VOLUME 0 · 集团战略总纲与三位一体主权计算架构总白皮书

MYRILUM 集团战略总纲与三位一体主权计算架构总白皮书：AI WorkOS 智能体操作系统、零依赖主权终端与亚秒级合规清算状态机的形式化闭环规范（v1.0）

AI WorkOS 智能体工作台、LingheOS v5.1 零依赖主权终端与灵核公链亚秒级状态机的形式化闭环、威胁边界及跨法域合规总纲

MYRILUM 集团首席架构师与跨学科形式化工程委员会（人工智能系统 · 应用密码学 · 分布式共识 · 金融监管科技 · 企业治理）



智能体工作操作系统
8 Apps · 21 Pkgs
Deterministic Harness & Context DNA

零依赖主权终端 v5.1
60 Specs · 0 Deps
169 Chains · 14 Zero-Trust MCP Tools

亚秒级并行清算公链
250 ms / 32 Lanes
Simplex BFT · 3.0B Gas · Chain 88888

集团法定主权合规锚定
UBI 80912065
D-U-N-S 374308629 · Non-Custodial R&D

协议与软件系统研发主体

MYRILUM LIMITED

中华人民共和国香港特别行政区《公司条例》（第 622 章）注册成立之法人团体（Body Corporate）

CR / UBI: 80912065 · D-U-N-S: 374308629
BR Cert: 80912065-000-07-26-0
Release: v1.0 Canonical Edition (2026)

REGISTERED OFFICE: UNIT 1603, 16/F THE L. PLAZA, 367-375 QUEEN'S RD CENTRAL, SHEUNG WAN, HONG KONG

协议研发主体登记要素、香港法律适用边界与链上存证指纹

VOL. 00 专著卷册定位与文献分级

VOL. 0 · GROUP MASTER ARCHITECTURE & GOVERNANCE WHITEPAPER

MYR-WP-MASTER-2026-V1.0-ZH · Canonical Release v1.0 (2026)

CHAIN 88888 链上密码学存证与安全守卫

LinghеSovereignSecurityGuardV5.latestWhitepaperAnchor()

Simplex BFT 250 ms · Verify Endpoint: `/v1/whitepapers/verify`

研发主体登记与密码学核验维度	官方核实唯一权威真值（**SSOT**）
协议与软件系统研发主体	`MYRILUM LIMITED` (香港法例第 622 章《公司条例》私人股份有限公司)
公司编号 / **UBI** 与邓白氏编码	CR/UBI: `80912065` · D-U-N-S®: `374308629`
商业登记证号码（第 **310** 章）	`80912065-000-07-26-0`
香港法定注册办事处	UNIT 1603, 16/F THE L. PLAZA, 367-375 QUEEN'S RD CENTRAL, SHEUNG WAN, HONG KONG
国际标准文献编号	`MYR-WP-MASTER-2026-V1.0-ZH` · GROUP MASTER ARCHITECTURE & GOVERNANCE WHITEPAPER · SOVEREIGN CHINESE EDITION (v1.0)
公链标识与不可变创世块摘要	ChainID `88888` (`0x15b38`) · Genesis SHA-256: `96208e9900b218935143be3024d2602566a86d61caa906d42399f35b83afd991`
LHKD 合成基准默克尔状态根	`0xa3e5fd1ee51db26128c49f848bc4eb6d71443fbfee51a40b9159832a21beae6e` (101.20% · 78,936,000.00 Synthetic Benchmark Vector)
LUSD 合成基准默克尔状态根	`0x5c3f82332fbffc0be49434232a9a97e2bf2c797423aa3fde4afd19b2c264f410` (100.50% · 10,050,000.00 Synthetic Benchmark Vector)
本卷 **Markdown** 母本 **SHA-256**	`182a1e6c8ebb9ceef15068f12fe99eb84c844cdd6b95de94c4cca17f6e0bfef7`

香港法律适用边界与纯底层技术规范声明（第 32、571、656、615、155/581 及 486 章）

1. 纯底层技术规范与非要约边界：本专著系由 MYRILUM LIMITED 仅以「协议与软件系统研发主体」身份编纂之分布式系统与密码学工程技术规范，不构成香港《公司（清盘及杂项条文）条例》（第 32 章）招股章程、《证券及期货条例》（第 571 章）证券或集体投资计划要约、《稳定币条例》（第 656 章）第 8 及第 9 条下指明稳定币之发行、要约或积极推广，亦不构成第 615 章虚拟资产服务。LHKD、LUSD 与 LHC 均为协议内生标准账本原语与非流通确定性基准测试状态。

2. 零利息非存款、终端非托管与隐私保护不变量：底层状态机在字节码层恒定锁定持有端零利息（r_holder(t) === 0，非第 155/581 章银行存款）；MYRILUM LingheOS Wallet 为 100% 客户端本地自托管零第三方运行时依赖软件；链上账本严格遵循《个人资料（隐私）条例》（第 486 章）实现零自然人隐私数据上链。

DOCUMENT NAVIGATION · 全卷结构化目录索引

全卷章节目录与形式化结构索引

瑞士国际主义网格学术目录 —— 支持在电子阅读器中点击任意章节目次跳转至对应形式化规范与数学证明章节。

00 摘要（**Executive & Scientific Abstract**） §00

00·1 全局形式化符号与跨系统原语公理表（**Global Mathematical Notation & Cross-Stack Primitives**） §00·1

01 第一性原理与集团三位一体主权计算动机 §01

› 1.1 企业级智能体协作与自治清算的三重结构性断层 §1.1

› 1.2 MYRILUM 三位一体因果验证闭环与正交职责分解 §1.2

› 1.3 主张成熟度分级、运行态边界与三个禁止等号 §1.3

02 第一支柱：**MYRILUM AI WorkOS** 确定性多智能体工作操作系统 §02

› 2.1 确定性执行引擎（`Harness`）、因果隐私账本与多端工程拓扑 §2.1

› 2.2 组织上下文基因核（`Context DNA`）与防幻觉可验证溯源交付架构 §2.2

› 2.3 单租户防篡改追加审计流与十维人工门禁（`Human Gate`）责任矩阵 §2.3

03 第二支柱：**MYRILUM LingheOS Wallet v5.1.0** 零依赖主权非托管终端 §03

› 3.1 零运行时供应链攻击面（`0 npm Dependencies`）与四端同构沙箱架构 §3.1

› 3.2 账户抽象矩阵（`EIP-7702` / `P-256` / `EIP-5792` / `ERC-7715`）与签名前钓鱼防火墙 §3.2

› 3.3 有限域 $GF(2^8)$ 门限密钥分片与链上 48 小时时间锁社交恢复 §3.3

04 第三支柱：**MYRILUM** 灵核公链（`ChainID 88888`）亚秒级并行清算状态机 §04

› 4.1 `Commonware Simplex BFT` 单槽确定性终局与 `0x76` 二维并行执行引擎 §4.1

› 4.2 协议内生合规原语（`TIP-403`）、联系汇率走廊与二叉默克尔储备核验模型 §4.2

› 4.3 双椭圆曲线密码学信任根（`EIP-7951 P-256` + `BN254 Groth16`）与全链意图清算海关 §4.3

05 跨栈因果协同协议：从企业认知推理到亚秒级可验证结算 §05

› 5.1 端到端七阶段确定性状态转换流水线与形式化组合不变性 §5.1

› 5.2 机器原生微支付（`x402`）与双边技术服务费确定性算术清分模型 §5.2

06 形式化信任假设、密码学微架构边界与热点争用退化分析 §06

› 6.1 四区域 `3-of-4` 拜占庭委员会网络几何延迟假设与主权时间锁边界 §6.1

› 6.2 分级侧信道防御模型：硅基硬件信任根（`Tier-1`）与受管运行时边界（`Tier-2`） §6.2

› 6.3 共享状态热点写冲突下的并行执行退化包络与确定性回退定理 §6.3

07 跨法域主权合规工程与双半球物理隔离（`Shared-Nothing`）治理架构 §07

› 7.1 香港法例全景合规矩阵（第 622、32、571、656、615、155/581 及 486 章）与非发行人安全港 §7.1

› 7.2 国际市场规则适配（美国 `Howey` 判例、`MiCA`、`BCBS SCO60` 及应用商店准则）与三级地理围栏 §7.2

› 7.3 中国境内纯人工智能工作台（`myrilum.cn`）独立法人运营与物理无共享隔离架构 §7.3

08 企业股权商业化模型、**GAAP/IFRS** 经常性现金流引擎与单位经济 §08

› 8.1 纯软件与算力基础设施股权价值捕获与 `IAS 7` 现金流勾稽公理 §8.1

› 8.2 三大经常性法币收入引擎与财务确认准则（`IFRS 15` / `ASC 606`） §8.2

09 集团白皮书全卷谱系、版本演进对账与密码学存证总索引 §09

› 9.1 四卷八册全球技术专著谱系与终端规范升级（`v5.0 -> v5.1.0`）对账说明 §9.1

› 9.2 分阶段工程路线图（`G0–G9` 门禁）与独立可复现密码学核验规程 §9.2

AP·A 标准与学术参考文献 §A

MYR-WP-MASTER-2026-V1.0-ZH · GROUP MASTER ARCHITECTURE & GOVERNANCE WHITEPAPER · SOVEREIGN CHINESE EDITION (v1.0)

MYRILUM 集团战略总纲与三位一体主权计算架构总白皮书：AI WorkOS 智能体操作系统、零依赖主权终端与亚秒级合规清算状态机的形式化闭环规范（v1.0）

文献主权编号：`MYR-WP-MASTER-2026-V1.0-ZH` · 卷册定位：`VOLUME 0`（集团战略与跨栈总架构白皮书 · 中文权威母本 `v1.0`）
协议与软件系统研发主体：`MYRILUM LIMITED`（香港法定唯一注册英文法团名称，未设注册中文法团名称；品牌中文译称“迈瑞伦” · 香港法例第 622 章《公司条例》私人股份有限公司 · 公司编号 / 唯一商业识别码 CR / UBI：`80912065` · 第 310 章商业登记证号：`80912065-000-07-26-0` · 邓白氏全球企业编码 D-U-N-S：`374308629`）
香港法定注册办事处：`UNIT 1603, 16/F THE L. PLAZA, 367-375 QUEEN'S RD CENTRAL, SHEUNG WAN, HONG KONG`
三位一体代码真源锚点：`MYRILUM AI WorkOS`（`8` 大应用端 · `21` 个核心模块包）· `MYRILUM LingheOS Wallet v5.1.0`（`0` 外部运行时依赖 · `60` 项确定性规范 · `169` 链 · `14` 项零信任 MCP 工具）· `MYRILUM Linghe Chain`（`ChainID = 88888` / `0x15b38` · 创世零块 SHA-256：`96208e9900b218935143be3024d2602566a86d61caa906d42399f35b83afd991`）

法定护栏 0.1 — 集团法律角色、非要约安全港、成熟度分轴与跨法域隔离总声明

1. 纯软件与底层协议研发主体定位：本集团总白皮书（`Volume 0`）系关于企业级多智能体工作操作系统、客户端自托管密码学终端及分布式拜占庭共识状态机之跨学科系统工程与形式化规范文献，由依中华人民共和国香港特别行政区《公司条例》（香港法例第 622 章，`Cap. 622`）注册成立之法人团体 `MYRILUM LIMITED`（香港法定唯一注册英文法团名称，未设第 622 章第 899(1) 条项下注册中文法团名称，品牌中文译称“迈瑞伦”，`BODY CORPORATE`）作为唯一协议与软件系统研发主体（`Protocol & Software R&D Author`）编纂发布（香港公司注册编号 / UBI：`80912065`，成立日期：`27 July 2026`；商业登记证号码：`80912065-000-07-26-0`；邓白氏编码 D-U-N-S：`374308629`）。`MYRILUM LIMITED` 之业务严格限定于企业软件许可、非托管终端工具研发及分布式验证基础设施工程技术输出，在任何司法管辖区均绝不接受、归集、持有或托管任何公众法币资金池，绝不运营任何虚拟资产交易所或自动化交易服务（ATS）撮合平台，亦绝不生成、存储、备份或触碰任何客户端私钥与助记词。
2. 香港法例与国际金融监管非要约边界（`Cap. 32` / `Cap. 571` / `Cap. 656` / `Cap. 615` / `Cap. 155`）：本文件在任何法域均不构成香港《公司（清盘及杂项条文）条例》（第 32 章）所指之招股章程，不构成《证券及期货条例》（第 571 章）项下之证券、期货合约、结构性产品或集体投资计划（CIS）认购要约或投资意见，不构成《稳定币条例》（第 656 章）第 8 条及第 9 条项下之受规管指明稳定币发行、要约或向公众积极推广，不构成《打击洗钱及恐怖分子资金筹集条例》（第 615 章）第 53ZRD 条项下之虚拟资产交易平台运营或受规管虚拟资产服务，亦不构成美国联邦证券法项下之投资合同或欧盟 `Regulation (EU) 2023/1114 (MiCA)` 第 16 条资产参考代币（ART）或第 48 条电子货币代币（EMT）公开发行文件。创世状态树内生之 `LHKD`（`0x20c0000000000000000000000000000000000002`）、`LUSD`（`0x20c0000000000000000000000000000000000001`）及 `LHC`（`0x20c0000000000000000000000000000000000000`）均严格界定为协议内生标准账本原语与 **100%** 合成非流通确定性基准测试状态，持有端强制执行零生息率不变量（$r_{\text{holder}} \equiv 0$，非第 155 章银行存款）。截至本版本，本集团未在本文献中承诺公开发行任何投机性代币。
3. 事实成熟度分轴原则与中国境内物理隔离红线：本文献严格区分代码已核验实现（`VERIFIED_IN_CODE`）、受控实验床实测基准（`BENCHMARKED_TESTBED`）、开放架构规范（`ARCHITECTURAL_SPEC`）与前置条件门禁路线图（`ROADMAP_GATED`），绝不将受控四节点共识基准数据混淆为无许可公众零售主网实时运行流量。同时，面向中国境内企业客户之纯人工智能工作台（`myrilum.cn`，工信部备案号：`京ICP备2026055724号-1`）由境内独立内资法人主体北京灵核智能体科技有限公司（统一社会信用代码：`91110108MAERKJRC8R`）独立运营，与香港 `MYRILUM LIMITED` 境外主权协议栈执行 **100%** 法人、网络、代码、数据库与结算账户物理无共享隔离（**Shared-Nothing Air-Gap**），境内版本彻底剔除一切区块链、密码学钱包、稳定币及跨境账本组件。全栈遵循香港《个人资料（私隐）条例》（第 486 章）数据最小化原则，链上状态严格维持零自然人个人身份信息（Zero Individual PII）。

第 00 节 · SECTION 00

摘要（Executive & Scientific Abstract）

当代人工智能与数字金融基础设施的演进正面临一个根本性的系统级断裂：在认知生产侧，大语言模型与多智能体工作流虽已具备强大的非结构化推理与多模态内容生成能力，但其底层本质仍是高方差的概率自回归采样器，普遍缺失跨会话组织记忆一致性、引用事实密码学溯源、单租户防篡改审计以及抵御间接提示词注入（Indirect Prompt Injection）的确定性执行边界；在价值清算侧，自治智能体集群的高频微粒化算力采购与跨机构商业履约，既无法承载传统代理行电汇（`T+1` 至 `T+3`）与卡组织网络（单笔固定清算底费 $0.15–$0.30）的结算摩擦，亦无法在第一代一维串行随机数（1D Nonce）通用公链上规避排队论延迟发散、波动性原生费率代币敞口以及应用层合规黑名单在组合调用下的穿透失效。认知层的“概率性失控”与清算层的“高摩擦失序”，共同阻碍了自治智能体从辅助对话工具向企业级受控生产力系统的跃迁。

