VOLUME 0 · GROUP MASTER ARCHITECTURE & SOVEREIGN GOVERNANCE WHITEPAPER

MYRILUM Group Master Architecture & Sovereign Governance Whitepaper: Formal Specification of the AI WorkOS Multi-Agent Operating System, Zero-Dependency Sovereign Client, and Sub-Second Regulated Settlement State Machine (v1.0)

Formal Architecture, Threat Boundaries, Multi-Jurisdictional Safe-Harbor Governance & Equity Economics of the MYRILUM Sovereign Trinity Stack

MYRILUM Group Principal Systems Architecture & Interdisciplinary Engineering Council (AI Systems · Applied Cryptography · Distributed Consensus · RegTech)



SOVEREIGN AI WORKOS
8 Apps · 21 Pkgs
Deterministic Harness & Context DNA

ZERO-TRUST WALLET v5.1
60 Specs · 0 Deps
169 Chains · 14 Zero-Trust MCP Tools

SUB-SECOND SETTLEMENT
250 ms / 32 Lanes
Simplex BFT · 3.0B Gas · Chain 88888

CORPORATE GOVERNANCE
UBI 80912065
D-U-N-S 374308629 · Non-Custodial R&D

PROTOCOL & SOFTWARE R&D AUTHOR

MYRILUM LIMITED

Hong Kong SAR Companies Ordinance (Cap. 622) · Body Corporate

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

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

Protocol R&D Entity Particulars, HK Statutory Boundary & Cryptographic Provenance

VOL. 00 MONOGRAPH ARCHITECTURAL TIER

VOL. 0 · GROUP MASTER ARCHITECTURE & GOVERNANCE WHITEPAPER

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

CHAIN 88888 ON-CHAIN VERIFICATION & GUARD

LingheSovereignSecurityGuardV5.latestWhitepaperAnchor()

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

Corporate / Cryptographic Field	Verified Canonical Record (SSOT)
Protocol & Software R&D Author	`MYRILUM LIMITED` (Hong Kong Companies Ordinance Cap. 622)
Company No. / UBI & D-U-N-S	CR/UBI: `80912065` · D-U-N-S®: `374308629`
Business Registration (Cap. 310)	`80912065-000-07-26-0`
Registered Office	UNIT 1603, 16/F THE L. PLAZA, 367-375 QUEEN'S RD CENTRAL, SHEUNG WAN, HONG KONG
Document Reference ID	`MYR-WP-MASTER-2026-V1.0-EN` · GROUP MASTER ARCHITECTURE & GOVERNANCE WHITEPAPER · INTERNATIONAL CANONICAL EDITION (v1.0)
Sovereign Network & Genesis Hash	ChainID `88888` (`0x15b38`) · Genesis SHA-256: `96208e9900b218935143be3024d2602566a86d61caa906d42399f35b83afd991`
LHKD Benchmark Merkle Root	`0xa3e5fd1ee51db26128c49f848bc4eb6d71443fbfee51a40b9159832a21beae6e` (101.20% · 78,936,000.00 Synthetic Benchmark Vector)
LUSD Benchmark Merkle Root	`0x5c3f82332fbffc0be49434232a9a97e2bf2c797423aa3fde4afd19b2c264f410` (100.50% · 10,050,000.00 Synthetic Benchmark Vector)
Canonical Source SHA-256	`522691a5113f695ad527669f22b8894e84737ff15e2496d9eea119252b8b3389`

HONG KONG STATUTORY BOUNDARY & PURE TECHNICAL SPECIFICATION NOTICE

1. Pure Technical Specification & Non-Offering Boundary: This monograph is an engineering and cryptographic specification authored by MYRILUM LIMITED solely as Protocol & Software R&D Author. Nothing herein constitutes a prospectus (Cap. 32), an offer of securities or collective investment schemes (Cap. 571), the issuance, offering, or active marketing of any specified stablecoin (Cap. 656 ss. 8 & 9), or a virtual asset service (Cap. 615). LHKD, LUSD, and LHC are enshrined protocol ledger primitives and non-circulating deterministic benchmark states.

2. Zero-Yield Non-Deposit, Non-Custodial Client & Privacy Invariants: Protocol state machines enforce zero holder yield (r_holder(t) === 0, non-deposit under Cap. 155 / Cap. 581), 100% client-side self-custodial key generation in MYRILUM LingheOS Wallet with zero runtime dependencies, and Zero Individual PII stored on-chain in compliance with the Personal Data (Privacy) Ordinance (Cap. 486).

TABLE OF CONTENTS · SWISS ARCHITECTURAL INDEX

CONTENTS & ARCHITECTURAL INDEX

Swiss Analytical Section Hierarchy — Select any entry in digital PDF viewers to navigate directly to the formal specification.

00 **Abstract** §00

00·1 **Global Mathematical Notation and Cross-Stack Primitives** §00·1

01 **First Principles and Motivation for the Sovereign Trinity Stack** §01

- 1.1 Three Structural Fault Lines in Enterprise Agentic Computing and Settlement §1.1
- 1.2 Orthogonal Decomposition of the MYRILUM Sovereign Trinity Closed Loop §1.2
- 1.3 Claim Maturity Taxonomy, Runtime State Separation, and Three Prohibited Equivalences §1.3

02 **Pillar I: MYRILUM AI WorkOS Deterministic Multi-Agent Operating System** §02

- 2.1 Deterministic Execution Harness, Causal Privacy Ledger, and Multi-Surface Topology §2.1
- 2.2 Organizational Context DNA and Anti-Hallucination Provenance Deliverables §2.2
- 2.3 Tenant-Isolated Append-Only Audit Stream and Ten-Dimensional Human Gate Accountability Matrix §2.3

03 **Pillar II: MYRILUM LingheOS Wallet v5.1.0 Zero-Dependency Sovereign Client** §03

