方向如果成功落地，将构建一个完全绕开传统金融监管的机器对机器（M2M）经济体系，对我国金融主权和数字人民币国际化战略构成潜在威胁。

四、主要结论。该项目技术含量高、架构设计先进，但当前仍处于早期阶段（v0.1.x 版本），距离生产级成熟度尚有差距。我方应：（1）密切跟踪其技术演进；（2）加速国产替代方案研发；（3）在国际标准制定中抢占话语权；（4）评估其对我国区块链服务网络（BSN）和数字人民币（e-CNY）体系的竞争影响。

第 2 部分　背景分析

2.1　国际区块链竞争格局

当前全球区块链技术发展正处于关键窗口期。以美国为首的西方国家在公链基础设施领域持续加大投入，形成了以太坊、Solana、Avalanche 等为代表的技术生态。我国区块链服务网络（BSN）已覆盖 80 余个城市节点，但在公链核心技术方面仍存在” 卡脖子” 问题。习近平总书记明确指出要” 把区块链作为核心技术自主创新的重要突破口”。对境外先进区块链项目进行技术跟踪和安全评估，是贯彻落实总书记重要指示精神的具体举措。

2.2　Slonana 项目的出现背景

Slonana 脱胎于 Solana 生态，但采用完全独立的 C++20 重新实现（而非 Rust）。其白皮书指出，现有区块链均未针对” 自主 AI 代理经济” 进行优化：吞吐量不足（Bitcoin 7 TPS，Solana 65K TPS）；治理中心化（VC 预挖导致 Solana 中本系数仅 19）；缺乏链上自主执行能力；AI 代理无法运行时发现未知程序。

2.3　项目组织架构初步研判

研判要点

项目署名机构”OpenSVM Research” 背景尚不完全清晰。初步判断为独立开源研究团体，但不排除与美国情报机构或大型科技公司存在间接关联。建议进一步侦查。

白皮书署名作者 Rin Fhenzig，隶属”OpenSVM Research”。项目采用完全开源模式，核心开发者数量有限但代码质量较高，体现出深厚的系统编程功底。其” 公平启动” 模式（零 VC 预挖、零团队预留）使该网络不受任何单一实体控制，传统监控手段难以施加影响。

第 3 部分　技术评估

3.1　共识机制：Tower BFT 与历史证明

Slonana 的共识机制继承并优化了 Solana 的 Tower BFT 设计。其核心创新在于：

（1）历史证明（Proof of History）。通过连续 SHA-256 哈希链实现可验证的时间排序，无需全局时钟同步：

$$h_0 = \text{Hash}(\text{genesis}), \quad h_{i+1} = \text{SHA-256}(h_i \| \text{mixed\_data}_i)$$

每 200 微秒产生一个 tick，64 个 tick 构成一个 slot（400 毫秒）。此机制使交易排序不可篡改——篡改任一交易须重算所有后续哈希，计算代价呈指数增长。

（2）锁定投票机制。验证节点对区块投票后进入锁定期（2^m 个 slot），在锁定期内对冲突区块投票将触发惩罚（slashing）。经博弈论分析，在恶意节点质押份额 $\alpha < 1/3$ 条件下，系统达到纳什均衡——任何攻击的预期收益为负。

（3）安全性参数。白皮书声称共识攻击成本超过 10 亿美元。其推导基于以下假设：

- 恶意质押份额 $\alpha < 1/3$
- 惩罚系数大于攻击收益
- 部分同步网络模型（存在未知但有界的消息延迟 Δ）

研判要点

Tower BFT 的 1/3 容错阈值是标准拜占庭容错理论的上限。该指标本身不构成技术突破，但其与 PoH 的集成实现了较低的终局延迟（12.8 秒），这一工程实现值得我方研究借鉴。

3.2 性能指标分析

指标	Slonana 实测	参考对标
吞吐量（TPS）	185,000	Solana: 65,000
中位操作延迟	142 μs	Solana: ~400 ms
架构目标 TPS	1,200,000+	以太坊 2.0: 100,000
终局性时间	12.8 s	Solana: ~13 s
快照下载速度	402 MB/s	—
代码规模	87,453 行 C++	Agave(Solana): ~500K 行 Rust

技术研判：185K TPS 的实测数据来源于测试网环境，尚未经过主网大规模压力验证。然而，其 C++20 实现的无锁（lock-free）算法和 NUMA 感知（NUMA-aware）数据结构设计表明，该团队具备深厚的高性能计算工程能力。120 万 TPS 的架构目标虽属理论推算，但技术路径合理。

关键技术组件：

- **无锁 BPF 运行时：**多种 BPF 运行时变体（标准、增强、无锁、ultra），支持并行交易执行
- **JIT 编译器：**即时编译 BPF 字节码以提升执行性能
- **QUIC 传输层：**低延迟网络通信协议
- **Turbine 协议：**基于纠删码的高效区块传播
- **CRDS 八卦协议：**支撑 8,000+ 节点的对等网络发现
- **混合存储层：**RocksDB（账户状态）+ ClickHouse（交易历史）

