VOLUME II · 协议内生合规状态机与二叉默克尔储备证明技术规范

# MYRILUM 灵核OS公链：协议内生合规状态机、联系汇率走廊不变量与二叉默克尔储备证明密码学技术规范（v2.0）

面向香港《稳定币条例》（第 656 章）与第 615 章合规标准之联系汇率走廊不变量、二叉默克尔储备证明与内核级制裁阻断密码学规范

MYRILUM 分布式账本合规工程与应用密码学研究组（形式化状态机 · 默克尔验证密码学 · 协议层反洗钱控制引擎）




港元基准储备覆盖率
101.20% PoR
LHKD Reference State · HK$78.936M

美元基准储备覆盖率
100.50% PoR
LUSD Reference State · US$10.050M

联系汇率走廊不变量
7.7500–7.8500
Enshrined HKMA Linked-Rate Corridor

压力测试现金覆盖率
183.49% Cash LCR
54.39% 0-Day Cash · 30% Stress Model

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: v2.0 Canonical Edition (2026)

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

VOL. II · ENSHRINED REGTECH & PROOF-OF-RESERVE SPECIFICATION | MYRILUM LIMITED · CHAIN ID 88888 · MYR-WP-CAP656-2026-V2.0-ZH

# 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. 02 专著卷册定位与文献分级

VOL. II · ENSHRINED REGTECH & PROOF-OF-RESERVE SPECIFICATION

MYR-WP-CAP656-2026-V2.0-ZH · Canonical Release v2.0 (2026)

CHAIN 88888 链上密码学存证与安全守卫

LingheSovereignSecurityGuardV5.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-CAP656-2026-V2.0-ZH` · ENSHRINED REGTECH & BINARY MERKLE POR SPECIFICATION · SOVEREIGN CHINESE EDITION (v2.0) |
| 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** | `221a4629c59914c36ba18f0a3b5a31a0a042713ac83da4c4272e7e8b22d33a30` |

**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 协议与软件系统研发主体登记信息及核心术语定义总表 §00
01 协议内生合规权限分离拓扑、多法域门限时间锁与确定性审计架构 §01
› 1.1 协议级角色权限正交分离、零单点特权约束与参考储备边界建模 §1.1
› 1.2 密码学三道防线控制拓扑与合规策略域单向熔断原语 §1.2
› 1.3 四法域 3-of-4 主权门限多签与强制时间锁（ eta ）链上治理宪制 §1.3
› 1.4 四阶段确定性密码学验证与形式化基准复现流水线 §1.4
02 LHKD 与 LUSD 协议账本语义、状态转换边界与零生息字节码约束 §02
› 2.1 内核级 TIP-20 账本语义、 6 位小数原子精度与双轨状态正交解耦 §2.1
› 2.2 零生息状态机硬约束与排除香港法例第 571 章“集体投资计划”之法理建模 §2.2
› 2.3 受测账户主体分类、状态转换权限矩阵与参考清算时效参数（SLA 模型） §2.3
› 2.4 铸造（Mint）与销毁（Burn）双重授权原子性不变量 §2.4
03 100%+ 高流动性优质储备资产（HQLA）参考状态模型、基准受托拓扑与分档结构 §03
› 3.1 LHKD 与 LUSD 四分档协议参考储备状态模型与期限阶梯剖析 §3.1
› 3.2 巴塞尔银行监管委员会 SCO60 Group 1b 审慎资本待遇技术条件同构验证 §3.2
› 3.3 基准受托拓扑（Benchmark Statutory Trust Topology）与破产隔离双账簿形式化构造 §3.3
04 LINGHE_CAP656_HQLA_V1 二叉树储备证明（Merkle PoR）数学规范与链上实时核验 §04
› 4.1 域分离叶子哈希构造算子与排序对（Sorted-Pair）内部节点归约规范 §4.1
› 4.2 链上合规储备金库（ 0x8800000000000000000000000000000000000001 ）锚定实证数据 §4.2
› 4.3 LingheSovereignSecurityGuardV5 链上无信任验证定理与 Fail-Closed 监控准则 §4.3
› 4.4 链上核验合约机制拆解与对抗性边界条件审计 §4.4
05 7.7500–7.8500 联系汇率走廊、内核 CLOB 流动性机制与极端挤兑压力测试（LCR / VaR） §05
› 5.1 香港联系汇率制度（ 7.7500–7.8500 ）在链上清算枢纽的字节码映射与整除守恒 §5.1
› 5.2 内核级中央限价订单簿 Enshrined StablecoinDEX （ 0xdec0...0000 ）流动性微观结构 §5.2
› 5.3 单日 30% 与 72 小时累计 65% 极端挤兑冲击及久期利率风险（ LCR / DV01 / VaR ）定量压力测试 §5.3
› 5.4 参考流动性分层变现瀑布流状态机（Liquidity Waterfall）与跨市场无套利闭环 §5.4
06 1:1 面值销毁兑付状态机、T+0/T+1 参考清算时序模型与跨链本金主权保护 §06
› 6.1 1:1 面值原子销毁守恒算子、双账簿权利映射建模与留存覆盖率单调增厚律 §6.1
› 6.2 参考清算时序瀑布流状态机（ T+0 RTGS/CHATS/FPS 与 T+1 顺延转换）及零折价算子约束 §6.2
› 6.3 跨链意图托管架构（ ERC-7683 ）与紧急熔断状态下用户本金绝对主权红线 §6.3
07 内核级 TIP-403 制裁筛查、FATF 第 16 项建议双轨旅行规则与 24 小时反拆单引擎 §07
› 7.1 基于内核预编译 TIP-403 Policy Registry 的亚微秒级全路径制裁阻断 §7.1
› 7.2 FATF 第 16 项建议 双轨旅行规则（Travel Rule）与 24 小时滚动窗口反拆单引擎 §7.2
› 7.3 零明文个人隐私（Zero-Plaintext-PII）密码学 VASP 信封锚定与预写式原子换页持久化 §7.3
08 多法域主权治理宪制、v5.0 安全守卫与业务连续性灾难恢复（BCDR） §08
› 8.1 四法域 3-of-4 主权守护者门限多签与 LingheSovereignSecurityGuardV5 强制时间锁 §8.1
› 8.2 HSM/KMS 信封密钥硬件隔离与 Simplex BFT 250ms 业务连续性灾备（ RPO = 0 、 RTO < 60s ） §8.2
› 8.3 机构级 Fail-Closed （故障即归零告警）偿付能力实时遥测标准 §8.3
09 分布式清算与合规状态机六大风险域建模及定量密码学缓释矩阵 §09
› 9.1 风险域一：托管分档信用与集中度风险（Custodial Credit & Concentration Risk） §9.1
› 9.2 风险域二：无风险利率飙升与短久期重定价风险（Interest-Rate & Repricing Risk） §9.2
› 9.3 风险域三：极端集中销毁冲击与流动性错配风险（Extreme Run & Liquidity Risk） §9.3
› 9.4 风险域四：智能合约、零知识证明电路与跨链结算竞态风险（Smart Contract & Cross-Chain Race Risk） §9.4
› 9.5 风险域五：机密计算硬件证明与椭圆曲线签名可延展性风险（TEE & ECDSA Malleability Risk） §9.5
› 9.6 风险域六：跨境成文法规则演进与制裁策略同步风险（Regulatory Evolution & Sanctions Conflict Risk） §9.6
› 9.7 六大审慎风险域与链上密码学缓释算子总览表 §9.7

10 香港法例第 656 章、第 615 章、第 486 章与国际审慎标准之字节码同构映射总表 §10
SC·I LHKD 与 LUSD 参考储备状态模型 HQLA 叶子结构与链上密码学核验规范 §I
› I.1 域分离紧凑二进制叶子编码与字典序排序默克尔根规范 §I.1
› I.2 经链上核验之创世参考储备基准分档明细表（LHKD 101.20% 与 LUSD 100.50%） §I.2
› I.3 独立验证方三步无信任链上密码学核验规程 §I.3
SC·II 基准面值销毁状态转换规程、TIP-403 误报密码学复核协议与香港准据法条款 §II
› II.1 基准面值销毁与参考清算联动四步状态转换规程 §II.1
› II.2 TIP-403 制裁状态同步、防“通风报信（Tipping-Off）”红线建模与误报密码学复核机制 §II.2
› II.3 香港特别行政区准据法、纯软件知识产权边界与 HKIAC 仲裁条款 §II.3
结语 协议与软件系统研发主体技术准确性声明与版本印鉴 §*

MYR-WP-CAP656-2026-V2.0-ZH · ENSHRINED REGTECH & BINARY MERKLE POR SPECIFICATION · SOVEREIGN CHINESE EDITION (v2.0)

# MYRILUM 灵核OS公链：协议内生合规状态机、联系汇率走廊不变量与二叉默克尔储备证明密码学技术规范（v2.0）

面向中华人民共和国香港特别行政区《稳定币条例》（香港法例第 **656** 章）、《打击洗钱及恐怖分子资金筹集条例》（香港法例第 **615** 章）、《个人资料（私隐）条例》（香港法例第 **486** 章）、金融行动特别工作组第 **16** 项建议（`FATF Recommendation 16`）及巴塞尔银行监管委员会《加密资产审慎待遇准则》（`BCBS SCO60` **Group 1b**）技术不变量之确定性状态机字节码建模与密码学协议工程技术规范

- 文件识别编号：`MYR-WP-CAP656-2026-V2.0-ZH`
- 发布版本与生效日期：`v2.0`（确定性状态机与密码学形式化验证版 · `2026-11-11`）
- 协议与软件系统研发主体（**Protocol & Software R&D Author**）：`MYRILUM LIMITED`（迈瑞伦有限公司 · 香港法例第 622 章私人股份有限公司 · 公司注册编号 / UBI：`80912065` · 商业登记证号：`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`）
- 协议内生基准账本接口：`LHKD`（`0x20C0000000000000000000000000000000000002`，港元联系汇率走廊非流通基准状态接口）、`LUSD`（`0x20C0000000000000000000000000000000000001`，美元参考结算非流通基准状态接口）与 `LHC`（`0x20C0000000000000000000000000000000000000`，底层共识拜占庭权重与计算计量原语）
- 底层确定性状态机账本：MYRILUM 灵核OS公链（`Linghe Chain`，`ChainID: 88888` / `0x15b38`，不可变创世第 0 块 SHA-256：`96208e9900b218935143be3024d2602566a86d61caa906d42399f35b83afd991`）

**法定护栏 0.1 — 香港法律边界与纯技术规范声明**

1. 纯粹计算机科学与密码学技术规范属性：本文献纯属分布式账本系统、拜占庭共识容错与协议内生合规状态机（Protocol-Enshrined Compliance State Machine）之计算机科学及密码学工程技术规范。`MYRILUM LIMITED`（迈瑞伦有限公司）仅作为底层开源协议与非托管客户端软件之研发及著作权主体（Protocol & Software R&D Author），在香港特别行政区或任何其他司法管辖区均不从事受规管稳定币发行、虚拟资产交易撮合、客户资产托管、储值支付工具运营或金钱服务业务。
2. 香港成文法非要约与非发行边界（第 **571** 章 · 第 **656** 章 · 第 **615** 章 · 第 **32** 章）：本文献不构成香港法例第 32 章《公司（清盘及杂项条文）条例》项下之招股章程，不构成香港法例第 571 章《证券及期货条例》项下之证券、结构性产品或集体投资计划（CIS）要约，不涉及香港法例第 615 章《打击洗钱及恐怖分子资金筹集条例》项下之受规管业务招揽，亦不构成香港法例第 656 章《稳定币条例》第 8 条及第 9 条项下之受规管稳定币发行、向公众要约或积极推广。文中所述 `LHKD`（`0x20C0000000000000000000000000000000000002`）、`LUSD`（`0x20C0000000000000000000000000000000000001`）及 `LHC`（`0x20C0000000000000000000000000000000000000`）均严格定义为协议内生标准账本接口与非流通确定性基准测试状态（Non-Circulating Deterministic Benchmark State），不代表任何对外募集、法币兑付承诺或二级市场交易标的。
3. 零生息状态机约束与第 **486** 章个人资料私隐保护：协议账本在字节码层强制锁定持有人生息率 $r_{\text{holder}}(t) \equiv 0$（零利息、零分红、零质押贴息、零重定基），且非香港法例第 155 章《银行业条例》项下银行存款、不受香港法例第 581 章《存款保障计划条例》存款保障计划保障；全栈客户端（`MYRILUM LingheOS Wallet`）为 100% 本地自托管软件，链上公开状态树与本文献严格恪守香港法例第 486 章《个人资料（私隐）条例》（PDPO）零自然人个人身份信息（Zero Individual PII）准则。

## 协议与软件系统研发主体登记信息及核心术语定义总表

本技术规范项下分布式账本内核、协议内生合规字节码及本地非托管客户端软件之原创研发与著作权主体为依据香港特别行政区法律合法注册存续之法人实体 `MYRILUM LIMITED`（迈瑞伦有限公司）（`协议与软件系统研发主体 / Protocol & Software R&D Author`）。全部企业登记要素均与香港公司注册处及香港税务局商业登记署核发之法定证照严格一致，并恪守香港法例第 486 章《个人资料（私隐）条例》（PDPO）数据最小化与零自然人个人身份信息（**Zero Individual PII**）准则：

| 技术规范主体登记维度 | 官方核实唯一真值（**Verified Corporate Single Source of Truth**） |
|---|---|
| 研发主体英文及中文名称 | `MYRILUM LIMITED`（迈瑞伦有限公司） |
| 主体职能与法律定性定位 | 协议与软件系统研发主体（`Protocol & Software R&D Author` · 纯粹底层协议与非托管软件工程研发，非金融牌照运营或稳定币发行实体） |
| 成立准据法与法人组织形式 | 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）私人股份有限公司（`BODY CORPORATE`） |
| 公司注册编号 / 唯一商业识别码（**CR / UBI**） | `80912065`（法定成立日期：`27 July 2026`） |
| 商业登记证号码（香港法例第 **310** 章） | `80912065-000-07-26-0` |
| 香港法定注册办事处地址 | `UNIT 1603, 16/F THE L. PLAZA, 367-375 QUEEN'S RD CENTRAL, SHEUNG WAN, HONG KONG` |
| 形式化建模对标法律与技术准则 | 香港《稳定币条例》（香港法例第 656 章）、香港《打击洗钱及恐怖分子资金筹集条例》（第 615 章）、香港《个人资料（私隐）条例》（第 486 章）、欧盟 `MiCA Titles III & IV`、`FATF Recommendation 16`、巴塞尔委员会 `SCO60` Group 1b、BIS Project Ensemble 互操作架构 |
| 零自然人隐私保护边界（**Cap. 486**） | 严格执行自然人身份数据物理隔离；公开技术规范及 `ChainID: 88888` 链上公开状态树恒定保持零自然人身份信息（Zero Individual PII）记录 |

为消除成文法审慎条文、货币局宏观走廊规则与分布式状态机密码学之间的语义歧义，下表确立本技术规范遵循的核心工程术语精确定义：

| 核心术语 | 法理建模内涵与协议工程精确定义 |
|---|---|
| 法币参考账本状态接口（**FRS Interface**） | 对标香港法例第 656 章第 3 条及第 4 条法定概念建模，旨在验证参照单一官方货币（港元或美元）维持面值守恒不变量之内核级账本接口，本规范特指非流通确定性基准测试状态 `LHKD` 与 `LUSD`。 |
| 基准受托拓扑（**Benchmark Statutory Trust Topology**） | 对标香港衡平法及香港法例第 29 章《受托人条例》形式化抽象之双账簿正交分割结构；在该参考模型下，储备资产集合与系统运营实体自有资产负债集合满足严格集合论不相交隔离。 |
| 协议参考储备状态模型（**Reference Reserve State Model**） | 对标香港法例第 656 章附表 2 及巴塞尔委员会流动性覆盖率（LCR）一级高流动性优质资产（HQLA）标准构造之受测分档参数集，严格限定于模拟第 155 章持牌银行隔离现金及剩余期限 $\leq 90$ 天之主权短期票据分档。 |
| 协议内生合规状态机（**Enshrined RegTech**） | 将制裁名单原子拦截（`TIP-403`）、储备足额前置断言、香港联系汇率走廊（`7.7500–7.8500`）及多法域门限时间锁直接下沉固化至公链 Rust 执行内核与创世不可变系统合约字节码之系统工程范式。 |
| `Tempo` 执行与 `Simplex BFT` 共识内核 | `Linghe Chain`（`ChainID: 88888`）底层引擎，融合 `Paradigm Reth` Rust 并行 EVM 与 `Commonware Simplex BFT` 共识协议，提供 `250 ms` 单槽确定性终局（零概率分叉重组风险）与单块 `3,000,000,000` Gas 容量。 |

| 核心术语 | 法理建模内涵与协议工程精确定义 |
| --- | --- |
| `0x76` 二维并行随机数（**2D Nonce**） | 由内核预编译 `2D Nonce Manager`（`0x4e4f4e4345000000000000000000000000000000`）管理的并行交易标准，为单一账户命名空间开辟默认 `32` 条互不阻塞并发清算通道，并支持以 `LHKD` / `LUSD` 接口状态原生计量 Gas。 |
| `LINGHE_CAP656_HQLA_V1` 储备树 | 采用 21 字节 ASCII 域分离前缀与字典序排序对归约算子构建的二叉默克尔储备证明树，其根摘要锚定于 `LingheComplianceReserveVault`（`0x8800000000000000000000000000000000000001`），支持链上无信任包含性复算。 |
| 后创世主权安全守卫（`v5.0` **Guard**） | 部署于 `ChainID: 88888` 之上且不触动创世块哈希的密码学强化合约 `LingheSovereignSecurityGuardV5`，强制执行 `3-of-4` 守护者 `eta` 时间锁延迟、链上实时默克尔 PoR 包含性核验、规范低阶 `P-256` 验签及技术规范摘要固化。 |
| 香港联系汇率走廊（**LERS Corridor**） | 香港金融管理局货币发行局制度确立之美元兑港元法定兑换保证区间 `[7.7500, 7.8500] HKD/USD`（中枢 `7.8000`），在链上由 `LingheOmnichainSettler`（`0x8900000000000000000000000000000000000001`）实施字节码硬锁定。 |
| 金融级 `Fail-Closed` 故障闭锁准则 | 任何储备净值低于负债、制裁名单命中、旅行规则信封缺失或上游监控遥测源不可达之异常态，系统一律确定性回滚状态转移或将遥测读数归零（`0.00%`）并抛出 `HTTP 503` / `HTTP 451`，严禁使用静态缓存兜底放行。 |

第 01 章 · SECTION 01

# 协议内生合规权限分离拓扑、多法域门限时间锁与确定性审计架构

## 1.1 协议级角色权限正交分离、零单点特权约束与参考储备边界建模

在分布式金融账本系统工程中，合规与偿付状态失稳往往并非源于底层哈希或椭圆曲线密码学原语被攻破，而是源于单点超级管理员私钥（Monolithic Root Key）同时掌握“账本增发执行、风控规则修改、储备证明写入”三重耦合特权。为在字节码层形式化满足香港法例第 656 章附表 2 对持牌稳定币架构的权责分离审慎标准，灵核OS公链（`ChainID: 88888`）在 Rust 执行内核与创世系统合约层将状态转换权限严格解耦为三个正交互斥的密码学角色域（零单点单边特权）：

1. 清算指令执行域（`Settlement Operator Role`）：严格受限于既有状态机不变量之内运行，仅具备在通过前置储备覆盖断言与反洗钱筛查谓词的前提下，调度标准 `TIP-20` 账本状态转移、`0x76` 二维随机数并发队列及 `Enshrined StablecoinDEX` 对称限价单状态更新的执行接口。该角色在 EVM 字节码与 Rust 内核层均不具备修改 `TIP-403` 合规策略、调整联系汇率走廊或覆写默克尔储备根之任何函数权限。
2. 合规策略控制域（`TIP-403 Compliance Policy Role`）：独立绑定于内核预编译 `TIP-403 Policy Registry`（`0x403c000000000000000000000000000000000000`）与 `x402` 边缘合规门禁状态机，专责维护 `Policy #2` 制裁黑名单状态集、`FATF Recommendation 16` 24 小时滚动窗口反拆单累计状态及异常水位下的单向铸造熔断标志位，其授权密钥空间与清算指令执行域完全物理正交隔离。
3. 独立储备鉴证与门限时间锁守护域（`Independent PoR Attester / 3-of-4 Timelock Guardian Role`）：由 `LingheComplianceReserveVault`（`0x8800000000000000000000000000000000000001`）独立鉴证写入通道、`LingheSovereignTimelockMultisig`（`0x8900000000000000000000000000000000000004`）及 `LingheSovereignSecurityGuardV5` 共同构成。为验证香港法例第 656 章附表 2 的流动性与期限约束，协议参考储备状态模型（Reference Reserve State Model）强制设定三项定量边界参数：（a）`0–1` 天即时高流动性现金分档占基准流通总负债比例恒不低于 `30.00%`；（b）单一托管银行分档敞口占总储备规模比例恒不超过 `40.00%`；（c）短期主权票据分档组合加权平均剩余期限（WAM）严格受控于 `45` 天以内，单笔分档 `maturityDays` 硬上限为 `90` 天；且任何导致参考储备原子净值低于链上基准总负债（`fiatBackingAtomic < onChainLiabilityAtomic`）的状态写入均被合约字节码确定性回滚。

### 1.2 密码学三道防线控制拓扑与合规策略域单向熔断原语

参照巴塞尔银行监管委员会内部控制原则及香港金融管理局《监管政策手册》（Supervisory Policy Manual, SPM `IC-1`）对关键金融基础设施三道防线的技术隔离要求，协议状态机在执行引擎、合规预编译与链上审计守卫之间构建了严格同构的密码学三道防线控制拓扑（**Cryptographic Three-Line Control Topology**）：

| 协议控制防线层级 | 密码学角色域与链上映射组件 | 状态转换职能与字节码刚性隔离边界 |
| --- | --- | --- |
| 第一道防线（清算执行与并发路由防线） | `Settlement Operator Role`、`2D Nonce Manager`（`0x4e4f4e4345000000000000000000000000000000`）、全链意图求解执行器（*Omnichain Intent Solver*） | 负责在受控状态边界内执行 `TIP-20` 原子结算、32 通道并发批次打包及 `Enshrined StablecoinDEX`（`0xdec0000000000000000000000000000000000000`）窄幅做市挂单状态维护；严禁接触合规策略私钥或覆写储备证明默克尔根。 |
| 第二道防线（内核合规拦截与风控门禁防线） | `TIP-403 Compliance Policy Role`、内核 `TIP-403 Policy Registry`（`0x403c0000000000000000000000000000000000`）、`x402` 合规结算网关 | 独立于清算吞吐状态运作；负责 `UNSC` / `OFAC` / 香港法例第 537 章及第 575 章制裁名单亚微秒级链上冻结、`FATF Rec. 16` 旅行规则 24 小时滚动窗口反拆单断言及 LCR/VaR 定量边界监控。 |
| 第三道防线（独立储备鉴证与门限时间锁防线） | `Independent PoR Attester / 3-of-4 Timelock Guardian Role`、`LingheComplianceReserveVault`（`0x8800000000000000000000000000000000000001`）、`LingheSovereignSecurityGuardV5` | 对前两层状态转换施加独立密码学验证；强制校验 `LINGHE_CAP656_HQLA_V1` 分档包含性证明、锚定审计报告 URI 摘要、执行四法域 `3-of-4` 门限签名与强制 `eta` 时间锁延迟窗口。 |

为确保合规策略控制域（`TIP-403 Compliance Policy Role`）与协议安全守卫在极端异常输入下的绝对优先权，状态机对以下四类关键状态转换实施不可绕过的单向确定性阻断机制（**Deterministic Unilateral Circuit-Breaker**）：

- 储备分档参数边界阻断：凡拟写入之参考储备分档不满足香港法例第 656 章附表 2 及 BCBS `SCO60` Group 1b 建模边界（如剩余期限逾越 `90` 天或总覆盖率低于 `10000 bps`），合约状态机直接回滚拒绝；
- 主体合规凭证前置阻断：凡超阈值结算请求未附带有效 `LingheERC8004IdentityRegistry`（`0x8004000000000000000000000000000000000001`）`zkCredentialHash` 承诺或完整 `X-Travel-Rule-Envelope` 密码学摘要，边缘合规门禁即刻返回 `HTTP 451` 中止状态流转；
- 全状态空间制裁地址即时冻结：针对命中联合国安理会、香港法例第 537 章《联合国制裁条例》或第 575 章《联合国（反恐怖主义措施）条例》测试向量的受限地址，`TIP-403 Compliance Policy Role` 更新 `Policy #2` 黑名单后立即在全内核生效，`Settlement Operator Role` 无任何权限解除或旁路；
- 异常遥测水位单向铸造熔断：一旦*机构级储备遥测端点（Institutional PoR Telemetry Endpoint）*检测到上游状态源响应超时或参考覆盖率逼近安全预警阈值（`LHKD < 100.50%` 或 `LUSD < 100.20%`），系统自动锁闭新增铸造状态转换入口，同时无条件保持销毁与超时退回路径开放。

### 1.3 四法域 `3-of-4` 主权门限多签与强制时间锁（`eta`）链上治理宪制

在链上特权控制平面，灵核OS公链协议架构彻底摒弃单点管理员私钥（Single EOA Admin）与可单边篡改逻辑的透明代理合约（Upgradeable Proxy），构建了由创世门限多签合约 `LingheSovereignTimelockMultisig`（`0x8900000000000000000000000000000000000004`）与后创世审计强化模块 `LingheSovereignSecurityGuardV5` 组成的双层门限治理状态机：