- 3.1 Zero-Dependency Supply-Chain Immunity and Four-Runtime Isomorphic Sandbox §3.1
- 3.2 Account Abstraction Matrix (`EIP-7702` / `P-256` / `EIP-5792` / `ERC-7715`) and Pre-Sign Phishing Firewall §3.2
- 3.3 Shamir $GF(2^8)$ Threshold Secret Sharing and 48-Hour Timelocked Guardian Recovery §3.3

04 **Pillar III: MYRILUM Linghe Chain (`ChainID 88888`) Sub-Second Parallel Settlement State Machine** §04

- 4.1 `Commonware Simplex BFT` Single-Slot Finality and Type- `0x76` 2D-Nonce Parallel EVM §4.1
- 4.2 Kernel-Enshrined RegTech (`TIP-403`), Linked-Rate Corridor, and Binary Merkle Solvency Proofs §4.2
- 4.3 Dual-Curve Cryptographic Roots (`EIP-7951 P-256` + `BN254 Groth16`) and Omnichain Settlement Customs §4.3

05 **Cross-Stack Causal Co-Design: From Enterprise Cognition to Sub-Second Verifiable Settlement** §05

- 5.1 Seven-Stage End-to-End Deterministic State-Transition Pipeline and Compositional Invariance §5.1
- 5.2 Machine-Native Micropayments (`x402`) and Bilateral Fee-for-Service Arithmetic Clearing §5.2

06 **Formal Trust Assumptions, Cryptographic Runtime Boundaries, and Hot-Spot Contention Degradation** §06

- 6.1 Four-Region `3-of-4` BFT Fiber-Geometry Assumptions and Mandatory Timelock Governance Bounds §6.1
- 6.2 Tiered Side-Channel Defense: Silicon Hardware Roots (`Tier-1`) vs. Managed JIT Runtime Boundaries (`Tier-2`) §6.2
- 6.3 Parallel Execution Degradation Under Hot-Spot Write Contention and Deterministic Serial Fallback §6.3

07 **Multi-Jurisdictional Regulatory Engineering and Shared-Nothing Dual-Hemisphere Isolation** §07

- 7.1 Hong Kong Statutory Compliance Matrix (`Cap. 622, 32, 571, 656, 615, 155/581 & 486`) and Non-Issuer Safe Harbor §7.1
- 7.2 International Regulatory Alignment (`Howey` , `MiCA` , `BCBS SCO60` & App Store Rules) and Tri-Mode Geofencing §7.2
- 7.3 Physically Air-Gapped Mainland China Pure-AI Enterprise Architecture (`myrilum.cn`) §7.3

08 **Corporate Equity Monetization, GAAP/IFRS Cash-Flow Engines, and Unit Economics** §08

- 8.1 Pure Software Equity Value Capture and `IAS 7` Cash-Flow Reconciliation Without Token Subsidies §8.1
- 8.2 Three Recurring Fiat Revenue Engines and `IFRS 15` / `ASC 606` Revenue Recognition §8.2

09 **Master Whitepaper Suite Lineage, Version Reconciliation, and Cryptographic Attestation Index** §09

- 9.1 Four-Volume Global Monograph Hierarchy and Client Specification Reconciliation (`v5.0 -> v5.1.0`) §9.1
- 9.2 Stage-Gated Engineering Roadmap (`G0-G9`) and Reproducible Cryptographic Verification Protocol §9.2

AP·A **Normative Standards and Academic References** §A

MYR-WP-MASTER-2026-V1.0-EN · GROUP MASTER ARCHITECTURE & GOVERNANCE WHITEPAPER · INTERNATIONAL CANONICAL EDITION (v1.0)

MYRILUM Group Master Architecture & Sovereign Governance Whitepaper: Formal Specification of the AI WorkOS Multi-Agent Operating System, Zero-Dependency Sovereign Client, and Sub-Second Regulated Settlement State Machine (v1.0)

Document Reference ID: `MYR-WP-MASTER-2026-V1.0-EN` · **Monograph Tier:** `VOLUME 0` (Group Master Architecture & Governance Whitepaper · International Canonical Edition `v1.0`)
Protocol & Software R&D Author: `MYRILUM LIMITED` (Sole Statutory Registered English Corporate Name under Cap. 622 s. 899(1); No Registered Chinese Corporate Name · Private Company Limited by Shares Incorporated in the Hong Kong SAR · Company Number / UBI: `80912065` · Cap. 310 Certificate: `80912065-000-07-26-0` · Dun & Bradstreet D-U-N-S Number: `374308629`)
Statutory Registered Office: `UNIT 1603, 16/F THE L. PLAZA, 367-375 QUEEN'S RD CENTRAL, SHEUNG WAN, HONG KONG`
Canonical Trinity Codebase Anchors: `MYRILUM AI WorkOS` (`8` Applications · `21` Modular Workspace Packages) · `MYRILUM LingheOS Wallet v5.1.0` (`0` Runtime npm Dependencies · `60` Verified Specifications · `169` Networks · `14` Zero-Trust MCP Tools) · `MYRILUM Linghe Chain` (`ChainID = 88888` / `0x15b38` · Immutable Genesis Block-0 SHA-256: `96208e9900b218935143be3024d2602566a86d61caa906d42399f35b83afd991`)

STATUTORY MANDATE 0.1 — Corporate R&D Scope, Non-Offering Safe Harbor, Maturity Separation & Jurisdictional Air-Gap Notice