本总白皮书（`Volume 0`）从第一性原理出发，提出并形式化定义 **MYRILUM** 集团三位一体主权计算与合规清算总架构（**The MYRILUM Sovereign Trinity Architecture**）。该架构由三个职责正交且通过密码学契约严密咬合的核心工程支柱组成：

1. 第一支柱——认知编排与企业治理层（`MYRILUM AI WorkOS`）：涵盖 `8` 大跨终端应用与 `21` 个模块化软件包，以确定性执行框架（`@myrilum/linghe-harness-core`）驱动多智能体会话状态机（`SessionTurnEngine`）、因果隐私账本（`PrivacyCausalLedger`）与配额权益计量器（`QuotaEntitlementMeter`）；通过组织上下文基因核（`@myrilum/linghe-context-dna`）与防幻觉交付物架构（`@myrilum/linghe-artifact-schema`），对 `6` 类企业交付模态实施规范化 `SHA-256` 摘要锚定与可验证外部信源绑定（`VerifiedCitationNode`），并由单租户严格防篡改追加审计流（`@myrilum/platform-audit`）与十维人工门禁（`Human Gate`）保障企业权责闭环。
2. 第二支柱——零信任终端与策略防火墙层（`MYRILUM LingheOS Wallet v5.1.0`）：采用净室工程构建 `0` 第三方运行时及开发期 `npm` 依赖的客户端自托管终端，横跨零依赖标准 Web 浏览器单页应用（SPA）、浏览器扩展、桌面原生与移动原生四大运行容器，完整落地 `60` 项确定性密码学与账户抽象规范（`OBL-001` 至 `OBL-060`），原生接入 `169` 条异构网络并提供 `14` 项零私钥暴露的模型上下文协议（MCP）工具。终端在非授信神经网络与私钥签名器之间确立确定性策略闸门，融合 `ERC-7715` 周期额度会话授权（效期硬上限 ≤ 30 天）、`EIP-5792` 原子批处理、`Permit2` 风险授权一键熔断、首尾字符相似地址投毒与 `EIP-712` 钓鱼拦截防火墙、有限域 $\mathrm{GF}(2^8)$ Shamir 门限分片备份以及链上 `48` 小时时间锁守护恢复。
3. 第三支柱——亚秒级并行合规状态机层（`MYRILUM Linghe Chain`，`ChainID = 88888` / `0x15b38`）：基于 `Commonware Simplex BFT` 四区域合成基准验证委员会与深度定制 `Paradigm Reth` Rust 并行执行引擎，达成 $\Delta_{\mathrm{slot}} = 250$ ms 单槽确定性终局（重组概率 $P_{\mathrm{reorg}} \equiv 0$）、单块 `3,000,000,000 Gas` 计算带宽及 `32` 通道类型 `0x76` 二维随机数并发清算（受控实验床实测 `20/20` 笔并发 `0x76` 微支付交易整批终局耗时 `~1,004 ms`）；内核层原生固化 `TIP-403` 亚微秒制裁阻断、香港联系汇率走廊 $[7.7500, 7.8500]$、`LINGHE_CAP656_HQLA_V1` 高流动性优质资产（High-Quality Liquid Assets, HQLA）二叉默克尔储备核验原语、`Osaka EIP-7951` 低阶 `P-256` 硬件飞地验签（`0x0000000000000000000000000000000000000000000000000000000000000100`）以及 `ERC-7683` 联合 `BN254 Groth16` 零知识配对（单次验证 `815,381 gas`）的异构跨链意图清算（实测履约耗时 `~936 ms`）。

在治理、风险披露与商业化维度，本文建立形式化信任假设、V8/JSC 受管运行时微架构侧信道分级边界与共享热点写冲突下的并行退化定理，确立香港境外技术栈与中国境内纯 AI 工作台（`myrilum.cn`）的 100% 物理无共享双轨合规模型，并严格论证不依赖任何代币发行补贴、完全符合国际财务报告准则（`IFRS 15` / `IAS 7` / `ASC 606`）的三大企业软件与基础设施经常性现金流引擎，构建兼具学术可证伪性、监管穿透力与长期股权护城河的集团总纲。

形式化公理符号表 · NOTATION

全局形式化符号与跨系统原语公理表（Global Mathematical Notation & Cross-Stack Primitives）

为消除跨学科语境歧义，表 0.1 统一界定贯穿 `MYRILUM AI WorkOS`、`LingheOS Wallet v5.1.0` 与 `Linghe Chain` 三大子系统的形式化代数符号、定义域及代码真源常量。全文记自然数集 $\mathbb{N}_0 = \{0, 1, 2, \dots\}$，无符号 b 比特整数集 $\mathbb{U}_b = \{0, 1, \dots, 2^b - 1\}$，$k$ 字节八位组空间 $\mathbb{B}^k = \{0,1\}^{8k}$，20 字节标准地址空间 $\mathcal{A} \equiv \mathbb{B}^{20}$，确定性字节串拼接算子为 $\Vert$。

符号 / 算子	代数定义域与精确常量	跨系统物理语义与唯一代码真源锚定
$\mathcal{S}_{\text{Trinity}}$	$(\mathcal{W}_{\text{os}}, \mathcal{K}_{\text{wallet}}, \mathcal{L}_{\text{chain}})$	MYRILUM 三位一体主权系统总元组：智能体工作台 $\mathcal{W}_{\text{os}}$、零信任终端 $\mathcal{K}_{\text{wallet}}$ 与确定性账本状态机 $\mathcal{L}_{\text{chain}}$
$\tau \in \mathcal{T}_{\text{tenant}}$	$\mathcal{T}_{\text{tenant}} \subset \mathbb{B}^{16}$	企业多租户强隔离作用域标识符（`TenantScope`），强制约束记忆基因库、配额计量器与追加审计流边界
$\mathcal{D}_{\text{DNA}}(\tau)$	$(\mathcal{D}_{\text{vis}}, \mathcal{D}_{\text{style}}, \mathcal{D}_{\text{audio}}, \mathcal{R}_{\text{learned}})$	租户 τ 之组织上下文基因四元组（视觉规范、写作语态、声学响度参数及带置信度权重的习得偏好规则集）
$\mathcal{A}_{\text{art}}, h_{\text{art}}$	$h_{\text{art}} = \text{SHA256}(\text{Canon}_{\text{JCS}}(\mathcal{A}_{\text{art}})) \in \mathbb{B}^{32}$	支持 `6` 类模态与 `7` 种标准格式的规范化企业交付物及其 RFC 8785 JCS 确定性 `SHA-256` 完整性摘要
$\mathcal{E}^{(n)}_{\text{audit}}$	$(\tau, n, t_n, a_n, o_n, h_{\text{payload}}, \text{corr}_n)$	单租户单调递增防篡改审计事件流（违反同租户性或序号唯一性立即触发确定性异常阻断）
$\mathcal{I}_{\text{AST}}$	$\mathcal{L}_{\text{NL}} \to \mathcal{I}_{\text{AST}}$	由非授信神经网络提议器生成的结构化意图抽象语法树，严禁包含任何私钥句柄或未解析裸字节码
$\Pi_{7715}(\pi, c, t)$	$\mathcal{P}_{7715} \times \mathcal{C}_{\text{call}} \times \mathbb{U}_{64} \to \{0,1\}$	`ERC-7715` 细粒度会话策略验证谓词：强校验目标合约白名单、周期原子额度上限及有效期 $\Delta t_{\text{exp}} \le 30$ days
$\Gamma_{\text{fw}}(\text{req}, \mathcal{H}_{\text{addr}})$	$\mathcal{Q}_{\text{sign}} \to \{\text{SAFE}, \text{WARN}, \text{BLOCK}\}$	`OBL-052` 签名前确定性防火墙：硬封禁裸 `eth_sign`、审计 `Permit2` / `SetCode` 并阻断首尾字符相似投毒地址
$\text{GF}(2^8)$	$\mathbb{F}_2[\zeta]/(\zeta^8 + \zeta^4 + \zeta^3 + \zeta + 1)$	不可约多项式为 `0x11b` 的伽罗瓦有限域，支撑 `OBL-057` Shamir k-of-n（$2 \le k \le n \le 16$）拉格朗日门限秘密分片
Δ_{rec}	$\Delta_{\text{rec}} \ge 48 \text{ hours} = 172,800 \text{ s}$	`OBL-058` 链上守护模块强制恢复冷静期时间锁下界；窗口期内原账户持有者享有任意时刻一票否决撤销权
$\sigma \in \mathbf{\Sigma}$	$(\sigma_{\text{acc}}, \sigma_{\text{tip20}}, \sigma_{\text{tip403}}, \sigma_{\text{nonce2d}}, \sigma_{\text{dex}}, \sigma_{\text{sys}})$	`Linghe Chain`（`ChainID = 88888` / `0x15b38`）六维正交世界状态元组，创世零块摘要为 `01a390d7...e2f1b`
$(N_{\text{val}}, f, q, \Delta_{\text{slot}})$	$N_{\text{val}} = 4,\ f = 1,\ q = 3,\ \Delta_{\text{slot}} = 250 \text{ ms}$	`Commonware Simplex BFT` 受控基准验证委员会规模、拜占庭容错上限、仲裁法定人数及单槽确定性终局周期
(k, ν)	$\mathbb{U}_{192} \times \mathbb{U}_{64}$（客户端活跃池 $\mathcal{K}_{32} \subset \mathbb{U}_{192}$）	类型 `0x76` 二维并行随机数流形坐标，由内核预编译 `0x4e4f4e43450000000000000000000000000000000000000000000000` 维护

符号 / 算子	代数定义域与精确常量	跨系统物理语义与唯一代码真源锚定
$\Phi_{403}(\psi, a)$	$\mathbb{U}_{64} \times \mathcal{A} \to \{0,1\}$	`TIP-403` Rust 内核级亚微秒制裁与白名单策略鉴权算子（`0x403c0000000000000000000000000000000000000000000000000000`）
(R_t, L_t, ρ_t)	$R_t, L_t \in \mathbb{N}_0$，$\rho_t = R_t/L_t \geq 1.0000$ $(L_t > 0)$	合成基准偿付状态模型 HQLA 测试值、基准负债值及覆盖率不变量（$L_t = 0$ 时 $\rho_t \triangleq 1.0000$，`0x8800000000000000000000000000000000000000000000000000000000000001`）
π_{HKMA}	$\pi_{\mathrm{HKMA}} \in [77500, 78500] \subset \mathbb{U}_{32}$	香港联系汇率制度标度区间不变量（精度 10^{-4} HKD/USD），固化于 `0x8900000000000000000000000000000000000000000000000000000000000001`
$(\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e)$	BN254 Optimal Ate, n_{P256} Low-s	双椭圆曲线密码学信任根：跨链零知识验证（`0x0000000000000000000000000000000000000000000000000000000000000008`）与硅基硬件验签（`0x0000000000000000000000000000000000000000000000000000000000000100`）
$\alpha \in [0,1]$	$\alpha = G_{\mathrm{serial}}/G_{\mathrm{slot}} \in [0,1]$ $(G_{\mathrm{slot}} > 0)$	单槽串行化存储冲突计算量占总槽位 Gas 比例，决定并行多通道吞吐向拓扑串行回退的包络曲线

第 01 章 · SECTION 01

第一性原理与集团三位一体主权计算动机

1.1 企业级智能体协作与自治清算的三重结构性断层

现代数字经济正在经历从“人类交互软件（Software-as-a-Tool）”向“自治智能体协同系统（Autonomous Agentic Systems）”的底层范式迁移。然而，当跨国金融机构、科技研发企业与高合规组织试图将生成式人工智能接入核心业务与资金清算链路时，现有技术栈暴露出三道彼此耦合的结构性断层：

断层一：多步概率推理的条件误差累积与企业记忆失忆症。大语言模型（LLM）本质上是基于条件概率分布 $P_\theta(x_t \mid x_{<t})$ 的随机序列生成器。设复杂企业工程交付流程包含 M 个串行子任务节点，记事件 V_i 表示第 i 步同时满足组织合规规范、品牌术语及事实出处完备，条件失效率为 $\epsilon_i = \Pr[\neg V_i \mid V_1, \ldots, V_{i-1}]$。即便每一步在给定前序合法条件下的单步条件可靠度均满足 $1 - \epsilon_i \leq p = 0.96$，在缺乏外部确定性状态机门禁的裸模型串联架构下，由概率链式法则，全链路零幻觉、零越权的联合概率仍随步数 M 呈指数坍缩：

$$P_{\mathrm{valid}}^{(M)} = \Pr[\cap_{i=1}^{M} V_i] = \prod_{i=1}^{M} (1 - \epsilon_i) \leq p^M \xrightarrow{M=25} 0.96^{25} \approx 0.3604$$

更严峻的是，市面通用对话工具缺乏严格按租户隔离的规范化组织记忆核与防篡改因果审计流，导致每次新会话均退化为零上下文猜测，无法满足受规管行业对交付物可追溯性与责任归属的底线要求。

断层二：神经网络提示词注入与非受限私钥托管的致命耦合。在早期智能体商业实验中，开发者往往将私钥明文或长期高权限 API 凭证直接注入智能体运行时环境变量。由于大语言模型在体系结构上无法严格分离“系统控制指令”与“外部检索非授信数据”，一旦智能体读取含有恶意对抗样本的网页、邮件或合同附件（Indirect Prompt Injection），攻击者即可劫持模型输出任意转账或无限额度代币授权调用，造成不可逆的资产瞬时清零；反之，若退回第三方中心化托管钱包，则直接引入托管机构挪用、单点破产与重度金融牌照合规负担。

断层三：传统延迟净额清算轨道与第一代串行公链的双重失灵。当自治智能体以亚美分颗粒度（$0.001–$0.10）高频按次采购可信 GPU 推理、实时金融行情或跨链流动性（`HTTP 402 Payment Required`）时，传统卡组织与跨境电汇网络固有的单笔固定清算底费 $c_{\mathrm{fixed}} \in [\$0.15, \$0.30]$ 使微观经济剩余恒为负值；而第一代通用公链受限于账户级一维串行 Nonce 队列与多槽位概率性终局，在单一机构金库并发调度 $K \geq 32$ 路智能体工作线程时，其 $M/G/1$ 平均排队等待时间随队列负载率 $\varrho_1 \to 1^-$ 双曲发散，且应用层外挂的 `ERC-20` 黑名单极易被包装合约与意图代付器穿透绕过。

为刻画一套面向企业与机构级自治经济的基础设施是否真正闭环，定义跨栈完备性示性泛函 $\mathcal{J}_{\text{Trinity}}:\mathfrak{S}\to\{0,1\}$ 为认知确定性与审计隔离（$\mathcal{C}_{\text{cog}}$，对应不变量 2.1）、终端零信任有界损耗（$\mathcal{C}_{\text{term}}$，对应定理 3.1）与内核级亚秒合规终局性（$\mathcal{C}_{\text{settle}}$，对应定理 5.1）三项可证伪谓词的逻辑合取：

$$\mathcal{J}_{\text{Trinity}}(\mathcal{S})=\mathbb{I}_{\mathcal{C}_{\text{cog}}}(\mathcal{W}_{\text{os}})\cdot\mathbb{I}_{\mathcal{C}_{\text{term}}}(\mathcal{K}_{\text{wallet}})\cdot\mathbb{I}_{\mathcal{C}_{\text{settle}}}(\mathcal{L}_{\text{chain}})\in\{0,1\}$$