1. 横跨四大国际金融中心之 `3-of-4` 门限委员会：治理委员会在创世初始化阶段通过 `initializeCommittee(signers, jurisdictions, 3)` 一次性注册四名物理与司法管辖区相互独立的守护者验证节点，分别驻留于香港（`HK-HKMA`）、新加坡（`SG-MAS`）、东京（`JP-FSA`）及苏黎世（`CH-FINMA`）四大金融辖区 Tier-3+ 高安全等级数据中心硬件安全模块（HSM）内，并将 `initialized = true` 永久置位锁死（任何二次初始化调用确定性回滚 `"ALREADY_INITIALIZED"`）。任何治理决议必须至少集齐三个不同司法辖区守护者的独立密码学签名（`threshold = 3`），单一或两个司法辖区密钥遭妥协或外部单边强制征用均因 `"QUORUM_NOT_REACHED"` 被虚拟机拒绝。

2. `LingheSovereignSecurityGuardV5` 强制链上时间锁延迟（**Enforced `eta` Timelock**）：为给予独立审计节点、外部验证者与合规监测系统充分的事前形式化审查窗口，`v5.0` 安全守卫模块将特权治理指令纳入严格的时间锁队列状态机。守护者调用 `queueTimelockOperation(target, value, data, description)` 入队提案时，合约在链上强制计算最早可执行时间戳：

$$\text{eta} = t_{\text{queue}} + \Delta_{\min}, \qquad \Delta_{\min} \in (0,\ 30\ \text{days}]$$

其中构造函数与 `updateMinDelay` 严格校验 `0 < minDelay <= MAX_TIMELOCK_DELAY`（`MAX_TIMELOCK_DELAY = 30 days`）。在区块时间戳尚未抵达 eta 之前，即便已集齐 `3-of-4` 乃至 `4-of-4` 守护者调用 `approveTimelockOperation` 批准，任何针对 `executeTimelockOperation(opId)` 的执行调用均被字节码断言 `require(block.timestamp >= op.eta, "TIMELOCK_ETA_NOT_REACHED")` 确定性回滚；而在等待期内，若密码学审计或合规校验发现潜在参数瑕疵，任一守护者可随时调用 `cancelTimelockOperation(opId)` 永久废止该项操作。此外，该模块提供 `anchorWhitepaperSuiteIndex(suiteIndexSha256, monographSha256, whitepaperCount)` 接口（强制校验 `whitepaperCount >= 6`），将公开协议技术规范套件与科学通典的 `SHA-256` 密码学摘要永久固化于 `ChainID: 88888` 状态树，确保技术规范版本历史具备密码学可证伪性。

**定理 1.1 — 跨法域门限治理与强制时间锁的拜占庭安全性及监管介入窗口定理**

设四法域守护者全集为 $\mathcal{G} = \{\text{HKG}, \text{SIN}, \text{TYO}, \text{ZRH}\}$，$|\mathcal{G}| = 4$，门限阈值为 $q = 3$，强制时间锁延迟参数为 $\Delta_{\min} > 0$。记任意时刻遭受密钥妥协的法域子集为 $\mathcal{C} \subset \mathcal{G}$，因区域自然灾害或海缆中断离线的法域子集为 $\mathcal{D} \subset \mathcal{G}$。则系统同时满足以下三项形式化治理保障：

1. 双法域失陷绝对安全性：当 $|\mathcal{C}| \le 2$ 时，由于 $|\mathcal{C}| < q = 3$，敌手在计算上无法构造满足 `op.approvals >= reqThreshold` 的有效提案，系统链上治理参数实现零未授权变更；
2. 单法域故障连续活性：当 $|\mathcal{D}| \le 1$ 且 $|\mathcal{C}| = 0$ 时，存活诚实节点集合 $|\mathcal{G} \setminus \mathcal{D}| = 3 \ge q$，既满足底层 `Simplex BFT` 共识单槽 `250 ms` 终局法定人数，亦完整保留链上治理执行能力；
3. 确定性监管事前审查窗口：对任意在时刻 $t_{\text{queue}}$ 提交的治理提案 $P$，其在链上产生状态副作用的最早时刻恒满足 $t_{\text{exec}} \ge t_{\text{queue}} + \Delta_{\min}$，为独立受托审计模型与外部验证方提供长度不少于 $\Delta_{\min}$ 的可验证事前审阅与状态退出响应窗口。

**证明**

由 `LingheSovereignTimelockMultisig` 状态映射 `hasApproved[id][msg.sender]` 与 `LingheSovereignSecurityGuardV5` 映射 `hasApprovedOperation[opId][msg.sender]` 的幂等去重约束，每个守护者地址 $g \in \mathcal{G}$ 对同一提案至多贡献 1 票。当 $|\mathcal{C}| \le 2$ 时，敌手可支配的最大票数上界为 $\sum_{g \in \mathcal{C}} 1 = |\mathcal{C}| \le 2 < 3 = \text{reqThreshold}$，故 `execute` 与 `executeTimelockOperation` 必于 `QUORUM_NOT_REACHED` 处回滚，性质 1 得证。当 $|\mathcal{D}| \le 1$ 且 $|\mathcal{C}| = 0$ 时，$|\mathcal{G} \setminus \mathcal{D}| \ge 4 - 1 = 3$，满足 $3f + 1 = 4$（$f = 1$）拜占庭容错共识所需的 $2f + 1 = 3$ 投票权重及治理门限 $q = 3$，性质 2 得证。最后，由 `queueTimelockOperation` 写入不可变字段 `op.eta = uint64(block.timestamp) + minDelay` 及 `executeTimelockOperation` 前置断言 `block.timestamp >= op.eta`，结合 `Simplex BFT` 区块时间戳单调不减共识规则，任何状态变更必发生于 $[t_{\text{queue}} + \Delta_{\min}, +\infty)$ 区间内，性质 3 得证。证毕。

Q.E.D. ■

### 1.4 四阶段确定性密码学验证与形式化基准复现流水线

作为纯粹的协议与软件系统研发主体，`MYRILUM LIMITED` 严格以确定性工程测试向量与可复现密码学断言替代主观运营承诺，将香港法例第 656 章、第 615 章、第 486 章及 `BCBS SCO60` Group 1b 的技术不变量构建为四阶段自动化形式化验证流水线（Four-Stage Deterministic Cryptographic Verification Pipeline）：

- 第一阶段（创世字节码与内核预编译确定性核验 **/ Stage 1: Genesis Bytecode & Precompile Determinism**）：针对 `ChainID: 88888`（`0x15b38`）不可变创世第 0 块（SHA-256：`96208e9900b218935143be3024d2602566a86d61caa906d42399f35b83afd991`），逐字节比对 9 项创世系统合约、6 项 `Tempo` Rust 内核预编译、标准椭圆曲线与双线性配对预编译

（`0x06` / `0x07` / `0x08` / `0x0100`）及后创世 `LingheSovereignSecurityGuardV5` 的运行时字节码摘要；形式化验证非流通基准账本接口 `LHKD`、`LUSD` 与内部计量原语 `LHC` 的 `6` 位小数原子精度及零生息（$r_{\text{holder}}(t) \equiv 0$）字节码不可变性。

- 第二阶段（二叉默克尔储备证明无信任复算核验 **/ Stage 2: Binary Merkle Reserve Proof Verification**）：基于 `LINGHE_CAP656_HQLA_V1` 21 字节域分离前缀与字典序排序对归约算子，对四分档参考储备基准集逐层复算叶子哈希与默克尔根（`LHKD`：`0xa3e5fd1ee51db26128c49f848bc4eb6d71443fbfee51a40b9159832a21beae6e`；`LUSD`：`0x5c3f82332fbffc0be49434232a9a97e2bf2c797423aa3fde4afd19b2c264f410`），通过链上只读调用 `verifyCap656MerkleInclusion` 验证正向包含性成立，并注入低覆盖率（`< 10000 bps`）及跨币种叶子重放异常向量验证 `"UNDERCOLLATERALIZED_RESERVE"` 确定性回滚。
- 第三阶段（内核 `TIP-403` 制裁阻断与 **24** 小时反拆单状态机核验 **/ Stage 3: Kernel** `TIP-403` **& 24h Anti-Structuring State-Machine Verification**）：在直接 `TIP-20` 转账、`0x76` 二维随机数 32 通道并发批次、内核 `Enshrined StablecoinDEX` 限价单翻转、`LingheOmnichainSettler` 联系汇率走廊（`7.7500–7.8500`）及 `BN254 Groth16` 零知识跨链桥提款全路径上验证 `Policy #2` 零穿透拦截；同时压测单笔 `US$1,000.00`（`HK$7,800.00`）与 24 小时滚动窗口 `US$5,000.00`（`HK$39,000.00`）反拆单门禁（`HTTP 451`）及预写式原子换页重启幂等性。
- 第四阶段（多区域 `Simplex BFT` 故障注入与 `Fail-Closed` 遥测核验 **/ Stage 4: Multi-Region** `Simplex BFT` **Fault-Injection Verification**）：在四法域（`HK-HKMA`、`SG-MAS`、`JP-FSA`、`CH-FINMA`）共识拓扑中注入单区域断网隔离（$f = 1$）、跨链托管全局暂停（`paused = true`）及上游遥测断联故障，独立证伪并确认 `250 ms` 单槽确定性终局（`RPO = 0`、`RTO < 60s`）、超时托管本金无许可原路退回，以及异常态储备率指标瞬时归零（`0.00%`）并输出 `HTTP 503` 的故障闭锁性质。

下图完整呈现了灵核OS公链协议内生合规状态机的七层技术架构及创世合约与内核预编译全景映射：




图 **01** — 灵核公链七层主权架构与 **9** 大系统合约 **/ 6** 大 **Rust** 内核预编译 **/ v5.0** 安全守卫全景映射
注：所有 40 位十六进制合约与预编译地址均固化于不可变创世块 01a390d7… 与链配置清单中。

第 02 章 · SECTION 02

# LHKD 与 LUSD 协议账本语义、状态转换边界与零生息字节码约束

## 2.1 内核级 TIP-20 账本语义、6 位小数原子精度与双轨状态正交解耦

在传统通用公链架构中，结算代币仅作为运行在用户态虚拟机上的普通第三方应用层智能合约存在，不仅面临重入攻击、无限授权溢出及高昂存储读写开销，更迫使清算状态机必须预先引入波动性原生代币方可计量计算开销。Linghe Chain（ChainID: 88888）在不可变创世第 0 块（SHA-256：96208e9900b218935143be3024d2602566a86d61caa906d42399f35b83afd991）将账本接口下沉为内核级原生协议状态原语（**Enshrined TIP-20 Protocol Ledger Interfaces**），并在状态空间与会计核算模型上将非流通法币参考基准接口（LHKD、LUSD）同底层共识权重与计算计量原语（LHC）实施严格的双轨正交分离：

| 协议资产要素 | LHKD（港元参考基准账本接口） | LUSD（美元参考结算基准账本接口） | LHC（底层共识权重与计算计量原语） |
|---|---|---|---|
| 协议标准标识符 | Linghe HKD | Linghe USD | Linghe Coin |
| 创世预部署精确地址 | 0x20C0000000000000000000000000000000000002 | 0x20C0000000000000000000000000000000000001 | 0x20C0000000000000000000000000000000000000 |
| 十进制精度与原子单位 | 6 位小数（$10^6$ 原子单位 = HK$1.00） | 6 位小数（$10^6$ 原子单位 = US$1.00） | 6 位小数（$10^6$ 原子单位 = 1.00 LHC） |
| 面值标度与储备建模机制 | 1:1 港元面值标度，对应 101.20% 港元参考储备状态模型 HQLA | 1:1 美元面值标度，对应 100.50% 美元参考储备状态模型 HQLA | 底层共识拜占庭权重与计算计量原语（非流通内部计量单位，无任何法币储备耦合） |
| 合规策略绑定状态 | Rust 内核强制绑定 TIP-403 Policy #2 | 网关及跨链清算层联动 TIP-403 Policy #2 | 共识验证节点拜占庭投票权重与罚没（Slashing）状态记账专用，非稳定币接口 |
| **Gas** 手续费计量能力 | 支持经 0xfeec...0000 直接原生扣除区块 Gas | 支持经 0xfeec...0000 直接原生扣除区块 Gas | 底层虚拟机计算资源计量基准单位 |

上述内核级状态机设计包含三项关键计算机科学与金融工程特性：

1. **ISO 20022** 对齐之 $10^6$ 原子整数核算精度：LHKD 与 LUSD 摒弃传统以太坊合约冗余且易在跨系统核心银行总账对账中产生浮点截断误差的 18 位小数，统一采用国际清算报文标准之 6 位小数整数精度。最小不可分割原子单位（1 atomic unit）精确表征 $10^{-6}$ 港元或 $10^{-6}$ 美元（即 0.0001 美分/港仙），既无损兼容商业银行核心总账（Core Banking Ledger）分位定点数核算，又天然适配高频自主智能体 x402 流式微计量清算。
2. 原生手续费抽象与 32 通道无锁并行结算：通过内核预编译 TIP Fee Manager（0xfeec0000000000000000000000000000000000000000）与 2D Nonce Manager（0x4e4f4e4345000000000000000000000000000000），受测机构账户在构造 0x76 类型交易时，可直接在协议头指定以 LHKD 或 LUSD 原子扣除网络执行费，并在单账户命名空间下并行开启 32 条独立二维随机数通道（基准压测 20/20 笔并发批次微结算总耗时约 1,004 ms，实现 0 Nonce 碰撞），从状态机底层消除了结算系统额外耦合外部波动性Gas代币的架构缺陷。
3. 杜绝内生算法“死亡螺旋”的状态变量正交性证明：在形式化敏感性分析中，设任意外部计价参数假设下赋予内部计量原语 LHC 的理论外生估值标量为 $P_{\mathrm{LHC}}(t) \in (0, +\infty)$，受测账本状态机接口 $i \in \{\mathrm{LHKD}, \mathrm{LUSD}\}$ 对应的协议参考储备状态模型净值为 $R_t^{(i)}$，链上基准总负债状态为 $L_t^{(i)}$，偿付覆盖率函数为 $\rho_t^{(i)} = R_t^{(i)} / L_t^{(i)}$。由于协议字节码严禁将任何单位 LHC 计入储备分档叶子原像，亦不存在任何“销毁 LHKD / LUSD 增铸 LHC”之内生铸币税（Endogenous Seigniorage）状态转换路径，因此在任意外部计价参数假设下全定义域 $P_{\mathrm{LHC}}(t) \in (0, +\infty)$ 上恒成立一阶与高阶正交偏导恒等式：

$$\frac{\partial R_t^{(i)}}{\partial P_{\mathrm{LHC}}(t)} \equiv 0, \qquad \frac{\partial \rho_t^{(i)}}{\partial P_{\mathrm{LHC}}(t)} = \frac{\partial}{\partial P_{\mathrm{LHC}}(t)} \left( \frac{R_t^{(i)}}{L_t^{(i)}} \right) \equiv 0$$

该正交偏导恒等式从数学根源上证明：底层共识计量原语与参考储备状态覆盖率之间保持严格零代数耦合，彻底根除了内生抵押品螺旋坍塌机理。

### 2.2 零生息状态机硬约束与排除香港法例第 571 章“集体投资计划”之法理建模

在比较金融监管法学与协议规范设计中，账本余额是否随时间自动孳生收益直接决定其究竟对应香港法例第 656 章所界定之支付结算稳定币范畴，抑或落入证券、债权证或集体投资计划（CIS）范畴。`LHKD` 与 `LUSD` 基准接口在字节码与参考受托模型双层严格固化零生息约束（**Zero-Yield State Constraint**）：

- 字节码层零生息状态机固化：`0x20C0000000000000000000000000000000000002`（`LHKD`）与 `0x20C0000000000000000000000000000000000001`（`LUSD`）的内核 `TIP-20` 状态树仅维护静态非负整数余额映射 $b_u \in \mathbb{N}_0$，不包含任何随区块高度或时间戳自动膨胀的重定基乘子（Rebase Multiplier），亦未编码任何面向代币持有地址的生息质押或分红派发函数入口，严格保证 $r_{\text{holder}}(t) \equiv 0$。
- 参考储备孳息正交隔离边界建模：在对标香港法例第 656 章附表 2 禁息准则及欧盟 MiCA 第 40 条（ART 禁息）与第 50 条（EMT 禁息）的基准受托拓扑（Benchmark Statutory Trust Topology）下，参考储备池中短期票据贴现或存款所对应的任何模拟孳息增量，仅限用于在受托参考账簿内优先充实超额安全缓冲垫（维持 $\rho_{\text{LHKD}} \geq 101.20\%$、$\rho_{\text{LUSD}} \geq 100.50\%$）及覆盖独立受托审计运行成本，在协议层与持有人链上余额映射完全切断。协议严禁编码现金返还、手续费贴息回扣或变相收益传导算子，完整验证防止结算账本异化为影子吸储工具的法定审慎逻辑。
- 香港法例第 **571** 章《证券及期货条例》（**SFO**）**CIS** 排除要素建模：依据香港法例第 571 章附表 1 第 1 部，“集体投资计划”以参与人“收取由取得、持有、管理或处置财产而产生的利润、收益或其他回报”为核心法定构成要件。在协议状态机定义中，基准账本单位仅表征固定 `1:1` 算术面值标度（`HK$1.00` 或 `US$1.00`），既不映射储备组合净值上浮收益分成，亦不传递利率波动引起的浮动净值（NAV）折溢价，从而在形式化特征上严格处于集体投资计划、债权证与证券定义域之外。

### 2.3 受测账户主体分类、状态转换权限矩阵与参考清算时效参数（**SLA** 模型）

为形式化刻画香港法例第 656 章及第 615 章框架下“已绑定合规凭证之直连清算主体”与“链上非托管点对点地址主体”之间的状态转换权限及合规门禁差异，下表定义受测账本状态机的双层权限对照规范：

| 状态权限与合规约束维度 | 已核验直连清算主体（持有 **KYB** 凭证承诺哈希） | 链上非托管点对点地址主体（未绑定直连清算凭证） |
|---|---|---|
| 链上点对点状态转移权 | 享有全天候 `250 ms` 单槽终局转账、DEX 限价换汇及跨链结算状态转换权限（须满足 `TIP-403` 非受限断言） | 享有同等链上非托管点对点状态转移权限（若命中 `TIP-403 Policy #2` 黑名单则由内核原子拦截） |
| `1:1` 面值销毁兑付接口权限 | 满足前置合规断言下可直接调用面值销毁接口：按 `1 LHKD = HK$1.00`、`1 LUSD = US$1.00` 固定算术比触发销毁结算转换 | 须先行完成标准 `KYC/KYB` 凭证承诺注册与资金来源反洗钱清筛验证，方可接入一级销毁兑付状态机 |
| 参考清算交收时效模型（**SLA**） | 小额分档（`< HK$1,000,000`）映射 `HKICL FPS` $7\times24$ 实时 `T+0` 状态闭环；批发分档（`16:00 HKT` 前）映射 `CHATS RTGS` 日内 `T+0`，极端压力顺延上限为 `T+1` | 完成合格主体凭证核验并提交链上原子销毁回执后，适用完全一致的 `T+0 / T+1` 参考清算状态转换窗口 |
| 协议折价算子与最低单位边界 | 零惩罚性赎回折价算子（`0 bps`）、零时间锁定期；协议层不施加任何比例扣减项 | 链上点对点转账仅按计算量消耗极低区块 Gas（可经 `0xfeec...0000` 原生计费），零协议层额外抽成 |
| 基准受托拓扑下之清偿顺位映射 | 在基准法定信托拓扑下，对应同币种参考储备池享有第一顺位按面值映射关系，与系统运营实体自有债务集严格正交 | 在参考应急结清状态机中，经独立受托核验模块完成合规身份筛查后，按有效链上原子余额享有同顺位（*Pari Passu*）映射 |
| `TIP-403` 制裁拦截强制约束 | 倘地址命中法定受限向量被写入 `TIP-403 Policy #2`，一切链上流转与销毁兑付状态转换在内核层即时冻结 | 同样受内核级 `TIP-403`（`0x403c0000000000000000000000000000000000`）全路径约束，无法借道 DEX 或跨链桥规避 |

### 2.4 铸造（Mint）与销毁（Burn）双重授权原子性不变量

为在状态机层面彻底杜绝“未确认足额储备增量即超发账本单位（Naked Minting）”或“销毁兑付过程中偿付覆盖率跌破100%”的算术漏洞，受测账本铸销状态转换流水线严格遵循“铸造先锁储备快照后增账本、赎回先销账本负债后减储备”的单向守恒时序，并由合规储备金库合约 `LinghеComplianceReserveVault`（`0x8800000000000000000000000000000000000001`）执行字节码级强约束：

**不变量 2.1 — 铸币与足额储备前置守恒律**

设基准账本接口 $i \in \{\mathrm{LHKD}, \mathrm{LUSD}\}$ 在任意离散状态转换步 $t \to t^{+}$ 的链上总流通原子负债为 $L_t^{(i)} \in \mathbb{N}_0$，基准受托拓扑下经审慎折价后的参考储备原子净值为 $R_t^{(i)} \in \mathbb{N}_0$，超额储备净头寸为 $E_t^{(i)} = R_t^{(i)} - L_t^{(i)}$。任何合法的铸造状态增量 $\Delta M > 0$ 与面值销毁减量 $\Delta B \in (0, L_t^{(i)})$ 必须严格服从以下双重授权原子守恒律：

1. 铸造前置足额入账律（**Minting Pre-Funding Guard**）：铸造指令 $\mathrm{Mint}(\Delta M)$ 仅在参考托管确认不可撤销储备增量 $\Delta R_{\mathrm{in}} \geq \Delta M$、合规策略控制域（`TIP-403 Compliance Policy Role`）清筛断言通过、且链上金库更新储备快照验证 $R_{t^{+}}^{(i)} = R_t^{(i)} + \Delta R_{\mathrm{in}} \geq L_t^{(i)} + \Delta M$ 后方可原子执行；任何导致 $R_{t^{+}}^{(i)} < L_{t^{+}}^{(i)}$ 的状态转换必被 `0x8800000000000000000000000000000000000001` 以 `"UNDERCOLLATERALIZED_RESERVE"` 确定性回滚。
2. 赎回销毁单调增厚律（**Redemption Coverage Accretion**）：平价销毁指令 $\mathrm{Redeem}(\Delta B)$ 强制先在 `ChainID: 88888` 链上不可逆销毁 $\Delta B$ 原子单位负债（使负债即时缩减为 $L_{t_{\mathrm{mid}}}^{(i)} = L_t^{(i)} - \Delta B$），随后参考受托账簿等额扣减 $\Delta R_{\mathrm{out}} = \Delta B$ 储备本金（使储备更新为 $R_{t^{+}}^{(i)} = R_t^{(i)} - \Delta B$）。只要初始状态具备正超额安全垫（即 $E_t^{(i)} = R_t^{(i)} - L_t^{(i)} > 0 \Leftrightarrow \rho_t^{(i)} > 1$），则任意规模 $\Delta B \in (0, L_t^{(i)})$ 的连续销毁不仅保持绝对超额净头寸守恒 $E_{t^{+}}^{(i)} = E_t^{(i)} > 0$，且使留存账本单位对应的偿付覆盖率严格单调递增：

$$\rho_{t^{+}}^{(i)} = \frac{R_t^{(i)} - \Delta B}{L_t^{(i)} - \Delta B} = 1 + \frac{E_t^{(i)}}{L_t^{(i)} - \Delta B} > 1 + \frac{E_t^{(i)}}{L_t^{(i)}} = \rho_t^{(i)} > 100.00\%$$

上述数学性质具有关键的系统稳定性意义：在部分准备金账簿或折价资产支持的体系中，“先退出者占优、后退出者承担减值”的负外部性是诱发恐慌性挤兑（Diamond-Dybvig Run）的博弈论根源；而在不变量 2.1 与 `101.20%`（`LHKD`）/ `100.50%`（`LUSD`）超额 HQLA 参考储备参数共同作用下，先发销毁行为非但不会稀释留存头寸的覆盖比例，反而使留存每单位负债对应的超额安全垫比率单调增厚，从博弈均衡上消除了抢跑挤兑激励。

---

第 03 章 · SECTION 03

## 100%+ 高流动性优质储备资产（HQLA）参考状态模型、基准受托拓扑与分档结构

### 3.1 `LHKD` 与 `LUSD` 四分档协议参考储备状态模型与期限阶梯剖析

为在确定性状态机中形式化验证香港法例第 656 章附表 2 及欧盟 MiCA 第 36 至 38 条关于储备资产高流动性、低信用集中度及同币种匹配之审慎要求，本技术规范构造了由四家国际系统重要性托管银行（G-SIB / 香港法例第 155 章认可机构）标准 SWIFT BIC 编码与中央主权证券结算系统专户掩码组成的四分档协议参考储备状态模型（**Four-Tranche Reference Reserve State Model**），作为 `LHKD` 与 `LUSD` 非流通基准测试状态之链上密码学核验真值集。