1. **Pure Software & Protocol R&D Author Scope**: This Group Master Whitepaper (`Volume 0`) is an interdisciplinary computer-science, cryptographic, and enterprise systems-engineering specification authored and published exclusively by `MYRILUM LIMITED` (sole statutory registered corporate name in English under Section 899(1) of the *Companies Ordinance*, `Cap. 622` of the Laws of Hong Kong, with no registered Chinese corporate name), a body corporate bearing Company Number / Unique Business Identifier (UBI) `80912065` (incorporated `27 July 2026`), *Business Registration Ordinance* (`Cap. 310`) Certificate `80912065-000-07-26-0`, and Dun & Bradstreet D-U-N-S Number `374308629`. `MYRILUM LIMITED` operates strictly as **Protocol & Non-Custodial Software R&D Author**: its activities are confined to enterprise software licensing, client-side self-custodial tooling, and distributed verification infrastructure R&D. At no time and in no jurisdiction does `MYRILUM LIMITED` accept, pool, hold, or custody public fiat funds, operate any virtual-asset exchange or automated trading service (ATS), or generate, store, back up, or access client private keys or seed phrases.
2. **Hong Kong & International Regulatory Non-Offering Boundary (`Cap. 32` / `Cap. 571` / `Cap. 656` / `Cap. 615` / `Cap. 155`)**: Nothing in this document constitutes a prospectus under the *Companies (Winding Up and Miscellaneous Provisions) Ordinance* (`Cap. 32`), an offer of securities, futures contracts, structured products, or interests in a collective investment scheme (CIS), or investment advice under the *Securities and Futures Ordinance* (`Cap. 571`), a regulated specified-stablecoin issuance, primary offering, or active marketing to the public under Sections 8 and 9 of the *Stablecoins Ordinance* (`Cap. 656`), a virtual asset trading platform (VATP) operation or regulated virtual asset service under Section 53ZRD of the *Anti-Money Laundering and Counter-Terrorist Financing Ordinance* (`Cap. 615`), an investment contract under U.S. federal securities law, or an offering document for any Article 16 asset-referenced token (ART) or Article 48 e-money token (EMT) under *Regulation (EU) 2023/1114* (`MiCA`). Within Genesis Block-0, `LHKD` (`0x20c0000000000000000000000000000000000002`), `LUSD` (`0x20c0000000000000000000000000000000000001`), and `LHC` (`0x20c0000000000000000000000000000000000000`

`000`) are strictly **enshrined protocol ledger primitives and 100% synthetic non-circulating deterministic benchmark states** enforcing a bytecode-locked zero-yield invariant ($r_{\text{holder}} \equiv 0$, non-deposit under `Cap. 155`). As of this release, `MYRILUM LIMITED` makes zero commitment to issue or sell any speculative token.

3. **Orthogonal Maturity Taxonomy & Mainland China Shared-Nothing Air-Gap**: This monograph strictly separates claims implemented and tested in source code (`VERIFIED_IN_CODE`), empirical latency measurements on controlled four-validator benchmark topologies (`BENCHMARKED_TESTBED`), formal interface specifications (`ARCHITECTURAL_SPEC`), and stage-gated future milestones (`ROADMAP_GATED`), never conflating controlled benchmark metrics with permissionless retail mainnet traffic. Furthermore, the Mainland China pure-AI enterprise edition (`myrilum.cn`, PRC MIIT ICP Filing `2026055724-1`) is independently operated onshore by PRC domestic legal entity **Beijing Linghe Agentic Technology Co., Ltd.** (Unified Social Credit Code `91110108MAERKJRC8R`) under a **100% corporate, network, codebase, database, and billing Shared-Nothing Air-Gap** from Hong Kong `MYRILUM LIMITED`, containing zero blockchain, wallet, stablecoin, or virtual-asset components. In strict compliance with the *Personal Data (Privacy) Ordinance* (`Cap. 486`), all on-chain states maintain Zero Individual Personally Identifiable Information (Zero Individual PII).

`SECTION 00 · EXECUTIVE ABSTRACT`

Abstract

Contemporary enterprise artificial intelligence and institutional financial infrastructure confront a foundational architectural fracture. On the cognitive plane, autoregressive Large Language Models (LLMs) and multi-agent workflows achieve remarkable unstructured reasoning yet remain inherently stochastic samplers: without external deterministic state machines, they exhibit multi-step error compounding, cross-session organizational amnesia, unverifiable source citations, and acute vulnerability to indirect prompt injection when connected to external execution tools. On the settlement plane, autonomous machine-to-machine procurement of confidential GPU inference, proprietary data streams, and cross-market liquidity cannot clear economically over legacy correspondent wire networks (`T+1` to `T+3`) or card rails imposing $0.15 to $0.30 fixed authorization floors, nor can it scale over first-generation sequential-nonce blockchains afflicted by $M/G/1$ queueing divergence, volatile native-token gas friction, and application-layer compliance wrappers that are trivially bypassed via smart-contract composition.

Starting from first principles, this Group Master Whitepaper (`Volume 0`) formalizes the **MYRILUM Sovereign Trinity Architecture**—a closed-loop computing and settlement stack composed of three orthogonally decoupled yet cryptographically interlocked engineering pillars:

1. **Pillar I — Enterprise Cognitive Orchestration & Governance (`MYRILUM AI WorkOS`)**: Spanning `8` multi-surface applications and `21` strongly typed workspace packages, `@myrilum/linghe-harness-core` encapsulates stochastic neural inference inside a deterministic execution harness driven by `SessionTurnEngine`, `PrivacyCausalLedger`, `CapabilityRouterRegistry`, `ArtifactDnaKernel`, and `QuotaEntitlementMeter`. Organizational brand and editorial memory are codified via `@myrilum/linghe-context-dna` under tenant-scoped `SHA-256` digests, while `@myrilum/linghe-artifact-schema` enforces anti-hallucination citation provenance (`VerifiedCitationNode`) across `6` enterprise deliverable modalities and `7` canonical file formats, backed by `@myrilum/platform-audit` single-tenant append-only audit streams and a ten-dimensional Human Gate accountability matrix.
2. **Pillar II — Zero-Trust Client & Deterministic Policy Firewall (`MYRILUM LingheOS Wallet v5.1.0`)**: Engineered under clean-room discipline with strictly `0` third-party runtime or development `npm` dependencies across four isomorphic client containers (zero-dependency standards-compliant Web browser application (SPA), Chromium MV3 Extension, macOS Native `WKWebView`, and iOS Native `WKWebView`), `LingheOS Wallet v5.1.0` verifies `60` public-standard capabilities (`OBL-001` through `OBL-060`) across `169` heterogeneous networks and exposes `14` zero-key-visibility Model Context Protocol (MCP) tools. An air-tight deterministic firewall interposes between

untrusted neural intent ASTs and signing keys, enforcing `ERC-7715` periodic and contract-allowlisted session bounds (≤ 30-day expiry), `EIP-5792` atomic call batching, `Permit2` batch approval lockdown, `EIP-712` / lookalike address-poisoning pre-sign interception, Shamir k-of-n secret sharing over $\mathrm{GF}(2^8)$, and `48`-hour owner-vetoable on-chain guardian recovery.