任一维度的缺失均导致 $\mathcal{J}_{\text{Trinity}}(\mathcal{S})=0$：仅有认知工作台而无主权终端与合规账本，智能体只能停留在沙盒文本生成而无法完成可验证价值闭环；仅有底层公链而无零信任终端防火墙与企业认知工作台，底层吞吐率则沦为缺乏真实企业生产力支撑的空转指标。

1.2 MYRILUM 三位一体因果验证闭环与正交职责分解

基于最小作用量与关注点正交分离原则，MYRILUM 集团在顶层架构中确立了“生成与验证严格解耦、认知与密钥物理隔离、合规下沉至状态转换内核”的三位一体系统拓扑（见图 1）。

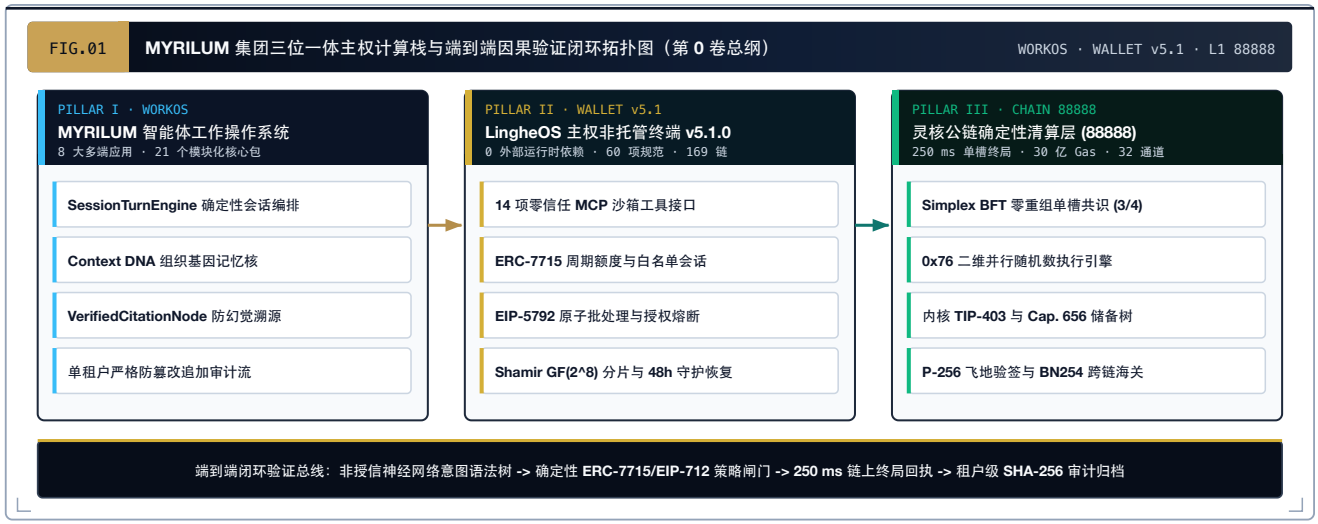


图 01 — MYRILUM 集团三位一体（AI WorkOS × 主权钱包 v5.1.0 × 灵核公链 88888）系统架构与因果验证闭环

注：三大子系统通过严格的无私钥零信任边界耦合；神经网络层永不触碰密钥材料，一切外部状态变更均须通过确定性密码学门禁。

定义 1.1 — MYRILUM 三位一体主权计算栈（The Sovereign Trinity Stack）

集团总技术栈定义为正交耦合三元组 $\mathcal{S}_{\text{Trinity}}=(\mathcal{W}_{\text{os}},\mathcal{K}_{\text{wallet}},\mathcal{L}_{\text{chain}})$：

1. 认知与治理工作台 $\mathcal{W}_{\text{os}}$（`MYRILUM AI WorkOS`）：负责多智能体任务编排、组织记忆基因（`Context DNA`）检索注入、防幻觉多模态交付物合成以及单租户不可变审计归档；该层对一切密码学私钥材料具有零可见性。
2. 非托管零信任终端 $\mathcal{K}_{\text{wallet}}$（`MYRILUM LingheOS Wallet v5.1.0`）：负责在客户端本地安全边界内管理密钥生命周期，通过 `14` 项零信任 MCP 接口接收来自 $\mathcal{W}_{\text{os}}$ 的结构化意图语法树 $\mathcal{I}_{\text{AST}}$，执行非模型确定性策略审计与硬件升级鉴权，输出规范化交易信封。
3. 亚秒级并行清算状态机 $\mathcal{L}_{\text{chain}}$（`MYRILUM Linghe Chain`，`ChainID = 88888`）：负责在 `250 ms` 单槽内完成拜占庭确定性共识、32 通道并发交易执行、内核级 `TIP-403` 合规拦截、硬件飞地与零知识配对证明验证，并向 $\mathcal{W}_{\text{os}}$ 返回不可抵赖的默克尔终局回执。

不变量 1.1 — 跨层单向信任降级与私钥零越界不变量

在 $\mathcal{S}_{\text{Trinity}}$ 的任意合法执行轨迹中，客户端根私钥与会话签名标量严格驻留于 $\mathcal{K}_{\text{wallet}}$ 本地受保护内存或硬件安全模块内；认知层 $\mathcal{W}_{\text{os}}$ 与公链网络层 $\mathcal{L}_{\text{chain}}$ 获取客户端私钥明文的信息熵恒等于零，且任何未经 $\mathcal{K}_{\text{wallet}}$ 确定性策略引擎签发的认知层输出均无法引发链上账本状态变异。

1.3 主张成熟度分级、运行态边界与三个禁止等号

为杜绝行业白皮书普遍存在的“将规划愿景伪装为既成事实、将实验室基准夸大为商业主网规模”的学术失范行为，本总白皮书严格执行技术成熟度与商业运行态双轴分离准则（表 1.1），并将底层分类映射锚定于机读真值台账。

成熟度等级代码	形式化判定标准与证据门槛	对应运行态边界（**Runtime Scope**）	本文献适用模块范围
`VERIFIED_IN_CODE`	已在对应代码仓库完整实现并通过自动化单元与契约门禁，零伪造桩代码	`INTERNAL_VERIFIED` / `ISOLATED_PROD`	`WorkOS` 核心 21 包、`LingheOS Wallet v5.1.0` 全部 `60` 项能力、境内隔离门禁
`BENCHMARKED_TESTBED`	已在受控四节点 `ChainID 88888` 基准拓扑完成实测延迟与 Gas 采样	`SANDBOX_BENCHMARK`（非公众零售主网）	`250 ms` 终局、`~1,004 ms` 并发微支付、`815,381 gas` 配对、`~936 ms` 跨链履约
`ARCHITECTURAL_SPEC`	数学公理、协议字节码接口与会计确认逻辑完备，待外部持牌方或买方接入	`COMMERCIAL_OR_LICENSED_INTERFACE`	持牌机构法币出入金客户端开放接口、三大经常性企业收入引擎
`ROADMAP_GATED`	取决于外部独立安全审计、特定法域监管牌照批复或创始人门禁签发	`GATED_PRE_RELEASE`（未激活）	跨大洲更多外部验证节点扩容、受规管法币稳定币商业化外部发行对接

与此同时，全集团所有工程与法务文档强制确立三个禁止等号（**Three Prohibited Equivalences**）：

1. 上链存证 ≠ 链下物理事实自动为真：链上哈希或默克尔根仅在密码学意义上证明特定数据在特定时刻已由特定签名主体提交且事后未被篡改（存在性与完整性证明），链下原始商业凭证或储备资产的真实性仍依赖于受规管托管机构鉴证、硬件飞地根证书及独立审计机制。
2. 投机性代币 ≠ 密码学可验证基础设施：分布式状态机、零知识证明与非托管硬件签名的核心工程价值在于消除跨机构对账摩擦与单点篡改风险，绝不以公开发行高波动投机代币为前提。
3. 链上合约治理 ≠ 免除法律责任主体的无序去中心化：任何自动化智能体行为与链上参数变更，均必须映射至明确的人类或法人授权主体、强制时间锁窗口及法定司法救济路径。

第 02 章 · SECTION 02

第一支柱：MYRILUM AI WorkOS 确定性多智能体工作操作系统

2.1 确定性执行引擎（`Harness`）、因果隐私账本与多端工程拓扑

`MYRILUM AI WorkOS` 是集团面向全球企业与专业组织构建的多智能体生产力中枢。在代码工程拓扑上，系统采用严格类型化模块化单仓架构，上层承载 `8` 大终端与业务应用（涵盖核心 Web 工作台 `platform-web`、异步分布式执行器 `platform-worker`、桌面客户端 `desktop-client`、移动客户端 `mobile-client`、营销创意工坊 `campaign-concept-studio`、会员与运营台 `member-operations`、文档中心 `docs-site` 及门户站点 `marketing-site`），底层沉淀为 `21` 个职责正交的核心领域包。

为攻克大语言模型在长链路多步任务中的状态漂移与权限失控，核心包 `@myrilum/linghe-harness-core` 将概率推理模型严密封装于确定性有限状态执行框架（Deterministic Execution Harness）之内。系统不再允许智能体自由循环调用外部副作用接口，而是由五大确定性内核组件协同驱动每一轮会话演进：

- 会话轮次状态机（`SessionTurnEngine`）：将多智能体协作分解为具有严格前置类型契约与超时预算的离散原子轮次（Turn），强制校验输入模式、上下文预算与输出结构完整度。
- 因果隐私账本（`PrivacyCausalLedger`）：为每一份进入上下文窗口的企业文档、检索片段与工具返回值打上租户作用域（`TenantScope`）与敏感度因果标签，从架构根源阻断跨租户上下文污染。

- 能力与模型路由注册表（`CapabilityRouterRegistry`）：通过统一抽象适配器层（`@myrilum/provider-adapters`）屏蔽底层异构商业大模型与私有化开源模型差异，支持按任务复杂度、延迟服务等级与数据驻留法域执行策略化路由。
- 交付物基因合成核（`ArtifactDnaKernel`）：将结构化中间表示编译为企业级版式文档，拒绝未通过模式校验的残缺输出进入交付态。
- 配额与权益原子计量器（`QuotaEntitlementMeter`）：联动 `@myrilum/entitlement` 与 `@myrilum/platform-billing`，在每轮推理与工具调用前后执行租户配额预扣、实际词元（Token）消耗核销与超限即停（Fail-Closed）熔断。

形式化地，设租户 τ 在第 j 轮会话前的确定性工作台状态为 $S_j = (\tau, C_j, Q_j, L_j)$，其中 C_j 为当前受控上下文有向无环图，$Q_j \in \mathbb{N}_0$ 为剩余可用算力配额，L_j 为只追加因果日志。当非授信模型推理算子 f_{LLM} 针对任务输入 u_j 产出候选动作提案 $\hat{a}_j$ 时，工作台状态转移函数 δ_{turn} 严格定义为：

$$S_{j+1} = \delta_{\mathrm{turn}}(S_j, u_j) = \begin{cases} (\tau,\ C_j \cup \{\mathrm{Sanitize}(\hat{a}_j)\},\ Q_j - \mathrm{Cost}(\hat{a}_j),\ L_j \Vdash e_{j+1}), & \text{若 } \mathrm{SchemaOk}(\hat{a}_j) \wedge \mathrm{PolicyOk}(\tau, \hat{a}_j) \wedge Q_j \geq \mathrm{Cost}(\hat{a}_j) \\ (\tau,\ C_j,\ Q_j,\ L_j \Vdash e_{j+1}^{(\mathrm{DENIED})}), & \text{其他情况（确定性拒绝并记录阻断原因码）} \end{cases}$$

2.2 组织上下文基因核（`Context DNA`）与防幻觉可验证溯源交付架构

通用人工智能工具难以进入大型机构生产核心的关键症结，在于其输出缺乏组织制度连续性与可核查事实锚点。`MYRILUM AI WorkOS` 通过 `@myrilum/linghe-context-dna` 与 `@myrilum/linghe-artifact-schema` 两大原创领域包建立了企业知识与交付物的数学标准化体系：

1. 多模态组织上下文基因核（`Context DNA`）：系统将企业的隐性品牌资产与公文纪律形式化编码为四维强类型结构 $\mathcal{D}_{\mathrm{DNA}}(\tau)$：
   - 品牌视觉基因（`BrandVisualDna`）：锁定主色、辅色、强调色、中性背景色十六进制标量、标题与正文字体族以及经过 `SHA-256` 校验的官方标识资产摘要；
   - 写作语态与修辞纪律（`WritingStyleDna`）：支持高管结论先行模式（`EXECUTIVE_DECISION_FIRST`）、技术深度剖析模式（`TECHNICAL_DEEP_DIVE`）与董事会简报模式（`BOARD_BRIEFING`），量化约束段落最大字符上限、单页幻灯片要点上限、禁用措辞黑名单与标准术语映射表；
   - 声学播报基因（`VoiceoverAudioDna`）：标准化声纹配置标识、参考音频 `SHA-256`、语速倍率、目标满刻度响度单位（Loudness Units relative to Full Scale, `LUFS`）与背景音乐闪避分贝数；
   - 持续演进偏好规则集（`LearnedPreferenceRule`）：从人类审阅者的历史修订动作中提炼术语替换、精炼度封顶、结论前置与禁用词拦截四类结构化规则，并附带置信度权重评分。
2. 六模态七格式规范化交付与防幻觉信源锚定：`@myrilum/linghe-artifact-schema` 原生定义研究报告（`REPORT`）、演示文稿（`SLIDE_DECK`）、视频成片（`VIDEO`）、电子表格（`SPREADSHEET`）、正式公文（`DOCUMENT`）与标准作业程序（`WORKFLOW_SOP`）六大交付模态，支持编译导出为 `docx`、`pptx`、`xlsx`、`pdf`、`mp4`、`md` 与 `json` 七种工业标准格式。每一个实质性外部论据均必须封装为可验证引用节点 `VerifiedCitationNode`，强制绑定信源地址、精确页码或锚点、原文摘录、信源正文 `contentSha256` 摘要及在线核验状态位 `httpVerified`。

设一份完成编译的企业交付物描述元组为 $\mathcal{A}_{\mathrm{art}} = (\tau, \mathrm{modality}, \mathrm{files}[], \mathrm{citations}[], \mathrm{tables}[])$，采用带长度前缀域分离的 RFC 8785 JSON 规范化方案（$\mathrm{Canon}_{\mathrm{JCS}}$），其跨系统规范化完整性指纹定义为：

$$h_{\mathrm{art}} = \mathrm{SHA256}(\mathrm{Canon}_{\mathrm{JCS}}(\tau,\ \mathrm{modality},\ \{\mathrm{sha256}(\mathrm{file}_u)\}_{u=1}^{U},\ \{\mathrm{contentSha256}(\mathrm{cit}_v)\}_{v=1}^{V},\ \{\mathrm{sha256}(\mathrm{tbl}_w)\}_{w=1}^{W}))$$

任何对交付文件字节流、引用原文或数值测算表的事后静默篡改，均会导致复算摘要与 h_{art} 发生雪崩式偏离，从而在企业内部合规复核或链上存证比对中被 `100%` 检出。

2.3 单租户防篡改追加审计流与十维人工门禁（`Human Gate`）责任矩阵

在机构内控与外部监管审查中，智能体系统的可审计性与人类最终控制权（Human-in-the-Loop Sovereignty）是不可逾越的法律底线。`@myrilum/platform-audit` 与 `@myrilum/identity-access` 在底层实现了单租户严格防篡改追加审计流：每一条 `AuditEvent` 均携带租户作用域、全局单调递增序号 `sequence`、执行主体类型（`USER` 或 `SYSTEM`）、目标对象

版本引用、执行结果（`SUCCEEDED` / `DENIED` / `FAILED`）、标准化原因码、因果关联标识 `correlationId` 以及载荷摘要 `payloadDigest`。