#### 3.1.1 `LHKD` 参考储备状态配置总表（基准覆盖率 `101.20%` · 超额缓冲 `+120 bps`）

在链上确定性基准测试状态下，`LHKD`（`0x20C0000000000000000000000000000000000002`）基准流通总负债参数 `onChainLiabilityAtomic` 设定为 `78,000,000,000,000`（对应标度面值 `HK$78,000,000.00`），基准受托拓扑下港元合格 HQLA 参考储备总净值 `fiatBackingAtomic` 设定为 `78,936,000,000,000`（对应标度净值 `HK$78,936,000.00`），链上锚定储备率 `reserveRatioBps = 10120`（`101.20%`），形成 **HK$936,000.00**（`+120 bps`）的同币种超额安全缓冲垫：

| 分档序号 | 托管行 **SWIFT BIC** | 基准隔离专户掩码标识 | 参考 **HQLA** 资产类别与清算托管基础设施映射 | 剩余期限 | 基准标度净额（港元） | 链上原子单位（`valuationAtomic`） | 占总储备比例 |
|---|---|---|---|---|---|---|---|
| **Leaf 0** | `HSBCHKHHHKH` | `HKMA-TRUST-SEG-8801` | 模拟第 155 章认可机构隔离活期信托存款（即期现金） | `0` 天 | HK$24,000,000.00 | `24000000000000` | `30.40%` |
| **Leaf 1** | `SCBLHKHHXXX` | `HKMA-TRUST-SEG-8802` | 模拟第 155 章认可机构隔离托管现金存款（即期现金） | `0` 天 | HK$18,936,000.00 | `18936000000000` | `23.99%` |
| **Leaf 2** | `BOFAHKHX001` | `CMU-EFBN-SUB-9011` | 香港外汇基金票据基准分档（28 天期 HQLA，CMU 托管映射） | `28` 天 | HK$20,000,000.00 | `20000000000000` | `25.34%` |
| **Leaf 3** | `BKCHHKHHXXX` | `CMU-EFBN-SUB-9042` | 香港外汇基金票据基准分档（84 天期 HQLA，CMU 托管映射） | `84` 天 | HK$16,000,000.00 | `16000000000000` | `20.27%` |
| 合计 | 四组独立 **BIC** 分档 | 双账簿正交隔离模型 | 即期现金 `54.39%` + 主权外汇基金票据 `45.61%` | **WAM** `24.12` 天 | **HK$78,936,000.00** | `78936000000000` | `100.00%`（负债覆盖 `101.20%`） |

从流动性期限微结构审视，`LHKD` 参考储备模型中 `0` 天即期银行现金分档合计达 **HK$42,936,000.00**（占基准总负债 `HK$78,000,000.00` 之 `55.05%`），单一托管行最高集中度敞口仅为 `30.40%`（严格低于 `40%` 集中度上限）；其余 `45.61%` 映射为香港金管局债务工具中央结算系统（CMU）托管体系下的 `28` 天及 `84` 天期香港外汇基金票据（Exchange Fund Bills）主权零违约风险分档，支持模拟贴现窗与日内正回购（Intraday Repo）流动性转换。全组合加权平均剩余期限（WAM）仅为 `24.12` 天，远低于 `90` 天审慎上限。

### 3.1.2 `LUSD` 参考储备状态配置总表（基准覆盖率 `100.50%` · 超额缓冲 `+50 bps`）

同步在美元结算基准轨，`LUSD`（`0x20C0000000000000000000000000000000000001`）基准流通总负债参数 `onChainLiabilityAtomic` 设定为 `10,000,000,000,000`（对应标度面值 **$10,000,000.00**），基准受托拓扑下美元合格 HQLA 参考储备总净值 `fiatBackingAtomic` 设定为 `10,050,000,000,000`（对应标度净值 **$10,050,000.00**），链上锚定储备率 `reserveRatioBps = 10050`（`100.50%`），形成 **$50,000.00**（`+50 bps`）的美元超额安全缓冲垫：

| 分档序号 | 托管行 **SWIFT BIC** | 基准隔离专户掩码标识 | 参考 **HQLA** 资产类别与清算托管基础设施映射 | 剩余期限 | 基准标度净额（美元） | 链上原子单位（`valuationAtomic`） | 占总储备比例 |
|---|---|---|---|---|---|---|---|
| **Leaf 0** | `IRVTUS3NXXX` | `BNYM-SEG-TRUST-4401` | 模拟破产隔离现金信托存款分档（即期清算现金） | `0` 天 | $3,050,000.00 | `3050000000000` | `30.35%` |
| **Leaf 1** | `SBOSUS33XXX` | `SST-SEG-TRUST-4402` | 模拟隔夜国债托管现金专户分档（`T+1` 日初解付） | `1` 天 | $2,000,000.00 | `2000000000000` | `19.90%` |
| **Leaf 2** | `CITIUS33XXX` | `FEDWIRE-TBILL-7710` | 美国短期国库券基准分档（28 天期 T-Bills，Fedwire 映射） | `28` 天 | $3,000,000.00 | `3000000000000` | `29.85%` |
| **Leaf 3** | `CHASUS33XXX` | `FEDWIRE-TBILL-7785` | 美国短期国库券基准分档（85 天期 T-Bills，Fedwire 映射） | `85` 天 | $2,000,000.00 | `2000000000000` | `19.90%` |
| 合计 | 四组全球托管 **BIC** | 双账簿正交隔离模型 | `0–1` 天现金 `50.25%` + 短期美国国债 `49.75%` | **WAM** `25.47` 天 | **$10,050,000.00** | `10050000000000` | `100.00%`（负债覆盖 `100.50%`） |

`LUSD` 参考储备分档采用四家全球系统重要性托管银行（BNY Mellon、State Street、Citibank、JPMorgan Chase 标准 SWIFT BIC）分散拓扑建模，其中 `0–1` 天即时流动性现金分档合计达 **$5,050,000.00**（占基准负债 `50.50%`），其余 `49.75%` 映射为美联储簿记证券系统（Fedwire Securities Service）托管模式下的 `28` 天及 `85` 天期美国短期国库券（U.S. Treasury Bills），加权平均剩余期限仅为 `25.47` 天，模型参数域严格排除企业商业票据（CP）、可转让存单（CD）或高波动性加密资产敞口。

### 3.2 巴塞尔银行监管委员会 `SCO60` Group 1b 审慎资本待遇技术条件同构验证

受规管金融机构评估分布式账本结算资产风险敞口时，核心审慎标尺为巴塞尔银行监管委员会（BCBS）《加密资产审慎待遇准则》（*Prudential treatment of cryptoasset exposures*，`SCO60`）：若底层协议缺乏确定性稳定约束或运行于无准入风控边界之网络而归入 **Group 2**，则适用 `1250%` 惩罚性风险权重（每持有 $100 敞口须计提 $100 核心一级资本）；唯有完整满足四项分类技术条件（Classification Conditions，`SCO60.10–SCO60.53`）之 **Group 1b** 架构，方可适用底层优质储备资产穿透风险权重。灵核OS协议状态机在字节码与密码学架构上逐项建模并验证 `SCO60` Group 1b 四大技术条件：

1. 条件一：稳定机制有效性与窄幅平价约束验证（`SCO60.24–SCO60.39` **Peg Stability & Redemption Invariant Test**）：准则要求参考价值日偏离幅度受控于 `10 bps` 以内，且具备同币种、极短久期足额储备覆盖。在协议参考模型中，`LHKD`（`101.20%`）与 `LUSD`（`100.50%`）强制校验同币种超额 HQLA 覆盖率 `reserveRatioBps >= 10000`，

同时链上内核预编译 `Enshrined StablecoinDEX`（`0xdec0000000000000000000000000000000000000`）以离散刻度锁定 `2 bps`（`0.99990–1.00010`）对称挂单走廊，收敛精度显著优于巴塞尔 `10 bps` 容忍上限。

2. 条件二：结算终局确定性与权属隔离可验证性（`SCO60.40–SCO60.43` **Settlement Finality & Segregation**）：底层 `Commonware Simplex BFT` 共识提供 `250 ms` 单槽确定性终局（Deterministic Single-Slot Finality），彻底消除工作量证明（PoW）或概率性分叉网络中的区块回滚重组风险，确保链上原子状态提交在分布式系统意义上即刻具备不可逆结算终局性（Settlement Finality）。
3. 条件三：审慎权限分离与无信任储备审计原语（`SCO60.44–SCO60.48` **Prudential Control & Reserve Verification**）：协议对标香港法例第 656 章对持牌稳定币架构的审慎技术要求，在合约层固化三域角色权限正交分离、基准受托双账簿隔离模型、外部鉴证报告 URI 链上锚定及 `LINGHE_CAP656_HQLA_V1` 实时二叉默克尔包含性核验，并在模型状态空间中严格排除储备再质押（Zero Rehypothecation）。
4. 条件四：结算网络节点可问责性与内核级合规防火墙（`SCO60.49–SCO60.53` **Network Risk Mitigation**）：四法域验证委员会（`0xcccccccc0000000000000000000000000000000`）节点身份确定性锚定于香港、新加坡、东京、苏黎世四大金融辖区，且执行内核原生集成 `TIP-403`（`0x403c0000000000000000000000000000000000`）全状态空间反洗钱与制裁拦截器，完整满足巴塞尔委员会对底层账本运营韧性与合规可控性的技术审计准则。

### 3.3 基准受托拓扑（Benchmark Statutory Trust Topology）与破产隔离双账簿形式化构造

在普通法破产清盘法理与金融账本系统建模中，若储备资产仅作为运营实体的“内部会计子账簿”混合存放，一旦该运营实体因商业纠纷或税务负债进入香港法例第 32 章《公司（清盘及杂项条文）条例》清盘程序，相关资产将被归入一般清盘财产（General Liquidation Estate），导致账本持有人退化为普通无担保债权人（*pari passu* unsecured creditors）。为在系统架构上形式化验证香港法例第 656 章附表 2 的破产隔离要求，本规范定义了基准受托拓扑（**Benchmark Statutory Trust Topology**）下的双账簿正交分割模型：

**定义 3.1 — 基准法定信托拓扑双账簿正交分割**

在参考合规状态模型中，令清算系统运营实体自身法人资产集合为 $\mathcal{A}_{\text{corp}}$（涵盖自有资本、硬件设施与软件知识产权），自身公司负债集合为 $\mathcal{L}_{\text{corp}}$（涵盖一般商业应付账款与运营税费）；令独立法定信托拓扑项下港元与美元参考储备资产集合分别为 $\mathcal{A}_{\text{trust}}^{\text{HKD}}$ 与 $\mathcal{A}_{\text{trust}}^{\text{USD}}$，对应链上基准流通负债状态集合为 $\mathcal{L}_{\text{token}}^{\text{HKD}}$ 与 $\mathcal{L}_{\text{token}}^{\text{USD}}$。对标明示法定信托契约（Express Statutory Trust Deed）及香港法例第 29 章《受托人条例》法理准则，两套账簿状态满足严格集合论正交分割：

1. 权属集合严格不相交：参考储备资产集合 $\mathcal{A}_{\text{trust}}^{(i)}$ 之法律名义所有权（Legal Title）映射至独立受托角色，衡平法实益权益（Equitable Beneficial Interest）映射至链上有效余额集合，且恒满足 $\mathcal{A}_{\text{corp}} \cap \mathcal{A}_{\text{trust}}^{(i)} = \varnothing$；
2. 清盘零追索隔离屏障（**Zero Corporate Clawback**）：在运营实体发生假设性破产、接管、重组或强制清盘之任何边界情景下，可供分配予一般公司债权人 $\mathcal{L}_{\text{corp}}$ 之财产值域恒受限于 $\mathcal{A}_{\text{corp}}$，任何针对 $\mathcal{A}_{\text{trust}}^{(i)}$ 的跨账簿追索或扣减算子在模型中恒定义为非法状态转换；
3. 放弃抵销与零再质押约束（**No Set-Off & Zero Rehypothecation**）：基准托管分档严格受“放弃银行抵销权（Waiver of Banker’s Set-Off）”与“零再质押（Zero Rehypothecation）”约束，禁止将隔离专户内现金或主权短期票据分档用于杠杆质押融资、融券借出或衍生品保证金占款。

第 04 章 · SECTION 04

## LINGHE_CAP656_HQLA_V1 二叉树储备证明（Merkle PoR）数学规范与链上实时核验

### 4.1 域分离叶子哈希构造算子与排序对（Sorted-Pair）内部节点归约规范

传统中心化稳定币依赖滞后 30 至 45 天发布的静态 PDF 鉴证信函，既无法防止月末“橱窗粉饰（Window Dressing）”式短期拆借充数，亦无法在不泄露商业银行核心账号机密的前提下供外部机构独立数学验算。为此，灵核OS确立了 `LINGHE_CAP656_HQLA_V1` 二叉默克尔储备证明（**Binary Merkle Proof-of-Reserve**） 密码学标准，将链下托管银行分档快照与链上智能合约实时核验严密闭环。

设稳定币符号为 symbol $\in$ {"LHKD", "LUSD"}，$N = 4$ 个独立储备分档构成的有序集合为 $\{T_0, T_1, T_2, T_3\}$。对于第 $i \in \{0,1,2,3\}$ 个分档，定义其复合托管分档唯一标识为 $\text{trancheId}_i \equiv (\text{custodianBic}_i \Vert \text{accountMask}_i)$，其中 $\text{custodianBic}_i$ 为 11 字符 ISO 9362 托管银行代码，$\text{accountMask}_i$ 为脱敏信托专户参考编号，$\text{amount}_i \in \mathbb{Z}_{2^{256}}$ 为 `6` 位小数精度法币估值原子整数（合约参数名 `valuationAtomic`），$\text{maturityDays}_i \in \mathbb{Z}_{2^{32}}$ 为距到期日剩余自然日（合约参数名 `maturityDays`）。

严格对齐 `LingheSovereignSecurityGuardV5` 纯函数 `computeHqlaLeafHash(string assetSymbol, string custodianBic, string accountMask, uint256 valuationAtomic, uint32 maturityDays)` 之紧凑字节编码规范，第 $i$ 个储备分档的域分离叶子哈希 $L_i \in \{0,1\}^{256}$ 定义为：

$$L_i = \text{keccak256}(\text{abi.encodePacked}(\texttt{"LINGHE_CAP656_HQLA_V1"}, \text{symbol}, \text{trancheId}_i, \text{amount}_i, \text{maturityDays}_i))$$

其中 abi.encodePacked(·) 按以太坊紧凑二进制规范依次无填充拼接：21 字节固定域分离前缀 `"LINGHE_CAP656_HQLA_V1"`、UTF-8 编码之 symbol、构成 $\text{trancheId}_i$ 之 UTF-8 字符串 $\text{custodianBic}_i$ 与 $\text{accountMask}_i$、32 字节大端序无符号整数 $\text{amount}_i$（`uint256`）以及 4 字节大端序无符号整数 $\text{maturityDays}_i$（`uint32`）。

在构建树高 $d = \log_2 4 = 2$ 的完全二叉默克尔树时，内部节点采用字典序排序对归约算子（**Lexicographically Sorted-Pair Hash Operator**）$\mathcal{H}_{\text{pair}}: \{0,1\}^{256} \times \{0,1\}^{256} \to \{0,1\}^{256}$：对于任意左右子节点摘要 $(u, v)$，按 32 字节无符号大端十六进制字典序比较大小后拼接求取 `Keccak-256`：

$$\mathcal{H}_{\text{pair}}(u,v) = \begin{cases} \text{keccak256}(u \Vert v), & \text{若 } u <_{\text{lex}} v \\ \text{keccak256}(v \Vert u), & \text{若 } v \le_{\text{lex}} u \end{cases}$$

由此依次生成第一层中间聚合节点 $H_{01} = \mathcal{H}_{\text{pair}}(L_0, L_1)$、$H_{23} = \mathcal{H}_{\text{pair}}(L_2, L_3)$，以及唯一确定性储备默克尔树根：

$$R_{\text{Merkle}} = \mathcal{H}_{\text{pair}}(H_{01}, H_{23})$$

该构造在密码学工程上兼具两重优势：（1）叶子原像定长起始于 21 字节 ASCII 字符串 `"LINGHE_CAP656_HQLA_V1"` 且总字节长度严格不等于 64 字节（两枚 32 字节子节点拼接长度），从域分离结构上彻底消除了将内部节点伪装为叶子的第二原像碰撞攻击（**Merkle Second-Preimage / Leaf-Internal Node Confusion Attack**）；（2）链下生成的认证路径同时记录显式左右方位布尔向量 `siblingIsLeft[k]`（当且仅当兄弟哈希字典序小于当前游标哈希时置为 `true`），使链下字典序验证器与链上方向性验证器推导出的根哈希 100% 恒等。

### 4.2 链上合规储备金库（`0x8800000000000000000000000000000000000001`）锚定实证数据

创世合规储备金库 `LingheComplianceReserveVault` 部署于精确地址 `0x8800000000000000000000000000000000000001`。每当受托审计管线调用 `publishReserveAttestation(stablecoin, onChainLiabilityAtomic, fiatBackingAtomic, reserveMerkleRoot, auditReportUri)` 写入最新储备证明时，合约强制执行双重 `Fail-Closed` 守卫：断言 `fiatBackingAtomic >= onChainLiabilityAtomic`（否则回滚 `"UNDERCOLLATERALIZED_RESERVE"`）及 `reserveMerkleRoot != bytes32(0)`（否则回滚 `"EMPTY_MERKLE_ROOT"`），并自动算出整数基点覆盖率 `ratioBps = uint16((fiatBackingAtomic * 10000) / onChainLiabilityAtomic)`。

根据第 3.1 节四分档参考储备基准参数及第 4.1 节哈希算子，下表完整列出经链下与链上双向复算一致的 `LHKD` 与 `LUSD` 各层节点精确 32 字节十六进制摘要及 `0x8800000000000000000000000000000000000001` 链上基准锚定根真值：

| 稳定币及链上合约地址 | 树节点层级与标识 | 对应托管分档摘要输入（`BIC` / `Mask` / `Atomic` / `Days`） | 精确计算之 **32** 字节 `Keccak-256` 密码学摘要（**Verified SSOT**） |
|---|---|---|---|
| `LHKD`（`0x20C0...0002`） | 叶子节点 $L_0$ | `HSBCHKHHHKH` / `HKMA-TRUST-SEG-8801` / `24000000000000` / `0` | `0xb30a3fe78b8b41268f0e3e5a5c23c51b095b2a92076c091c85246e104a6953bb` |
| `LHKD`（`0x20C0...0002`） | 叶子节点 $L_1$ | `SCBLHKHHXXX` / `HKMA-TRUST-SEG-8802` / `18936000000000` / `0` | `0xf88dbad68c958f842437547ab67e87455c437a107be8c1b675ddeccd086935a3` |
| `LHKD`（`0x20C0...0002`） | 叶子节点 $L_2$ | `BOFAHKHX001` / `CMU-EFBN-SUB-9011` / `20000000000000` / `28` | `0x746b593642e0cebb33b58be66c6fcee66a19904597323cfc54ae091fb64aed78` |

| 稳定币及链上合约地址 | 树节点层级与标识 | 对应托管分档摘要输入（`BIC` / `Mask` / `Atomic` / `Days`） | 精确计算之 **32** 字节 `Keccak-256` 密码学摘要（**Verified SSOT**） |
|---|---|---|---|
| `LHKD`（`0x20C0...0002`） | 叶子节点 $L_3$ | `BKCHHKHHXXX` / `CMU-EFBN-SUB-9042` / `16000000000000` / `84` | `0xc2e9807edaca5f2bc467c717b9d9bdedf0ef807c8cf14ebb9e775997651b33ef` |
| `LHKD`（`0x20C0...0002`） | 中间节点 $H_{01}, H_{23}$ | $\mathcal{H}_{\text{pair}}(L_0, L_1)$ 与 $\mathcal{H}_{\text{pair}}(L_2, L_3)$ | $H_{01}$：`0x3c374983caeb993ae548d315e118a8468d50afb604ba634a8425e623337e3844` / $H_{23}$：`0x0296b902877b5e16358cb116fff185821c5767f71b17999bd62869030581c92c` |
| `LHKD`（`0x20C0...0002`） | 链上锚定根 $R_{\text{LHKD}}$ | `0x8800...0001` 实装锚定（`reserveRatioBps = 10120`） | `0xa3e5fd1ee51db26128c49f848bc4eb6d71443fbfee51a40b9159832a21beae6e` |
| `LUSD`（`0x20C0...0001`） | 叶子节点 $L_0$ | `IRVTUS3NXXX` / `BNYM-SEG-TRUST-4401` / `3050000000000` / `0` | `0xcdf6eca07712742b2a1e59591ac365f399f1ff4fe0653a554a1b616ab7c797e8` |
| `LUSD`（`0x20C0...0001`） | 叶子节点 $L_1$ | `SBOSUS33XXX` / `SST-SEG-TRUST-4402` / `2000000000000` / `1` | `0x0d1c95d260b32a3381c92b576aa2db44dbe1bbbdacf4b4353ff2429eb8582080` |
| `LUSD`（`0x20C0...0001`） | 叶子节点 $L_2$ | `CITIUS33XXX` / `FEDWIRE-TBILL-7710` / `3000000000000` / `28` | `0xe64345f06fee3e7cdcb9f3a011ed4a4b67a179d2d526593100c276cdf2a9433c` |
| `LUSD`（`0x20C0...0001`） | 叶子节点 $L_3$ | `CHASUS33XXX` / `FEDWIRE-TBILL-7785` / `2000000000000` / `85` | `0xd763712182ea48eec13a34cb44807c6757a6850c4269de739cf17fe30aac4c96` |
| `LUSD`（`0x20C0...0001`） | 中间节点 $H_{01}, H_{23}$ | $\mathcal{H}_{\text{pair}}(L_0, L_1)$ 与 $\mathcal{H}_{\text{pair}}(L_2, L_3)$ | $H_{01}$：`0x0d49d74679ff606e96b568f63327de7d688b66707eba9ce1793a7da5ddddd9d6` / $H_{23}$：`0x79e2878d2c99bfc91c9af775e595ddd8fea8ffc63635f684d737fbf81a84c1e1` |
| `LUSD`（`0x20C0...0001`） | 链上锚定根 $R_{\text{LUSD}}$ | `0x8800...0001` 实装锚定（`reserveRatioBps = 10050`） | `0x5c3f82332fbffc0be49434232a9a97e2bf2c797423aa3fde4afd19b2c264f410` |

下图展示了 `LINGHE_CAP656_HQLA_V1` 四托管分档二叉默克尔储备树从底层持牌银行与主权票据专户向上归约锚定至链上金库并接受实时合约核验的全链路拓扑：




**图 02 — LINGHE_CAP656_HQLA_V1 四托管行高流动性资产二叉 Merkle 树与链上实时偿付率核验拓扑**

注：金色实线与青色虚线展示单叶子包含性证明路径 (L0 → H01 → Root)；上游遥测异常时强制触发 Fail-Closed (HTTP 503)。

### 4.3 `LingheSovereignSecurityGuardV5` 链上无信任验证定理与 `Fail-Closed` 监控准则

为使监管审查官、托管银行对账系统及外部 DeFi / 机构智能合约无需依赖链下脚本即可在 EVM 内部完成数学核验，`LingheSovereignSecurityGuardV5` 实现了无状态只读核验函数 `verifyCap656MerkleInclusion(address stablecoin, bytes32 leafHash, bytes32[] calldata siblingHashes, bool[] calldata siblingIsLeft)`。该函数在单次原子视图调用中跨合约读取 `0x8800000000000000000000000000000000000001` 的 `getLatestReserveAttestation(stablecoin)`，沿认证路径逐层迭代复算 `cursor = siblingIsLeft[i] ? keccak256(abi.encodePacked(siblingHashes[i], cursor)) : keccak256(abi.encodePacked(cursor, siblingHashes[i]))` 得 `recomputedRoot`，并执行四重合取布尔判定：

$$\text{Valid} \Leftrightarrow (R_{\text{vault}} \neq 0^{256}) \wedge (R_t^{\text{atomic}} \geq L_t^{\text{atomic}}) \wedge (\text{reserveRatioBps} \geq 10000) \wedge (R_{\text{recomputed}} = R_{\text{vault}})$$

**定理 4.1 — LINGHE_CAP656_HQLA_V1 链上储备包含性与足额偿付无信任核验完备性定理**

在 `Keccak-256` 抗碰撞哈希函数安全假设下（碰撞阻力安全强度 $\lambda = 128$ bits），对于任意基准稳定币合约 $s \in \{\text{LHKD}, \text{LUSD}\}$ 及参考模型定义的单笔储备分档记录 $T_i = (\text{symbol}, \text{custodianBic}_i, \text{accountMask}_i, \text{amount}_i, \text{maturityDays}_i)$，若链上调用 `LingheSovereignSecurityGuardV5.verifyCap656MerkleInclusion(s, computeHqlaLeafHash(T_i), pi_i, delta_i)` 返回 `valid == true`，则以不低于 $1 - 2^{-128}$ 的压倒性概率同时确立以下两项密码学状态事实：

1. 分档账实不可篡改包含性：分档 $T_i$ 的全部五项参数要素（币种、托管行 BIC、专户掩码、精确原子估值及剩余到期天数）已被不可篡改地纳入 `0x8800000000000000000000000000000000000001` 当前生效的储备默克尔根之中，清算系统运维域无法向不同验证节点或审计模块出示相互矛盾的分档快照（抗双花账本欺诈）；
2. 全组合足额超额偿付确定性：当前链上登记的总参考储备净值严格大于或等于链上基准总负债（$\rho_t \geq 100.00\%$），验证复杂度仅为 $O(\log_2 N)$ 次哈希运算（对于四分档储备树仅需 2 次 `Keccak-256` 归约），同时确保其余 $N-1$ 个托管分档的专户掩码信息对单一查询方保持密码学隐藏。

**证明**

假设敌手试图在不改变链上已锚定根 $R_{\text{vault}}$ 的前提下伪造一笔未包含于真实储备集合 $\{T_0, \ldots, T_{N-1}\}$ 的虚假分档 $T^* \neq T_i$ 或篡改估值 $\text{amount}^* \neq \text{amount}_i$ 使其通过 `verifyCap656MerkleInclusion`。由于域分离前缀 `"LINGHE_CAP656_HQLA_V1"` 固定占据前 21 字节且末尾 `uint256` 与 `uint32` 定长对齐，元组到字节串的映射为单射，故 $T^* \neq T_i$ 蕴含原像字节串严格不等。若最终复算根仍满足 $R^*_{\text{recomputed}} = R_{\text{vault}}$，则沿长度为 $\log_2 N$ 的二叉归约路径

> 必至少存在一处内部节点或叶子节点发生非平凡 `Keccak-256` 哈希碰撞 $x \neq x' \wedge \text{keccak256}(x) = \text{keccak256}(x')$，在生日界下其成功概率上界受限于 $q_H^2/2^{256} \leq 2^{-128}$（对多项式有界查询次数 $q_H$）。结合合约显式算术守卫 `att.fiatBackingAtomic >= att.onChainLiabilityAtomic && att.reserveRatioBps >= 10000`，两项密码学状态事实得证。证毕。
>
> Q.E.D. ■