3. **Pillar III — Sub-Second Parallel Regulated State Machine (`MYRILUM Linghe Chain`, `ChainID = 88888` / `0x15b38`)**: Combining `Commonware Simplex BFT` across a four-region synthetic benchmark validator committee with a customized `Paradigm Reth` Rust execution kernel, `Linghe Chain` achieves $\Delta_{\text{slot}} = 250$ ms single-slot deterministic finality ($P_{\text{reorg}} \equiv 0$), a `3,000,000,000` per-slot gas ceiling, and `32` concurrent type-`0x76` 2D-nonce settlement lanes (`20/20` concurrent `0x76` micropayment transactions finalized in `~1,004 ms` on the controlled benchmark testbed). Kernel precompiles natively enforce sub-microsecond `TIP-403` sanctions screening, the `[7.7500, 7.8500] HKD/USD` Linked Exchange Rate corridor, `LINGHE_CAP656_HQLA_V1` High-Quality Liquid Assets (HQLA) binary Merkle solvency proofs, canonical low-s `Osaka EIP-7951` `P-256` hardware enclave verification (`0x0000000000000000000000000000000000000100`), and `ERC-7683` + `BN254 Groth16` (`815,381 gas`) omnichain intent fulfillment (`~936 ms` benchmark latency).

Beyond protocol mechanics, we formalize explicit trust assumptions, V8/JavaScriptCore JIT microarchitectural side-channel tiering, Amdahl-Brent contention degradation envelopes under shared-state write conflicts, Shared-Nothing jurisdictional isolation between global and Mainland China deployments, and three token-independent `IFRS 15` / `IAS 7` / `ASC 606` corporate equity cash-flow engines.

FORMAL NOTATION & PRIMITIVES

Global Mathematical Notation and Cross-Stack Primitives

To maintain formal precision across artificial-intelligence orchestration, client-side cryptography, and distributed consensus, Table 0.1 defines the canonical algebraic notation, domains, and repository Single-Source-of-Truth (SSOT) constants referenced throughout this volume. Here $\mathbb{N}_0 = \{0, 1, 2, \ldots\}$, $\mathbb{U}_b = \{0, 1, \ldots, 2^b - 1\}$ denotes unsigned b-bit integers, $\mathbb{B}^k = \{0,1\}^{8k}$ denotes k-byte octet strings, $\mathcal{A} \equiv \mathbb{B}^{20}$ denotes canonical 20-byte addresses, and $\Vert$ denotes deterministic byte concatenation.

Symbol / Operator	Algebraic Domain & Exact Constant	Cross-Stack Semantics & Canonical SSOT Anchor
$\mathcal{S}_{\text{Trinity}}$	$(\mathcal{W}_{\text{os}}, \mathcal{K}_{\text{wallet}}, \mathcal{L}_{\text{chain}})$	Complete MYRILUM Sovereign Trinity tuple: Enterprise AI WorkOS $\mathcal{W}_{\text{os}}$, Sovereign Wallet $\mathcal{K}_{\text{wallet}}$, and L1 State Machine $\mathcal{L}_{\text{chain}}$.
$\tau \in \mathcal{T}_{\text{tenant}}$	$\mathcal{T}_{\text{tenant}} \subset \mathbb{B}^{16}$	Strongly isolated enterprise `TenantScope` governing organizational memory, quota meters, and append-only audit streams.
$\mathcal{D}_{\text{DNA}}(\tau)$	$(\mathcal{D}_{\text{vis}}, \mathcal{D}_{\text{style}}, \mathcal{D}_{\text{audio}}, \mathcal{R}_{\text{learned}})$	Tenant τ Context DNA four-tuple: visual brand tokens, writing tone rules, audio loudness profile, and weighted learned preferences.
$\mathcal{A}_{\text{art}}, h_{\text{art}}$	$h_{\text{art}} = \text{SHA256}(\text{Canon}_{\text{JCS}}(\mathcal{A}_{\text{art}})) \in \mathbb{B}^{32}$	Enterprise deliverable spanning `6` modalities and `7` file formats with RFC 8785 JCS canonical `SHA-256` digest and citation tree.