不变量 2.1 — 单租户审计流隔离与非破坏性更正不变量

设租户 τ 当前审计日志序列为 $\mathcal{E}_{\text{audit}} = (e_1, e_2, \ldots, e_m)$。对于任意待追加候选事件 e^*，追加算子 `appendAuditEvent` 在写入前强制验证：(i) 同租户同源性 $\forall e_i \in \mathcal{E}_{\text{audit}}, \text{tenant}(e_i) = \text{tenant}(e^*)$，违者立即抛出 `AUDIT_TENANT_MISMATCH` 异常；(ii) 标识与序号严格唯一性 $\forall e_i, \text{id}(e_i) \neq \text{id}(e^*) \wedge \text{seq}(e_i) \neq \text{seq}(e^*)$，违者立即抛出 `DUPLICATE_AUDIT_EVENT` 异常；(iii) 历史事件严禁原地覆写或物理删除，任何冲正与勘误必须以新序号追加并通过 `correctionOfAuditEventId` 指向被更正事件，保留完整取证链条。

围绕“智能体身份绝不等于法律人格，一切机器动作必须归属于明确自然人或法人责任主体”的治理铁律，表 2.1 确立了全集团跨产品线强制执行的十维人工门禁（`Human Gate`）权限矩阵。

业务动作类别	智能体自主执行权限边界	强制人工门禁（**Human Gate**）与安全兜底机制
1. 资料检索、需求拆解与方案比选	允许在租户授权语料与公开信源内自主执行	用户可随时干预覆盖并审阅完整 `VerifiedCitationNode` 溯源链
2. 商业报价单与法律合同草案起草	仅允许生成带草案水印的结构化初稿	严禁自动对外发出具有法律约束力之要约；须经授权自然人审签
3. 低风险可逆工具调用与格式转换	允许在租户配额 `QuotaEntitlementMeter` 内执行	触及单轮算力或频次阈值立即按 `fail-closed` 熔断挂起
4. 签署具法律约束力之企业协议	绝对禁止智能体独立签署	必须由法定代表人或获授权签署人通过硬件身份核验确认
5. 不可逆资金划转与链上大额结算	禁止突破 `ERC-7715` 微额会话上限单独执行	超出预设会话微额白名单立即强制触发人工硬件签名或多签审批
6. 重要存证签发、撤销与状态更正	仅允许辅助生成待审证明载荷与哈希摘要	必须经人工复核、填写法定理由码并通过非破坏性追加事件记录
7. 违规处罚、保证金扣减与追责	绝对禁止算法单方终局裁决	必须遵循明确证据标准、人工合规官裁决与独立申诉复议程序
8. 商业履约争议最终裁决	仅允许提供时间线与哈希比对辅助分析报告	移交独立人工仲裁机制或管辖法院司法救济
9. 跨组织或跨边界敏感数据共享	默认全面封禁（`DEFAULT_DENY`）	必须取得数据所有权主体针对特定目的与期限的显式二次授权
10. 核心协议升级与风控规则变更	绝对禁止单节点或单智能体即时生效	强制执行 `3-of-4` 多法域多签加时间锁延迟生效（eta）与公开审计

第 03 章 · SECTION 03

第二支柱：MYRILUM LingheOS Wallet v5.1.0 零依赖主权非托管终端

3.1 零运行时供应链攻击面（`0 npm Dependencies`）与四端同构沙箱架构

在加密货币与机构数字资产历史上，终端侧最致命的系统性灾难并非源于椭圆曲线离散对数难题被攻破，而是源于现代前端生态臃肿的第三方传递性依赖树投毒（如恶意篡改深层 `npm` 子包窃取内存助记词）。假设一个常规 Web3 钱包客户端引入 D 个外部运行时软件包（行业典型值 $D \in [400, 1200]$），记各依赖包在单版本周期内遭供应链投毒的算术平均概率为 $\bar{p}_{\text{dep}} = \frac{1}{D}\sum_{i=1}^{D} p_{\text{dep},i} = 10^{-4}$；由初等不等式 $1 - x \leq e^{-x}$（$x \in [0, 1]$），客户端暴露于恶意代码注入的概率满足严格下界：

$$P_{\text{compromise}}(D) = 1 - \prod_{i=1}^{D}(1 - p_{\text{dep},i}) \geq 1 - e^{-D \cdot \bar{p}_{\text{dep}}} \xrightarrow{D=800} 1 - e^{-0.08} \approx 7.69\%$$

为在数学根源上将第三方运行时供应链攻击概率压缩至 $P_{\text{compromise}}(0) \equiv 0$，`MYRILUM LingheOS Wallet v5.1.0` 严格遵循净室工程规范（Clean-Room Engineering），在客户端仓库彻底消除第三方运行时及开发期 `npm` 依赖（`0` 外部运行时或开发期 `npm` 依赖），所有密码学编码、ABI 递归解析、二进制交易序列化、矢量金融图表与零信任协议栈均基于原生语言标准库与宿主操作系统底层原生密码接口从零自研实现，并通过 `60` 项确定性功能与安全规范（`OBL-001` 至 `OBL-060`）全量自动化验证。

在工程部署形态上，`LingheOS Wallet v5.1.0` 构建了单一代码真源驱动的四端同构安全沙箱容器：(i) 零依赖标准 Web 浏览器单页应用（SPA）；(ii) Chromium `Manifest V3` 独立隔离世界扩展（强制设定 `all_frames: false`、严格源绑定 `postMessage`，并通过 `EIP-6963` 多钱包发现协议诚实声明 `isMetaMask = false`，杜绝提供者伪装污染）；(iii) macOS 原生 `WKWebView` 桌面安全容器；(iv) iOS 原生 `WKWebView` 移动安全容器。终端原生支持 `169` 条异构公链网络（涵盖 `Linghe Chain 88888`、主流 EVM 生态及基于 `SLIP-0010 Ed25519` 的非 EVM 网络），确保机构与个人用户在任意设备上享有字节级一致的安全语义。

3.2 账户抽象矩阵（`EIP-7702` / `P-256` / `EIP-5792` / `ERC-7715`）与签名前钓鱼防火墙

面向智能体自治协作与高频机构业务，`LingheOS Wallet v5.1.0` 完整实现了新一代以太坊与主权公链账户抽象标准栈，并在认知层智能体与底层签名器之间构筑了不可绕过的确定性纵深防御体系（见图 2）：

- 双模智能账户与硬件通行密钥（`OBL-002`、`OBL-049`、`OBL-055`）：原生支持 `EIP-7702` 类型 `0x04` 账户代码委托授权（`0x05` 授权元组）与 `Osaka EIP-7951` `WebAuthn Passkey`（提取公钥基础设施标准 `SubjectPublicKeyInfo` 即 `SPKI` 格式之 `P-256` 公钥并强制执行低阶 s 规范化），同时完整实现 `EIP-5792` 原子批处理调用接口（`wallet_getCapabilities` / `wallet_sendCalls` / `wallet_getCallsStatus`，单批次支持 $1 \ldots 32$ 笔调用编译为 `ERC-7579` `0x01` 批处理载荷）及 `ERC-4337 v0.7` 定值账本原语代付打包器（沙盒基准态支持零原生代币余额下以非流通基准测试状态单元 `LUSD` 或 `LHKD` 报价核算执行费，并在获准法域兼容外部独立持牌机构发行的合规结算代币）。
- 细粒度有界会话授权（`OBL-050` — `ERC-7715`）：针对 AI 智能体自动化执行需求，`grantErc7715Permissions` 支持签发受严格三维边界约束的会话凭证 `permissionsContext`：(i) 显式目标合约与函数选择器白名单（`contract-call-allowlist`）；(ii) 原生资产或 `ERC-20` 原子累计配额上限；(iii) 强制不超 `30` 天的绝对失效时间戳（$0 < t_{\text{exp}} - t_{\text{now}} \leq 30 \times 86,400$ s），支持随时一键即时吊销。
- 存量授权健康度审计与一键批量熔断（`OBL-051`）：内置授权审计引擎自动扫描 `ERC-20`、`ERC-721`、`ERC-1155` 及标准 `Permit2`（`0x000000000022d473030f116ddee9f6b43ac78ba3`）存量授权，精准识别无限额度授权（$\geq 2^{255}$）、未验证合约支出方、全集合 NFT 授权及休眠超 `90` 天高危授权，输出 `0–100` 健康评分并一键编码 `approve(spender, 0)` 与 `Permit2.lockdown` 原子批处理撤销交易。
- 签名前钓鱼抽干与首尾相似地址投毒防火墙（`OBL-052`、`OBL-053`）：在任何签名请求触达密钥模块前，`simulateAndAuditSignRequest` 执行四重确定性拦截：(i) 硬件级永久封禁无结构裸哈希盲签 `eth_sign`（风险分 `100`，直接返回 `BLOCK: RAW_ETH_SIGN_FORBIDDEN`）；(ii) 深度解构 `EIP-712` 结构化报文，对针对未验证支取方的无限额 `Permit` / `PermitSingle` / `PermitBatch` 离线授权及非授信 `EIP-7702 SetCode` 代码委托直接返回 `BLOCK`，并对有界离线授权或 `domain.chainId` 异常触发 `WARN` 挂起人工复核；(iii) 首尾字符相似地址投毒检测——若目标地址不在近期已知交易对手集合中，但其 `0x` 后前 ≥ 3 位十六进制字符与末尾 ≥ 4 位十六进制字符同时匹配某一历史真实对手地址而中间字节相异，立即判定为高危投毒攻击并返回 `BLOCK: ADDRESS_POISONING_LOOKALIKE`（风险分 `94`）；(iv) `EIP-4361` 以太坊登录（Sign-In with Ethereum, `SIWE`）报文强制核验请求源域名 `host` 一致性与时效窗口，并兼容 `ERC-6492` 反事实未部署智能账户魔法后缀封装。

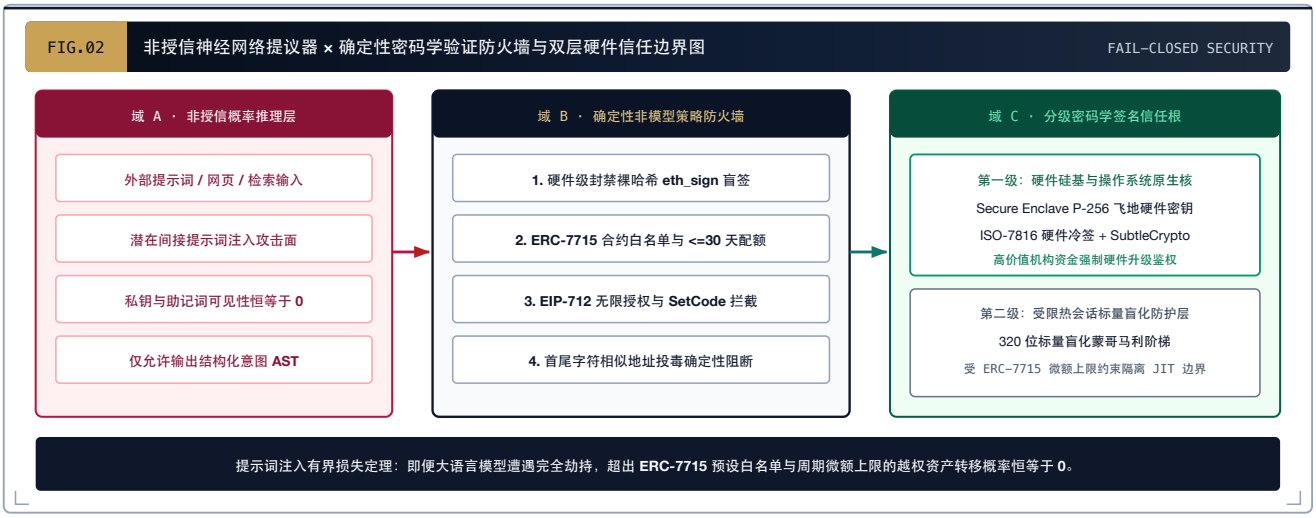


图 02 — 非授信神经网络提议器 × 确定性密码学策略验证器与分级硬件侧信道防御边界

注：严格区分操作系统 C++/硅基硬件恒定时间原语（Tier-1）与受 V8/JSC BigInt JIT 微架构边界制约的 320 位标量盲化热会话层（Tier-2）。

定理 3.1 — 间接提示词注入攻击下的智能体有界损失不变量（Prompt-Injection Bounded-Loss Theorem）

设认知层 $\mathcal{W}_{\text{os}}$ 在时刻 t 遭遇任意强度的对抗性提示词注入劫持，向终端 `14` 项零信任 MCP 接口提交任意恶意构造调用序列 $\{m_1, \dots, m_r\}$。设由人类通过硬件升级鉴权预先签发的良构最小权限会话策略 $\pi = (\mathcal{A}_{\text{allow}}, \mathcal{F}_{\text{allow}}, Q_{\text{cap}}, t_{\text{exp}})$ 满足：(i) MCP 工具仅能生成待审策略草案，无法自主激活或提权实时签名策略；(ii) $\mathcal{F}_{\text{allow}} \neq \varnothing$ 仅包含收款方受限的确定性函数选择器，禁用空载荷裸转账且目标合约无存量无限授权（配合 `OBL-058` 链上滚动 24 小时支出硬上限 Q_{daily}，会话周期最多跨越 $K_{\text{win}} = \lceil (t_{\text{exp}} - t_0)/86400 \rceil \leq 30$ 个窗口）；(iii) 自动签名管线在任何 `OBL-052` 判定 $\Gamma_{\text{fw}}(m_j) \neq \text{SAFE}$（含 `BLOCK` 与 `WARN`）时立即按 `fail-closed` 挂起，且会话代付执行费上界为 F_{gas}。在底层签名方案满足标准选择消息存在性不可伪造（`EUF-CMA`，安全参数 λ）前提下，攻击者窃取助记词概率恒为零，且总经济敞口满足上界：

$$\mathcal{L}_{\max}(\text{Adv}_{\text{LLM}} \mid \pi) \leq \mathbb{I}(t < t_{\text{exp}}) \cdot (\min(Q_{\text{cap}},\, K_{\text{win}}\, Q_{\text{daily}}) + F_{\text{gas}}), \quad \Pr[\text{Target}(m_j) \notin \mathcal{A}_{\text{allow}} \wedge \text{Accepted}(m_j)] \leq \text{negl}(\lambda)$$

证明

由零信任 MCP 分发契约（`OBL-008`、`OBL-060`），全部 `14` 项工具处理函数运行于与密钥存储隔离的无特权路由域（其中 `wallet_grant_erc7715_permission` 仅构造未激活策略描述对象），上下文空间不含任何导出助记词或原始私钥标量之函数绑定。对于任一候选调用 m_j，确定性验证器 `validateExecutionAgainstErc7715` 执行纯布尔与整数集合判定：当 $\text{to}(m_j) \notin \mathcal{A}_{\text{allow}}$、空载荷转账或选择器 $\text{sel}(m_j) \notin \mathcal{F}_{\text{allow}}$、时钟 $t \geq t_{\text{exp}}$ 或累计消耗 $u_{\text{used}} + \text{val}(m_j) > Q_{\text{cap}}$ 时，直接输出 `allowed = false` 中止签名；若攻击者试图构造裸哈希或离线 `Permit` 报文绕过转账限额，`OBL-052` 返回 `BLOCK` 或 `WARN`（均满足 $\Gamma_{\text{fw}}(m_j) \neq \text{SAFE}$），阻断自动签名；链上执行侧另有 `OBL-058` 强制拦截突破 Q_{daily} 之调用。除非敌手以可忽略概率 $\text{negl}(\lambda)$ 攻破椭圆曲线 `EUF-CMA` 难题伪造签名，否则任何越界指令均无法生效，证毕。