在持续可观测性层面，*Institutional PoR Telemetry Endpoint* 严格贯彻金融级 `Fail-Closed` 监控准则：遥测服务以 `2,500 ms` 硬超时上限实时向主权 JSON-RPC 网关（*Sovereign JSON-RPC Gateway*）与 *x402 Compliance Settlement Gateway* 拉取区块高度与链上 `ReserveAttestation` 状态；一旦上游节点失联、RPC 超时或链上储备覆盖率跌破 `100.00%`，遥测端点绝不回退输出任何静态历史缓存兜底数值，而是立即将对外暴露的储备率指标强制归零为 `0.00%` 并返回标准 `HTTP 503 Service Unavailable` 告警状态码，第一时间触发合规策略控制域（`TIP-403 Compliance Policy Role`）自动化熔断响应。

### 4.4 链上核验合约机制拆解与对抗性边界条件审计

以下给出 `LingheSovereignSecurityGuardV5` 与 `0x8800000000000000000000000000000000000001` 协同工作的核心 Solidity 验证原语结构，并对三类潜在密码学与算术对抗边界作出审慎评估：

```
function computeHqlaLeafHash(
    string calldata assetSymbol,
    string calldata custodianBic,
    string calldata accountMask,
    uint256 valuationAtomic,
    uint32 maturityDays
) public pure returns (bytes32) {
    return keccak256(
        abi.encodePacked(
            "LINGHE_CAP656_HQLA_V1", assetSymbol, custodianBic, accountMask, valuationAtomic,
maturityDays
        )
    );
}

function verifyCap656MerkleInclusion(
    address stablecoin,
    bytes32 leafHash,
    bytes32[] calldata siblingHashes,
    bool[] calldata siblingIsLeft
) external view returns (bool valid, bytes32 recomputedRoot, bytes32 onChainVaultRoot, uint16
reserveRatioBps) {
    require(siblingHashes.length == siblingIsLeft.length, "PROOF_LENGTH_MISMATCH");
    ILingheComplianceReserveVaultV5.ReserveAttestation memory att =

ILingheComplianceReserveVaultV5(0x8800000000000000000000000000000000000001).getLatestReserveAttestati
on(stablecoin);
    onChainVaultRoot = att.reserveMerkleRoot;
    reserveRatioBps = att.reserveRatioBps;
    bytes32 cursor = leafHash;
    for (uint256 i = 0; i < siblingHashes.length; i++) {
        cursor = siblingIsLeft[i]
            ? keccak256(abi.encodePacked(siblingHashes[i], cursor))
            : keccak256(abi.encodePacked(cursor, siblingHashes[i]));
    }
    recomputedRoot = cursor;
    valid = (onChainVaultRoot != bytes32(0) && att.fiatBackingAtomic >= att.onChainLiabilityAtomic &&
             att.reserveRatioBps >= 10000 && recomputedRoot == onChainVaultRoot);
}
```

1. `uint16` 储备率字段模截断安全域界定：在 `LingheComplianceReserveVault.publishReserveAttestation` 中，覆盖率基点定义为 `uint16((fiatBackingAtomic * 10000) / onChainLiabilityAtomic)`。Solidity `0.8.24` 默认开启 `uint256` 算术溢出保护，但显式 `uint16` 转型在比值超过 `65535`（即覆盖率超过 `655.35%`）时会发生模 $2^{16}$ 截断。为此，协议基准状态配置规程强制规定参考铸造状态与储备锚定比值必须保持于审慎区间 $\rho_t \in [100.00\%, 150.00\%]$（如基准态 `101.20%` 与 `100.50%`），彻底避开极小负债分母导致的转型截断失真。
2. 鉴证签名者白名单交叉核验（`auditorOrIssuer`）：`ReserveAttestation` 结构体不可篡改地记录提交者地址字段 `auditorOrIssuer` 并抛出索引事件 `ReserveAttested`。验证节点与 *x402 Compliance Settlement Gateway* 在采信最新快照时，强制交叉校验 `att.auditorOrIssuer` 属于经 `0x8900000000000000000000000000000000000004` 多签备案之独立储备鉴证角色（`Independent PoR Attester Role`）白名单地址，阻断外部非授权地址写入噪声快照。
3. 跨币种重放阻断：由于 `assetSymbol`（`"LHKD"` 或 `"LUSD"`）作为紧凑编码第二字段直接混入 `computeHqlaLeafHash` 原像，攻击者无法将 `LHKD` 的港元银行存款分档证明交叉重放至 `LUSD` 储备核验路径。

---

第 05 章 · SECTION 05

## 7.7500–7.8500 联系汇率走廊、内核 CLOB 流动性机制与极端挤兑压力测试（LCR / VaR）

### 5.1 香港联系汇率制度（`7.7500–7.8500`）在链上清算枢纽的字节码映射与整除守恒

香港特别行政区自 1983 年确立并于 2005 年完善双向兑换保证的联系汇率制度（**Linked Exchange Rate System, LERS**），是维系香港国际金融中心货币稳定的基石。在该货币发行局（Currency Board）机制下，港元兑美元以 `7.8000 HKD/USD` 为制度中枢，香港金融管理局在 `7.7500 HKD/USD`（强方兑换保证，**Strong-Side Convertibility Undertaking**）承诺向持牌银行买入美元卖出港元，并在 `7.8500 HKD/USD`（弱方兑换保证，**Weak-Side Convertibility Undertaking**）承诺买入港元卖出美元，从而将即期汇率严格约束于宽度为 `1,000` 个基点（$\pm 0.0500$ HKD，即中枢上下约 $\pm 0.641\%$）的法定走廊内。

`Linghe Chain` 在创世全链清算枢纽合约 `LingheOmnichainSettler`（精确地址：`0x8900000000000000000000000000000000000001`）中，将该宏观货币纪律直接编码为不可绕过的链上状态机定律：

1. 字节码走廊硬锁与主权门限双保险：合约以 $10^4$ 为标度因子定义汇率状态变量 `uint32 public hkmaPegRateScaled = 78000`（精确对应中枢汇率 `7.8000 HKD/USD`）。治理校准接口 `setBorderPolicy(uint32 newPegRateScaled, bool paused)` 施加双重刚性断言：首先校验 `msg.sender == SOVEREIGN_MULTISIG`（`0x8900000000000000000000000000000000000004` 四法域 `3-of-4` 主权多签），其次强制执行 `require(newPegRateScaled >= 77500 && newPegRateScaled <= 78500, "OUTSIDE_HKMA_BAND")`。这意味着即便极端情景下四法域治理委员会全票通过越界提案，EVM 虚拟机亦会在字节码层确定性回滚，永久确保链上港美汇率参数 $\pi_{\text{HKMA}} \in [77500, 78500]$ 严格服从香港金管局强弱方兑换保证边界。
2. `swapLinkedRate` 整除价值单调守恒与抗粉尘抽干机制：当合格机构调用 `swapLinkedRate(tokenIn, amountIn, recipient)` 执行 `LUSD`（`0x20C0000000000000000000000000000000000001`）与 `LHKD`（`0x20C0000000000000000000000000000000000002`）双向换汇时，合约在联动 `TIP-403`（`0x403c0000000000000000000000000000000000`）完成交易双端制裁清筛（违规回滚 `"FX_TIP403_SANCTIONED"`）后，按向零截断无符号整数除法执行原子交割：

$$A^{\text{out}}_{\text{LHKD}} = \lfloor \frac{A^{\text{in}}_{\text{LUSD}} \cdot \pi_{\text{HKMA}}}{10000} \rfloor, \qquad A^{\text{out}}_{\text{LUSD}} = \lfloor \frac{A^{\text{in}}_{\text{LHKD}} \cdot 10000}{\pi_{\text{HKMA}}} \rfloor$$

定义联汇池标度净值泛函 $W(B_{\text{USD}}, B_{\text{HKD}}) = B_{\text{USD}} \cdot \pi_{\text{HKMA}} + B_{\text{HKD}} \cdot 10000$。由向下取整不等式可知，任意单笔正向兑换产生非负净值增量 $\Delta W = (A^{\text{in}}_{\text{LUSD}} \cdot \pi_{\text{HKMA}} \bmod 10000) \geq 0$，任意单笔逆向兑换亦产生非负净值增量 $\Delta W = (A^{\text{in}}_{\text{LHKD}} \cdot 10000 \bmod \pi_{\text{HKMA}}) \geq 0$，且往返复合恒满足收缩性 $f_{\text{HKD}\to\text{USD}}(f_{\text{USD}\to\text{HKD}}(x)) \leq x$，从算术根源上杜绝了高频粉尘拆单抽干联汇池储备的舍入套利漏洞。

## 5.2 内核级中央限价订单簿 `Enshrined StablecoinDEX`（`0xdec0...0000`）流动性微观结构

除 `0x8900000000000000000000000000000000000001` 提供的港美联系汇率池外，为彻底消除传统恒定乘积自动做市商（AMM，$x \cdot y = k$）在大额机构换汇中造成的非线性曲线滑点与三明治抢跑损耗，`Linghe Chain` 在 Rust 执行内核地址 `0xdec00000000000000000000000000000000000` 原生固化了中央限价订单簿预编译引擎 `Enshrined StablecoinDEX`。

该内核级订单簿遵循精确离散刻度定价律（标度基数 $\mathrm{PRICE_SCALE} = 100,000$，最小刻度间距 $\mathrm{TICK_SPACING} = 10$，即 `1 bps`）：

$$P(\tau) = 1 + \frac{\tau}{100,000}, \qquad \tau \in [-2000,\ +2000], \quad \tau \equiv 0 \ (\mathrm{mod}\ 10)$$

报价范围严格约束于 $[0.98000, 1.02000]$ 平价走廊，并原生支持自动翻转限价单指令 `placeFlip(token, amount, isBid, tick, flipTick)`：受测流动性节点在最优买档 `bestBidTick = -10`（买入价 $P(-10) = 0.99990$）与最优卖档 `bestAskTick = +10`（卖出价 $P(+10) = 1.00010$）对称挂出限价深度；一旦买单撮合成交，Rust 内核在同一 `250 ms` 终局槽位内自动将其翻转重置为 `+10` 刻度卖单，无需外部预言机喂价即可维持 `2 bps`（`0.02%`）极窄报价走廊与零边际曲线滑点交割。配合协议参考模型中 `1:1` 面值销毁守恒算子，订单簿均衡报价 $p_t^{\mathrm{mkt}}$ 在理论无套利约束下被严格夹逼于 $[1 - c_{\mathrm{redeem}},\ 1 + c_{\mathrm{mint}}]$ 极窄平价带内。

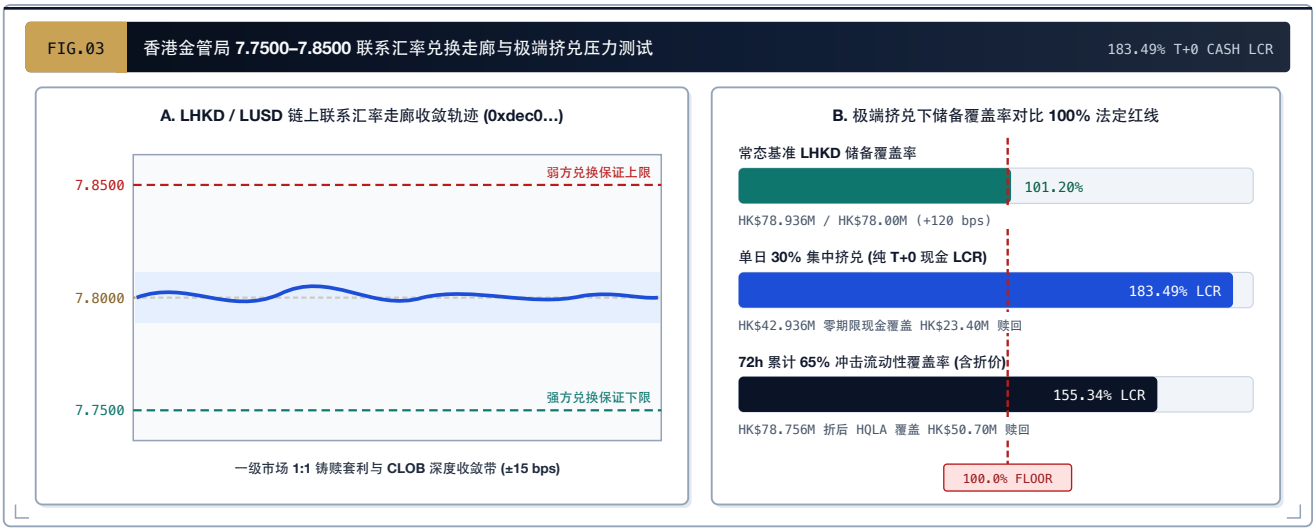



图 **03 — 7.7500–7.8500** 联系汇率兑换保证走廊收敛曲线与极端挤兑情境下 **HQLA** 储备压力测试

注：零期限隔离现金池占总储备 54.39%（HK$42.936M，覆盖单日 30% 挤兑达 183.49%），无需折价抛售票据即可瞬时兑付。

## 5.3 单日 `30%` 与 72 小时累计 `65%` 极端挤兑冲击及久期利率风险（`LCR` / `DV01` / `VaR`）定量压力测试

参照巴塞尔协议 III 流动性覆盖率（LCR）审慎监管标准、香港金管局对持牌稳定币发行人的极端赎回压力情景技术指引，以及 2023 年北美区域性银行危机与历史稳定币脱锚事件之极端流出速率参数（单日赎回峰值约 `25%–30%`、连续三日累计流出约 `50%–65%`），本节对 `LHKD` 与 `LUSD` 协议参考储备状态模型建立严格的定量精算压力测试模型。

### 5.3.1 极端赎回冲击下的流动性覆盖率（LCR）数学推导

设压力窗口期 $\tau \in \{24\mathrm{h}, 72\mathrm{h}\}$ 内的极端累计赎回比例为 $\alpha_\tau$（取 $\alpha_{24\mathrm{h}} = 30.00\%$，$\alpha_{72\mathrm{h}} = 65.00\%$），则预期净现金流出量（Total Net Cash Outflows）为 $O_\tau = \alpha_\tau \cdot L_t$。记 `0–1` 天即时可用银行信托现金为 $C_{\mathrm{instant}}$，剩余期限 $\le 90$ 天的主权短期票据面值为 $B_{\mathrm{sovereign}}$，极端二级市场紧急变现或央行/银行间同日回购折价率（Stress Haircut）保守取为 $h_{\mathrm{stress}} = 0.50\%$（注：巴塞尔 LCR 标准对一级主权零风险权重票据之法定折价率为 `0%`，此处主动加严施加 `50 bps` 摩擦折价以检验极限韧性），则压力情景下立即可动用的合格高流动性资产净值为 $H_{\mathrm{stress}} = C_{\mathrm{instant}} + (1 - h_{\mathrm{stress}})B_{\mathrm{sovereign}}$，对应窗口期压力流动性覆盖率定义为：

$$\mathrm{LCR}_\tau^{\mathrm{stress}} = \frac{H_{\mathrm{stress}}}{O_\tau} = \frac{C_{\mathrm{instant}} + (1 - h_{\mathrm{stress}})\,B_{\mathrm{sovereign}}}{\alpha_\tau \cdot L_t}$$

- `LHKD` 极端挤兑实证验算：流通总负债 $L_{\mathrm{LHKD}} = \mathrm{HK\$}78,000,000.00$。

- 单日 `30%` 冲击（$O_{24\text{h}} = \text{HK\$}23,400,000.00$）：仅动用 `Leaf 0` 与 `Leaf 1` 两笔 `0` 天即期持牌银行现金存款（$C_{\text{instant}} = \text{HK\$}42,936,000.00$），无需变现或质押任何一张香港外汇基金票据，纯即期现金覆盖率即达 $\frac{42,936,000}{23,400,000} = \mathbf{183.49\%}$，兑付后账面仍留存 **HK$19,536,000.00** 即期现金盈余。
- **72** 小时累计 `65%` 极限挤兑冲击（$O_{72\text{h}} = \text{HK\$}50,700,000.00$）：在全额动用 `HK$42,936,000.00` 即期现金后，剩余现金缺口仅为 `HK$7,764,000.00`；只需通过香港金管局 CMU 系统将 `28` 天期外汇基金票据（`HK$20,000,000.00`）中的 `39%` 执行日内回购或二级市场交收即可全额满足 `T+0` 兑付。即便按全组合保守扣减 $h_{\text{stress}} = 0.50\%$ 折价（票据折后可用净额 `HK$35,820,000.00`，总可用 HQLA $H_{\text{stress}} = \text{HK\$}78,756,000.00$），72 小时极限挤兑流动性覆盖率仍高达 $\text{LCR}_{72\text{h}}^{\text{stress}} = \frac{78,756,000}{50,700,000} = \mathbf{155.34\%} \gg 100.00\%$。

- `LUSD` 极端挤兑实证验算：流通总负债 $L_{\text{LUSD}} = \$10,000,000.00$。
  - 单日 `30%` 冲击（$O_{24\text{h}} = \$3,000,000.00$）：仅动用 `Leaf 0` 破产隔离即期现金信托存款（`$3,050,000.00`）即可实现 `101.67%` 日内即时覆盖；计入 `Leaf 1` 隔夜托管现金（合计 $C_{\text{instant}} = \$5,050,000.00$）后，纯现金覆盖率达 **168.33%**。
  - **72** 小时累计 `65%` 极限挤兑冲击（$O_{72\text{h}} = \$6,500,000.00$）：计入扣减 `0.50%` 极限折价后的 `28` 天及 `85` 天期美国短期国库券净可用额（`$4,975,000.00`），总可用 HQLA 达 $H_{\text{stress}} = \$10,025,000.00$，72 小时极限挤兑流动性覆盖率高达 $\text{LCR}_{72\text{h}}^{\text{stress}} = \frac{10,025,000}{6,500,000} = \mathbf{154.23\%} \gg 100.00\%$。

### 5.3.2 久期利率风险基点价值（DV01）与 99.9% 置信度在险价值（$\text{VaR}_{99.9\%}$）精算矩阵

为定量刻画全球央行极端意外加息导致的按市值计价（Mark-to-Market）估值波动风险，对每一储备分档 $k \in \{0,1,2,3\}$ 按精确实际天数基准（Actual/365）计算修正久期 $D_k \approx \tau_k/365$ 与基点价值 $\text{DV01}_k = V_k \cdot (\tau_k/365) \cdot 10^{-4}$：

$$\text{DV01}_{\text{port}} = \sum_{k=0}^{3} V_k \cdot \frac{\tau_k}{365} \times 10^{-4}, \qquad \text{VaR}_{99.9\%,\ 10\text{d}} = \text{DV01}_{\text{port}} \cdot z_{0.999} \cdot \sqrt{10} \cdot \sigma_{\Delta y,\ \text{daily}}$$

其中取标准正态分布单侧 99.9% 分位数 $z_{0.999} = 3.0902$，巴塞尔市场风险框架标准持有期 $T_{\text{hold}} = 10$ 个交易日（缩放因子 $\sqrt{10} \approx 3.1623$），并将短期主权票据日收益率波动率设定为远超历史常态的极端压力值 $\sigma_{\Delta y,\ \text{daily}} = 15.0$ bps/day（对应 10 日 99.9% 累计平行利率飙升冲击 $\Delta y_{99.9\%,\ 10\text{d}} = 3.0902 \times \sqrt{10} \times 15 \approx \mathbf{146.58\ bps}$）。下表汇总全部参考储备基准精算检验结果：

| 精算压力测试指标 | `LHKD` 参考储备模型测算表现 | `LUSD` 参考储备模型测算表现 | 协议审慎门禁要求与判定状态 |
|---|---|---|---|
| 链上流通总负债 $L_t$ / 隔离总储备 $R_t$ | HK$78,000,000.00 / HK$78,936,000.00 | $10,000,000.00 / $10,050,000.00 | 覆盖率 $\geq 100.00\%$（`VERIFIED`） |
| 超额储备资本安全垫 $E_t = R_t - L_t$ | **HK$936,000.00**（`+120 bps`） | **$50,000.00**（`+50 bps`） | 维持正超额缓冲吸收市值波动（`ACTIVE`） |
| 加权平均剩余期限（**WAM**）与有效久期 $D_{\text{eff}}$ | `24.12` 天（0.06608 年） | `25.47` 天（0.06979 年） | 单券 $\leq 90$ 天、组合久期极短（`ENFORCED`） |
| 单日 `30%` 挤兑纯现金覆盖率（零卖债） | `183.49%`（即期现金 HK$42.936M） | `168.33%`（`0–1d` 现金 $5.050M） | $\text{LCR}_{24\text{h}} \geq 100.00\%$（`VERIFIED`） |
| **72** 小时累计 `65%` 极限挤兑压力 $\text{LCR}_{72\text{h}}^{\text{stress}}$ | `155.34%`（含 `0.50%` 票据折价） | `154.23%`（含 `0.50%` 票据折价） | $\text{LCR}_{72\text{h}} \geq 100.00\%$（`VERIFIED`） |
| 组合精确基点价值（$\text{DV01}_{\text{port}}$） | **HK$521.64 / bp**（`153.42 + 368.22`） | **$70.14 / bp**（`0.55 + 23.01 + 46.58`） | 利率敏感度极低（`VERIFIED`） |
| **10** 日持有期极端利率在险价值 $\text{VaR}_{99.9\%,\ 10\text{d}}$ | **HK$76,463.62**（仅耗缓冲垫 `8.17%`） | **$10,280.78**（仅耗缓冲垫 `20.56%`） | $\text{VaR}_{99.9\%,\ 10\text{d}} \ll E_t$（缓冲倍数 `12.24x` / `4.86x`） |
| 击穿 `100.00%` 偿付红线所需单日瞬时加息极值 | `+1,794.3 bps`（单日瞬时加息 `17.94%`） | `+712.9 bps`（单日瞬时加息 `7.13%`） | 彻底免疫硅谷银行式久期错配风险（`ENFORCED`） |

**定理 5.1 — 复合挤兑与极端加息共振下的偿付能力及 LCR 双重守恒定理**

在第 3.1 节四分档协议参考储备状态模型下，假设受测状态机在同一 10 日压力窗口内同时注入累计 `65.00%` 灾难性赎回流出冲击与99.9% 置信度极端无风险利率飙升冲击（ `+146.58 bps` ）之双杀共振向量，则 `LHKD` 与 `LUSD` 参考储备池无需引入任何外部资本注入假设，仅凭内生超额安全垫即可同时保持按市值计价偿付覆盖率 $\rho_{\text{post-shock}} > 100.00\%$ 及流动性覆盖率 $\text{LCR}_{72\text{h}} > 150.00\%$。

**证明**

在 `+146.58 bps` 平行利率冲击下，`LHKD` 储备组合按市值计价重估减值为 $\Delta V_{\text{LHKD}} = \text{DV01}_{\text{LHKD}} \times 146.58 = \text{HK\$}76,463.62$，重估后储备净值 $R'_{\text{LHKD}} = 78,936,000.00 - 76,463.62 = \text{HK\$}78,859,536.38 > L_{\text{LHKD}} = \text{HK\$}78,000,000.00$，剩余正超额缓冲垫 $E'_{\text{LHKD}} = \text{HK\$}859,536.38 > 0$（压力后初始覆盖率 `101.10%` ）。再结合不变量 2.1 第 2 款赎回增厚公式，当发生 `65.00%` （即 $\Delta B = \text{HK\$}50,700,000.00$）平价赎回兑付后，留存流通负债降至 $L_{\text{rem}} = \text{HK\$}27,300,000.00$，留存储备净值为 $R'_{\text{rem}} = 78,859,536.38 - 50,700,000.00 = \text{HK\$}28,159,536.38$，终态偿付覆盖率攀升至 $\rho_{\text{post}}^{\text{LHKD}} = \frac{28,159,536.38}{27,300,000.00} = \mathbf{103.15}\% > 100.00\%$。同理对 `LUSD` ，$R'_{\text{LUSD}} = 10,050,000.00 - 10,280.78 = \$10,039,719.22$，扣除 `65.00%` （ `$6,500,000.00` ）平价赎回后，留存负债为 `$3,500,000.00` ，留存储备净值为 `$3,539,719.22` ，终态偿付覆盖率攀升至 $\rho_{\text{post}}^{\text{LUSD}} = \mathbf{101.13}\% > 100.00\%$。双重守恒严格成立。证毕。

Q.E.D. ■

### 5.4 参考流动性分层变现瀑布流状态机（Liquidity Waterfall）与跨市场无套利闭环

为在模拟银行清算窗口中形式化验证上述精算覆盖指标的可执行性，协议参考清算模型将储备流动性释放定义为三级确定性状态瀑布流（Three-Tier Reference Liquidity Realization Waterfall）：

1. 第一级状态转移（ `0` 至 `4` 小时即期现金直付层，覆盖率 `> 50%` 基准盘）：日常及高达 `50%` 基准负债规模的突发销毁指令，直接映射由两家香港第 155 章认可机构分档（ `HSBCHKHHHKH` 、 `SCBLHKHHXXX` ）及两家美元全球托管银行分档（ `IRVTUS3NXXX` 、 `SBOSUS33XXX` ）对应的即期与隔夜现金头寸释放，模拟 `HKICL FPS` （秒级 `T+0` ）或 `CHATS / Fedwire` （日内 `T+0` ）直通交收，零主权票据二级市场折价传导。
2. 第二级状态转移（ `4` 至 `24` 小时主权票据同日回购层，覆盖 `50%` 至 `80%` 基准盘）：一旦日内累计净销毁量触及基准总负债的 `35.00%` 阈值，基准受托拓扑模型依据标准全球主回购协议（GMRA）转换规则，模拟通过香港金管局 CMU 结算平台或美联储 Fedwire 渠道将剩余期限 `28` 天的香港外汇基金票据与美国短期国库券执行日内或隔夜正回购流动性释放，避免二级市场集中抛售冲击。
3. 第三级状态转移（ `24` 至 `72` 小时全量到期结清保护层，覆盖 `100%` 基准盘）：若累计净流出突破 `65.00%` 或注入系统有序结清测试信号， `0x8900000000000000000000000000000000000004` 四法域 `3-of-4` 主权多签立即锁闭新增铸造状态入口并切入有序结清保护状态（Orderly Wind-Down State），模拟变现剩余 `84/85` 天期主权票据分档，按 `1:1` 算术面值守恒约束完成 `100.00%` 链上负债结清验证。