Symbol / Operator	Algebraic Domain & Exact Constant	Cross-Stack Semantics & Canonical SSOT Anchor
$\mathcal{E}_{\text{audit}}^{(n)}$	$(\tau, n, t_n, a_n, o_n, h_{\text{payload}}, \text{corr}_n)$	Single-tenant monotonically sequenced append-only audit event stream failing closed on scope mismatch or sequence collision.
$\mathcal{I}_{\text{AST}}$	$\mathcal{L}_{\text{NL}} \to \mathcal{I}_{\text{AST}}$	Structured intent Abstract Syntax Tree emitted by untrusted neural proposers with zero private-key or raw-digest access.
$\Pi_{7715}(\pi, c, t)$	$\mathcal{P}_{7715} \times \mathcal{C}_{\text{call}} \times \mathbb{U}_{64} \to \{0,1\}$	`ERC-7715` deterministic session-permission verifier enforcing target contract allowlists, periodic atomic caps, and $\Delta t_{\text{exp}} \leq 30$ days.
$\Gamma_{\text{fw}}(\text{req}, \mathcal{H}_{\text{addr}})$	$\mathcal{Q}_{\text{sign}} \to \{\texttt{SAFE}, \texttt{WARN}, \texttt{BLOCK}\}$	`OBL-052` pre-sign firewall blocking raw `eth_sign`, auditing `Permit2` / `SetCode`, and intercepting prefix/suffix address poisoning.
$\text{GF}(2^8)$	$\mathbb{F}_2[\zeta]/(\zeta^8 + \zeta^4 + \zeta^3 + \zeta + 1)$	Finite Galois field modulo Rijndael polynomial `0x11b` powering `OBL-057` Shamir k-of-n ($2 \leq k \leq n \leq 16$) secret sharing.
Δ_{rec}	$\Delta_{\text{rec}} \geq 48 \text{ hours} = 172,800 \text{ s}$	Mandatory `OBL-058` on-chain guardian recovery timelock floor during which the active owner retains instant unilateral veto power.
$\sigma \in \mathbf{\Sigma}$	$(\sigma_{\text{acc}}, \sigma_{\text{tip20}}, \sigma_{\text{tip403}}, \sigma_{\text{nonce2d}}, \sigma_{\text{dex}}, \sigma_{\text{sys}})$	Six-dimensional world state of `Linghe Chain` (`ChainID = 88888` / `0x15b38`), anchored to Genesis SHA-256 `01a390d7...e2f1b`.
$(N_{\text{val}}, f, q, \Delta_{\text{slot}})$	$N_{\text{val}} = 4,\ f = 1,\ q = 3,\ \Delta_{\text{slot}} = 250 \text{ ms}$	`Commonware Simplex BFT` controlled benchmark committee size, Byzantine fault bound, quorum threshold, and single-slot finality period.
(k, ν)	$\mathbb{U}_{192} \times \mathbb{U}_{64}$ (active pool $\mathcal{K}_{32} \subset \mathbb{U}_{192}$)	Type-`0x76` 2D parallel nonce manifold coordinates maintained by kernel precompile `0x4e4f4e434500000000000000000000000000000000000000`.
$\Phi_{403}(\psi, a)$	$\mathbb{U}_{64} \times \mathcal{A} \to \{0,1\}$	Kernel-enshrined `TIP-403` sub-microsecond sanctions and policy predicate (`0x403c0000000000000000000000000000000000000000`).
(R_t, L_t, ρ_t)	$R_t, L_t \in \mathbb{N}_0,\ \rho_t = R_t / L_t \geq 1.0000\ (L_t > 0)$	Synthetic solvency benchmark HQLA vector, benchmark liability, and coverage invariant ($\rho_t \triangleq 1.0000$ if $L_t = 0$; `0x8800000000000000000000000000000000000001`).
π_{HKMA}	$\pi_{\text{HKMA}} \in [77500, 78500] \subset \mathbb{U}_{32}$	Enshrined HKMA Linked Exchange Rate corridor parameter (10^{-4} HKD/USD scale) in `0x8900000000000000000000000000000000000001`.
$(\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e)$	$\text{BN254 Optimal Ate},\ n_{\text{P256}}\ \text{Low-}s$	Dual elliptic-curve cryptographic roots: ZK light-client pairing (`0x0000000000000000000000000000000000000008`) and silicon TEE verify (`0x0000000000000000000000000000000000000100`).

Symbol / Operator	Algebraic Domain & Exact Constant	Cross-Stack Semantics & Canonical SSOT Anchor
$\alpha \in [0,1]$	$\alpha = G_{\text{serial}}/G_{\text{slot}} \in [0,1]\ (G_{\text{slot}} > 0)$	Per-slot serialized conflict gas fraction over total slot gas governing degradation from K-lane concurrency to topological serial order.

SECTION 01

First Principles and Motivation for the Sovereign Trinity Stack

1.1 Three Structural Fault Lines in Enterprise Agentic Computing and Settlement

Global digital infrastructure is undergoing a structural transition from human-driven interactive software toward autonomous multi-agent execution workflows. Yet enterprises, financial institutions, and regulated organizations attempting to deploy autonomous agents across mission-critical operations encounter three compounded structural fault lines:

Fault Line I: Conditional Hallucination Compounding and Organizational Amnesia in Unbounded Neural Chains. Autoregressive foundation models sample token sequences probabilistically according to $P_\theta(x_t \mid x_{<t})$. Consider an enterprise workflow comprising M sequential reasoning, retrieval, and tool-invocation steps. Let event V_i denote that step i satisfies factual accuracy, brand policy, and schema validity, with conditional failure probability $\epsilon_i = \Pr[\neg V_i \mid V_1, \ldots, V_{i-1}]$. Even if each step satisfies conditional single-step reliability $1 - \epsilon_i \le p = 0.96$ given valid predecessors, by the probability chain rule an unverified neural pipeline without deterministic intermediate state-machine gates suffers exponential reliability decay across depth M:

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

Furthermore, generic conversational interfaces lack tenant-isolated canonical memory structures and cryptographically verifiable citation graphs, causing each session to regress toward ungrounded improvisation unacceptable in legal, financial, or boardroom deliverables.

Fault Line II: Catastrophic Coupling of Indirect Prompt Injection and Unbounded Key Custody. Early agentic payment prototypes routinely inject raw private keys or unrestricted API bearer secrets directly into the agent runtime environment. Because transformer attention mechanisms cannot algebraically segregate system control instructions from untrusted external data ingested via web pages, emails, or RAG documents (Indirect Prompt Injection), a single adversarial payload can hijack the model into signing arbitrary asset transfers or unlimited `Permit` approvals. Conversely, retreating to centralized third-party custodial wallets reintroduces counterparty insolvency exposure, commingled balance-sheet risk, and heavy financial-licensing overhead.

Fault Line III: Simultaneous Breakdown of Legacy Deferred-Net Rails and Sequential Blockchains. Autonomous agents procuring verifiable inference or market data at sub-cent granularity ($0.001–$0.10 per `HTTP 402` call) face negative net utility over legacy card and correspondent banking rails whose fixed clearing floors $c_{\text{fixed}} \in [\$0.15, \$0.30]$ exceed transaction principal. Meanwhile, first-generation blockchains impose scalar 1D account nonces whose $M/G/1$ Pollaczek-Khinchine queueing latency diverges hyperbolically as multi-threaded treasury utilization approaches unity ($\varrho_1 \to 1^-$), force corporate balance sheets to hold volatile native gas coins, and rely on contract-level blacklists easily circumvented through wrapper indirection.