Q.E.D. ■

3.3 有限域 $\text{GF}(2^8)$ 门限密钥分片与链上 48 小时时间锁社交恢复

为彻底破解自托管模式下“单点助记词遗失导致资产永久灭失”与“单点备份被盗导致资产瞬时失窃”的二元悖论，`LinghеOS Wallet v5.1.0` 在离线密码学层与链上模块层构建了双重主权灾备机制：

1. 有限域 $\text{GF}(2^8)$ **Shamir** k-of-n 门限秘密分片（`OBL-057`）：基于 Adi Shamir 多项式插值理论，在以 Rijndael 不可约多项式 $P(\zeta) = \zeta^8 + \zeta^4 + \zeta^3 + \zeta + 1$（十六进制 `0x11b`）构造的伽罗瓦有限域 $\text{GF}(2^8)$ 上，对秘密字节流 $S = (s_0, s_1, \dots, s_{L-1}) \in \mathbb{B}^L$（$1 \leq L \leq 256$）的每一字节独立均匀采样 $k-1$ 个随机系数 $(a_{l,1}, \dots, a_{l,k-1}) \xleftarrow{\$} \text{GF}(2^8)^{k-1}$，构造次数至多为 $k-1$ 的随机多项式 $f_l(x) = s_l \oplus \bigoplus_{d=1}^{k-1} (a_{l,d} \otimes x^d)$（记 $\otimes$ 为有限域乘法），在互异非零横坐标

$x_i = i \in \{1, \ldots, n\}$ 处求值并生成 n 份附带 `32` 位 `SHA-256` 传输完整性校验和的分片（$2 \le k \le n \le 16$）。集齐任意 k 份分片后，经校验和筛除传输损坏分片，通过拉格朗日插值在 $x = 0$ 处唯一重构秘密字节（重构后进一步核对账户公钥承诺以阻断恶意守护人篡改分片）：

$$s_l = f_l(0) = \oplus_{i=1}^{k} \left(y_{l,i} \otimes \bigotimes_{\substack{1 \le j \le k \\ j \ne i}} \left(x_j \otimes (x_i \oplus x_j)^{-1} \right) \right) \quad \text{in } \mathrm{GF}(2^8)$$

任意少于 k 份分片的泄露在香农信息论意义上保持完美保密性（Perfect Secrecy），敌手对 s_l 的后验分布严格等于均匀先验分布。

2. 链上 `ERC-7579` + `ERC-7201` **48** 小时时间锁守护恢复与日限额熔断（`OBL-058`）：链上智能账户恢复模块采用 `ERC-7201` 命名空间存储消除代理升级槽位碰撞，绝对禁止任何研发方或管理员后门（`owner` 严格限定为智能账户自身）。当守护人达成 k-of-n 门限提议更换失联密钥时，系统强制进入不少于 $\Delta_{\text{rec}} = 48$ hours 的公开时间锁窗口；在此期间，若原账户持有者并未失联（例如遭遇守护人恶意串谋），原持有者可在任意一秒调用 `cancelRecovery()` 实施即时一票否决。同时模块内置按代币维度的滚动 24 小时支出硬上限（`DailySpendCapExceeded`），配合 `OBL-056` 基于先进先出（`FIFO`）与最高成本先出（`HIFO`）批次核算的 `SHA-256` 密封财税审计报表导出器，全面满足家族办公室与企业金库的内控合规要求。

表 3.1 完整汇总了覆盖全部 `60` 项终端规范（`OBL-001` 至 `OBL-060`）与全部 `14` 项零信任 MCP 工具接口的演进矩阵。

规范域编号	核心密码学与终端安全模块	遵循公开标准 / 算法不变量	零信任 **MCP** 工具映射（共 **14** 项）
`OBL-001` – `003`	多链密钥核、Passkey 与硬件冷签	`BIP-39/32`、`SLIP-0010`、`EIP-7702`、`P-256`、`ISO-7816 WebHID`	`wallet_get_status`、`wallet_get_portfolio`
`OBL-004` – `008`	递归解码、双语意图编译与全链微支付	`EIP-137`、`ERC-4626`、`ERC-7579`、`x402`、`TIP-403`、`BN254`	`wallet_decode_calldata`、`wallet_compile_intent`、`wallet_verify_session_policy`、`wallet_quote_dex`、`wallet_x402_mcp_challenge`、`wallet_check_tip403_compliance`、`wallet_omnichain_x402_invoke`、`wallet_zk_light_client_bridge`
`OBL-009` – `048`	`169` 链同构网络矩阵、加密金库与终端底座	`AES-256-GCM`、`PBKDF2-SHA256`（60 万次迭代）、`EIP-6963`、三级区域围栏	经由 `wallet_get_status`、`wallet_get_portfolio` 与 `wallet_quote_dex` 受控只读暴露
`OBL-049` – `050`	原子批处理调用与细粒度周期会话授权	`EIP-5792`（1–32 笔原子打包）、`ERC-7715`（≤ 30 天有界配额）	`wallet_build_eip5792_batch`、`wallet_grant_erc7715_permission`
`OBL-051` – `053`	授权健康度批量熔断、防钓鱼与反事实登录	`Permit2 lockdown`、`EIP-712` 首尾防投毒、`EIP-4361`、`ERC-6492`	`wallet_audit_approvals_and_revoke`、`wallet_simulate_sign_firewall`
`OBL-054` – `060`	免 Gas 跨链单、定值原语代付、财税、灾备与网关	`ERC-7683`、`ERC-4337 v0.7`、`FIFO/HIFO SHA-256`、`Shamir GF(2^8)`、`48h` 守护	同构内嵌于终端安全中心与 `64 KB` 有界本地零信任分发网关

第 04 章 · SECTION 04

第三支柱：MYRILUM 灵核公链（ChainID 88888）亚秒级并行清算状态机

4.1 Commonware Simplex BFT 单槽确定性终局与 0x76 二维并行执行引擎

作为集团三位一体架构的底层价值与状态锚定基座，MYRILUM Linghe Chain（ChainID = 88888，十六进制 0x15b38；不可变创世零块 SHA-256：96208e9900b218935143be3024d2602566a86d61caa906d42399f35b83afd991）专为主权级智能体高频微清算与跨机构实时全额交收（Real-Time Gross Settlement, RTGS）而设计。

在共识层，协议采用 Commonware Simplex BFT 三阶段流水线拜占庭容错协议，受控基准测试床由 HK-HKMA、SG-MAS、JP-FSA 与 CH-FINMA 四组区域延迟与合规仿真节点配置标签（注册于内核预编译 0xcccccccc0000000000000000000000000000000000000000，$N_{\mathrm{val}} = 4, f = 1, q = 3$）驱动——非背书声明：上述四组标识符纯属由 MYRILUM LIMITED 在隔离基准测试床内独立运行的合成地域延迟与监管规则仿真配置画像（**Synthetic Regional Simulation Profile Tags**），绝不代表香港金融管理局（**HKMA**）、新加坡金融管理局（**MAS**）、日本金融厅（**JFSA**）或瑞士金融市场监督管理局（**FINMA**）参与节点运行、存在任何关联关系、授予牌照或作出任何形式之官方认可与背书。通过全网格一步公证广播与本地超时虚拟空块跳过证书（Dummy Skip Certificate）快速跨槽机制，协议达成单槽 $\Delta_{\mathrm{slot}} = 250\ \mathrm{ms}$ 确定性终局——一旦高度 h 聚合生成 3-of-4 Ed25519 终局证书，账本重组概率严格满足 $P_{\mathrm{reorg}} \equiv 0$（恢复点目标 Recovery Point Objective, $\mathrm{RPO} = 0$）。

在执行层，底层内核基于模块化 Rust 执行引擎 Paradigm Reth 深度构建，单槽计算容量上限设定为 $G_{\max} = 3,000,000,000$ Gas（理论持续计算吞吐带宽达 1.2×10^{10} Gas/s）。为彻底根除传统 EVM 一维标量 Nonce 对企业金库并发智能体线程造成的队头阻塞，协议在架构层引入 **EIP-2718** 类型 0x76 二维无符号随机数空间 $(k, \nu) \in \mathbb{U}_{192} \times \mathbb{U}_{64}$（由内核预编译 0x4e4f4e4345000000000000000000000000000000 维护）：通道 $k = 0$ 保持对传统串行交易的完全向后兼容，而单账户默认激活并发通道池 $\mathcal{K}_{32} = \{1, \ldots, 32\} \subset \mathbb{U}_{192}$ 允许同一企业金库同时开启 $K = 32$ 条互不阻塞的独立并发清算泳道。由 Pollaczek–Khinchine 排队论公式，当聚合到达率为 λ 的微支付流均匀分布至 K 条读写集正交的并发通道时，单通道排队负载率由 $\varrho_1 = \lambda/\mu_1$ 骤降至 $\varrho_K = \lambda/(K\mu_1)$，稳态平均排队等待时延实现超线性坍缩：

$$\frac{\mathbb{E}[W_q^{(2D,K)}]}{\mathbb{E}[W_q^{(1D)}]} = \frac{1-\varrho_1}{K(1-\varrho_1/K)} \ll \frac{1}{K} \quad (\text{当 } \varrho_1 \to 1^-)$$

配合原生多账本原语费用管理器 TIP Fee Manager（0xfeec000000000000000000000000000000000000）与 0x78 域分离第三方 Gas 代付签名，机构智能体可在基准环境下直接以协议内生定值参考基准原语结清 Gas，无需在资产负债表上预持波动性原生代币。在受控 ChainID 88888 基准测试床中，同一金库并发广播 20/20 笔 0x76 微支付交易全部达成确定性终局仅耗时 ~1,004 ms，零 Nonce 碰撞且零队列停滞。

4.2 协议内生合规原语（TIP-403）、联系汇率走廊与二叉默克尔储备核验模型

区别于在通用公链应用层松散拼装可被轻易绕过的黑名单合约，灵核公链将金融监管不变量直接下沉固化至创世状态空间与 Rust 执行内核字节码边界：

1. 三类创世账本原语正交隔离、零通胀与零生息不变量：创世零块将共识质押计量原语 LHC（0x20c0000000000000000000000000000000000000，无通胀增发质押奖励、无散户委托资金池、无企业利润回购销毁承诺）与非流通定值清算参考基准原语 LUSD（0x20c0000000000000000000000000000000000001）及 LHKD（0x20c0000000000000000000000000000000000002）严格正交解耦（全部采用 6 位小数精度并携带 EIP-3541 "0xef" 内核哨兵字节码）。如法定护栏 0.1 所述，LUSD 与 LHKD 严格作为非流通确定性基准测试状态，持有端强制锁定 $r_{\mathrm{holder}}(t) \equiv 0$。
2. 内核级 TIP-403 亚微秒策略拦截与双轨旅行规则存证：每一次价值转移均在 Rust 执行内核层强制调用 TIP-403 策略注册表（0x403c0000000000000000000000000000000000）），对任意深度的合约嵌套调用（CALL / DELEGATECALL）具备零穿透不可绕过性；同时针对单笔满 US$1,000.00（HK$7,800.00）或 24 小时滑动窗口累计满 US$5,000.00（HK$39,000.00）防拆分阈值之转账，强制要求锚定 FATF Recommendation 16 零明文隐私（Zero-PII）密码学信封哈希。
3. 二叉默克尔偿付覆盖率与联系汇率走廊字节码不变量：合规储备锚定金库（0x8800000000000000000000000000000000000001）采用 LINGHE_CAP656_HQLA_V1 域分离二叉默克尔树实时核验分项储备净值。合成测试向量显式声明：在受控确定性基准测试床中，创世预置的 LHKD 基准负债测试向量 HK$78,000,000.00 与参考储备测试向量 HK$78,936,000.00（算术覆盖率 101.20%，默克尔根 0xa3e5fd1ee51db26128c49f848bc4eb6d71443fbfee51a40b9159832a

`21beae6e`）以及 `LUSD` 基准负债测试向量 `US$10,000,000.00` 与参考储备测试向量 `US$10,050,000.00`（算术覆盖率 `100.50%`，默克尔根 `0x5c3f82332fbffc0be49434232a9a97e2bf2c797423aa3fde4afd19b2c264f410`）**100%** 系用于验证智能合约算术不变量的合成密码学测试向量（**Synthetic Deterministic Test Vectors**），对应 `0` 真实银行存款、`0` 受托法币资产与 `0` 对外发行货币负债；同时全链清算海关（`0x8900000000000000000000000000000000000001`）在字节码层恒定锁定香港联系汇率强弱方兑换走廊（当 $L_t = 0$ 时约定 $\rho_t := +\infty$）：

$$\forall t \geq 0: \quad L_t^{(\mathrm{LHKD})} > 0 \Longrightarrow \rho_t^{(\mathrm{LHKD})} = \frac{R_t^{(\mathrm{LHKD})}}{L_t^{(\mathrm{LHKD})}} \geq 1.0000, \quad L_t^{(\mathrm{LUSD})} > 0 \Longrightarrow \rho_t^{(\mathrm{LUSD})} = \frac{R_t^{(\mathrm{LUSD})}}{L_t^{(\mathrm{LUSD})}} \geq 1.0000, \quad \pi_{\mathrm{HKMA}}(t) \in [77500, 78500]$$

4.3 双椭圆曲线密码学信任根（`EIP-7951 P-256` + `BN254 Groth16`）与全链意图清算海关

为打通硅基机密算力核验与多链流动性互操作，灵核公链在底层预编译与创世系统合约层构建了双椭圆曲线密码学引擎（实测延迟对数对比见图 3，完整创世确定性地址空间见表 4.1）：

- 硅基硬件飞地两阶段证明注册与 `ERC-8004` 智能体服务清分：系统采用严谨的两阶段密码学解耦设计——第一阶段（飞地根证明注册）：硬件证明验证合约（`0x8900000000000000000000000000000000000003`）调用 `Osaka EIP-7951` 原生预编译（`0x0000000000000000000000000000000000000100`），并配合后创世安全守卫 `LingheSovereignSecurityGuardV5` 强制核验低阶标量规范性约束 $0 < s \leq \lfloor n_{\mathrm{P256}}/2 \rfloor$，链上验证机密计算 GPU 飞地（如 NVIDIA H100 / AWS Nitro）硬件根报价并注册受信任飞地运行时签名密钥 `runtimeSigner`；第二阶段（高频任务履约结算）：验证托管金库（`0x8004000000000000000000000000000000000003`）核验已注册 `runtimeSigner` 对推理输出摘要 `outputHash` 的确定性授权，联动 `ERC-8004` 智能体身份（`0x8004000000000000000000000000000000000001`）与支付加权信誉账本（`0x8004000000000000000000000000000000000002`）完成原子技术服务费清分。
- `ERC-7683` 双向跨链意图海关与 `BN254 Groth16` 零知识轻客户端桥：零知识桥合约（`0x8900000000000000000000000000000000000002`）调用 EVM 预编译 `0x0000000000000000000000000000000000000008` 执行四配对等式核验，实测单次链上证明验证仅消耗 `815,381 gas`（占单槽 30 亿 Gas 上限的 `0.027%`）；配合覆盖六大外部 EVM 网络与 Solana 的双向防抢跑托管机制，异构源链免 Gas 跨链意图端到端履约基准耗时仅为 `~936 ms`。