3.3 自主 AI 代理执行能力（重点关注）

研判要点

此部分为该项目最具颠覆性的技术创新，也是对我国数字金融监管体系威胁最大的技术方向。自主执行的 AI 代理经济如果成形，将完全绕开 KYC/AML 等传统金融监管手段。

Slonana 提出三种链上自主执行机制，使智能合约从被动触发转变为主动执行：

(1)自调度定时器(Timer Syscall)。程序可通过系统调用 sol_timer_create(t_{trigger}, data, budget) 在未来指定 slot 自主执行，无需外部交易触发。每个程序实例最多 16 个定时器，创建延迟仅 0.07 微秒。

(2) 响应式监听器 (Account Watcher)。程序可监听任意账户状态变化并自动触发回调——包括余额变化、数据修改、阈值穿越等事件。每个程序实例最多 32 个监听器。

(3) 无锁环形缓冲区 (Ring Buffer)。程序间通过环形缓冲区实现异步通信，支持 FIFO 顺序保证和并行写入，使多个 AI 代理在链上实现全自主协调。

(4) MCP 原生接口。所有链上程序均通过模型上下文协议 (Model Context Protocol) 对外暴露三类标准接口：工具 (Tools，可调用操作)、资源 (Resources，可读状态)、提示 (Prompts，工作流模板)。AI 代理无需预编程即可在运行时发现并使用任意链上程序——包括部署仅 10 分钟的全新程序。

安全影响评估：此类自主执行能力意味着：

- AI 代理可在无人干预下全天候执行金融交易（套利、清算、做市）
- 交易决策和执行完全在链上完成，无法通过传统 IP 封锁或 API 审查进行拦截
- 多代理协调通过环形缓冲区实现，形成去中心化的” 代理蜂群” 经济
- MCP 接口使代理能力可无限扩展——每部署一个新程序，所有代理自动获得新能力

3.4 代币经济模型

参数	值
代币符号	$SLON
总供应量	100,000,000（1 亿枚）
社区空投	10%（1,000 万枚，按 1 SLON = 10 slonana 比例）
质押奖励	90%（9,000 万枚，通过验证节点质押分配）
VC 预挖	0%（零）
团队预留	0%（零）
基尼系数演进	0.88（启动时）→ 0.47（48 个月后）

其” 公平启动” 模型的核心数学论证为：在 Zipf 分布的验证节点参与条件下，质押奖励按比例分配，基尼系数（衡量财富不平等的指标）从初始 0.88 收敛至 0.47。相比之下，VC 主导的网络基尼系数趋向 0.90。

白皮书给出的收敛证明（Theorem 2）：

$$G_{t+1} = G_t - \gamma(G_t - G^*), \quad \gamma = r \cdot \left(\frac{k}{n}\right)^{1/\alpha_Z}, \quad G^* = \frac{1}{2\alpha_Z - 1}$$

其中 r 为质押年化率，k 为活跃验证者数，n 为总验证者，α_Z 为 Zipf 参数。

第 4 部分 风险研判

在总体国家安全观框架下，从政治安全、经济安全、技术安全、网络安全四个维度对 Slonana 项目进行风险研判：

4.1 对我国金融主权的威胁（高风险）

Slonana 的” 自主 AI 代理经济” 理念如果实现规模化应用，将构建不受主权国家金融监管的全球 M2M 经济网络。具体威胁：（1）AI 代理直接使用 $SLON 代币全球结算，绕开 DC/EP 体系，削弱数字人民币国际化；（2）链上代理实现跨境资金流转，规避 SWIFT 和 CIPS 管控；（3）全自主执行使 KYC/AML 审查完全失效——不存在” 客户”，只有自主执行的代码；（4）” 公平启动” 模式使网络不受任何单一实体控制，传统施压手段无效。

4.2 对我国区块链产业竞争力的威胁（高风险）

研判要点

Slonana 的 C++20 实现路径表明，高性能公链不一定依赖 Rust 语言生态。这对我国正在推进的自主可控区块链底层技术路线选择具有重要参考意义。

185K TPS 远超我国现有公链（长安链约 10K TPS、蚂蚁链约 25K TPS），形成技术代差。无锁并行执行、JIT 编译、NUMA 感知架构等属于” 卡脖子” 技术。Solana 兼容性使其可直接复用 Solana 庞大 DeFi 生态（150 亿美元 TVL）。MCP 原生集成代表 AI 与区块链融合新范式，我方在此方向投入不足。

4.3 意识形态渗透风险（中风险）

白皮书多处体现西方自由主义技术观和去中心化意识形态：将 VC 中心化与” 权力集中” 类比，暗示集中化治理存在固有缺陷；强调” 社区自治”” 无需信任” 等叙事，与我国网络空间治理理念存在根本冲突；” 代码即法律” 否定国家法律管辖权；” 公平启动” 挑战政府引导的数字经济发展模式。