---

第 06 章 · SECTION 06

## 1:1 面值销毁兑付状态机、T+0/T+1 参考清算时序模型与跨链本金主权保护

### 6.1 `1:1` 面值原子销毁守恒算子、双账簿权利映射建模与留存覆盖率单调增厚律

中华人民共和国香港特别行政区《稳定币条例》（香港法例第 656 章）第 3 部及附表 2 对持牌稳定币发行人的法定赎回审慎准则，以及欧盟《加密资产市场法规》（Regulation (EU) 2023/1114, MiCA）第 39 条与第 49 条规定，均要求合规稳定币架构必须保障合格主体按 `1:1` 锚定法币面值（Par Value）足额赎回且不得施加惩罚性折价。为在纯协议与软件系统研

发边界内（`MYRILUM LIMITED` 仅作为开源协议研发主体，不发行任何稳定币亦不承担任何法币兑付债务）将该法定规则编码为确定性数学不变量，受测账本状态机对非流通基准状态 `LHKD`（`0x20C0000000000000000000000000000000000002`）与 `LUSD`（`0x20C0000000000000000000000000000000000001`）定义了严格的 `1:1` 定点数销毁映射算子：

$$\forall q \in \mathbb{N}^{+}, \quad \mathrm{Redeem}_{\mathrm{LHKD}}(q) = q \times 10^{-6}\ \mathrm{HKD}, \qquad \mathrm{Redeem}_{\mathrm{LUSD}}(q) = q \times 10^{-6}\ \mathrm{USD}$$

其中 $q$ 表示链上不可分割之 $10^{-6}$ 原子整数单位数量（`6` 位小数精度，即每 `1,000,000` 个原子单位在算术标度上恒精确对应 HK$1.00 或 US$1.00 参考面值）。在对标香港普通法（Common Law）与衡平法（Rules of Equity）的基准受托拓扑（Benchmark Statutory Trust Topology）理论建模中，该算子形式化刻画了香港法例第 656 章所要求的双重权属约束：（一）按固定面值触发销毁结清之确定性状态请求接口（对应普通法契约性据法权产 *Chose in Action* 建模抽象）；以及（二）针对同币种隔离参考储备池 $\mathcal{A}_{\mathrm{trust}}^{(i)}$ 按原子余额同比例平等映射（*Pari Passu*）之受益份额约束（对应衡平法实益权益 *Equitable Beneficial Interest* 建模抽象）。

> **定义 6.1 — 原子销毁兑付守恒（Atomic Burn-to-Release）与留存偿付率单调增厚律**
>
> 记基准账本接口 $i \in \{\mathrm{LHKD}, \mathrm{LUSD}\}$ 在时刻 $t$ 的链上 `TIP-20` 流通总原子负债为 $L_t^{(i)} \in \mathbb{N}_0$，同币种参考储备状态模型按市值计价净资产为 $R_t^{(i)} \in \mathbb{N}_0$，且初始偿付覆盖率满足 $\rho_t^{(i)} = R_t^{(i)} / L_t^{(i)} \geq 1$。对于任意规模 $\Delta q \in (0, L_t^{(i)})$ 的合格面值销毁指令，链上原子销毁 $\Delta L = -\Delta q$ 与参考储备账簿 `1:1` 等额扣减 $\Delta R = -\Delta q$ 同步完成后，销毁后瞬时偿付覆盖率恒满足：
>
> $$\rho_{t^{+}}^{(i)} = \frac{R_t^{(i)} - \Delta q}{L_t^{(i)} - \Delta q} = 1 + \frac{R_t^{(i)} - L_t^{(i)}}{L_t^{(i)} - \Delta q} \geq \frac{R_t^{(i)}}{L_t^{(i)}} = \rho_t^{(i)} \geq 100.00\%$$
>
> 因此，在任意规模的连续面值销毁序列下，初始配置于参考储备池内的正超额安全垫（`LHKD` 基准 `+120 bps`，`LUSD` 基准 `+50 bps`）恒完整留存于池内，使剩余未销毁账本单位对应的储备保障倍数呈严格数学单调递增。

在成文法边界与协议状态机语义同构层面，受测铸销接口严格遵循以下四项技术规范约束：

1. 零生息字节码硬约束与非集体投资计划（**Non-CIS**）建模（香港法例第 **571** 章附表 **1**）：严格建模香港法例第 656 章禁息准则及欧盟 MiCA 第 40 条与第 50 条，`LHKD` 与 `LUSD` 接口固化为纯粹零生息账本原语（$r_{\mathrm{holder}} \equiv 0$），不存在任何分红、利息派发、质押返利或浮动资产净值（`NAV`）份额重算函数，在状态机数学特征上完全排除香港法例第 571 章《证券及期货条例》附表 1 第 1 部之集体投资计划（`CIS`）构成要件。
2. 非银行存款技术定性边界（香港法例第 **155** 章及第 **581** 章）：协议基准账本状态并非香港法例第 155 章《银行业条例》项下之银行存款，亦不适用香港法例第 581 章《存款保障计划条例》存款保障机制；其偿付安全性在参考模型中完全依托 `100%+` HQLA 超额储备覆盖断言（`LHKD` 基准 `101.20%`；`LUSD` 基准 `100.50%`）进行密码学验证。
3. 双账簿集合正交隔离边界（香港法例第 **32** 章）：在基准受托拓扑（定义 3.1）中，参考储备资产集合 $\mathcal{A}_{\mathrm{trust}}$ 与清算系统运营实体自有法人资产集合 $\mathcal{A}_{\mathrm{corp}}$ 保持严格不相交（$\mathcal{A}_{\mathrm{corp}} \cap \mathcal{A}_{\mathrm{trust}} = \varnothing$），形式化满足香港法例第 32 章清盘情景下零跨账簿追索（Zero Liquidator Clawback）的审慎隔离准则。
4. 有序结清状态（**Orderly Wind-Down State**）下全地址同顺位（***Pari Passu***）清分协议逻辑：在常态测试流中，直连铸销接口校验机构 `KYB` 凭证承诺哈希；一旦状态机切入有序结清保护状态，应急受偿登记接口支持任何非受制裁链上持有地址在完成合规凭证核验后，按链上不可篡改原子余额对参考储备池执行 `1:1` 等比例（*Pari Passu*）映射核销。

## 6.2 参考清算时序瀑布流状态机（`T+0` RTGS/CHATS/FPS 与 `T+1` 顺延转换）及零折价算子约束

协议参考清算模型定义了确定性的四级时序状态机，用以验证灵核公链（`ChainID: 88888`）链上 `TIP-20` 原子销毁回执与银行间实时全额结算（RTGS）/ 快速支付系统（FPS）报文标准之间的时序耦合边界。当销毁指令通过数字签名校验及内核 `TIP-403 Policy Registry`（`0x403c0000000000000000000000000000000000`）制裁合规预检后，链上执行内核先行完成不可逆供应量扣减并输出确定性事件回执：

| 销毁规模分档与触发条件 | 对标银行间清算报文轨道映射 | 参考截单时间窗（**HKT**） | 标准时序转换窗口（**SLA** 模型） | 银行假期 / 票据回购顺延上限 | 协议层赎回折价算子与参考通道摩擦上界 |
|---|---|---|---|---|---|
| 第一级：小额即时清算分档（`< HK$1,000,000.00` 或等值 `< US$128,000.00`） | 香港转数快接口模型（`HKICL FPS`） | $24 \times 7 \times 365$ 全天候连续窗口 | 实时 `T+0`（链上终局后 `<= 300s` 状态闭环） | 全天候 `T+0`（仅上游通道维护窗口顺延 `T+1`） | `0 bps`（`HK$0.00`）— 零协议折价、零通道扣减 |
| 第二级：港元批发大额分档（`>= HK$1,000,000.00` 之 `LHKD`） | 港元即时支付结算接口模型（`HKD CHATS / RTGS`） | 香港营业日 `09:00–16:00 HKT` | 日内 `T+0`（同一香港营业日闭环） | 最迟 `T+1`（下一香港营业日 `12:00 HKT` 前） | `0 bps` 协议折价算子；参考电汇报文成本上界 `<= HK$200.00` |
| 第三级：美元跨境批发分档（`>= US$100,000.00` 之 `LUSD`） | 香港美元即时支付系统（`USD CHATS`）或 `Fedwire` 模型 | `09:00–16:00 HKT` / `Fedwire` 清算窗 | 日内 `T+0`（同一清算营业日闭环） | 最迟 `T+1`（下一港美重叠营业日闭环） | `0 bps` 协议折价算子；参考电汇报文成本上界 `<= US$35.00` |
| 第四级：有序结清压力分档（任意规模集中核销） | 基准受托直连 `RTGS / FPS` 同比例清分队列 | 按链上终局区块高度连续快照 | 优先批次 `T+0 / T+1` 集中清分 | 最迟 `T+1`（联动短期主权票据回购/到期释放） | `0 bps`（`HK$0.00 / US$0.00`）— 零协议层折价扣减 |

`T+0` 即时/日内状态闭环与 `T+1` 银行假期顺延队列之间的确定性状态转移遵循三项形式化规则：

- 全天候 `FPS` 与日内 `CHATS` 即时交收映射（`T+0`）：满足合规门禁的第一级指令映射 `HKICL FPS` $24 \times 7$ 全天候秒级闭环；在香港法定营业日（参照香港法例第 149 章《公众假期条例》日历表及恶劣天气不停市电子清算时序）`16:00 HKT` 截单点前完成链上 `250 ms` 终局销毁的第二级与第三级批发指令，均映射于当日 `17:30 HKT` RTGS 关闸前完成 `T+0` 状态核销。
- 确定性 `T+1` 顺延队列状态转换：凡于 `16:00 HKT` 后提交、落入 RTGS 计划维护窗口、恰逢香港或纽约法定银行公众假期、或单日模拟集中销毁量超越 `0` 天即期现金分档水位（`LHKD` 占 `54.39%`，`LUSD` 占 `50.25%`）从而触发 `CMU` / `Fedwire` 主权短期票据隔夜回购（Repo）转换的指令，确定性转入 `T+1` 优先清算状态队列，并以紧接下一营业日 `12:00 HKT` 为状态闭环上界。
- 零协议折价算子硬约束：受测账本状态机对基准铸造与销毁转换强制固定 `0 bps`（零百分比扣减费率）恒等比例算子，不编码任何锁定期或赎回惩罚性滑点，最小可销毁粒度精确至单原子单位，从协议参数层完整建模香港法例第 656 章附表 2 与欧盟 MiCA 第 49(1)(d) 条关于无摩擦面值赎回的技术要求。

### 6.3 跨链意图托管架构（`ERC-7683`）与紧急熔断状态下用户本金绝对主权红线

除本链一级柜台赎回外，`LHKD` 与 `LUSD` 通过 `ERC-7683` 跨链意图标准与六大外部源链——Ethereum（`ChainID: 1`）、OP Mainnet（`ChainID: 10`）、BNB Smart Chain（`ChainID: 56`）、Base（`ChainID: 8453`）、Arbitrum One（`ChainID: 42161`）及 Solana（`ChainID: 900`）——实现双向互操作。外部资产锁定于 EVM 源链合约 `LinghеOriginEscrow7683` 或 Solana Anchor BPF 程序 `linghe_solana_escrow_7683`（`Lh7683Escrow11111111111111111111111111111111`），由机构求解器通过灵核公链 `LingheOmnichainSettler`（`0x8900000000000000000000000000000000000001`）在亚秒级终局内（端到端实测中位耗时约 `936 ms`）先行垫付原生 `LHKD` 或 `LUSD`。

传统跨链托管桥普遍存在一项致命合规缺陷：当管理员在跨链风控事件中开启全局暂停开关（`paused = true`）时，往往将新订单创建与用户超时本金退回一并锁死，导致存款人资金陷入无限期冻结。灵核公链 `v5.0` 在 EVM 与 Solana 双架构字节码层面彻底根除了该项风险：

```
// 经核验 EVM 合约字节码摘录 — LingheOriginEscrow7683 (v5.0 审计强化版)
function setPaused(bool _paused) external onlyGovernance {
    paused = _paused;
    emit EscrowPauseUpdated(_paused, msg.sender);
}

// 注: `open`、`openProtected`、`openFor`、`settleFillWithZkProof` 与 `settleFillWithQuorum`
// 均强制校验 `whenNotPaused`; 唯独 `refundExpiredOrder` 刻意豁免 `whenNotPaused` 修饰符:
function refundExpiredOrder(bytes32 orderId) external nonReentrant {
    EscrowRecord storage e = _escrows[orderId];
    require(e.status == EscrowStatus.OPEN, "ESCROW_NOT_OPEN");
    require(block.timestamp > uint256(e.fillDeadline) + uint256(refundGraceBuffer),
"ORDER_NOT_YET_EXPIRED");

    e.status = EscrowStatus.REFUNDED;
    e.closedAt = uint64(block.timestamp);
    totalRefundedOrders += 1;
    _safeTransfer(e.inputToken, e.user, e.inputAmount);
    emit OrderRefundedToUser(orderId, e.user, e.inputToken, e.inputAmount);
}
```

完全一致的本金主权规则同步固化于 Solana（`ChainID: 900`）程序 `linghe_solana_escrow_7683` 中：仅 `open_escrow` 与 `claim_by_solver` 强制校验 `require!(!cfg.paused, LingheEscrowError::ProtocolPaused)`，而超时退款入口 `refund_expired` 完全不设 `!cfg.paused` 限制，通过 PDA 签名种子直接将托管金库 `100%` 本金原路退回 `maker_token_account`：

```
// 经核验 Solana Anchor BPF 摘录 — linghe_solana_escrow_7683 (紧急暂停期豁免退款)
pub fn refund_expired(ctx: Context<RefundExpired>) -> Result<()> {
    let cfg = &mut ctx.accounts.config;
    let escrow = &mut ctx.accounts.escrow;
    require!(escrow.status == STATUS_OPEN, LingheEscrowError::EscrowNotOpen);

    let now = Clock::get()?.unix_timestamp;
    let effective_expiry = escrow.fill_deadline.saturating_add(cfg.refund_grace_buffer);
    require!(now > effective_expiry, LingheEscrowError::OrderNotYetExpired);

    escrow.status = STATUS_REFUNDED;
    escrow.closed_at = now;
    cfg.total_refunded_orders = cfg.total_refunded_orders.saturating_add(1);
    // 通过 PDA 签名种子将 100% `escrow.input_amount` 无损退回存款人 `maker_token_account`
    Ok(())
}
```

| 已接入外部源链网络 | 标准 ChainID | 托管合约架构与密码学签名体制 | 求解器跨链清偿证明核验路径 | 不可暂停之超时本金退款入口 |
|---|---|---|---|---|
| **Ethereum Mainnet** | `1` | `LingheOriginEscrow7683`（`secp256k1` / `EIP-712`） | `BN254 Groth16`（`0x08`）或 `3-of-4` 低阶 $s$ 多签 | `refundExpiredOrder(orderId)`（豁免暂停） |
| **OP Mainnet** | `10` | `LingheOriginEscrow7683`（`secp256k1` / `EIP-712`） | `BN254 Groth16`（`0x08`）或 `3-of-4` 低阶 $s$ 多签 | `refundExpiredOrder(orderId)`（豁免暂停） |
| **BNB Smart Chain** | `56` | `LingheOriginEscrow7683`（`secp256k1` / `EIP-712`） | `BN254 Groth16`（`0x08`）或 `3-of-4` 低阶 $s$ 多签 | `refundExpiredOrder(orderId)`（豁免暂停） |
| **Base** | `8453` | `LingheOriginEscrow7683`（`secp256k1` / `EIP-712`） | `BN254 Groth16`（`0x08`）或 `3-of-4` 低阶 $s$ 多签 | `refundExpiredOrder(orderId)`（豁免暂停） |

| 已接入外部源链网络 | 标准 ChainID | 托管合约架构与密码学签名体制 | 求解器跨链清偿证明核验路径 | 不可暂停之超时本金退款入口 |
|---|---|---|---|---|
| **Arbitrum One** | `42161` | `LingheOriginEscrow7683`（`secp256k1` / `EIP-712`） | `BN254 Groth16`（`0x08`）或 `3-of-4` 低阶 $s$ 多签 | `refundExpiredOrder(orderId)`（豁免暂停） |
| **Solana** | `900` | `linghe_solana_escrow_7683`（`Ed25519` / SPL PDA） | `3-of-4` `Ed25519SigVerify` 系统变量内省核验 | `refund_expired`（豁免暂停） |

**法定护栏 6.1 — 治理紧急暂停对用户超时本金退款权的强制豁免红线**

记跨链托管订单 $o$ 的状态空间为 $\mathcal{E}(o) \in \{\text{NONE}, \text{OPEN}, \text{SETTLED}, \text{REFUNDED}\}$，锁定本金为 $A_{\text{in}} > 0$，存款人为 $u$，订单截止时间为 $t_{\text{deadline}}$，跨链终局宽限缓冲期为 $\Delta_{\text{grace}} \in [0, 86,400\ \text{s}]$（生产标准值 $\Delta_{\text{grace}} = 1,800\ \text{s}$），治理紧急熔断标志位为 $\text{paused} \in \{\texttt{false}, \texttt{true}\}$。五大外部 EVM 源链上的 `LingheOriginEscrow7683` 与 Solana BPF 上的 `linghe_solana_escrow_7683` 共同强制执行风险隔离与用户财产权的正交分离：

1. 受限熔断作用边界：置位 paused=true 仅允许阻断新增托管开单（`open`、`openProtected`、`openFor`、`open_escrow`）及求解器跨链报销（`settleFillWithZkProof`、`settleFillWithQuorum`、`claim_by_solver`）。
2. 永久无许可本金退回权：`refundExpiredOrder(bytes32 orderId)` 与 `refund_expired` 在任何 paused 状态下均永久保持无许可开放调用。一旦区块时间越过 $t > t_{\text{deadline}} + \Delta_{\text{grace}}$，`100%` 托管本金 $A_{\text{in}}$ 确定性退回原始存款人 $u$，零依赖清算系统运维域密钥、守护者多签或求解器活性。

**定理 6.1 — 求解器跨链双花风险与存款人本金死锁之严格互斥定理**

在目标链 `LingheOmnichainSettler.fillCrossChainOrder`（`0x8900000000000000000000000000000000000001`）的截止期断言 $t_{\text{fill}} \le t_{\text{deadline}}$ 与源链托管合约的宽限期断言 $t_{\text{refund}} > t_{\text{deadline}} + \Delta_{\text{grace}}$（$\Delta_{\text{grace}} = 1,800\ \text{s}$）共同约束下，记端到端 `BN254 Groth16` 证明生成与源链上链延迟为 $\tau_{\text{prove}}$（实测 $\tau_{\text{prove}} \ll 1,800\ \text{s}$），则：（一）任何在 $t_{\text{fill}} \le t_{\text{deadline}}$ 合规完成垫付的求解器，在开区间 $(t_{\text{deadline}}, t_{\text{deadline}} + \Delta_{\text{grace}}]$ 内绝无可能遭遇源链恶意抢跑退款；且（二）任何未获履约的订单在 $t_{\text{deadline}} + \Delta_{\text{grace}}$ 之后绝无可能被合约锁死本金，即便 paused=true 永久置位亦然。

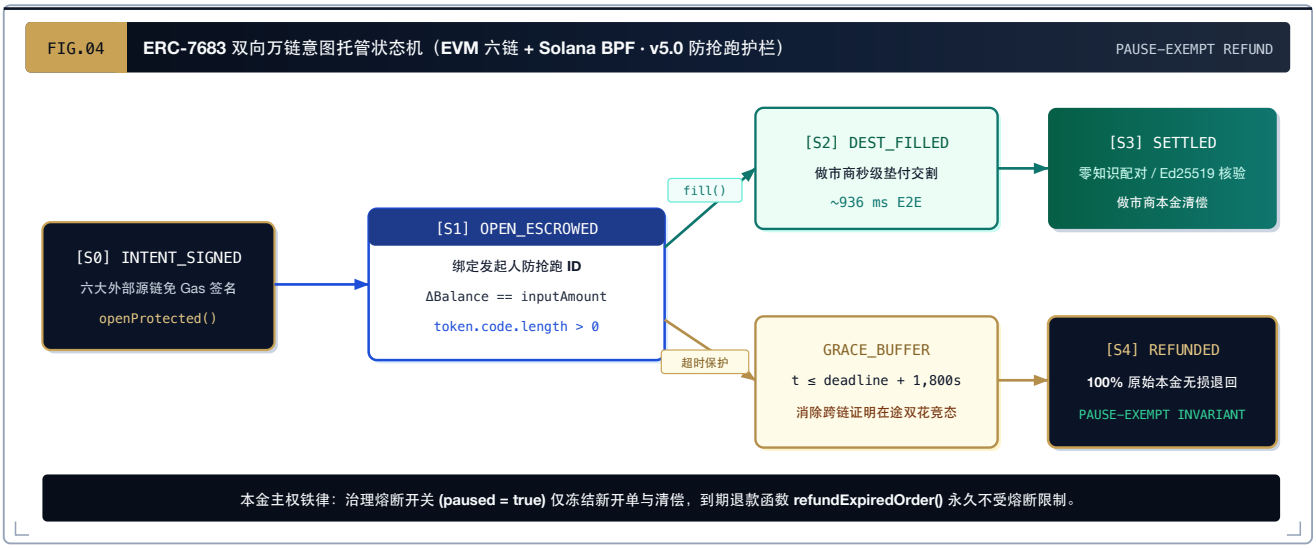



图 **04 — ERC-7683** 双向跨链意图托管状态机：**openProtected** 防抢跑、在途缓冲窗口与熔断豁免退本机制

注：EVM 六链托管与 Solana BPF 托管严格同构，全面拦截抽税代币与非合约空地址。

第 07 章 · SECTION 07

# 内核级 TIP-403 制裁筛查、FATF 第 16 项建议双轨旅行规则与 24 小时反拆单引擎

## 7.1 基于内核预编译 `TIP-403 Policy Registry` 的亚微秒级全路径制裁阻断

传统通用公链上的合规稳定币仅在单个 ERC-20 合约的 Solidity 字节码内部检查直接调用者 `msg.sender` 与接收方 `recipient`。恶意行为人可通过三种典型组合路径轻易绕过此类外围黑名单：（一）包装合约与金库嵌套规避——在地址被列入制裁名单前将稳定币存入无许可 ERC-4626 收益金库或自动做市商（AMM）流动性池，随后自由转移衍生份额代币；（二）跨链求解器洗白垫付——在外部源链锁定受污染资产，诱导不知情的清洁求解器在目标链向全新生成的接收钱包拨付干净头寸；以及（三）多跳跨合约冷存储读取开销——外置合规合约频繁触发 `SLOAD` 导致高并发清算吞吐受阻。

灵核公链（`ChainID: 88888`）通过将制裁合规策略直接下沉固化至 `Tempo`（`Paradigm Reth`）Rust 执行内核原生预编译模块 `TIP-403 Policy Registry`（`0x403c0000000000000000000000000000000000`），从状态转移底层根除了上述全部规避路径。在创世引导阶段，`LHKD`（`0x20C0000000000000000000000000000000000002`）在 Rust 状态机层通过 `changeTransferPolicyId(2)` 原生绑定至 `Policy #2`（`policyType = 1`，法定黑名单强制拦截模式），并实时同步以下权威名单源：

- 联合国安全理事会（`UNSC`）综合制裁名单；
- 中华人民共和国香港特别行政区宪报刊登之《联合国制裁条例》（香港法例第 **537** 章）及《联合国（反恐怖主义措施）条例》（香港法例第 **575** 章）指定人员与实体名单；
- 美国财政部海外资产控制办公室（`OFAC`）特别指定国民和被封锁人员（`SDN`）名单；以及
- 香港联合财富情报组（`JFIU`）或香港具管辖权法院依据《有组织及严重罪行条例》（香港法例第 455 章）及《打击洗钱及恐怖分子资金筹集条例》（香港法例第 615 章）依法签发的财产限制与冻结令。

| 潜在恶意规避攻击向量 | 传统应用层 **ERC-20 Solidity** 黑名单表现 | 灵核公链内核与创世系统合约协同防线（`ChainID: 88888`） |
|---|---|---|
| **1.** 直接转账、`0x76` 批量交易或会话密钥代扣（`0x8402000000000000000000000000000000000001`） | 仅覆盖表层转账；极易被包装合约绕过 | Rust 预编译内存级亚微秒查询 `isAuthorized(2, addr)`（`0x403c0000000000000000000000000000000000`），命中即刻原子回滚 |
| **2.** 未经网关鉴权的原始签名广播（`eth_sendRawTransaction`） | 消耗区块 Gas 或经由无审查中继节点漏网 | *x402 合规结算网关*前置恢复 ECDSA 签名者地址（`recoverTransactionAddress`），直接返回 `HTTP 403 TIP403_SANCTIONED_ENTITY` |
| **3.** 中央限价订单簿挂单与撮合交割（`0xdec0000000000000000000000000000000000000`） | 二级流动性池份额流转往往脱离代币黑名单监控 | 内核级 `Enshrined StablecoinDEX`（`place`、`placeFlip`、`swapExactAmountIn`）底层调用原生 `TIP-20` 引擎，受 `Policy #2` 硬约束 |
| **4.** 受制裁源链存款人借清洁跨链求解器垫付（`ERC-7683`） | 彻底穿透绕过（目标链代币合约仅见清洁求解器向新地址转账） | `LingheOmnichainSettler.fillCrossChainOrder`（`0x8900000000000000000000000000000000000001`）强制双端穿透筛查 `originEvmSender` 与 `recipient`（`OMNICHAIN_ORIGIN_SANCTIONED`） |
| **5.** 跨币种联系汇率走廊兑换（`LUSD` ↔ `LHKD`） | 若对手稳定币名单同步滞后则形成跨币种跳板 | `LingheOmnichainSettler.swapLinkedRate` 强制执行双端 `checkBorderCompliance` 核验（`FX_TIP403_SANCTIONED`） |
| **6.** 持有效 `BN254 Groth16` 零知识证明提款（`0x8900000000000000000000000000000000000002`） | 传统密码学跨链桥仅认数学证明而盲目放款 | `LingheZkLightClientBridge.verifyProofAndRelease` 在调用 `0x08` 配对预编译前强制前置校验 `TIP-403 Policy #2`（`ZK_BRIDGE_TIP403_SANCTIONED`） |