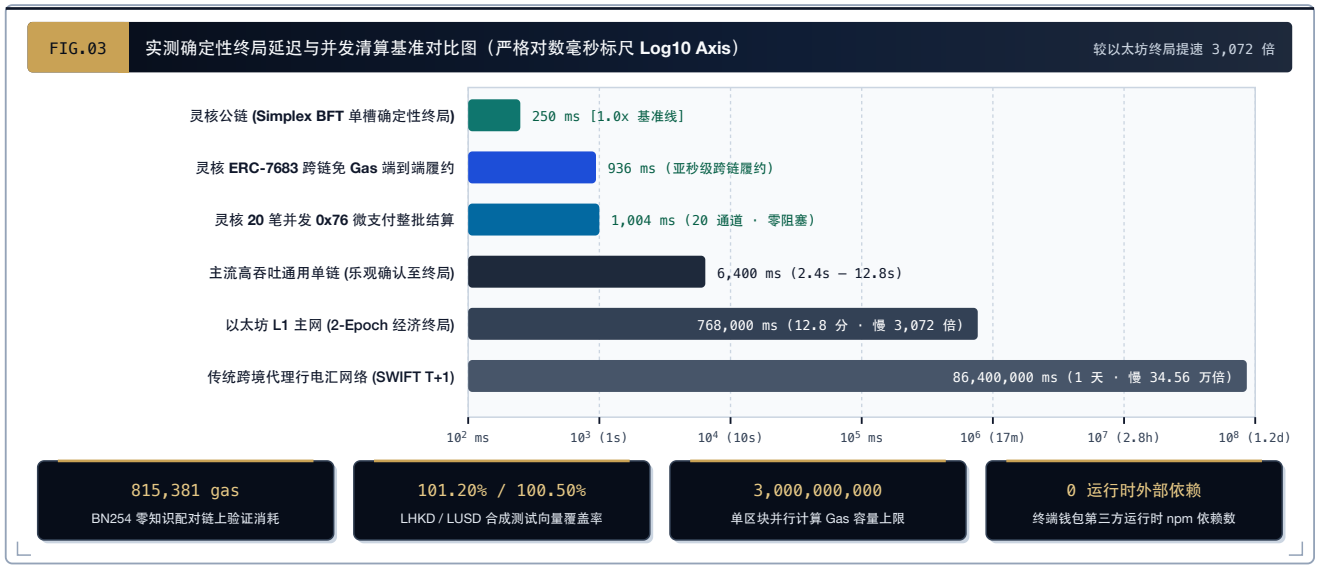


图 **03** — 灵核公链实测终局延迟、**20** 通道并发微支付吞吐与全球主流清算网络对数坐标对比

注：横轴严格遵循 Log10(ms) 数学对数刻度（100 ms 至 100,000,000 ms）；基准数据采集自受控 ChainID 88888 端到端测试套件。

架构层级	模块名称与功能语义	创世确定性标准地址（**SSOT**）
原生账本原语层	`LHC`（零通胀共识质押计量原语）/ `LUSD` / `LHKD`（非流通确定性合成基准状态）	`0x20c0000000000000000000000000000000000000` – `0x20c0000000000000000000000000000000000002`

架构层级	模块名称与功能语义	创世确定性标准地址（**SSOT**）
密码学预编译层	`BN254` 椭圆曲线加/乘/配对（`Groth16`）与 `Osaka EIP-7951` `P-256` 硬件验签	`0x0000000000000000000000000000000000000006` – `0x0000000000000000000000000000000000000008`、`0x0000000000000000000000000000000000000100`
Rust 执行内核层	`TIP-403` 制裁拦截、`2D Nonce` 管理器、账户密钥链、验证者配置、多原语费用管理器与沙盒参考中央限价订单簿（CLOB）	`0x403c0000000000000000000000000000000000`、`0x4e4f4e4345500000000000000000000000000000`、`0xaaaaaaaa00000000000000000000000000000000`、`0xcccccccc00000000000000000000000000000000`、`0xfeec0000000000000000000000000000000000`、`0xdec0000000000000000000000000000000000000`
智能体经济层	`ERC-8004` 身份注册表、支付加权信誉账本、服务费验证托管金库与有界会话管理器	`0x8004000000000000000000000000000000000001` – `0x8004000000000000000000000000000000000003`、`0x8402000000000000000000000000000000000001`
合规与全链海关层	`Cap. 656` 储备默克尔锚定金库、`ERC-7683` 清算海关、`ZK` 轻客户端桥、`P-256` 验证器、`3-of-4` 主权多签与标准 `Permit2`	`0x8800000000000000000000000000000000000001`、`0x8900000000000000000000000000000000000001` – `0x8900000000000000000000000000000000000004`、`0x000000000022d473030f116ddee9f6b43ac78ba3`

第 05 章 · SECTION 05

跨栈因果协同协议：从企业认知推理到亚秒级可验证结算

5.1 端到端七阶段确定性状态转换流水线与形式化组合不变性

将三大支柱串联为一个不可分割的工程整体时，一笔企业级跨机构智能体协作任务（例如：跨国研究团队在 `AI WorkOS` 中调度外部机密算力模型完成行业尽调报告并实时结清推理服务费）严格沿携带唯一全链路幂等追踪号 $\kappa_j \in \mathbb{B}^{16}$（`correlationId`）的七阶段确定性因果流水线演进：

1. 阶段 **I**（受控认知规划）：`WorkOS` 会话引擎 `SessionTurnEngine` 载入租户 τ 之 `Context DNA`，预冻结词元算力配额并生成不含任何密钥权限的结构化任务意图语法树 $\mathcal{I}_{\mathrm{AST}}$ 与追踪号 κ_j。
2. 阶段 **II**（零信任 **MCP** 挑战握手）：外部算力服务端返回符合 `HTTP 402` 规范的机器计费挑战票据（含目标结算地址、原子金额、链标识及到期槽位），`WorkOS` 将票据与 $\mathcal{I}_{\mathrm{AST}}$ 经 `64 KB` 有界本地受限通道提交至 `LingheOS Wallet v5.1.0` 的 `wallet_x402_mcp_challenge` 接口。
3. 阶段 **III**（非模型确定性策略与防钓鱼审计）：终端顺序执行 `OBL-052` 防火墙（核验无裸盲签、无同形/首尾近似地址投毒、无越权 `Permit`）与 `OBL-050` `ERC-7715` 会话配额谓词 Π_{7715}，以及前置 `wallet_check_tip403_compliance` 合规预检。
4. 阶段 **IV**（并发通道分配与签名封装）：校验全绿后，终端从激活池中分配空闲二维随机数通道 $k \in \mathcal{K}_{32}$，构造类型 `0x76` 定值参考基准原语代付交易（或异构链 `ERC-7683` 免 Gas 意图单）并完成本地签名。
5. 阶段 **V**（**250 ms** 内核合规与单槽终局）：`Linghe Chain` 在单槽内执行 `TIP-403` 内核筛查、联系汇率走廊校验与并行状态写集提交，生成不可逆 `Simplex BFT` 终局证书与状态根 $\mathcal{R}(\sigma')$。
6. 阶段 **VI**（硬件飞地两阶段核验与服务费清分）：算力飞地（其硬件根报价已预先通过 `0x8900000000000000000000000000000000000003` 与 `0x0000000000000000000000000000000000000100` 低阶 `P-256` 验签绑定 `runtimeSigner`）核验付款终局后在硅基 TEE 内完成推理，由已注册 `runtimeSigner` 对 `outputHash` 授权提交至 `0x8004000000000000000000000000000000000003` 触发原子清分。
7. 阶段 **VII**（防幻觉交付合成与幂等双账本归档）：`WorkOS` 校验交付物引用树生成 `JCS` 规范化 `SHA-256` 密封摘要 h_{art}，并以追踪号 κ_j 幂等关联链上终局交易哈希与状态根 $\mathcal{R}(\sigma')$ 写入 `@myrilum/platform-audit` 单租户只追加审计流。

定义跨栈乘积状态空间 $\mathbf{\Omega} = \mathcal{S}_{\text{os}} \times \mathbf{\Sigma} \times \mathscr{M}_{\text{pipe}}$（其中 $\mathscr{M}_{\text{pipe}}$ 表示携带追踪号 κ_j 的阶段间有界消息信封空间）。将四级子算子自然提升为 $\mathbf{\Omega} \to \mathbf{\Omega}$ 上的全函数自同态后，端到端跨栈复合状态转移总算子 $\Psi_{\text{E2E}} : \mathbf{\Omega} \times \mathcal{U} \to \mathbf{\Omega}$ 严格良定义为：

$$\Psi_{\text{E2E}}(\omega_j, u_j) = (\hat{\Upsilon}_{\text{audit}} \circ \hat{\Upsilon}_{\text{L1}} \circ \hat{\Upsilon}_{\text{MCP}} \circ \hat{\delta}_{\text{turn}})(\omega_j, u_j), \quad \omega_j = (S_j, \sigma, m_j) \in \mathbf{\Omega}$$

定理 5.1 — 跨栈失败即停前缀安全性与幂等审计终态收敛定理

对于任意由租户 τ 发起、携带唯一追踪号 κ_j 的跨栈任务请求 u_j，提升后复合算子 $\omega_{j+1} = (S_{j+1}, \sigma', m_{j+1}) = \Psi_{\text{E2E}}(\omega_j, u_j)$ 同时满足两项形式化保证：(i) 失败即停前缀安全性（**Fail-Closed Prefix Safety**）——当且仅当认知配额与模式完备、终端 `ERC-7715 / OBL-052` 安全谓词成立且公链内核 `TIP-403` 与偿付覆盖率不变量（$L_{t'} > 0 \Longrightarrow \rho_{t'} \geq 1.0000$）全部成立时，链上状态方可发生非平凡价值转移 $\sigma \to \sigma'$；(ii) 基于 `correlationId` 的幂等审计收敛性（**Idempotent Audit Convergence**）——一旦阶段 V 达成单槽确定性终局（$P_{\text{reorg}} \equiv 0$），无论阶段 VI–VII 期间是否遭遇网络抖动或进程重启，基于 κ_j 的确定性对账恢复规程必在不产生重复扣款的前提下收敛至唯一单调序号审计事件 $e^* \in S_{j+1}$，双向密码学绑定 h_{art} 与链上终局状态根 $\mathscr{R}(\sigma')$。

证明

i. 在乘积空间 $\mathbf{\Omega}$ 上，每一级提升算子对失败信封 $m = \perp$ 均定义为恒等映射：若 $\hat{\delta}_{\text{turn}}$ 配额或模式核验拒绝，则输出 $(S'_j, \sigma, \perp)$，后续算子保持 $\sigma' = \sigma$；若 $\hat{\Upsilon}_{\text{MCP}}$ 拦截越权或钓鱼载荷，终端不产出有效签名，$\sigma' = \sigma$；若链上 $\hat{\Upsilon}_{\text{L1}}$ 触发 `TIP-403` 或偿付率违例，Rust 执行内核原子回滚调用写集，故前缀安全性严格成立。(ii) 一旦 `Simplex BFT` 聚合 `3-of-4` 终局证书，$\mathscr{R}(\sigma')$ 永久不可逆；若客户端或工作台在阶段 VII 落盘前中断，重启恢复器通过确定性键 (τ, κ_j) 查询链上已终局回执并调用幂等受保护的 `appendAuditEvent`，由不变量 2.1 之单调序号锁与去重约束，系统必唯一写入一条绑定 $(h_{\text{art}}, \mathscr{R}(\sigma'))$ 的审计记录且不会重放已消耗的二维随机数 (k, ν)，证毕。

Q.E.D. ■

5.2 机器原生微支付（`x402`）与双边技术服务费确定性算术清分模型

在智能体技能编排与算力执行协同调用中，创世验证托管合约（`0x8004000000000000000000000000000000000003`）执行按次双边商业技术服务费清分（**Bilateral Fee-for-Service Split**）——其中技能授权费率参数满足合约硬约束 $\beta_{\text{bps}} \in \{0, \ldots, 5000\}$，不构成任何资金池归集、份额化收益权或被动投资分红，且 `MYRILUM LIMITED` 协议层抽成恒等于 `0%`。对于总额为 $V \in \mathbb{N}_+$（6 位精度原子单位）的单次托管服务费，合约执行确定性向下取整与余数守恒清分：

$$V_{\text{royalty}} = \left\lfloor \frac{V \cdot \beta_{\text{bps}}}{10,000} \right\rfloor, \quad V_{\text{executor}} = V - V_{\text{royalty}}, \quad V_{\text{royalty}} + V_{\text{executor}} \equiv V$$

在标准基准参数 $\beta_{\text{bps}} = 2,000$（即上层技能知识产权授权方 `skillAuthor` 获 `20%` 技术许可费、底层算力执行节点 `agentPayee` 获 `80%` 推理算力服务费）下，上述恒等式在任意不可整除微额结算中严格保证零粉尘残余锁死（**Zero Dust Accumulation**）；同时唯有经 `0x8900000000000000000000000000000000000003`（底层调用 `0x0000000000000000000000000000000000000100` `P-256` 硬件证明注册）绑定的有效 `runtimeSigner` 交付真实推理摘要方可解锁结算并累算 `ERC-8004` 履约信誉，从博弈论根源挫败女巫刷单自证攻击（Sybil Wash-Trading）。

第 06 章 · SECTION 06

形式化信任假设、密码学微架构边界与热点争用退化分析

真正的工程权威源自对系统物理极限与信任前提的绝对诚实。本章主动站在全球密码学专家、分布式系统审稿人与攻防安全红队的严苛视角，显式界定全栈三大核心子系统的精确信任边界与最坏情况退化特性。

6.1 四区域 `3-of-4` 拜占庭委员会网络几何延迟假设与主权时间锁边界

在分布式共识层，本文献所报告的 $\Delta_{\text{slot}} = 250$ ms 单槽终局与跨链履约基准建立在以下显式形式化前提之上：

1. 四节点验证委员会规模、光速网络几何与非共谋假设：受控基准拓扑配置 $N_{\text{val}} = 4$ 个分布于香港、新加坡、东京与苏黎世区域的验证节点，拜占庭容错上界为 $f = \lfloor (N_{\text{val}} - 1)/3 \rfloor = 1$，法定仲裁门限 $q = 2f + 1 = 3$。安全性（**Safety /** 零双花分叉）在任意异步网络延迟与跨洋光缆分区下无条件成立，前提是同一时期遭攻陷或串谋的验证节点数不超过 $f = 1$；活性与网络几何预算（**Liveness & Fiber Geometry**）在 Dwork-Lynch-Stockmeyer 部分同步模型下自全局稳定时间（Global Stabilization Time, GST）后成立：由于法定门限 $q = 3$，亚太三核心节点（香港–新加坡–东京，专线单向传播时延 ≤ 35 ms）在诚实亚太提案节点轮次内即可独立闭环完成三阶段公证与终局聚合（稳态耗散远低于 $\Delta_{\text{slot}} = 250$ ms），而苏黎世跨洲节点（单向约 `85–95 ms`）异步追赶同步状态；当提案轮次轮转至苏黎世或遭遇单节点离线故障时，`Simplex BFT` 本地超时虚拟空块跳过证书将最坏跨槽切换时延严格约束在 ≤ 500 ms 以内。若未来委员会向更大节点规模 $N_{\text{val}} \gg 4$ 演进，全网格广播复杂度 $O(N_{\text{val}}^2)$ 需配合门限聚合签名（如 BLS）升级并重新披露实测曲线。
2. 创世多签与后创世时间锁守卫双层治理边界：创世零块在 `0x8900000000000000000000000000000000000004` 预置 `3-of-4` 主权多签基础治理原语，并由后创世部署的安全守卫合约 `LingheSovereignSecurityGuardV5` 强制接管关键协议变更路径，废除单点管理员即时改写逻辑——一切受保护参数调整必须先排入链上公开时间锁队列并满足生效约束 $\text{eta} = t_{\text{queue}} + \Delta_{\min}$（$\Delta_{\min} \in (0, 30\ \text{days}]$），确保所有非托管终端用户与外部接入机构享有确定性的链上公开预警与无许可资产退出窗口。