Let $\mathfrak{S}$ denote the space of candidate enterprise agentic architectures. We define the cross-stack completeness indicator functional $\mathcal{J}_{\text{Trinity}} : \mathfrak{S} \to \{0,1\}$ as the conjunction of three falsifiable predicates—deterministic cognitive orchestration & audit isolation ($\mathcal{C}_{\text{cog}}$, Invariant 2.1), zero-trust bounded client loss ($\mathcal{C}_{\text{term}}$, Theorem 3.1), and kernel-regulated sub-second finality ($\mathcal{C}_{\text{settle}}$, Theorem 5.1):

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

Omitting any single pillar collapses $\mathcal{J}_{\text{Trinity}}(\mathcal{S})$ to zero: cognitive software without a sovereign policy firewall cannot safely touch value, whereas a high-speed blockchain without enterprise cognitive workflows and zero-dependency client security remains disconnected from real institutional productivity.

1.2 Orthogonal Decomposition of the MYRILUM Sovereign Trinity Closed Loop

Guided by the principle of least action and strict separation of concerns, the MYRILUM Group establishes a unified architecture in which **probabilistic generation is decoupled from deterministic verification, neural cognition is air-gapped from cryptographic keys, and regulatory invariants are enshrined at the state-transition kernel** (Figure 1).

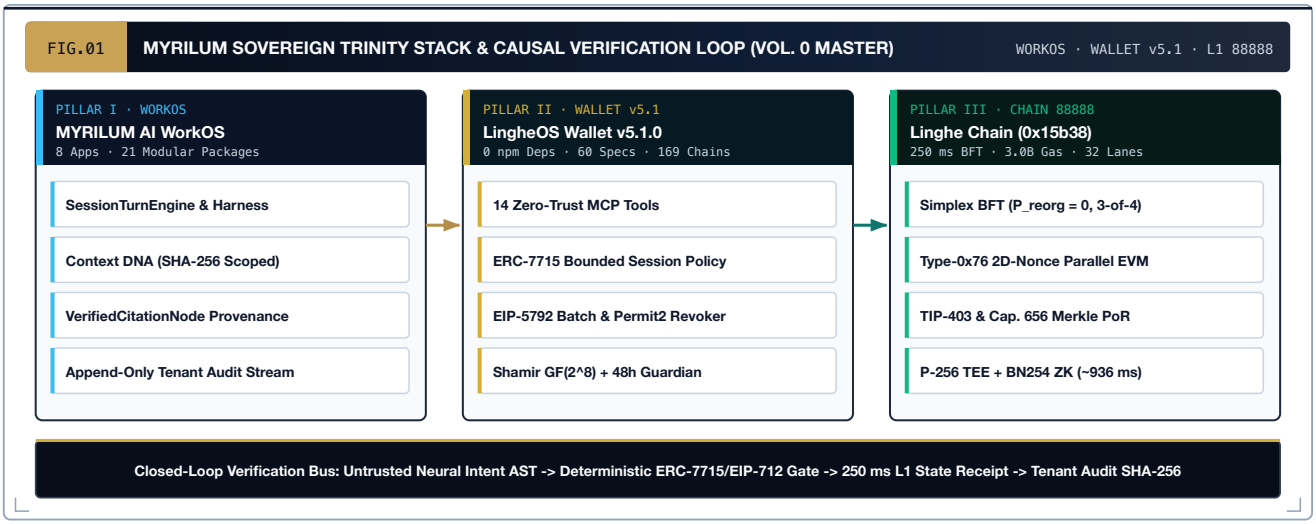


FIGURE 01 — MYRILUM Sovereign Trinity Stack (AI WorkOS × Sovereign Wallet v5.1.0 × Linghe Chain 88888) & Causal Verification Loop

Note: All three subsystems couple strictly across zero-key-visibility boundaries; neural models never access private keys or bypass deterministic policy verification.

DEFINITION 1.1 — The MYRILUM Sovereign Trinity Stack

The group architecture is formally defined as the orthogonally coupled triple $\mathcal{S}_{\text{Trinity}} = (\mathcal{W}_{\text{os}}, \mathcal{K}_{\text{wallet}}, \mathcal{L}_{\text{chain}})$:

1. **Enterprise Cognitive & Governance Plane** $\mathcal{W}_{\text{os}}$ **(`MYRILUM AI WorkOS`)**: Orchestrates multi-agent task execution, tenant-scoped `Context DNA` injection, citation-verified multi-modal deliverable synthesis, and append-only tenant audit logging, operating with strictly zero visibility into cryptographic private keys.
2. **Zero-Trust Sovereign Client Plane** $\mathcal{K}_{\text{wallet}}$ **(`MYRILUM LingheOS Wallet v5.1.0`)**: Governs local self-custodial key lifecycles within a zero-dependency sandbox, ingesting structured intent ASTs $\mathcal{I}_{\text{AST}}$ from $\mathcal{W}_{\text{os}}$ across `14` Zero-Trust MCP tools, enforcing non-LLM `ERC-7715` / `EIP-712` policy firewalls and hardware step-up authentication before emitting signed envelopes.
3. **Sub-Second Regulated Settlement Plane** $\mathcal{L}_{\text{chain}}$ **(`MYRILUM Linghe Chain`, `ChainID = 88888`)**: Executes `250 ms` single-slot BFT consensus, 32-lane `0x76` parallel state transitions, kernel `TIP-403` compliance screening, and dual-curve (`P-256` TEE + `BN254` ZK) verification, returning non-repudiable Merkle finality receipts to $\mathcal{W}_{\text{os}}$.