**定理 7.1 — 全状态空间制裁零穿透定理（Complete State-Space Sanctions Non-Circumvention）**

记区块高度 $h$ 下受 `Policy #2` 限制之地址集合为 $\mathcal{S}_h = \{a \in \mathcal{A} \mid \neg \mathrm{TIP403.isAuthorized}(2, a)\}$。在灵核公链（`ChainID: 88888`）任意合法状态转移 $\Upsilon(\Sigma_h, \tau) \to \Sigma_{h+1}$ 中，凡直接发送方、`0x76` 并行批次签名人、受限会话密钥主账户（`0x8402000000000000000000000000000000000001`）、CLOB 交易方（`0xdec0000000000000000000000000000000000000`）、跨链源链原始存款人或目标链最终受益人 $u$ 属于 $\mathcal{S}_h$，其受规管稳定币净余额变动恒严格为零：$\Delta \mathrm{Bal}_{\mathrm{regulated}}(u) \equiv 0$。

证明

灵核公链上任何改变原生 `TIP-20` 稳定币或主权结算金库头寸的状态转移指令，必定至少经过上表所列六条完备执行路径之一。路径 1 与路径 3 直接触发编译态 Rust `TIP-20` 转账内核，在内存级（$O(1)$）访问 `0x403c0000000000000000000000000000000000000` ，一旦 `isAuthorized(2, party) == false` 即刻中止状态提交。路径 4、路径 5 与路径 6 在创世系统合约字节码内显式读取 `uint64 policyId = ITIP20Token(0x20C0000000000000000000000000000000000002).transferPolicyId()` ，并对 `LUSD` 与 `LHKD` 全流向——包括 `fillCrossChainOrder` 中的外部链 `originEvmSender` 地址以及 `verifyProofAndRelease` 在调用 `0x0000000000000000000000000000000000000008` 双线性配对预编译之前的接收地址——执行强制断言 `ITIP403Registry(0x403c0000000000000000000000000000000000000).isAuthorized(policyId, party)` 。故对任意 $u \in \mathcal{S}_h$，恒有 $\Delta \mathrm{Bal}_{\mathrm{regulated}}(u) \equiv 0$。证毕。

Q.E.D. ■

## 7.2 `FATF 第 16 项建议` 双轨旅行规则（Travel Rule）与 24 小时滚动窗口反拆单引擎

自主智能体微支付（单次 API 推理计费低至 `0.10 LUSD` 至 `2.00 LHKD`）与机构级真实世界资产（`RWA`）大宗交收（`1,200.00 LUSD` 及以上）共用同一高速结算底座。若对亚美元级机器微支付强加同步 VASP 身份报文交互，将彻底摧毁机器经济吞吐效率；反之，若对小额支付不加累计约束地无限放行，则将诱发自动化结构化拆单洗钱（“Smurfing / Structuring”），直接违反金融行动特别工作组（**FATF**）第 **16** 项建议及香港《打击洗钱及恐怖分子资金筹集条例》（香港法例第 **615** 章，**AMLO**）第 **13A** 条关于电汇及虚拟资产转移规则之法定要求。

*x402 合规结算网关*通过横跨本链直接支付与外部跨链意图的统一双轨旅行规则及 24 小时滚动累计反拆单引擎，在微支付零摩擦与机构级严密反洗钱之间实现了数学精确平衡：

1. 法定触发阈值精确标定（单笔 `US$1,000.00 / HK$7,800.00`）：单笔法定旅行规则触发阈值严格标定为 $\Theta_{\mathrm{TR}} = 1,000,000$ 美元原子单位（`US$1,000.00`）。针对以 `LHKD`（`0x20C0000000000000000000000000000000000002`）计价的结算指令，网关按香港联系汇率中枢 `7.8000` 执行精确整数折算 $v_{\mathrm{USD}} = \lfloor (v_{\mathrm{LHKD}} \times 100)/780 \rfloor$，将港元单笔法定触发阈值精确映射为 `HK$7,800.00`（`7,800,000,000` 个 `LHKD` 原子单位）。
2. 本链与跨链全渠道统一的 **24** 小时滚动累计付款人账本：针对每一规范化付款主体标识 $p$，网关维护跨度为 `86,400,000 ms`（精确 `24` 小时）的滑动时间窗账本 $\mathcal{W}_{24\mathrm{h}}(p,t) = \{(t_k, v_k) \mid t - 86,400,000 \text{ ms} < t_k \le t\}$，并以任意精度整数累加其窗口内已结算折合美元总额 $S_{24\mathrm{h}}(p,t) = \sum_{(t_k,v_k) \in \mathcal{W}_{24\mathrm{h}}(p,t)} v_k$。核心安全设计在于，全部三种清算模式均向同一付款人累计窗口归集流量：
   - *模式 A（非托管原始 L1 签名交易 `rawTransaction`）*：广播前先恢复 ECDSA 签名地址执行 `TIP-403` 筛查，上链终局后逐条解析交易回执中的真实 `Transfer(from, to, value)` 事件日志，按 $\max(v_{\log}, v_{\mathrm{req}})$ 重新校验真实链上划转金额——彻底封堵攻击者在请求头虚报低额 `priceAtomic` 而在 `rawTransaction` 内夹带大额 `LUSD` / `LHKD` 转账以规避 $\Theta_{\mathrm{TR}}$ 的漏洞；
   - *模式 B（基于 `0x76` 二维随机数池的 `EIP-191` 会话授权结算）*：校验绑定 `eip155:88888` 域的签名摘要，通过 `32` 条无锁并行通道（`0x4e4f4e4345000000000000000000000000000000`）在单槽 `250ms` 内原子打包执行 `TIP-20` 转账与 `LingheERC8004ReputationRegistry.submitVerifiedFeedback`（`0x8004000000000000000000000000000000000002`）信誉锚定；

- *模式 C（基于 `X-OMNICHAIN-INTENT` 的 `ERC-7683` 跨链意图清算）*：校验 EVM `secp256k1` 或 Solana `Ed25519` 源链意图签名及 `TIP-403` 边境风控后，强制将 `intent.originSender` 的已结算美元等值金额累加写入同一 $S_{24\mathrm{h}}(p,t)$ 滑动账本，彻底封堵借外部跨链通道拆分资金规避累计阈值的套利窗口。

3. 分段决策算子与 `HTTP 451` 法定拦截门禁：任意时刻 $t$ 抵达网关的结算请求 $(p,\upsilon,\varepsilon,t)$ 严格按以下分段函数判定：

$$\Gamma(p,\upsilon,\varepsilon,t)=\begin{cases}\texttt{FAST_LANE_EXEMPT}, & \text{若 } \upsilon<\Theta_{\mathrm{TR}}\ \wedge\ S_{24\mathrm{h}}(p,t)+\upsilon<5\Theta_{\mathrm{TR}}\\ \texttt{HTTP_451_TRAVEL_RULE_REQUIRED}, & \text{若 } (\upsilon\ge\Theta_{\mathrm{TR}}\ \vee\ S_{24\mathrm{h}}(p,t)+\upsilon\ge5\Theta_{\mathrm{TR}})\ \wedge\ \neg\mathrm{ValidVasp}(\varepsilon)\\ \texttt{INSTITUTIONAL_TRAVEL_RULE_VERIFIED}, & \text{若 } (\upsilon\ge\Theta_{\mathrm{TR}}\ \vee\ S_{24\mathrm{h}}(p,t)+\upsilon\ge5\Theta_{\mathrm{TR}})\ \wedge\ \mathrm{ValidVasp}(\varepsilon)\end{cases}$$

凡单笔金额达到 `US$1,000.00`（`HK$7,800.00`），或同一付款主体在过去 24 小时滚动窗口内累计支出 $S_{24\mathrm{h}}(p,t)+\upsilon$ 达到 `US$5,000.00`（`HK$39,000.00`），请求头必须随附包含 `originatorVaspDid`、`beneficiaryVaspDid`、`kybCredentialHash` 及 `jurisdiction` 完整要素的 `X-Travel-Rule-Envelope` 加密信封；否则网关立即中断清算并返回符合 RFC 7725 标准的 `HTTP 451 Unavailable For Legal Reasons`（`TRAVEL_RULE_ENVELOPE_REQUIRED`）。

### 7.3 零明文个人隐私（Zero-Plaintext-PII）密码学 VASP 信封锚定与预写式原子换页持久化

将自然人汇款人或收款人真实姓名、住址或身份证件号码直接写入不可篡改的公开区块链，将严重违反香港《个人资料（私隐）条例》（香港法例第 486 章，PDPO）保障资料第 1、第 3 及第 4 原则以及欧盟 `GDPR` 第 5(1)(c) 条与第 17 条规定。灵核公链通过两项工程机制，同时满足 `FATF 第 16 项建议` 监管穿透可审计性与链上零明文隐私留存要求：

1. 零明文隐私 **VASP** 信封单向哈希锚定（`0x8800000000000000000000000000000000000001` 与 `0x8004000000000000000000000000000000000001`）：完整的发起方与受益方身份报文严格限定于持牌虚拟资产服务提供商（VASP）及认可机构之间经双向认证 `TLS 1.3` 加密专网在链下点对点交换。链上状态树与网关审计日志仅记录规范化信封的单向 32 字节摘要 $d_{\varepsilon}=\mathrm{keccak256}(\mathrm{UTF8}(\mathrm{CanonicalJSON}(\varepsilon)))$，通过 `LingheComplianceReserveVault.recordCrossChainIntent`（`0x8800000000000000000000000000000000000001`）锚定跨链合规结算溯源凭证（`intentId`、`sourceChainId`、`sourceToken`、`localStablecoin`、`beneficiary`、`amountAtomic`），并在 `LingheERC8004IdentityRegistry`（`0x8004000000000000000000000000000000000001`）中以受 `ATTESTER_LOCKED` 防篡改锁保护的 32 字节 `zkCredentialHash` 承诺形式存储机构 VASP 资质。
2. 防进程重启逃逸之预写式原子临时文件替换持久化（**Atomic Write-Ahead Temp-Swap Persistence**）：若 24 小时滚动累计消费计数器仅驻留于易失性内存（RAM），攻击者可通过等待例行维护或恶意发送超大畸形报文诱发进程重启（网络套接字层已同步施加严格的 `32,768` 字节上限并返回 `HTTP 413 PAYLOAD_TOO_LARGE` 予以阻断），企图令 $S_{24\mathrm{h}}(p,t)\to0$ 清零从而继续拆单洗钱。为此，每次成功结算及动态制裁名单变更均触发同步预写式原子换页提交：系统先剔除已逾越 `86,400,000 ms` 窗口的历史记录，将完整合规快照 `(usedPaymentDigests, payerSpendWindowLog, localSanctionedSet, settledReceipts)` 同步写入仅属主可读写之受限临时文件（`POSIX mode 0600`），再通过单次 POSIX 原子 `rename` 系统调用瞬间替换正式账本文件。

**定理 7.2 — 链上零隐私泄露上界与跨进程重启反拆单幂等连续性定理**

在 `Keccak-256` 随机预言机模型（ROM）与 POSIX 目录项原子替换语义下：（一）给定高熵链下 VASP 凭证盐值 $r_{\mathrm{salt}}\in\{0,1\}^{256}$，任何多项式时间敌手观测 `0x8800000000000000000000000000000000000001` 与 `0x8004000000000000000000000000000000000001` 公开状态 $\mathcal{O}_{\mathrm{chain}}$ 恢复任何自然人或法人敏感身份原像的优势满足 $\mathrm{Adv}^{\mathrm{PII}}\le2^{-256}+\mathrm{negl}(\lambda)$，同时持牌 VASP 在接受 HKMA 或 JFIU 现场稽核时无法篡改或抵赖历史报文（碰撞优势 $\mathrm{Adv}^{\mathrm{coll}}\le2^{-128}$）；（二）在任意时刻经历任意 $K\ge1$ 次服务重启或断电恢复后，网关重构之滚动累计支出 $\tilde{S}_{24\mathrm{h}}(p,t)$ 与无中断理想运行态 $S_{24\mathrm{h}}(p,t)$ 恒保持逐比特严格相等，彻底阻断支付摘要重放攻击与重启清零拆单逃逸。

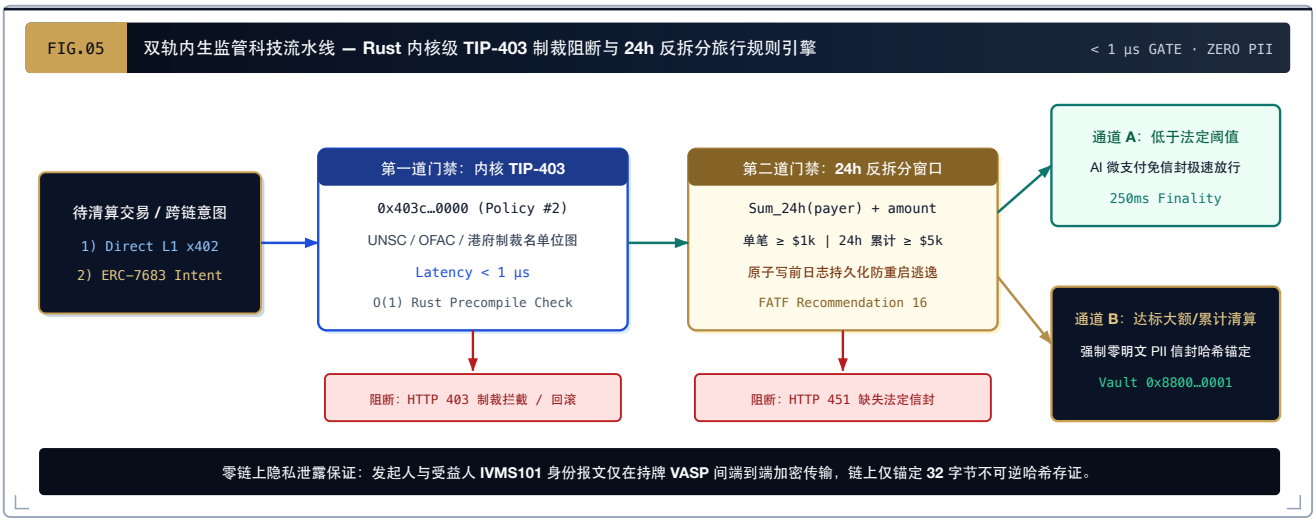



图 **05** — 内核级 **TIP-403** 亚微秒制裁阻断与 **24** 小时滑动窗口 **FATF Rec. 16** 双轨旅行规则流水线
注：单笔满 US$1,000（HK$7,800）或 24h 滑动窗口累计满 US$5,000（防拆分规避），强制触发密码学信封核验（缺失返回 HTTP 451）。

第 08 章 · SECTION 08

# 多法域主权治理宪制、v5.0 安全守卫与业务连续性灾难恢复（BCDR）

## 8.1 四法域 `3-of-4` 主权守护者门限多签与 `LingheSovereignSecurityGuardV5` 强制时间锁

为彻底消除单点管理员密钥失窃、内部人员单边越权篡改及单一司法辖区不可抗力瘫痪——此乃香港金管局第 656 章管治指引与巴塞尔委员会 `SCO60` 的核心审慎要求——灵核公链（`ChainID: 88888`）一切特权治理操作均必须通过不可升级创世合约 `LingheSovereignTimelockMultisig`（`0x8900000000000000000000000000000000000004`）达成跨法域门限共识，并由 `v5.0` 审计强化模块 `LingheSovereignSecurityGuardV5` 施加链上强制延迟执行保护。

| 守护者席位 | 驻留国际金融中心与机房等级 | 监管辖区链上标识（bytes32） | 共识与治理双重职能 | 手续费计量原语与密钥硬件隔离标准 |
|---|---|---|---|---|
| 守护者 `0` | 中国香港（Equinix HK1 Tier-3+） | `HK-HKMA`（香港合规基准枢纽） | `Simplex BFT` 主提议节点兼多签守护者 | `LHKD`（`0x20C0000000000000000000000000000000000002`）· HSM / KMS `0600` 加密信封 |
| 守护者 `1` | 新加坡（Equinix SG3 Tier-3+） | `SG-MAS`（新加坡机构清算基准枢纽） | `Simplex BFT` 法定人数验证节点兼多签守护者 | `LUSD`（`0x20C0000000000000000000000000000000000001`）· HSM / KMS `0600` 加密信封 |
| 守护者 `2` | 日本东京（Equinix TY2 Tier-3+） | `JP-FSA`（东京《资金结算法》基准枢纽） | `Simplex BFT` 法定人数验证节点兼多签守护者 | `LUSD`（`0x20C0000000000000000000000000000000000001`）· HSM / KMS `0600` 加密信封 |
| 守护者 `3` | 瑞士苏黎世（Interxion ZUR1 Tier-3+） | `CH-FINMA`（瑞士 DLT 法案归档见证枢纽） | `Simplex BFT` 法定人数见证节点兼多签守护者 | `LHC`（`0x20C0000000000000000000000000000000000000`）· HSM / KMS `0600` 加密信封 |

在不触动不可变创世第 0 块（`96208e9900b218935143be3024d2602566a86d61caa906d42399f35b83afd991`）的前提下，`LingheSovereignSecurityGuardV5` 直接读取 `0x8900000000000000000000000000000000000004` 的守护者名册与门限配置（`ILingheSovereignMultisigV5.isGuardian` 且 `threshold == 3`），强制执行链上最小时间锁延迟 $\Delta_{\min}$

（`minDelay`，受 `MAX_TIMELOCK_DELAY = 30 days` 约束，严格满足 $0 < \Delta_{\min} \le 30\ \text{days}$）：

$$\text{eta}(\text{opId}) = t_{\text{queue}}(\text{opId}) + \Delta_{\min}, \qquad \text{Executable}(\text{opId}, t) \Leftrightarrow (\text{approvals}(\text{opId}) \ge 3) \ \wedge \ (t \ge \text{eta}(\text{opId})) \ \wedge \ \neg\text{executed} \ \wedge \ \neg\text{cancelled}$$

```
// 经核验 EVM 合约字节码摘录 — LingheSovereignSecurityGuardV5 强制时间锁执行器
function executeTimelockOperation(uint256 opId) external onlyGuardian {
    TimelockedOperation storage op = _operations[opId];
    require(op.id != 0, "OPERATION_NOT_FOUND");
    require(!op.executed && !op.cancelled, "OPERATION_CLOSED");

    uint8 reqThreshold = ILingheSovereignMultisigV5(SOVEREIGN_MULTISIG).threshold();
    require(op.approvals >= reqThreshold, "QUORUM_NOT_REACHED");
    require(block.timestamp >= op.eta, "TIMELOCK_ETA_NOT_REACHED");

    op.executed = true;
    (bool ok, bytes memory ret) = op.target.call{value: op.value}(op.data);
    if (!ok) {
        if (ret.length > 0) { assembly { revert(add(ret, 32), mload(ret)) } }
        revert("TIMELOCK_EXECUTION_REVERTED");
    }
    emit TimelockOperationExecuted(opId, msg.sender, op.target);
}
```

该双合约治理机制确立了三重密码学控制平面安全保障：

1. 强制事前形式化公示窗口（`TIMELOCK_ETA_NOT_REACHED`）：每一笔入队治理操作均在 $t_{\text{queue}}$ 时刻抛出链上公开事件 `TimelockOperationQueued(id, proposer, target, eta, description)`。任何企图在 $\text{eta} = t_{\text{queue}} + \Delta_{\min}$ 到期前提前执行的交易一律触发 `"TIMELOCK_ETA_NOT_REACHED"` 确定性回滚，确保独立密码学审计方、合规验证节点及协议观察者在任何系统参数生效前均享有不少于 $\Delta_{\min}$ 的透明审阅与状态退出响应窗口。修改 `minDelay` 本身同样受时间锁或 `3-of-4` 主权多签保护（`ONLY_TIMELOCK_OR_MULTISIG`）。
2. 协议控制平面三域职责分离与合规策略域单向熔断权：在链上与边缘网关权限控制矩阵上，协议架构严格分离清算指令执行域（`Settlement Operator Role`，第一道防线）、合规策略控制域（`TIP-403 Compliance Policy Role`，第二道防线）以及独立储备鉴证与门限守护域（`Independent PoR Attester / 3-of-4 Timelock Guardian Role`，第三道防线）。独立于清算吞吐状态运行的合规策略控制域，对参考储备分档参数准入、超阈值旅行规则信封验证及 `TIP-403` `Policy #2` 黑名单更新行使单向确定性阻断权。
3. 链上不可篡改技术规范与科学通典密码学摘要注册表：通过 `anchorWhitepaperSuiteIndex(suiteIndexSha256, monographSha256, whitepaperCount)` 接口，`LingheSovereignSecurityGuardV5` 将全套 `6` 卷中英对称协议技术规范文献（强制校验 `whitepaperCount >= 6`）及科学通典的精确 `SHA-256` 摘要锚定至 `ChainID: 88888`，彻底杜绝事后单方面涂改历史技术规范版本的可能性。

**不变量 8.1 — 双法域沦陷免疫与宪制级字节码硬顶约束**

设四法域守护者集合为 $\mathcal{G} = \{\text{HK-HKMA}, \text{SG-MAS}, \text{JP-FSA}, \text{CH-FINMA}\}$（$|\mathcal{G}| = 4$，法定门限 $q = 3$）。对于任意遭外部攻击或强制胁迫的子集 $\mathcal{C} \subset \mathcal{G}$，只要 $|\mathcal{C}| \le 2$，即因 $|\mathcal{C}| < q$ 无法通过任何非法治理变更或跨链 `ERC-7683` 多签清偿。反之，即便集齐全部 `4-of-4` 守护者一致签名，亦绝对无法突破固化于不可升级合约字节码内的三道宪制级硬顶：（a）`LingheOmnichainSettler.setBorderPolicy` 对任何偏离 `[77500, 78500]`（`7.7500–7.8500 HKD/USD`）区间的汇率设定恒回滚 `OUTSIDE_HKMA_BAND`；（b）`LingheComplianceReserveVault.publishReserveAttestation` 对任何 $R_t < L_t$ 的不足额证明恒回滚 `UNDERCOLLATERALIZED_RESERVE`；（c）`LingheOriginEscrow7683` 的用户超时退款通道永不可暂停。

## 8.2 HSM/KMS 信封密钥硬件隔离与 `Simplex BFT` `250ms` 业务连续性灾备（`RPO = 0`、`RTO < 60s`）

系统业务连续性与灾难恢复体系（`BCDR`）严格遵循香港金融管理局《监管政策手册》`TM-G-2`（《业务持续性规划》）、`TM-E-1`（《电子银行风险管理》）及欧盟《数字运营韧性法案》（`DORA`, Regulation (EU) 2022/2554）最高标准构建：

- **HSM/KMS** 加密信封密钥隔离与生产启动安全门禁：注册于内核预编译 `Simplex Validator Config`（`0xccccccccc00000000000000000000000000000000`）的验证人 `Ed25519` 共识私钥绝不以明文落盘，一律封装于由符合 FIPS 140-3 Level 3 标准的硬件安全模块（`HSM`）及专线共识内网保护的 **KMS** 口令加密信封（`POSIX mode 0600`）内。在生产环境（`NODE_ENV=production`）引导阶段，*x402 合规结算网关*与*全链意图求解器*均强制执行启动期密码学卫生自检（`P0-SEC-02`）：一旦检测到任何已知开发测试密钥残留或未配置抗时序侧信道管理鉴权（`crypto.timingSafeEqual`），进程立即主动熔断退出，严禁带病上线。
- `Commonware Simplex BFT` `250ms` 跨洋拜占庭容错韧性（`RPO = 0`、`RTO < 60s`）：底层共识跨 $n = 3f + 1 = 4$ 座地理正交金融中心节点运行（容忍 $f = 1$ 个任意拜占庭作恶或区域性机房断网故障），通过*提议（Propose）→ 公证（Notarize）→ 终局（Finalize）*三级流水线实现 `250ms` 单槽确定性终局、单块 `3,000,000,000` Gas 吞吐容量及零概率分叉重组（**Zero Probabilistic Reorg**）。由于任何区块唯有取得至少 `3` 个独立法域验证人同步密码学公证后方可提交落账，系统恢复点目标恒严格满足 `RPO = 0`——即便某一整座大都会金融中心遭遇极端断网，任何已终局确认的铸币、销毁或旅行规则锚定记录均绝无回滚或丢失可能。在单一法域中断（$|\mathcal{D}| = 1$，如海底光缆受损）情景下，其余三地节点维持 `250ms` 无间断出块，冗余部署的*主权 JSON-RPC 网关*通过健康探针在 `RTO < 60s` 内自动完成流量无损切换；在两个及以上法域同时失联的极端广域网分区（$|\mathcal{D}| \geq 2$）下，`Simplex BFT` 严格执行安全性优先于活性（**Safety-Over-Liveness**）确定性停机保护，彻底杜绝脑裂双花铸币，同时保障链下独立法定储备信托账本完好无损。