6.2 分级侧信道防御模型：硅基硬件信任根（`Tier-1`）与受管运行时边界（`Tier-2`）

在应用密码学审查中，任何宣称在纯浏览器 JavaScript 虚拟机内对任意物理微架构侧信道实现“绝对恒定时间”的表述均违背现代即时编译器（JIT）底层事实。为此，`MYRILUM LingheOS Wallet v5.1.0` 建立了诚实、严密的双层密码学侧信道防御分级架构（**Two-Tier Cryptographic Side-Channel Boundary**）：

- 第一级：硅基硬件飞地与操作系统原生恒定时间核（`Tier-1 Hardware / OS Native Root`）：
  - 本地金库主密钥派生与静态加密完全委托宿主浏览器及操作系统底层 C++/汇编原生实现的 `WebCrypto SubtleCrypto` 接口（`PBKDF2-HMAC-SHA256` 强制 `600,000` 次迭代与不可导出 `AES-256-GCM` 认证加密）；
  - 机构金库强制硬件独占模式：高价值机构金库与核心策略审批强制绑定设备硅基安全飞地（如 Apple `Secure Enclave` 硬件隔离生成的不可导出 `NIST P-256` 通行密钥，链上经 `0x0000000000000000000000000000000000000100` 核验）或通过 `64` 字节分帧 `ISO-7816 WebHID` 应用协议数据单元（Application Protocol Data Units, APDUs）驱动物理气隙硬件冷签名器完成离线签名，在机构安全策略下显式禁用纯软件签名回退，确保主私钥标量永不进入宿主通用内存。
- 第二级：受限热会话 **320** 位标量盲化蒙哥马利阶梯层（`Tier-2 Scalar-Blinded Montgomery Ladder Session Plane`）：
  - 为支撑高频微额 `x402` 受托会话签名，终端纯原生椭圆曲线引擎对每次 `secp256k1` / `secp256r1` 标量乘法引入 **62** 位密码学安全随机数（**CSPRNG**）乘法标量盲化 $k' = (k \bmod n) + (3 \cdot 2^{62} + r_{62}) \cdot n$（$r_{62} \leftarrow_{\$} \{0, \ldots, 2^{62} - 1\}$，恒定锁定比特长度 $\lfloor \log_2 k' \rfloor + 1 = 320$），并在固定 320 步平衡步幅蒙哥马利阶梯（Balanced-Stride Montgomery Ladder）上执行倍点与加点运算；
  - 显式微架构与仿射求逆边界披露：由于仿射坐标点加运算内部调用基于扩展欧几里得算法的模逆函数（`modInv`），且 V8 与 JavaScriptCore 引擎内部对原生大整数 `BigInt` 采用可变长机器字数组分配、动态 JIT 分层编译与垃圾回收（GC）调度，在共享物理 CPU L1/LLC 缓存的同驻恶意进程高精度微架构计时探测（如 Prime+Probe）极端威胁模型下，纯受管语言运行时无法等同于物理安全芯片。因此，架构规范强制将 `Tier-2` 严格限制于受 `ERC-7715` 微额周期上限与合约白名单约束的短期可随时吊销会话密钥内；凡触及大额资金划转、白名单变更或守护人配置，一律强制触发 `Tier-1` 硅基硬件升级鉴权（Hardware Step-Up Authentication）。

6.3 共享状态热点写冲突下的并行执行退化包络与确定性回退定理

灵核公链的 `32` 通道二维随机数（`0x76`）消除了发送方账户级排队阻塞，但多核状态机的并行加速比在物理上仍受制于目标合约存储槽写集冲突（例如：同一毫秒内大量交易同时竞价修改沙盒参考订单簿 `0xdec0000000000000000000000000000000000000`）。

设单个 `250 ms` 共识槽内包含 m 笔已排序交易，$\alpha = G_{\text{serial}} / G_{\text{slot}} \in [0, 1]$ 为存在读写/写写存储键交集而必须按因果拓扑顺序串行执行的 Gas 工作量占比，并记乐观并发控制（Optimistic Concurrency Control, OCC）冲突检测与中止重调度归一化开销因子为 $\delta_{\text{occ}}(\alpha) \geq 0$。由广义阿姆达尔–布伦特并行调度上界（Amdahl–Brent Serialization Envelope），在 K 条并发

执行通道下的有效状态吞吐加速比 $S(\alpha, K)$ 满足：

$$S(\alpha, K) = \frac{1}{\alpha + \frac{1-\alpha}{K} + \delta_{\text{occ}}(\alpha)}, \quad \text{其中} \lim_{\alpha \to 0^+} \delta_{\text{occ}}(\alpha) = 0 \Longrightarrow \lim_{\alpha \to 0^+} S(\alpha, K) = K$$

对于读写集正交的智能体 `x402` 微支付与分片托管清分（$\alpha \approx 0, \delta_{\text{occ}} \approx 0$），系统释放接近 $K = 32$ 通道的并发吞吐；而在极端单一热点合约争用场景（$\alpha \to 1$）下，调度器确定性地退化为按区块内规范拓扑序串行执行，并由 EIP-1559 动态基础费率拥塞反馈与单通道执行时间片预算共同护航，确保单槽执行耗时始终收敛于 `250 ms` 共识预算之内，绝不引发共识死锁、非确定性状态根分叉或账本安全性违例。

表 6.1 汇总了全系统显式非主张边界与触发即停（Kill Criteria）安全熔断准则。

审计维度	显式系统边界披露（**What We Explicitly Bound**）	触发即停熔断红线（**Mandatory Kill Criteria**）
链下储备与预言机边界	链上默克尔根证明报表结构一致性与 $\geq 100\%$ 算术覆盖（基准值纯属合成测试向量），不替代持牌银行现场审计	一旦持牌部署环境下 $\rho_t < 100.00\%$ 或汇率越出 $[7.7500, 7.8500]$，内核字节码立即阻断铸造与跨链交割
智能体自治权限边界	认知模型默认被视为可被注入劫持的非授信提议器，无独立法律人格	若任何路径允许 AI 在无授权主体、无额度上限、无审计日志下划转资金，立即下线该能力
终端密码学运行时边界	严格区分 `Tier-1` 硅基硬件/OS 原生密码核与 `Tier-2` 320 位标量盲化受管热会话层	严禁机构大额金库启用纯软件签名回退或跳过 `Tier-1` 硅基硬件升级鉴权
商业可持续性边界	单位毛利必须完全依靠企业软件订阅、风控套件许可与基础设施 SLA 服务费独立为正	若任一业务线必须依赖发行代币补贴或承诺投资回报方能存续，立即否决立项

第 07 章 · SECTION 07

跨法域主权合规工程与双半球物理隔离（`Shared-Nothing`）治理架构

7.1 香港法例全景合规矩阵（第 622、32、571、656、615、155/581 及 486 章）与非发行人安全港

作为立足中国香港特别行政区的国际化科技研发企业，`MYRILUM LIMITED` 将香港现行成文法体系逐条映射为可验证的系统架构边界（表 7.1），确保在输出世界级主权协议与企业软件的同时严守纯技术研发安全港。

香港法例章号与法定名称	核心监管红线与受规管行为界定	**MYRILUM** 架构级合规隔离与技术映射
第 **622** 章《公司条例》及第 **310** 章《商业登记条例》	独立法人资格、法定注册名称及真实商业登记披露	`MYRILUM LIMITED` 依第 622 章第 899(1) 条仅以唯一英文法定公司名称注册（UBI: `80912065`，BR: `80912065-000-07-26-0`，邓白氏: `374308629`），主体权责透明清晰
第 **32** 章《公司（清盘及杂项条文）条例》（CWUMPO）及第 **571** 章《证券及期货条例》	禁止无牌招股章程、证券/期货合约要约、集体投资计划（CIS）、第 III 部自动化交易服务（ATS）及第 4/9 类投资顾问与资产管理	纯计算机科学工程规范；零公众募资、零期货/衍生品发行、零资金池分成、零订单撮合经纪与零投资顾问邀约
第 **656** 章《稳定币条例》（第 8 及第 9 条）	禁止无牌在香港发行指明稳定币，或向香港公众要约/积极推广非持牌指明稳定币	`MYRILUM LIMITED` 严守非发行人纯协议与软件研发主体定位；`LHKD` / `LUSD` 仅为非流通确定性合成基准测试状态，法币适配器仅为面向未来独立持牌机构的开放客户端接口
第 **615** 章《打击洗钱及恐怖分子资金筹集条例》（AMLO 第 5B 部第 53ZRD 条）	规管虚拟资产交易平台（VATP）托管/撮合业务及 `FATF Rec. 16` 旅行规则要求	客户端 `100%` 自托管软件（零客户私钥/资产触碰、零中心化撮合、零交易佣金抽成，非 VATP）；协议内生提供 `TIP-403` 拦截与 24h 防拆分哈希信封原语

香港法例章号与法定名称	核心监管红线与受规管行为界定	**MYRILUM** 架构级合规隔离与技术映射
第 **155** 章《银行业条例》及第 **581** 章《存款保障计划条例》	禁止非认可机构接受公众计息存款或吸收公众可偿还资金	不接受任何公众资金；底层状态机字节码恒定锁死持有端零利率 $r_{\text{holder}}(t) \equiv 0$
第 **486** 章《个人资料（私隐）条例》	个人资料收集最小化、目的限定及跨境传输安全保障	链上状态与跨链证明严格执行 **Zero Individual PII**（仅锚定不可逆 32 字节密码学摘要）

7.2 国际市场规则适配（美国 `Howey` 判例、`MiCA`、`BCBS SCO60` 及应用商店准则）与三级地理围栏

面向全球多元司法辖区与主流移动分发渠道，系统在协议与客户端层面实施精细化的法域自适应合规控制：

- 美国证券法 `Howey` 四要件结构性阻断与欧盟 `MiCA` / 巴塞尔 `SCO60` 技术对齐：企业软件客户按标准商业合同支付确定性软件订阅与算力服务费；协议内生原语 `LHC` 无通胀质押资金池或利润回购、`LUSD` / `LHKD` 锁死零生息（$r_{\text{holder}} \equiv 0$）、`ERC-8004` 仅执行按次双边算力与知识产权服务费清分（`MYRILUM` 零抽成），从结构上切断“金钱投入共同事业并依赖发行方经营努力获取投资回报”之认定链条。同时，储备证明数据结构在技术规范上兼容巴塞尔委员会 `BCBS SCO60` 审慎分类及欧盟 `MiCA` 储备核验数据格式（`MYRILUM LIMITED` 不在欧洲经济区开展任何 `MiCA` 第 16 条资产参考代币或第 48 条电子货币代币公开发行要约）。
- 客户端三级司法地理围栏与 **Apple App Store** 审核准则精确对齐（`OBL-005`）：`MYRILUM LingheOS Wallet v5.1.0` 内置确定性区域策略引擎，支持三种分级运行画像：(i) `GLOBAL_PRO` 模式——仅面向司法辖区允许的专业机构环境开放完整链上深度分析与非托管签名工具；(ii) `HK_RETAIL_STRICT` 模式——面向香港普通环境自动屏蔽未获当地零售许可的高杠杆衍生品、生息金库与事件合约入口；(iii) `APP_STORE_SAFE` 模式——严格遵循 **Apple App Store Review Guidelines** 第 `3.1.1` 条（应用内购买边界，绝不使用 `x402` 或任何加密资产在移动端应用内解锁数字软件功能或 **SaaS** 订阅权益）、第 `3.1.5(i)–(v)` 条（非托管钱包、交易、交易所、衍生品与加密应用规范）及第 `5.3` 条（博彩与事件合约限制），确保移动分发包保持纯粹合规的非托管工具属性，零未持牌法币出入金、零未授权交易撮合与零违规数字内容内购绕行。

7.3 中国境内纯人工智能工作台（`myrilum.cn`）独立法人运营与物理无共享隔离架构

针对跨法域运营中最高等级的数据合规与金融监管边界要求，本架构在顶层确立了境外全球主权研发栈（`MYRILUM LIMITED` · `myrilum.com`）与中国境内纯人工智能企业工作台（`myrilum.cn` · 工信部备案号：`京ICP备2026055724号-1`）**100%** 物理无共享隔离（**Shared-Nothing Air-Gap Architecture**）（见图 4）：

1. 独立境内法人主体与四平面物理隔离：中国境内门户 `myrilum.cn` 由独立设立的中国境内法人实体北京灵核智能体科技有限公司（统一社会信用代码：`91110108MAERKJRC8R`）依法独立运营并以人民币对公账户及增值税发票体系开展纯企业软件商业结算。境内系统在代码构建产物、境内专有网络（VPC）、独立加密数据库与密钥管理系统四个平面实施彻底物理隔离；境内构建产物 `0%` 包含任何区块链节点客户端、智能合约 ABI、加密钱包、助记词派生器、`x402` 链上微支付或跨链桥代码。
2. 境内法律法规与国标双标识全面遵循：境内纯 AI 工作台严格遵守《网络安全法》《数据安全法》《个人信息保护法》（PIPL）及《生成式人工智能服务管理暂行办法》。全量企业业务文档、`Context DNA` 与审计日志 `100%` 加密驻留于中国境内合规数据中心，底层推理请求路由至中国境内合规大模型接口并受 `providerNotice` 透明告知门禁管控（面向公众开放之生成式服务上线备案纳入 `G8` 属地合规门禁）；若个别跨国企业租户自愿启用外部联邦单点登录（SSO），涉及必要身份核验字段之跨境交互严格履行《个人信息保护法》第 38–39 条事前告知、单独同意与安全评估机制（政企私有化底座版则 `100%` 局域网物理闭环零出境）；同时全量生成合成文档、演示文稿与音视频严格执行强制性国家标准 **GB 45438-2025**《网络安全技术 人工智能生成合成内容标识办法》显式标识与文件元数据隐式双标识。



图 **04** — 全球与中国境内物理隔离（**Shared-Nothing**）双轨合规架构及企业股权三大经常性收入引擎

注：境外与境内系统实施代码仓、云网络、数据库与密钥空间的 100% 物理无共享隔离；企业商业化完全独立于任何代币发行或利差补贴。

第 08 章 · SECTION 08

企业股权商业化模型、GAAP/IFRS 经常性现金流引擎与单位经济

8.1 纯软件与算力基础设施股权价值捕获与 IAS 7 现金流勾稽公理

在国际机构投资人与香港联交所（如主板第 18C 章特专科技公司上市准则）的财务审计视角下，依赖持续增发代币补贴维持表象活跃度的项目不具备内生造血能力。MYRILUM LIMITED 确立纯企业股权价值捕获与独立主体核算公理：境外全球技术许可与基础设施 SLA 收入由香港 MYRILUM LIMITED 独立签约入账；中国境内纯 AI 企业软件收入由境内独立法人北京灵核智能体科技有限公司依法独立签约纳税入账，境内外主体账务清晰隔离、绝无违规跨境资金混同，且全集团代币发行补贴项恒定锁死为 $S_{\text{token}} \equiv 0$。