INVARIANT 1.1 — Unidirectional Trust Isolation and Zero Private-Key Extrusion

Across every admissible execution trace of $\mathcal{S}_{\text{Trinity}}$, root mnemonics and signing scalars remain strictly confined within $\mathcal{K}_{\text{wallet}}$ protected local memory or silicon hardware enclaves; mutual information between private key material and the observable state of $\mathcal{W}_{\text{os}}$ or $\mathcal{L}_{\text{chain}}$ is identically zero, and no cognitive output of $\mathcal{W}_{\text{os}}$ can mutate on-chain state without satisfying the deterministic non-LLM verification predicates of $\mathcal{K}_{\text{wallet}}$.

1.3 Claim Maturity Taxonomy, Runtime State Separation, and Three Prohibited Equivalences

To uphold rigorous scientific falsifiability and eliminate the industry malpractice of conflating architectural roadmaps or laboratory benchmarks with live public retail deployments, every substantive claim in this specification is classified along two orthogonal axes: **Technical Maturity** and **Operational Runtime Scope** (Table 1.1), backed by a machine-readable repository truth ledger.

Maturity Classification	Formal Verification Criterion & Evidence Standard	Operational Runtime Scope	Applicable Modules in This Volume
`VERIFIED_IN_CODE`	Deterministically implemented in repository source code and verified via automated test suites with zero mock stubs.	`INTERNAL_VERIFIED` / `ISOLATED_PROD`	`WorkOS` 21 core packages, `LingheOS Wallet v5.1.0` all `60` specs, Mainland isolation gates.
`BENCHMARKED_TESTBED`	Empirically measured on controlled 4-validator `ChainID 88888` benchmark topology with reproducible latency and gas telemetry.	`SANDBOX_BENCHMARK` (Non-retail mainnet)	`250 ms` finality, `~1,004 ms` 20-tx parallel burst, `815,381 gas` ZK verify, `~936 ms` omnichain fill.
`ARCHITECTURAL_SPEC`	Mathematically complete state-machine, client interface, or accounting specification ready for licensed counterparty integration.	`COMMERCIAL_OR_LICENSED_INTERFACE`	Open client adapters for licensed fiat institutions; three corporate `IFRS 15` revenue engines.
`ROADMAP_GATED`	Contingent upon external regulatory licensing, independent third-party security audit, or explicit Human Gate sign-off.	`GATED_PRE_RELEASE` (Inactive)	External validator set expansion across continents; licensed commercial stablecoin issuer integration.

Furthermore, all MYRILUM engineering and governance specifications enforce **Three Prohibited Equivalences**:

1. **On-Chain Recording** $\neq$ **Off-Chain Factual Truth**: A blockchain state root or Merkle commitment cryptographically proves existence, timestamped ordering, and post-submission immutability of a signed statement, but never substitutes for physical custodian audits, hardware enclave root certificates, or legal verification of underlying off-chain facts.
2. **Speculative Token** $\neq$ **Cryptographic Verification Infrastructure**: Deterministic consensus, zero-knowledge proofs, and self-custodial hardware signatures derive institutional utility from eliminating reconciliation and tampering risk—never from speculative token issuance.
3. **On-Chain Governance** $\neq$ **Unaccountable Decentralization**: Every automated agent action and protocol parameter transition must map deterministically to an identifiable human or corporate principal, mandatory timelock disclosure, and lawful dispute-resolution venue.

SECTION 02

Pillar I: MYRILUM AI WorkOS Deterministic Multi-Agent Operating System

2.1 Deterministic Execution Harness, Causal Privacy Ledger, and Multi-Surface Topology

`MYRILUM AI WorkOS` serves as the enterprise cognitive operating system of the group. Architecturally organized as a strongly typed modular monorepo, the platform powers `8` user-facing and worker applications (`platform-web`, `platform-worker`, `desktop-client`, `mobile-client`, `campaign-concept-studio`, `member-operations`, `docs-site`, and `marketing-site`) built atop `21` domain-isolated workspace packages.

To eliminate stochastic drift and unauthorized side effects in multi-agent workflows, `@myrilum/linghe-harness-core` wraps foundation models inside a **Deterministic Execution Harness** governed by five specialized kernel subsystems:

- **Session Turn State Machine (`SessionTurnEngine`)**: Partitions multi-agent collaboration into discrete, strongly typed execution turns subject to pre-turn schema validation, context-window token budgets, and deterministic timeout bounds.
- **Causal Privacy Ledger (`PrivacyCausalLedger`)**: Attaches immutable `TenantScope` and sensitivity lineage tags to every ingested document, retrieved chunk, and tool output, structurally preventing cross-tenant context contamination.
- **Capability & Provider Router (`CapabilityRouterRegistry`)**: Coupled with `@myrilum/provider-adapters`, abstracts heterogeneous commercial and self-hosted open-weights foundation models behind deterministic SLA, cost, and data-residency routing policies.
- **Canonical Artifact Kernel (`ArtifactDnaKernel`)**: Compiles validated intermediate representations into publication-grade enterprise deliverables while rejecting malformed or unverified outputs fail-closed.
- **Atomic Quota & Entitlement Meter (`QuotaEntitlementMeter`)**: Integrated with `@myrilum/entitlement` and `@myrilum/platform-billing`, enforces pre-execution quota reservation, exact post-turn metering, and immediate fail-closed suspension upon budget exhaustion.

Formally, let the deterministic WorkOS state of tenant τ prior to turn j be $S_j = (\tau, C_j, Q_j, L_j)$, where C_j denotes the causally tagged context DAG, $Q_j \in \mathbb{N}_0$ denotes remaining compute entitlement, and L_j denotes the append-only audit log. Given user or workflow input u_j and candidate neural proposal $\hat{a}_j = f_{\text{LLM}}(C_j, u_j)$, the state transition operator δ_{turn} is defined strictly as:

$$S_{j+1} = \delta_{\text{turn}}(S_j, u_j) = \begin{cases} (\tau,\ C_j \cup \{\text{Sanitize}(\hat{a}_j)\},\ Q_j - \text{Cost}(\hat{a}_j),\ L_j \Vert\ e_{j+1}), & \text{if SchemaOk}(\hat{a}_j) \wedge \text{PolicyOk}(\tau, \hat{a}_j) \wedge Q_j \geq \text{Cost}(\hat{a}_j) \\ (\tau,\ C_j,\ Q_j,\ L_j \Vert\ e_{j+1}^{(\text{DENIED})}), & \text{otherwise (fail-closed rejection with deterministic reason code)} \end{cases}$$