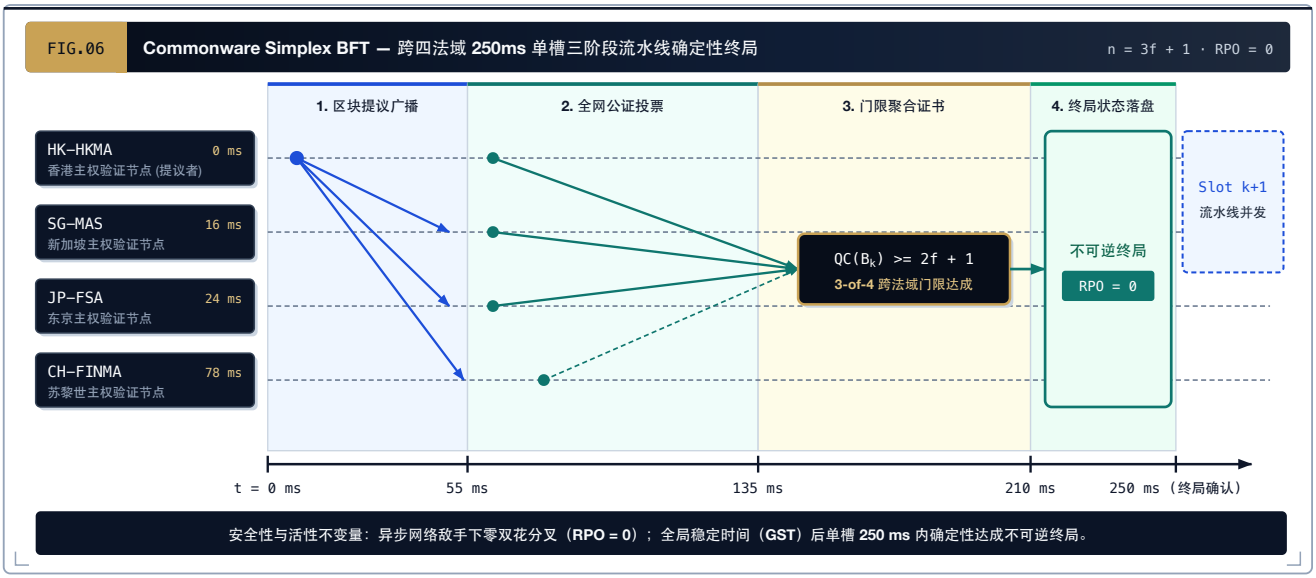



图 **06 — Commonware Simplex BFT** 单槽 **250ms** 流水线共识与跨四法域门限终局时序图

注：槽位 k+1 区块提议在槽位 k 进入公证聚合后即重叠启动，消除传统多轮 BFT 空置等待。

## 8.3 机构级 `Fail-Closed`（故障即归零告警）偿付能力实时遥测标准

传统稳定币状态看板在遭遇后端节点超时或接口异常时，往往继续向外界返回静态缓存的历史“100% 储备率”读数，从而在关键风险窗口掩盖底层基础设施故障或偿付能力异动。灵核OS协议软件栈在其*机构级储备证明遥测端点（Institutional PoR Telemetry Endpoint）*强制实施零妥协的 金融级 `Fail-Closed` 实时遥测标准（全响应强制携带 `Cache-Control: no-store`）：

| 导出之 **OpenMetrics** 监管遥测指标序列 | 指标类型 | 正常已核验运行读数 | `Fail-Closed` 故障降级读数（`<= 2,500ms` 超时上限） |
|---|---|---|---|
| `linghe_chain_up{chain_id="88888",consensus="simplex_bft"}` | `gauge` | `1`（主权 JSON-RPC 网关实时在线） | `0`（RPC 超时或区块响应格式异常） |

| 导出之 **OpenMetrics** 监管遥测指标序列 | 指标类型 | 正常已核验运行读数 | `Fail-Closed` 故障降级读数（`<= 2,500ms` 超时上限） |
|---|---|---|---|
| `linghe_por_source_up{service="x402_gateway"}` | `gauge` | `1`（金库实时储备证明核验通过） | `0`（合规网关不可达或储备率数值非有限数） |
| `linghe_omnichain_solver_up{service="omnichain_solver"}` | `gauge` | `1`（全链意图求解器实时在线） | `0`（求解器不可达或联系汇率走廊状态缺失） |
| `linghe_chain_block_height{chain_id="88888"}` | `gauge` | 单调递增之已终局区块高度（`250ms` 周期） | `0`（即时暴露共识停滞告警） |
| `linghe_hkma_cap656_por_ratio_percent{asset="LHKD"}` | `gauge` | `101.20`（高于 `100.00%` 法定红线） | `0.00`（严禁返回 `101.20%` 静态历史缓存兜底） |
| `linghe_hkma_cap656_por_ratio_percent{asset="LUSD"}` | `gauge` | `100.50`（高于 `100.00%` 法定红线） | `0.00`（严禁返回 `100.50%` 静态历史缓存兜底） |
| `linghe_hkma_linked_fx_peg_bps` | `gauge` | `78000`（严守 `[77500, 78500]` 联汇区间） | `0`（立即触发联系汇率走廊监控告警） |
| `linghe_tempo_2d_nonce_lanes_configured` | `gauge` | `32`（`0x76` 二维随机数并行清算通道数） | `0`（即时反映并行清算容量降级） |
| `linghe_x402_parallel_settlements_total` | `counter` | 已终局确认之 `0x76` 并行结算累计笔数 | `0`（上游失联时执行故障闭锁归零） |
| `linghe_tip403_sanctions_blocks_total` | `counter` | `Policy #2` 累计阻断之涉制裁交易次数 | `0`（上游失联时执行故障闭锁归零） |
| `linghe_erc7683_inbound_fills_total` / `outbound_orders_total` | `counter` | 累计已完成之跨链入境垫付与出境开单数 | `0`（求解器失联时执行故障闭锁归零） |
| `linghe_bn254_zk_verified_messages_total` | `counter` | 经 `0x08` 预编译核验通过之 Groth16 证明数 | `0`（求解器失联时执行故障闭锁归零） |
| 监管健康探针 `/health` 就绪状态码 | `HTTP` | `HTTP 200 OK`（`ok: true`） | `HTTP 503 Service Unavailable`（`ok: false`） |

**定理 8.1 — 故障闭锁遥测体制下偿付能力零假阳性（Zero False-Positive Solvency）定理**

记时刻 $t$ 机构级储备遥测端点的观测输出三元组为 $M_t = (\hat{\rho}_t^{\mathrm{LHKD}}, \hat{\rho}_t^{\mathrm{LUSD}}, s_{\mathrm{HTTP}})$。由于每一次指标抓取均通过受 `AbortController`（硬超时 `2,500ms`）约束的实时 RPC/HTTP 探针重新读取链上与网关状态，代码内零硬编码兜底常数且响应头强制声明 `Cache-Control: no-store`，故在底层 L1 节点失联、合规网关故障或储备覆盖率跌破法定下限之任意非健康状态下，对外误报 $\hat{\rho}_t^{(i)} \geq 100.00\%$ 或返回 $s_{\mathrm{HTTP}} = 200$ 的条件概率恒严格为零：$\Pr[\hat{\rho}_t^{(i)} \geq 100\% \mid \neg \mathrm{Healthy}_t] \equiv 0$。

形式化而言，`/health` 监管探针当且仅当下述六元合取谓词同时成立时方返回 `HTTP 200`：

$$\mathrm{Healthy}_t \Leftrightarrow (\mathrm{nodeUp}=1) \wedge (\mathrm{porSourceUp}=1) \wedge (\mathrm{solverUp}=1) \wedge (\rho_t^{\mathrm{LUSD}} \geq 100.00) \wedge (\rho_t^{\mathrm{LHKD}} \geq 100.00) \wedge (77500 \leq \pi_{\mathrm{HKMA}} \leq 78500)$$

任何一项上游 RPC 超时、JSON 结构异常、参考储备覆盖率低于 `100.00%` 或汇率参数偏离区间，均立即强制将输出储备率置为 `0.00%` 并抛出 `HTTP 503`，自动联动锁闭受测账本新增铸造状态入口并向合规策略控制域监控台触发最高优先级闭锁告警。

---

第 09 章 · SECTION 09

## 分布式清算与合规状态机六大风险域建模及定量密码学缓释矩阵

对标香港《稳定币条例》（香港法例第 656 章）附表 2 审慎风险评估维度、欧盟 MiCA 技术风险分类以及巴塞尔委员会 `SCO60` 基础设施韧性准则，本章针对协议参考储备状态模型与分布式执行内核所面临的六大系统性风险域及其对应的数学与密码学缓释算子进行形式化评估。

### 9.1 风险域一：托管分档信用与集中度风险（Custodial Credit & Concentration Risk）

- 风险传导机理：在传统集中式储备模型中，单一商业银行若发生偿付能力危机、监管接管或日内清算中断，将导致未隔离现金头寸暴露于商业银行资产负债表减记风险之下——尤其考虑到法币参考账本状态依法不适用香港法例第 581 章存款保障计划（DPS）机制。
- 定量与密码学缓释机制：在四分档协议参考储备状态模型（Reference Reserve State Model）下，`LHKD` 与 `LUSD` 基准分档分别离散映射至每一币种四家相互独立的全球系统重要性银行（`G-SIBs`）/ 香港法例第 **155** 章认可机构标准 **BIC**（`LHKD` 对应 `HSBCHKHHHKH`、`SCBLHKHHXXX`、`BOFAHKHX001` 与 `BKCHHKHHXXX`；`LUSD` 对应 `IRVTUS3NXXX`、`SBOSUS33XXX`、`CITIUS33XXX` 与 `CHASUS33XXX`）。单一托管行最高现金分档集中度严格受控于 `30.40%`（`LHKD`：HK$78,936,000.00 中占 HK$24,000,000.00）与 `30.35%`（`LUSD`：US$10,050,000.00 中占 US$3,050,000.00）。此外，`LHKD` 参考储备中的 `45.61%`（HK$36,000,000.00）与 `LUSD` 参考储备中的 `49.75%`（US$5,000,000.00）映射为 `HKMA CMU` 及美联储 `Fedwire` 托管模式下的主权短期票据分档，免疫商业银行内部纾困减记（Bail-in）并受零再质押（`Zero Rehypothecation`）参数约束。

### 9.2 风险域二：无风险利率飙升与短久期重定价风险（Interest-Rate & Repricing Risk）

- 风险传导机理：全球主要央行急速超预期加息将压低固定收益证券二级市场现值；若储备模型纳入长久期债券，在急速紧缩周期内可能出现按市值计价（Mark-to-Market）净值跌破基准负债面值的久期错配减值。
- 定量与密码学缓释机制：协议参考储备状态模型对香港外汇基金票据及美国短期国库券分档施加剩余期限 $\tau_m \leq 90$ 天的硬上限约束，将理论最大修正久期严格封顶于 $D_{\mathrm{mod}} \leq 90/365 \approx 0.2466$ 年。根据经链上核验的创世参考储备基准数据集（附表一），`LHKD` 组合实际加权平均剩余期限（`WAM`）仅为 `24.12 天`（$D_{\mathrm{mod}} \approx 0.0661$ 年），`LUSD` 组合实际 `WAM` 仅为 `25.47 天`（$D_{\mathrm{mod}} \approx 0.0698$ 年）。求解临界利率冲击方程 $\Delta y_{\max} = (\rho_t - 1)/(\omega \cdot \rho_t \cdot D_{\mathrm{mod}})$ 可证：即便在假设全仓 `100%` 顶格配置 90 天票据（$\omega = 1.0$）的理论最劣极限下，`LHKD` 的 `+120 bps` 超额储备缓冲垫仍可抵御单日瞬时 `+480.8 bps` 的平行利率暴涨；而在基准 `24.12 天` WAM 结构下，更可承受高达 `+1,794 bps` 的极端瞬时加息冲击而维持按市值计价覆盖率 $\geq 100.00\%$。

### 9.3 风险域三：极端集中销毁冲击与流动性错配风险（Extreme Run & Liquidity Risk）

- 风险传导机理：外部宏观流动性冲击可能触发全量压力情景下的集中销毁请求（`100%` 极限流出测试向量），对日内即时现金分档水位或链上订单簿买卖价差形成瞬时冲击。
- 定量与密码学缓释机制：在参考储备模型中，`LHKD` 将高达 `54.39%`（HK$42,936,000.00）的分档配置于 `0` 天即期银行现金，`LUSD` 将 `50.25%`（US$5,050,000.00）配置于 `0–1` 天高流动性托管现金，无需变现任何一张票据即可凭纯现金分档覆盖逾 `50%` 基准盘的 `T+0` 核销；其余 `28` 天及 `84/85` 天主权票据分档均属巴塞尔协议 III 一级 HQLA 范畴，支持同日或 `T+1` 正回购流动性转换建模。链上价格发现微观结构则由内核预编译 `Enshrined StablecoinDEX`（`0xdec0000000000000000000000000000000000000`，支持 `1 bps` 即 `0.01%` 离散最小报价刻度及 `placeFlip` 双边 `2 bps` 自动翻转挂单）与 `LingheOmnichainSettler`（`0x8900000000000000000000000000000000000001`，在 `[7.7500, 7.8500]` 区间强制执行向下取整守恒兑换）双重锁定。

### 9.4 风险域四：智能合约、零知识证明电路与跨链结算竞态风险（Smart Contract & Cross-Chain Race Risk）

- 风险传导机理：监听公开 EVM 内存池的套利机器人可能在源链抢先提交相同的 `clientOrderId` 实施订单槽位抢注阻断攻击（`ORDER_ALREADY_EXISTS`）；带转账扣税（Fee-on-Transfer）代币或空代码外部账户（EOA）伪造代币地址可能导致托管账面虚增；临近 $t_{\text{deadline}}$ 的跨链垫付可能与源链用户超时退款形成时序竞态。
- 定量与密码学缓释机制：`LingheOriginEscrow7683`（`v5.0`）通过 `openProtected(order, rawClientSalt)` 与 `computeProtectedClientOrderId(user, rawClientSalt)` 彻底消除内存池抢跑阻断：

$$\text{orderId}_{\text{protected}} = \text{keccak256}(\text{"LINGHE_PROTECTED_CLIENT_ID_V5"} \Vert \text{chainId} \Vert \text{escrowAddr} \Vert \text{user} \Vert \text{rawClientSalt})$$

由于调用者地址 `user = msg.sender` 被密码学硬绑定于哈希原像内部，抢跑者复制完全相同的交易载荷仅会在其自身地址命名空间下生成截然不同的 `orderId`，绝无可能抢占原调用者订单槽位。入金记账强制断言 `d.inputToken.code.length > 0`（`NOT_CONTRACT_TOKEN`）及精确余额差 `(balAfter − balBefore) == d.inputAmount`（`FEE_ON_TRANSFER_UNSUPPORTED`）。跨链履约与超时退款竞态则由 `refundGraceBuffer`（$\Delta_{\text{grace}} = 1,800\ \text{s} \le 86,400\ \text{s}$）在数学上彻底隔离为互不相交的时间区间 $[0, t_{\text{deadline}}] \cap (t_{\text{deadline}} + \Delta_{\text{grace}}, \infty) = \varnothing$。在 Solana 端（`linghe_solana_escrow_7683`），原生 `Ed25519SigVerify` 指令内省严格校验 `sig_ix_idx == u16::MAX` 及偏移量边界 `offset >= header_end`（`2 + 14 * num_sigs`），彻底阻断跨指令签名偏移伪造攻击。

### 9.5 风险域五：机密计算硬件证明与椭圆曲线签名可延展性风险（TEE & ECDSA Malleability Risk）

- 风险传导机理：底层椭圆曲线验签预编译默认同时接受同一消息摘要的正负对称签名对 $(r, s)$ 与 $(r, n-s)$，可能导致 NIST `P-256`（`secp256r1`）硬件证明（`0x0000000000000000000000000000000000000100`）或 `secp256k1` 免 Gas 授权出现签名哈希可延展性重放；此外，第三方开源前端依赖包投毒可能窃取终端用户签名私钥。
- 定量与密码学缓释机制：`LingheSovereignSecurityGuardV5.verifyCanonicalP256Signature` 在调用 `0x0000000000000000000000000000000000000100` 前强制执行规范低阶 $s$ 值（**Canonical Low-$s$**）边界检查：

$$0 < r < n_{\text{P256}}, \qquad 0 < s \le \lfloor \frac{n_{\text{P256}}}{2} \rfloor = \texttt{0x7FFFFFFF800000007FFFFFFFFFFFFFFFDE737D56D38BCF4279DCE5617E3192A8}$$

```
// 经核验 EVM 合约字节码摘录 — LingheSovereignSecurityGuardV5 规范低阶 S 值 P-256 验签器
function verifyCanonicalP256Signature(
    bytes32 messageSha256,
    bytes32 r,
    bytes32 s,
    bytes32 qx,
    bytes32 qy
) external view returns (bool) {
    uint256 rVal = uint256(r);
    uint256 sVal = uint256(s);
    if (rVal == 0 || rVal >= P256_ORDER_N) return false;
    if (sVal == 0 || sVal > P256_HALF_N) return false;

    bytes memory input = abi.encodePacked(messageSha256, r, s, qx, qy);
    (bool ok, bytes memory ret) = P256_PRECOMPILE.staticcall(input);
    if (!ok || ret.length != 32) return false;
    return abi.decode(ret, (uint256)) == 1;
}
```

同理，`LingheOriginEscrow7683._recoverLowS` 强制执行 `uint256(s) <= SECP256K1_HALF_N` 及守护者地址严格升序校验（`recovered > prevGuardian`），以 $O(N)$ 复杂度杜绝重复签名凑数。硬件可信执行环境（`NVIDIA H100 CC` / `AWS Nitro`）必须在 `0x8900000000000000000000000000000000000003` 持有激活态芯片原厂根证书与 `PCR0` 度量哈希白名单；终端 `MYRILUM LingheOS Wallet` 则坚持 `0` 第三方运行时 `npm` 依赖，私钥全程受硬件级 Touch ID 与 `AES-256-GCM`（`600,000` 次迭代 `PBKDF2-HMAC-SHA256`）本地沙箱加密保护。

### 9.6 风险域六：跨境成文法规则演进与制裁策略同步风险（Regulatory Evolution & Sanctions Conflict Risk）

- 风险传导机理：香港法例第 656 章附属技术指引细化、欧盟 MiCA 监管技术标准（`RTS`）迭代或跨司法管辖区制裁名单更新，要求分布式账本合规状态机具备确定性、低延迟的参数重配置与受限状态隔离能力。
- 协议架构与法律边界缓释机制：在法律主体边界上，`MYRILUM LIMITED` 严格界定为底层开源协议与本地非托管软件系统研发主体，在香港或任何司法管辖区均不从事受规管稳定币发行、资金归集或向公众要约活动；协议内生之 `LHKD`、`LUSD` 与 `LHC` 恒定保持为非流通确定性基准测试状态（Non-Circulating Deterministic Benchmark State）。在状态机规则可演进性上，内核预编译 `TIP-403 Policy Registry`（`0x403c000000000000000000000000000000000000`）支持合规策略控制域在 `250 ms` 单槽终局内原子同步最新法定制裁测试集，并配套基于 `EIP-191` 签名挑战的误报复核规程（详见附表二）及四法域 `3-of-4` 时间锁参数治理边界。

### 9.7 六大审慎风险域与链上密码学缓释算子总览表

| 审慎风险域 | 核心极端压力测试向量 | 协议内生定量 / 密码学硬边界 | 链上强制执行合约与预编译地址 | 缓释后残余风险评级 |
|---|---|---|---|---|
| **1.** 托管集中度风险 | 单一商业托管分档信用中断冲击 | 每币种 `4` 组 G-SIB/认可机构 BIC 分散建模；单行现金上限 `30.40%`；零再质押约束 | `0x8800000000000000000000000000000000000001`（`LINGHE_CAP656_HQLA_V1`） | 低（**LOW**）· 双账簿正交隔离 |
| **2.** 利率飙升风险 | 全球央行急速大幅平行加息冲击 | 单券 $\tau_m \le 90$d；基准 WAM `24.12d` / `25.47d`；最劣可抗 `+480.8 bps` 冲击 | `publishReserveAttestation`（`reserveRatioBps >= 10000`） | 极微（**NEGLIGIBLE**）· `101.20%` / `100.50%` |
| **3.** 极端流出风险 | `100%` 基准盘同步集中销毁测试 | `54.39%`（`LHKD`）与 `50.25%`（`LUSD`）`0–1d` 现金分档 + 一级 HQLA 回购瀑布流模型 | `0xdec0000000000000000000000000000000000000`（`1 bps CLOB`）+ 基准受托模型 | 低（**LOW**）· `T+0` / 最迟 `T+1` |

| 审慎风险域 | 核心极端压力测试向量 | 协议内生定量 / 密码学硬边界 | 链上强制执行合约与预编译地址 | 缓释后残余风险评级 |
|---|---|---|---|---|
| **4.** 跨链与证明竞态 | 内存池抢注阻断 / 履约退款竞态 | 用户盐值绑定 `openProtected` + `1,800s` 宽限期 + 永不暂停之 `refundExpiredOrder` | `LingheOriginEscrow7683` 与 `0x8900000000000000000000000000000000000002` | 极微（**NEGLIGIBLE**）· 时序区间互斥 |
| **5.** 飞地与签名延展 | 高阶 $s$ 镜像签名伪造 / 供应链投毒 | 规范低阶 $0 < s \le \lfloor n_{P256}/2 \rfloor$ + `PCR0` 度量白名单 + 钱包 `0` 外部运行时依赖 | `LingheSovereignSecurityGuardV5` + `0x0000000000000000000000000000000000000100` | 极微（**NEGLIGIBLE**）· 硬件信任根锚定 |
| **6.** 制裁与规则演进 | 跨法域名单同步 / 小额拆单逃逸 | 内核 `TIP-403 Policy #2` + `US$1,000` / `US$5,000` 24h WAL 旅行规则 + 策略域单向熔断 | `0x403c0000000000000000000000000000000000000` + `HTTP 451` 合规网关 | 受控（**CONTROLLED**）· 非流通基准闭环 |