设会计期间 T 内服务 M_{ent} 家企业与机构客户，定义单客户经常性软件许可与基础设施订阅收入为 $R_{\text{sub},i}$，按实际消耗并由我方承担主要责任（Principal）计量的算力编排与验证增购收入为 $R_{\text{meter},i}$，对应边际云资源与推理履约直接营业成本为 $C_{\text{cogs},i}$。遵循《国际会计准则第 7 号——现金流量表》（IAS 7 / ASC 230），单客户单位毛利（Gross Profit, GP_i）、企业经营活动现金流（OCF_{corp}）与自由现金流（FCF_{corp}）满足严格为正的单位毛利约束与精确现金流勾稽关系（其中 C_{opex} 为研发及管理期间费用，T_{tax} 为实缴企业所得税，D_{da} 为非付现折旧摊销，ΔNWC 为含预收合同负债变动在内的净营运资本增加额，CapEx 为资本性支出）：

$$\text{GP}_i = R_{\text{sub},i} + R_{\text{meter},i} - C_{\text{cogs},i} > 0, \qquad \text{FCF}_{\text{corp}}(T) = \underbrace{\left(\sum_{i=1}^{M_{\text{ent}}} \text{GP}_i - C_{\text{opex}}(T) - T_{\text{tax}}(T) + D_{\text{da}}(T) - \Delta\text{NWC}(T)\right)}_{\widetilde{\text{OCF}_{\text{corp}}(T)}} - \text{CapEx}(T) \quad (S_{\text{token}} \equiv 0)$$

通过 @myrilum/linghe-harness-core 内置的 QuotaEntitlementMeter 前置额度预扣与组织上下文前缀缓存优化，每一次受管推理与节点核验调用均在执行前锁定正向单位毛利（$\text{GP}_i > 0$），从机制上杜绝算力倒挂亏损。

8.2 三大经常性法币收入引擎与财务确认准则（IFRS 15 / ASC 606）

表 8.1 严格按照《国际财务报告准则第 15 号——客户合同收入》（IFRS 15 / ASC 606）五步法履约义务拆分、独立售价（SSP）分摊及主要责任人/代理人（Principal vs. Agent）判定准则，界定了三大核心法币收入引擎。

商业化收入引擎	目标机构买方画像	标准化计费原语与开放核心边界	IFRS 15 / ASC 606 收入确认模式与毛利结构
引擎一：企业级 **AI WorkOS** 订阅与专属私有化部署	跨国企业、金融机构投研与法务部、咨询事务所与大型组织	年度合同订阅价值（ACV / ARR）+ Context DNA 企业记忆库扩容 + 预付工作流算力包 + 本地/专属 VPC 私有化授权与年度维保（PCS）	云端 SaaS 属持续访问权（IFRS 15.35），按履约期分期确认；私有化部署按独立售价（SSP）拆分为控制权转移时点确认的功能性知识产权使用权（IFRS 15.B58）与分期确认的维保服务；预付算力包先计入合同负债（递延收入），仅在我方承担履约主责（IFRS 15.B34–B38）时按总额法核销确认（客户自带密钥 BYOK 或端侧点对点 x402 直付不计入过手收入）
引擎二：机构级非托管策略风控台与合规审计商业套件	家族办公室、持牌资管人、支付/稳定币牌照申请机构、企业财资部	开放核心（**Open-Core**）模式：基础个人自托管客户端保持开放免费；商业版按年收取多席位 RBAC ERC-7715 策略管理台、TIP-403 /旅行规则网关、储备证明（Proof-of-Reserve, PoR）核验器、HSM 连接器及 FIFO/HIFO 财税模块许可费	纯非托管企业软件授权与支持服务，按许可期间分期或交付履约确认（100% 零资金池托管风险；稳态软件目标毛利率 > 85% [ARCHITECTURAL_SPEC]）
引擎三：多链高吞吐 **RPC**、硬件飞地验签与归档基础设施 **SLA**	量化与算法团队、机密 GPU 算力云、跨链做市商与金融科技平台	即期商业化覆盖 169 条外部异构网络低延迟专属 RPC 集群、P-256 硬件飞地批量验签通道 SLA 与合规索引数据流；受规管结算网络商业节点服务受 G9 牌照门禁前置约束（[ROADMAP_GATED]）	按基础设施服务等级协议（SLA）履约期分期确认（IFRS 15.35(a)），并依可变对价准则（IFRS 15.50–56）计提可用性赔付抵减准备

第 09 章 · SECTION 09

集团白皮书全卷谱系、版本演进对账与密码学存证总索引

9.1 四卷八册全球技术专著谱系与终端规范升级（v5.0 -> v5.1.0）对账说明

随着本集团战略与总架构白皮书（Volume 0）的正式编纂定稿，MYRILUM 构建了层次严密、中英双语结构 1:1 完全对称的“境外四卷八册全球主权专著系列 + 中国境内独立纯 **AI** 专著”完整出版文献体系（表 9.1）：

- 第 **0** 卷（Volume 0 · 本卷）：集团顶层战略总纲，统合 MYRILUM AI WorkOS、LingheOS Wallet v5.1.0 与 Linghe Chain 88888 三位一体闭环架构、跨栈乘积空间因果证明、微架构侧信道与共识网络边界、双半球物理隔离治理及 IFRS 15 / IAS 7 企业股权经济模型。
- 第 **I** 卷（Volume I · 旗舰协议黄皮书）：深入展开灵核公链六维状态空间、五阶段交易执行语义、Simplex BFT 共识活性/安全性数学证明及双椭圆曲线密码学完整代数推导。
- 第 **II** 卷（Volume II · 内生监管科技与储备证明规范）：专项形式化证明面向香港《稳定币条例》（Cap. 656）附表 2 之联系汇率走廊不变量、二叉默克尔储备核验树与内核级反洗钱控制引擎。
- 第 **III** 卷（Volume III · 系统总架构与实测性能基准精要）：面向机构技术决策者提供精炼的架构速览与端到端实测对数延迟基准数据对照。

版本演进与法定商号对账说明 — 终端规范 `v5.0 -> v5.1.0` 无损衔接与冻结摘要保护

1. 终端能力演进对账：第 I、II、III 卷（`v2.0` 冻结版）编纂于 `v5.0` 审计基线时期，彼时文中引述客户端包含 `48` 项能力与 `10` 个零信任 MCP 工具。此后，在不改变灵核公链创世零块摘要（`96208e9900b218935143be3024d2602566a86d61caa906d42399f35b83afd991`）及第 I–III 卷已冻结链上密码学指纹的前提下，团队完成了向 `MYRILUM LingheOS Wallet v5.1.0` 的向后兼容净室升级，新增 `OBL-049` 至 `OBL-060` 共 `12` 项公开标准能力（累计达 `60` 项确定性规范）并将零信任 MCP 工具扩展至 `14` 项（见表 3.1）。
2. 法定英文注册名称精确口径：依据香港《公司条例》（第 622 章）第 899(1) 条，`MYRILUM LIMITED`（UBI：`80912065`）在香港公司注册处仅登记唯一英文法定公司名称（“迈瑞伦”仅作为非注册中文品牌音译标识）；早期已冻结之第 I–III 卷中文版局部括号内出现的中文描述性译名仅作非正式参考释义，为 `100%` 保持第 I–III 卷既有 `SHA-256` 存证指纹零变动而原样封存，全卷法定主体识别一律以本总纲披露之唯一英文注册名称 `MYRILUM LIMITED` 为准。

卷册与法域归属	国际标准文献编号（**DocCode**）	语种	核心架构覆盖范围与密码学锚定状态
Volume 0（集团总纲）	`MYR-WP-MASTER-2026-V1.0-ZH` / `EN`	简体中文（国际版）/ 英文	集团三位一体总架构、形式化威胁边界、跨法域隔离与股权现金流模型（锚定 `WHITEPAPER_PUBLICATION_INDEX.json`）
Volume I（协议黄皮书）	`MYR-WP-TECH-2026-V2.0-ZH` / `EN`	简体中文（国际版）/ 英文	`Simplex BFT` 250 ms 共识、`0x76` 二维并行 EVM、`BN254` 与 `P-256` 完整数学证明（已冻结 SHA-256）
Volume II（合规与储备规范）	`MYR-WP-CAP656-2026-V2.0-ZH` / `EN`	简体中文（国际版）/ 英文	`Cap. 656` 偿付覆盖率不变量、`[7.7500, 7.8500]` 走廊与 `TIP-403` 内核拦截规范（已冻结 SHA-256）
Volume III（架构基准精要）	`MYR-WP-EXEC-2026-V2.0-ZH` / `EN`	简体中文（国际版）/ 英文	亚秒级状态机系统精要与跨链 `~936 ms` 实测对数延迟基准专著（已冻结 SHA-256）
中国境内独立专著	`MYR-WP-CN-AI-2026-V1.0-ZH`	简体中文（境内版）	由北京灵核智能体科技有限公司面向 `myrilum.cn`（京ICP备2026055724号-1）发布之纯企业级 AI WorkOS 技术白皮书

9.2 分阶段工程路线图（`G0–G9` 门禁）与独立可复现密码学核验规程

MYRILUM 拒绝以未经验证的营销时间表替代严谨的工程发布纪律，所有模块从代码合入到外部商业启用均受十级确定性发布关卡（`G0–G9`）刚性约束（表 9.2）。任何外部审计师、机构尽调团队或学术同行均可通过公开出版索引清单 `WHITEPAPER_PUBLICATION_INDEX.json` 独立复算四卷八册全部 Markdown 母本与 PDF 成书的 `SHA-256` 摘要，并对照后创世安全守卫合约 `LingheSovereignSecurityGuardV5.latestWhitepaperAnchor()` 及在线确定性核验端点 `/v1/whitepapers/verify` 验证文献完整性。

门禁阶段	工程、安全与法务准入条件（**Deterministic Gate Invariant**）	当前客观状态
`G0–G2` 范围、主张与真源关	完成跨三仓真值台账锚定，全量核心主张实现成熟度分级且反证与边界显式可见	已达成（`VERIFIED`）
`G3–G5` 原型、权责与安全关	`WorkOS` 21 包、`Wallet v5.1.0` 60 项零依赖规范与 `Chain 88888` 受控基准测试床全绿闭环；十维 `Human Gate` 落地	已达成（`VERIFIED`）
`G6–G7` 经济与司法隔离关	确立零代币补贴三大 `IFRS 15` 收入引擎；完成香港与境内 `Shared-Nothing` 物理隔离架构验证	已达成（`VERIFIED`）

门禁阶段	工程、安全与法务准入条件（**Deterministic Gate Invariant**）	当前客观状态
`G8` 外部独立审查与渠道核验关	Apple Developer Program 组织开发者资质（邓白氏 `374308629`）人工核验闭环、第三方独立安全渗透审计与专项法律意见书	推进中（`IN_REVIEW`）
`G9` 商业化规模签发关	满足目标法域全部监管牌照/备案前置条件与创始人门禁正式签发后，按区域策略分批开放机构生产级服务	门禁待启（`GATED`）

附录 A · APPENDIX A

标准与学术参考文献

1. Dwork, C., Lynch, N., & Stockmeyer, L. (1988). Consensus in the Presence of Partial Synchrony. *Journal of the ACM*, 35(2), 288–323.
2. Chan, B. Y., & Pass, R. (2023). Simplex Consensus: A Simple and Fast Consensus Protocol. *Cryptology ePrint Archive*, Paper 2023/463.
3. Shamir, A. (1979). How to Share a Secret. *Communications of the ACM*, 22(11), 612–613.
4. Groth, J. (2016). On the Size of Pairing-Based Non-Interactive Arguments. *Advances in Cryptology — EUROCRYPT 2016*, LNCS 9666, 305–326.
5. Montgomery, P. L. (1987). Speeding the Pollard and Elliptic Curve Methods of Factorization. *Mathematics of Computation*, 48(177), 243–264.
6. National Institute of Standards and Technology (NIST). (2023). *Digital Signature Standard (DSS)*, FIPS PUB 186-5 (`secp256r1` / `Ed25519`).
7. Ethereum Foundation & Open Web Standards. *EIP-712: Typed Structured Data Hashing and Signing*; *EIP-2718: Typed Transaction Envelope*; *EIP-4337: Account Abstraction Using Alt Mempool v0.7*; *EIP-4361: Sign-In with Ethereum*; *EIP-5792: Wallet Call API v2.0*; *ERC-6492: Signature Validation for Predeploy Contracts*; *EIP-6963: Multi Injected Provider Discovery*; *ERC-7579: Minimal Modular Smart Accounts*; *ERC-7683: Cross Chain Intents*; *EIP-7702: Set EOA Account Code*; *ERC-7715: Grant Permissions from Wallets*; *EIP-7951: Precompile for secp256r1 Curve Support*; *ERC-8004 (Draft): Trustless Agents*; *HTTP 402 / x402 Machine Payment Protocol*.
8. Laws of Hong Kong. *Companies Ordinance* (`Cap. 622`); *Companies (Winding Up and Miscellaneous Provisions) Ordinance* (`Cap. 32`); *Personal Data (Privacy) Ordinance* (`Cap. 486`).
9. Laws of Hong Kong. *Securities and Futures Ordinance* (`Cap. 571`); *Anti-Money Laundering and Counter-Terrorist Financing Ordinance* (`Cap. 615`); *Banking Ordinance* (`Cap. 155`).
10. Laws of Hong Kong. *Stablecoins Ordinance* (`Cap. 656`), Sections 8, 9 & Schedule 2.
11. Hong Kong Monetary Authority (HKMA). *Linked Exchange Rate System Operational Mechanism* (`7.7500–7.8500 HKD/USD` Convertibility Undertakings).
12. Financial Action Task Force (FATF). *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers* (`Recommendation 16` Travel Rule).
13. Basel Committee on Banking Supervision (BCBS). *Prudential Treatment of Cryptoasset Exposures* (`SCO60`).
14. European Parliament and Council. *Regulation (EU) 2023/1114 on Markets in Crypto-Assets (`MiCA`)*.
15. International Accounting Standards Board (IASB) & Financial Accounting Standards Board (FASB). *IFRS 15 / ASC 606: Revenue from Contracts with Customers*; *IAS 7 / ASC 230: Statement of Cash Flows*.
16. Greshake, K., et al. (2023). Not What You've Signed Up For: Compromising Real-World LLM-Integrated Applications with Indirect Prompt Injection. *Proceedings of the 16th ACM Workshop on Artificial Intelligence and Security (AISec)*.
17. Pollaczek, F. (1930). Über eine Aufgabe der Wahrscheinlichkeitstheorie. *Mathematische Zeitschrift*, 32(1), 64–100.

18. Amdahl, G. M. (1967). Validity of the Single Processor Approach to Achieving Large Scale Computing Capabilities. *AFIPS Conference Proceedings*, 30, 483–485.



VOL. 0 · GROUP MASTER ARCHITECTURE & GOVERNANCE WHITEPAPER

250 ms 单槽确定性终局 · 二叉默克尔储备核验原语 · 协议内生合规状态机

链上密码学核验凭据与协议研发主体登记卡

FROZEN SSOT · v1.0

协议与软件研发主体
MYRILUM LIMITED (HK Cap. 622 Body Corporate)

公司注册与商业登记证号
CR/UBI: 80912065 · BR: 80912065-000-07-26-0

主权网络与链标识
ChainID: 88888 (0x15b38)

后创世链上存证守卫
LingheSovereignSecurityGuardV5.
latestWhitepaperAnchor()

不可变创世零块 **SHA-256**
96208e9900b218935143be3024d2602566a86d61caa906d42399f35b83afd991

本卷 **Markdown** 母本 **SHA-256**
182a1e6c8ebb9ceef15068f12fe99eb84c844cdd6b95de94c4cca17f6e0bfef7

确定性在线核验端点
/v1/whitepapers/verify

香港法定注册办事处
UNIT 1603, 16/F THE L. PLAZA, 367-375 QUEEN'S RD CENTRAL, SHEUNG WAN, HK

© 2026 MYRILUM LIMITED. All Rights Reserved. HK Cap. 656 & EU MiCA Zero-Yield Settlement Architecture · Zero Individual PII

VOL. 0 · GROUP MASTER ARCHITECTURE & GOVERNANCE WHITEPAPER | CRYPTOGRAPHIC PROVENANCE COLOPHON · MYR-WP-MASTER-2026-V1.0-ZH