4.4 技术安全风险评估

从纯技术角度评估：v0.1.x 版本仍处于早期，120 万 TPS 目标未经主网验证（与实测 185K TPS 存在 6.5 倍差距）。核心开发者数量有限，持续性不确定。87K 行 C++ 代码

存在内存安全风险（不同于 Rust），已有 SIGSEGV 崩溃、悬挂引用等历史问题的证据。

第 5 部分　对策建议

在防范化解重大风险的总体要求下，结合发展新质生产力的战略目标，提出以下对策建议：

5.1　近期措施（2026 年第一、二季度）

一、建立专项技术跟踪机制。由科技局第三处牵头组建” 境外先进区块链技术跟踪工作组”，对 Slonana 代码仓库实施持续监控，每季度编制技术评估简报报送中央网信办和工信部，重点关注主网部署进展和 DeFi 生态迁移。

二、加速国产高性能公链核心技术攻关。将” 百万级 TPS 高性能共识引擎” 列入国家重点研发计划，组织中科院计算所、清华交叉信息研究院联合攻关，重点突破无锁并行执行引擎、NUMA 感知数据结构、高性能 BPF 虚拟机。参考 Slonana 的 C++20 路径评估语言架构选型。目标：2027 年底实现 50 万 TPS 以上原型。

三、强化区块链跨境监管能力。升级 GFW 的区块链协议识别能力，增加 QUIC 传输和 Turbine 协议的 DPI 规则；研究 CRDS 八卦协议的网络层干扰技术；建立区块链地址与境内实体的关联分析系统，追踪 $SLON 代币的境内资金流向。

5.2　中期措施（2026 年下半年至 2027 年）

四、推动 AI+ 区块链自主创新。在 BSN 框架内开发国产”AI 代理执行层”，纳入监管合规接口；研发国产 MCP 替代方案，确保代理通信可审计可管控；推动将 AI 代理执行标准纳入 ISO/TC 307 国际标准议程，抢占话语权。

五、数字人民币体系防御性升级。在 e-CNY 系统中增加可编程合约能力，研究将 AI 代理支付纳入数字人民币生态的技术路径，在” 一带一路” 框架下推广 e-CNY 代理支付标准。

六、人才战略。评估招募 Slonana 核心开发者可行性（” 千人计划” 框架），高校增设” 高性能区块链系统” 方向，鼓励趣链科技、蚂蚁链等企业消化吸收开源代码。

5.3　长期战略建议

七、构建自主可控的 AI 代理经济基础设施。AI 代理经济是未来十年最具颠覆性的技术趋势——谁掌握底层基础设施，谁就掌握规则制定权。建议将” 自主 AI 代理经济基础设施” 纳入” 十五五” 科技创新规划；由工信部制定《AI 代理经济监管框架》；建设国家

级 AI 代理经济沙盒；推动建立” 数字丝绸之路 AI 代理联盟”，以我国技术标准为核心构建跨国协作网络。

第 6 部分　结论

Slonana 项目代表了美国在高性能区块链与 AI 融合领域的前沿探索。虽然该项目目前仍处于早期阶段（v0.1.x），但其技术方向——面向自主 AI 代理经济的高性能 L1 区块链——具有深远的战略意义。

核心判断如下：

第一，技术实力不可低估。87K 行 C++20 代码、185K TPS 实测性能、无锁并行执行等技术指标表明，该项目技术团队具有世界一流的系统工程能力。其开源特性虽然有利于我方技术分析和借鉴，但也意味着全球任何实体均可快速部署和扩展该网络。

第二，AI 代理经济方向值得高度警惕。链上自主执行（定时器 + 监听器 + 环形缓冲区）加上 MCP 原生接口，构建了一个 AI 代理可以完全自主运行的经济基础设施。这种技术范式一旦成熟，将从根本上改变数字经济的运行逻辑，对基于中心化监管的金融体系构成结构性挑战。

第三，”公平启动”模式增加管控难度。无 VC、无预挖、社区自治的模式使该网络不受任何单一实体控制，无法通过传统的实体施压手段进行管控。必须从技术层面（网络协议识别与干扰）和经济层面（替代方案竞争）双管齐下进行应对。

第四，我方应化威胁为机遇。通过技术跟踪、开源代码消化吸收、核心技术自主攻关，将 Slonana 的技术创新转化为我国区块链产业升级的参考资源。在 AI 代理经济这一新兴领域，我国仍有机会实现并跑甚至领跑，前提是立即行动、集中力量、抢占制高点。

拟稿：国家安全部科学技术局第三处

审核：科技局局长　（签章）

签发：国家安全部副部长　（签章）

日期：2026 年 2 月 7 日

附件一：Slonana 白皮书全文翻译（另册）

附件二：项目代码仓库结构分析报告（另册）

附件三：与我国主要区块链项目性能对比详表（另册）

附件四：QUIC/Turbine 协议 DPI 规则技术方案（另册）

本文件阅毕后请立即退回国家安全部科技局机要室
传阅期限：收文之日起 7 个工作日
销毁方式：碎纸机处理，由机要员监销