第 10 章 · SECTION 10

## 香港法例第 656 章、第 615 章、第 486 章与国际审慎标准之字节码同构映射总表

下表将香港特别行政区相关成文法、欧盟《加密资产市场法规》（Regulation (EU) 2023/1114, MiCA）、FATF 国际反洗钱准则及巴塞尔委员会 `SCO60` 的 16 项核心技术规范条文，逐条映射至灵核公链（`ChainID: 88888`）经核验的链上合约/预编译地址、字节码强制执行谓词与可复现密码学证据：

| 序号 | 对标成文法条与国际审慎标准 | 形式化建模之实质性技术准则 | 经核验链上合约 / 内核预编译地址 | 密码学 / 字节码强制执行算子 | 独立可验证审计遥测与密码学回执 |
|---|---|---|---|---|---|
| 1 | 香港第 **656** 章第 **8** 及 **9** 条；第 **622** 章著作权主体 | 纯技术研发非发行边界与香港研发法人登记要素不可变锚定 | `MYRILUM LIMITED` 协议研发主体锚点（`LingheSovereignSecurityGuardV5`） | `anchorWhitepaperSuiteIndex`（`CR/UBI 80912065`、`BR 80912065-000-07-26-0`） | 链上 `WhitepaperSuiteAnchored` 事件与非流通基准状态声明 |
| 2 | 香港第 **656** 章第 **14** 条及附表 **2** 准则建模；**MiCA** 第 **19** 及 **51** 条 | 技术规范文档套件完整性密码学固化与防篡改摘要校验 | `LingheSovereignSecurityGuardV5` + 创世块 `01a390d7...2f1b` | `require(suiteIndexSha256 != bytes32(0) && whitepaperCount >= 6)` | 全套 6 卷中英双语技术规范公开 `SHA-256` 校验回执 |
| 3 | 香港第 **656** 章附表 **2**（全额储备）；欧盟 **MiCA** 第 **36** 条 | 参考储备净值在任意状态转换后均不低于链上基准总负债（$\geq 100\%$） | `0x8800000000000000000000000000000000000001`（`LingheComplianceReserveVault`） | `require(fiatBackingAtomic >= onChainLiabilityAtomic)`（`reserveRatioBps >= 10000`） | `LHKD 10120 bps`（`101.20%`）、`LUSD 10050 bps`（`100.50%`）基准链上读数 |
| 4 | 香港第 **656** 章附表 **2**（资产隔离）；欧盟 **MiCA** 第 **37** 条 | 基准法定信托双账簿正交隔离模型与四分档独立 BIC 拓扑核验 | `0x8800000000000000000000000000000000000001` + `LingheSovereignSecurityGuardV5` | `verifyCap656MerkleInclusion` 校验 `LINGHE_CAP656_HQLA_V1` 分档叶子 | 四分档二叉默克尔根（`0xa3e5...eae6e` 与 `0x5c3f...64f410`） |

| 序号 | 对标成文法条与国际审慎标准 | 形式化建模之实质性技术准则 | 经核验链上合约 / 内核预编译地址 | 密码学 / 字节码强制执行算子 | 独立可验证审计遥测与密码学回执 |
|---|---|---|---|---|---|
| 5 | 香港第 656 章附表 2（资产质量）；欧盟 MiCA 第 38 条 | 极短期高流动性 HQLA 期限约束（$\tau_m \le 90$ 天）且零内部计量原语耦合 | 0x20C0000000000000000000000000000000000002（LHKD）/ 0x20C0000000000000000000000000000000000001（LUSD） | computeHqlaLeafHash(..., maturityDays)，$\tau_m \in \{0,1,28,84,85\}$；$\partial R_t / \partial P_{\mathrm{LHC}} \equiv 0$ | 附表一默克尔叶子 maturityDays 包含性证明与基准鉴证 URI |
| 6 | 香港第 656 章附表 2（面值赎回）；欧盟 MiCA 第 39 及 49 条 | 1:1 定点数原子销毁守恒映射（T+0 / T+1 时序模型），0 bps 协议折价算子 | 0x20C0000000000000000000000000000000000002 与 0x20C0000000000000000000000000000000000001 | 链上 TIP-20 原子销毁守恒算子与留存覆盖率单调增厚律 | 链上 Transfer 销毁事件回执与参考清算状态转移日志 |
| 7 | 香港第 656 章禁息准则；欧盟 MiCA 第 40 及 50 条；第 571 章附表 1 | 字节码层强制锁定持有人零生息率（$r_{\mathrm{holder}} \equiv 0$）；排除 CIS 构成要件 | 0x20C0000000000000000000000000000000000002 与 0x20C0000000000000000000000000000000000001 | 纯粹非重定基 6 位精度 TIP-20 账本；零生息或质押分红函数入口 | 不可变 TIP-20 ABI 接口审计确认零利息派发逻辑 |
| 8 | 香港金融管理局联系汇率制度（LERS） | 字节码硬锁定 7.7500–7.8500 HKD/USD 强弱方兑换保证走廊 | 0x8900000000000000000000000000000000000001（LingheOmnichainSettler） | require(newPegRateScaled >= 77500 && newPegRateScaled <= 78500) 及向下取整守恒 | linghe_hkma_linked_fx_peg_bps = 78000 及 LinkedRateSwapped 事件 |
| 9 | 香港第 537 章（UNSO）；第 575 章（UNATMO）；OFAC / JFIU | 对指定受限地址向量实施即时冻结与全状态空间零穿透阻断 | 0x403c0000000000000000000000000000000000（TIP-403 Policy Registry） | isAuthorized(2, account) 贯穿内核 TIP-20、DEX、Settler 与 ZK 跨链桥 | linghe_tip403_sanctions_blocks_total 计数器及确定性回滚日志 |
| 10 | FATF 第 16 项建议；香港第 615 章第 13A 条（AMLO） | 单笔 $\ge \mathrm{US\$1,000}$（HK$7,800）旅行规则与 24h 滚动窗口反拆单断言 | 0x8800000000000000000000000000000000000001 + *x402 合规结算网关* | 分段算子 $\Gamma(p, v, \mathcal{E}, t)$、86,400,000ms WAL 滑动窗及 HTTP 451 门禁 | HTTP 451 TRAVEL_RULE_ENVELOPE_REQUIRED 审计日志与 CrossChainIntentSettled |
| 11 | 香港第 486 章（PDPO 第 1、3、4 原则）；欧盟 GDPR 第 5 及 17 条 | 个人资料最小化原则；严禁将自然人明文个人身份信息写入公开状态树 | 0x8004000000000000000000000000000000000001（LingheERC8004IdentityRegistry） | attestAgentCompliance 仅锚定 32 字节 zkCredentialHash 与 keccak256 信封摘要 | 链上状态树扫描确认零自然人明文 PII 字符串留存 |
| 12 | 香港第 656 章附表 2（权限治理）；BCBS SCO60 | 跨司法辖区门限治理、eta 时间锁事前公示及零单点管理员私钥 | 0x8900000000000000000000000000000000000004 + LingheSovereignSecurityGuardV5 | 四法域 3-of-4（HK-HKMA、SG-MAS、JP-FSA、CH-FINMA）+ block.timestamp >= op.eta | TimelockOperationQueued / TimelockOperationExecuted 链上治理回执 |
| 13 | 香港金管局 SPM TM-G-2 与 TM-E-1；欧盟 DORA（Reg. 2022/2554） | 分布式共识韧性（RPO = 0、RTO < 60s）及故障闭锁实时遥测 | 0xcccccccc0000000000000000000000000000（Simplex Validator Config） | Commonware Simplex BFT（250ms 单槽终局）+ HTTP 503 / 0.00% 故障归零探针 | linghe_chain_up、linghe_por_source_up 及 HTTP 503 故障注入验证回执 |

| 序号 | 对标成文法条与国际审慎标准 | 形式化建模之实质性技术准则 | 经核验链上合约 / 内核预编译地址 | 密码学 / 字节码强制执行算子 | 独立可验证审计遥测与密码学回执 |
|---|---|---|---|---|---|
| **14** | 跨链用户本金主权保护（香港第 **656** 章 / 欧盟 **MiCA** 第 **47** 条） | 跨链合约紧急暂停或求解器离线期间严禁锁死用户托管本金 | `LinghеOriginEscrow7683`（EVM）与 `linghe_solana_escrow_7683`（Solana） | `openProtected` + `refundGraceBuffer`（`1,800s`）+ 豁免暂停之 `refundExpiredOrder` | `paused == true` 期间成功触发 `OrderRefundedToUser` / `OrderRefundedEvent` 回执 |
| **15** | **NIST FIPS 186-5** 与硬件机密计算完整性（`EIP-7951`） | 硬件信任根度量核验及彻底消除椭圆曲线 ECDSA 签名可延展性 | `0x8900000000000000000000000000000000000003` + `0x0000000000000000000000000000000000000100` | `verifyCanonicalP256Signature` 强制校验 $0 < s \le \text{P256_HALF_N}$ 及 `PCR0` 度量 | `HardwareEnclaveAttested` 与 `EnclaveProofVerified`（`0x8004000000000000000000000000000000000003`） |
| **16** | 香港第 **615** 章非托管软件边界与原生手续费抽象 | 客户端本地自托管密钥隔离与免波动代币耦合之原生 Gas 计量 | `0xfeec0000000000000000000000000000000000000000` 与 `0x4e4f4e4345000000000000000000000000000000` | 原生 `LHKD` / `LUSD` 计量 Gas + `32` 通道 `0x76` 2D Nonce + 钱包 `0` 外部 `npm` 依赖 | 基准压测 `20/20` 并发批次（耗时约 `1,004ms`，`0` 随机数冲突丢包） |

法定附表一 · SCHEDULE I

# LHKD 与 LUSD 参考储备状态模型 HQLA 叶子结构与链上密码学核验规范

## I.1 域分离紧凑二进制叶子编码与字典序排序默克尔根规范

为支持独立密码学审计员、分布式系统研究人员及自动化合规验证工具在不向公开状态树暴露底层商业银行完整账号的前提下，以数学确定性独立复算核验 `100%+` 储备覆盖不变量，每一独立参考储备分档 $i \in \{0, 1, 2, 3\}$ 严格遵循固化于 `LinghеSovereignSecurityGuardV5` 合约中的 Solidity 紧凑字节编码规范生成叶子摘要：

```
// 经核验 EVM 合约字节码摘录 — LinghеSovereignSecurityGuardV5 储备叶子哈希与包含性核验器
function computeHqlaLeafHash(
    string calldata assetSymbol,
    string calldata custodianBic,
    string calldata accountMask,
    uint256 valuationAtomic,
    uint32 maturityDays
) public pure returns (bytes32) {
    return keccak256(
        abi.encodePacked(
            "LINGHE_CAP656_HQLA_V1",
            assetSymbol,
            custodianBic,
            accountMask,
            valuationAtomic,
            maturityDays
        )
    );
}
```

形式化而言，每一枚分档叶子摘要 $\ell_i \in \{0,1\}^{256}$ 由六个顺序紧凑拼接字段构成——域分离前缀 `"LINGHE_CAP656_HQLA_V1"`（`21` 字节 ASCII）、币种符号 `assetSymbol`（`UTF-8`）、ISO 9362 托管银行识别码 `custodianBic`（`11` 字节 ASCII）、脱敏参考专户标识 `accountMask`（`UTF-8`）、大端序 `uint256` 原子估值 `valuationAtomic`（`32` 字节）以及大端序 `uint32` 剩余到期天数 `maturityDays`（`4` 字节，$\le 90$）：

$$\ell_i = \text{keccak256}(\texttt{"LINGHE_CAP656_HQLA_V1"} \,\|\, \text{assetSymbol}_i \,\|\, \text{custodianBic}_i \,\|\, \text{accountMask}_i \,\|\, \text{valuationAtomic}_i \,\|\, \text{maturityDays}_i)$$

内部节点按规范字节字典序排序对归约算子 $\text{HashSorted}(x, y) = \text{keccak256}(\min(x, y) \,\|\, \max(x, y))$ 逐层向上聚合，确保与排序对验证器及显式左右位置（`siblingIsLeft`）验证器双向等价兼容：

$$H_{0,1} = \text{HashSorted}(\ell_0, \ell_1), \qquad H_{2,3} = \text{HashSorted}(\ell_2, \ell_3), \qquad R_{\text{Merkle}} = \text{HashSorted}(H_{0,1}, H_{2,3})$$

### I.2 经链上核验之创世参考储备基准分档明细表（`LHKD` `101.20%` 与 `LUSD` `100.50%`）

**A.** `LHKD`（`0x20C0000000000000000000000000000000000002`）— 链上基准总负债：`78,000,000.00 LHKD`（`78,000,000,000,000` 原子单位）

| 叶子索引 | 托管银行 **SWIFT BIC** | 脱敏参考专户掩码标识 | 参考 **HQLA** 储备资产建模分类 | 剩余期限（`uint32`） | 基准标度估值（法币 / `uint256` 原子单位） | 经核验 `LINGHE_CAP656_HQLA_V1` 叶子摘要 $\ell_i$ |
|---|---|---|---|---|---|---|
| `0` | `HSBCHKHHHKH` | `HKMA-TRUST-SEG-8801` | 模拟第 155 章认可机构破产隔离活期信托现金分档 | `0` 天 | HK$24,000,000.00（`24000000000000`） | `0xb30a3fe78b8b41268f0e3e5a5c23c51b095b2a92076c091c85246e104a6953bb` |
| `1` | `SCBLHKHHXXX` | `HKMA-TRUST-SEG-8802` | 模拟第 155 章认可机构独立托管清算现金分档 | `0` 天 | HK$18,936,000.00（`18936000000000`） | `0xf88dbad68c958f842437547ab67e87455c437a107be8c1b675ddeccd086935a3` |
| `2` | `BOFAHKHX001` | `CMU-EFBN-SUB-9011` | 香港外汇基金票据基准分档（28 天期一级 HQLA） | `28` 天 | HK$20,000,000.00（`20000000000000`） | `0x746b593642e0cebb33b58be66c6fcee66a19904597323cfc54ae091fb64aed78` |
| `3` | `BKCHHKHHXXX` | `CMU-EFBN-SUB-9042` | 香港外汇基金票据基准分档（84 天期一级 HQLA） | `84` 天 | HK$16,000,000.00（`16000000000000`） | `0xc2e9807edaca5f2bc467c717b9d9bdedf0ef807c8cf14ebb9e775997651b33ef` |

- 第一层内部聚合节点：
  - $H_{0,1}^{\text{LHKD}} = \text{keccak256}(\ell_0 \,\|\, \ell_1) =$ `0x3c374983caeb993ae548d315e118a8468d50afb604ba634a8425e623337e3844`（因字节序 $\ell_0 < \ell_1$）；
  - $H_{2,3}^{\text{LHKD}} = \text{keccak256}(\ell_2 \,\|\, \ell_3) =$ `0x0296b902877b5e16358cb116fff185821c5767f71b17999bd62869030581c92c`（因字节序 $\ell_2 < \ell_3$）。
- 锚定于链上金库 `0x8800000000000000000000000000000000000001` 之 `LHKD` 默克尔根：
  - $R_{\text{Merkle}}^{\text{LHKD}} = \text{keccak256}(H_{2,3}^{\text{LHKD}} \,\|\, H_{0,1}^{\text{LHKD}}) =$ `0xa3e5fd1ee51db26128c49f848bc4eb6d71443fbfee51a40b9159832a21beae6e`（因字节序 $H_{2,3}^{\text{LHKD}} < H_{0,1}^{\text{LHKD}}$）；
  - 参考储备模型总净值：**HK$78,936,000.00**（`78,936,000,000,000` 原子单位）；基准偿付覆盖率：`101.20%`（`10120 bps`）；链上基准锚定 URI 字段：`linghe://compliance/por/lhkd-cap656-hkma-sandbox.pdf`。

**B.** `LUSD`（`0x20C0000000000000000000000000000000000001`）— 链上基准总负债：`10,000,000.00 LUSD`（`10,000,000,000,000` 原子单位）

| 叶子索引 | 托管银行 **SWIFT BIC** | 脱敏参考专户掩码标识 | 参考 **HQLA** 储备资产建模分类 | 剩余期限（`uint32`） | 基准标度估值（法币 / `uint256` 原子单位） | 经核验 `LINGHE_CAP656_HQLA_V1` 叶子摘要 $\ell_i$ |
|---|---|---|---|---|---|---|
| `0` | `IRVTUS3NXXX` | `BNYM-SEG-TRUST-4401` | 模拟破产隔离现金信托存款分档 | `0` 天 | US$3,050,000.00（`3050000000000`） | `0xcdf6eca07712742b2a1e59591ac365f399f1ff4fe0653a554a1b616ab7c797e8` |
| `1` | `SBOSUS33XXX` | `SST-SEG-TRUST-4402` | 模拟隔夜司库现金专户托管分档 | `1` 天 | US$2,000,000.00（`2000000000000`） | `0x0d1c95d260b32a3381c92b576aa2db44dbe1bbbdacf4b4353ff2429eb8582080` |
| `2` | `CITIUS33XXX` | `FEDWIRE-TBILL-7710` | 美国短期国库券基准分档（28 天期 T-Bill 一级 HQLA） | `28` 天 | US$3,000,000.00（`3000000000000`） | `0xe64345f06fee3e7cdcb9f3a011ed4a4b67a179d2d526593100c276cdf2a9433c` |
| `3` | `CHASUS33XXX` | `FEDWIRE-TBILL-7785` | 美国短期国库券基准分档（85 天期 T-Bill 一级 HQLA） | `85` 天 | US$2,000,000.00（`2000000000000`） | `0xd763712182ea48eec13a34cb44807c6757a6850c4269de739cf17fe30aac4c96` |

- 第一层内部聚合节点：
  - $H_{0,1}^{\mathrm{LUSD}} = \mathrm{keccak256}(\ell_1 \,\|\, \ell_0) =$ `0x0d49d74679ff606e96b568f63327de7d688b66707eba9ce1793a7da5ddddd9d6`（因字节序 $\ell_1 < \ell_0$）；
  - $H_{2,3}^{\mathrm{LUSD}} = \mathrm{keccak256}(\ell_3 \,\|\, \ell_2) =$ `0x79e2878d2c99bfc91c9af775e595ddd8fea8ffc63635f684d737fbf81a84c1e1`（因字节序 $\ell_3 < \ell_2$）。
- 锚定于链上金库 `0x8800000000000000000000000000000000000001` 之 `LUSD` 默克尔根：
  - $R_{\mathrm{Merkle}}^{\mathrm{LUSD}} = \mathrm{keccak256}(H_{0,1}^{\mathrm{LUSD}} \,\|\, H_{2,3}^{\mathrm{LUSD}}) =$ `0x5c3f82332fbffc0be49434232a9a97e2bf2c797423aa3fde4afd19b2c264f410`（因字节序 $H_{0,1}^{\mathrm{LUSD}} < H_{2,3}^{\mathrm{LUSD}}$）；
  - 参考储备模型总净值：**US$10,050,000.00**（`10,050,000,000,000` 原子单位）；基准偿付覆盖率：`100.50%`（`10050 bps`）；链上基准锚定 URI 字段：`linghe://compliance/por/lusd-2026-q4-attestation.pdf`。

### I.3 独立验证方三步无信任链上密码学核验规程

任何外部密码学审计工具、协议研究人员或合规验证节点均无需依赖中心化后台状态背书，可通过以下三步确定性只读流程独立完成储备包含性与足额性验证：

1. 获取规范默克尔证明包：向 *x402 合规结算网关* 发起只读查询 `GET /v1/compliance/por-merkle-proof?asset=LHKD&leafIndex=0`（或指定 `asset=LUSD` 及任意 `leafIndex` $\in \{0,1,2,3\}$），获取 `(leaf, leafHash, merkleProof, computedMerkleRoot)`。以 `LHKD` 第 `0` 号基准分档（`HSBCHKHHHKH`）为例，`merkleProof` 返回第一层兄弟节点 `(position: "right", siblingHash: 0xf88d...35a3)` 与第二层兄弟节点 `(position: "left", siblingHash: 0x0296...c92c)`。
2. 链上复算域分离叶子摘要：在 `ChainID: 88888` 上通过只读 `eth_call` 调用 `LingheSovereignSecurityGuardV5.computeHqlaLeafHash("LHKD", "HSBCHKHHHKH", "HKMA-TRUST-SEG-8801", 24000000000000, 0)`，确认返回值与 `0xb30a3fe78b8b41268f0e3e5a5c23c51b095b2a92076c091c85246e104a6953bb` 逐字节

完全一致。

3. 链上断言金库默克尔根匹配及 `>= 100%` 足额覆盖：调用 `LingheSovereignSecurityGuardV5.verifyCap656MerkleInclusion(0x20C000000000000000000000000000000000002, leafHash, [sibling0, sibling1], [false, true])`，该合约实时跨合约读取 `0x8800000000000000000000000000000000000001` 上的 `getLatestReserveAttestation`，当且仅当 `recomputedRoot == onChainVaultRoot`、`fiatBackingAtomic >= onChainLiabilityAtomic` 且 `reserveRatioBps >= 10000` 同时满足时，方返回 `(valid: true, recomputedRoot, onChainVaultRoot, reserveRatioBps: 10120)`。

---

法定附表二 · SCHEDULE II

# 基准面值销毁状态转换规程、TIP-403 误报密码学复核协议与香港准据法条款

## II.1 基准面值销毁与参考清算联动四步状态转换规程

| 状态转换阶段 | 协议角色域 / 系统模块 | 合规门禁断言与链上密码学执行动作 | 参考时序目标上限（SLA 模型） |
|---|---|---|---|
| 第一阶段：机构凭证承诺注册与路由绑定 | 受测直连账户与合规策略控制域（`TIP-403 Compliance Policy Role`） | 对标香港法例第 615 章机构 `KYC/KYB` 数据结构，在 `0x8004...0001` 锚定零明文隐私 `zkCredentialHash` 承诺并映射同名清算路由标识 | 前置初始化状态（首次调用前完成） |
| 第二阶段：签名销毁指令与 `TIP-403` 合规门禁 | 调用账户与 *x402 合规结算网关* | 校验账户签名，确认 `0x403c0000000000000000000000000000000000000` 中 `isAuthorized(2, holder) == true`；若单笔 $v \geq \text{US\$1,000.00}$（`HK$7,800.00`）同步核验 VASP 旅行规则信封摘要 | `< 1 秒`（`250ms` L1 状态读取） |
| 第三阶段：链上基准负债原子销毁 | 灵核公链执行内核（`ChainID: 88888`） | 原子执行 `LHKD`（`0x20C0000000000000000000000000000000000002`）或 `LUSD`（`0x20C0000000000000000000000000000000000001`）`TIP-20` 原子余额扣减并输出不可篡改销毁回执 | `250 ms`（`Simplex BFT` 单槽确定性终局） |
| 第四阶段：`1:1` 面值守恒参考储备核销 | 基准受托拓扑模型与参考清算接口 | 按 `100%` 算术面值（`HK$1.00` / `US$1.00`，`0 bps` 协议折价算子）模拟 `HKICL FPS`（`< HK$1M`）或 `CHATS / Fedwire` RTGS（`>= HK$1M` 且于 `<= 16:00 HKT` 提交）同步扣减参考储备 | 实时 / 日内 `T+0`（最迟 `T+1 12:00 HKT`） |

## II.2 `TIP-403` 制裁状态同步、防“通风报信（Tipping-Off）”红线建模与误报密码学复核机制

1. 即时内核层阻断与香港成文法防“通风报信（**Tipping-Off**）”技术建模：一旦目标地址被写入 `TIP-403 Policy #2`（`modifyPolicyBlacklist(2, targetAddress, true)`），涉及该地址的一切本链 `TIP-20` 转移、CLOB 挂单撮合、跨链意图交割及销毁转换均在 Rust 内核层原子中止。对标香港《有组织及严重罪行条例》（香港法例第 **455** 章）第 **25A(5)** 条、《贩毒（追讨得益）条例》（香港法例第 **405** 章）第 **25A(5)** 条及《联合国（反恐怖主义措施）条例》（香港法例第 **575** 章）第 **12(5)** 条关于严禁“通风报信（Tipping-off）”之法定约束，网关错误响应严格仅输出标准化拒绝代码，零泄露底层情报触发规则细节。

2. 启发式地址聚类误报之密码学挑战—应答复核协议（`5` 个香港营业日参考窗口）：针对链上地址图谱聚类启发式算法可能引发的非制裁关联误判，协议规范定义了标准化密码学复核载荷结构：（a）法人注册或主体资质哈希凭证；（b）证明申请人对受限地址享有排他私钥控制权的 `EIP-191` 挑战—应答数字签名；以及（c）可独立追溯之链上历史交易有向无环图（DAG）干净来源证明。在参考合规工作流模型中，凡确认属启发式聚类误判而非具法律约束力之法定名单向量者，于 `5` 个香港营业日参考周期内生成状态解封提案。
3. 法定名单移除与双域门限协同解封断言：凡对应宪报刊登之 `UNSC`、香港法例第 537 章、第 575 章、`OFAC` 或 `JFIU` 名单测试向量的受限状态，在协议状态机中执行解封转换（`modifyPolicyBlacklist(2, targetAddress, false)`）必须同时满足合规策略控制域（`TIP-403 Compliance Policy Role`）签名验证与四法域 `3-of-4` 主权守护者多签合约（`0x8900000000000000000000000000000000000004`）门限批准之双重密码学前置条件。

### II.3 香港特别行政区准据法、纯软件知识产权边界与 `HKIAC` 仲裁条款

1. 准据法（**Governing Law**）：本密码学与协议工程技术规范、底层开源状态机参考代码与非托管客户端软件著作权声明，以及由此产生或与之相关的任何非契约性法律关系，均受中华人民共和国香港特别行政区法律管辖并按其解释。
2. 纯研发非金融服务范围确认与香港国际仲裁中心（`HKIAC`）终局仲裁：鉴于 `MYRILUM LIMITED` 仅作为协议与软件系统研发主体（Protocol & Software R&D Author），不从事任何稳定币发行、法币资金归集托管、兑付承诺或受规管虚拟资产交易服务，凡因本技术规范文本解释、开源软件许可边界或知识产权归属引起或与之相关的任何争议，当事方应首先通过向 `MYRILUM LIMITED` 香港法定注册办事处送达书面通知的方式启动 `30` 个公历日善意磋商；逾期未能协商解决者，应提交香港国际仲裁中心（`HKIAC`），按照提交仲裁通知时现行有效的《香港国际仲裁中心机构仲裁规则（HKIAC Administered Arbitration Rules）》通过仲裁终局解决：
   - 仲裁地及法定开庭地：中华人民共和国香港特别行政区；
   - 仲裁庭组成：由按照《HKIAC 规则》指定的三（`3`）名仲裁员组成；
   - 仲裁语言：中文或英文。
3. 香港高等法院原讼法庭法定管辖保留：上述仲裁条款概不限制具管辖权司法或执法机关依据香港法例第 537 章、第 575 章、第 455 章或相关知识产权保护与衡平法禁制令救济条文，向中华人民共和国香港特别行政区高等法院原讼法庭（**Court of First Instance of the High Court**）行使法定专属管辖权或申请紧急临时禁制令（Interim Injunction）。

---

协议与软件系统研发主体技术准确性声明与版本印鉴

下述协议与软件系统研发主体（**Protocol & Software R&D Author**）确认，经执行全链路确定性合约字节码编译校验、`LINGHE_CAP656_HQLA_V1` 二叉默克尔储备树原像复算及多区域拜占庭容错故障注入测试，本技术规范所载之企业主体登记要素、`ChainID: 88888` 创世与系统合约地址、密码学算子定义及形式化数学不变量均与代码唯一真源（SSOT）严格一致。依据香港法例第 656 章第 8 条及第 9 条、第 571 章及第 615 章之法律边界，`MYRILUM LIMITED` 在香港或任何司法管辖区均不从事受规管稳定币发行或金融牌照业务；本文献及链上非流通确定性基准测试状态（`LHKD`、`LUSD`、`LHC`）纯属计算机科学与密码学协议技术规范，不构成任何代币销售、公众要约、集体投资计划或法币兑付承诺。

- 协议与软件系统研发主体（**Protocol & Software R&D Author**）：`MYRILUM LIMITED`（迈瑞伦有限公司）· 公司注册编号 / UBI `80912065` · 商业登记证号 `80912065-000-07-26-0`
- 法人组织形式与成立法例：于 `2026 年 7 月 27 日` 依据香港法例第 622 章《公司条例》注册成立之私人股份有限公司（`BODY CORPORATE`）
- 香港法定注册办事处地址：`UNIT 1603, 16/F THE L. PLAZA, 367-375 QUEEN'S RD CENTRAL, SHEUNG WAN, HONG KONG`
- 底层确定性验证账本与创世区块锚定：MYRILUM 灵核OS公链（`Linghe Chain`，`ChainID: 88888` / `0x15b38`）· 创世第 0 块 SHA-256 `96208e9900b218935143be3024d2602566a86d61caa906d42399f35b83afd991`
- 发布版次与生效日期：`v2.0` 协议内生合规状态机与密码学技术规范正式版 · `2026 年 11 月 11 日`




VOL. II · ENSHRINED REGTECH & PROOF-OF-RESERVE SPECIFICATION

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 · v2.0

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**

221a4629c59914c36ba18f0a3b5a31a0a042713ac83da4c4272e7e8b22d33a30

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