2.2 Organizational Context DNA and Anti-Hallucination Provenance Deliverables

Enterprise adoption of generative AI requires institutional continuity and audit-grade factual provenance. `MYRILUM AI WorkOS` formalizes organizational identity and deliverable integrity through `@myrilum/linghe-context-dna` and `@myrilum/linghe-artifact-schema`:

1. **Multi-Modal Organizational Context DNA (`Context DNA`)**: Institutional standards are encoded into a strongly typed four-component tuple $\mathcal{D}_{\text{DNA}}(\tau)$:
   - **Brand Visual DNA (`BrandVisualDna`)**: Locks primary, secondary, accent, and neutral hex palettes, heading/body typography, and `SHA-256`-verified corporate emblem digests;
   - **Writing Style DNA (`WritingStyleDna`)**: Enforces explicit rhetorical modes (`EXECUTIVE_DECISION_FIRST`, `TECHNICAL_DEEP_DIVE`, `BOARD_BRIEFING`), paragraph character ceilings, per-slide bullet caps, forbidden phrase blacklists, and canonical terminology maps;

- **Voiceover Audio DNA (`VoiceoverAudioDna`)**: Standardizes voice profile identifiers, reference audio `SHA-256` digests, speaking-rate multipliers, target Loudness Units relative to Full Scale (`LUFS`), and background-music ducking thresholds;
- **Learned Preference Rules (`LearnedPreferenceRule`)**: Extracts structured terminology-replacement, conciseness, conclusion-first, and forbidden-phrase rules with explicit `confidenceScore` weights from human editorial feedback.

2. **Six-Modality, Seven-Format Deliverables & Verified Citation Nodes**: `@myrilum/linghe-artifact-schema` standardizes six enterprise deliverable modalities (`REPORT`, `SLIDE_DECK`, `VIDEO`, `SPREADSHEET`, `DOCUMENT`, `WORKFLOW_SOP`) across seven canonical output formats (`docx`, `pptx`, `xlsx`, `pdf`, `mp4`, `md`, `json`). Every external factual assertion must be anchored to a `VerifiedCitationNode` binding the source URL, exact page or section anchor, verbatim excerpt, `contentSha256` digest, and `httpVerified` status flag.

For any compiled enterprise deliverable $\mathcal{A}_{\text{art}} = (\tau, \text{modality}, \text{files}[], \text{citations}[], \text{tables}[])$, applying length-delimited RFC 8785 JSON Canonicalization ($\text{Canon}_{\text{JCS}}$) yields its deterministic cross-stack integrity digest:

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

Any silent post-generation mutation of an exported binary file, cited source excerpt, or verified numeric table induces an avalanche mismatch against h_{art}, guaranteeing `100%` tamper detection during internal compliance review or on-chain anchor verification.

2.3 Tenant-Isolated Append-Only Audit Stream and Ten-Dimensional Human Gate Accountability Matrix

Institutional governance demands non-destructive auditability and unambiguous human sovereignty. Within `@myrilum/platform-audit` and `@myrilum/identity-access`, every `AuditEvent` records `TenantScope`, strictly monotonic `sequence`, actor classification (`USER` or `SYSTEM`), versioned object reference, execution outcome (`SUCCEEDED` / `DENIED` / `FAILED`), standardized `reasonCode`, `correlationId`, and `payloadDigest`.

> **INVARIANT 2.1 — Single-Tenant Audit Isolation and Non-Destructive Correction Lineage**
>
> Let $\mathcal{E}_{\text{audit}} = (e_1, e_2, \ldots, e_m)$ denote the active audit log of tenant τ. For any candidate event e^*, the `appendAuditEvent` transition enforces prior to commit: (i) strict tenant homogeneity $\forall e_i \in \mathcal{E}_{\text{audit}},\ \text{tenant}(e_i) = \text{tenant}(e^*)$, throwing `AUDIT_TENANT_MISMATCH` on violation; (ii) identifier and sequence uniqueness $\forall e_i,\ \text{id}(e_i) \neq \text{id}(e^*) \wedge \text{seq}(e_i) \neq \text{seq}(e^*)$, throwing `DUPLICATE_AUDIT_EVENT` on collision; and (iii) strict append-only immutability—prior events are never overwritten or deleted, and any subsequent amendment must append a new sequenced event referencing `correctionOfAuditEventId`.

Enforcing the foundational legal axiom that **an AI agent identity is never a legal person and every automated operation must map to an accountable human or corporate principal**, Table 2.1 specifies the ten-dimensional Human Gate matrix enforced across all MYRILUM products.

Operational Action Category	Autonomous AI Execution Scope	Mandatory Human Gate & Fail-Closed Safeguard
1. Research retrieval, task decomposition & matching	Permitted within authorized tenant corpora and public sources	Human operator retains instant override and full `VerifiedCitationNode` inspection
2. Commercial quotations & legal contract drafting	Restricted to watermarked structured draft generation	Strictly prohibited from binding external transmission without authorized human sign-off
3. Low-risk reversible tool execution & formatting	Permitted within `QuotaEntitlementMeter` bounds	Suspends fail-closed immediately upon hitting per-turn compute or rate ceilings

Operational Action Category	Autonomous AI Execution Scope	Mandatory Human Gate & Fail-Closed Safeguard
4. Execution of legally binding corporate agreements	**Strictly prohibited for autonomous agents**	Requires explicit hardware-authenticated signature by an authorized corporate officer
5. Irreversible fund transfers & high-value settlement	Prohibited beyond micro-bounded `ERC-7715` session caps	Any transfer exceeding allowlisted micro-caps mandates human hardware or multisig approval
6. Issuance, revocation, or amendment of attestations	Restricted to preparing candidate payloads and digests	Requires human compliance review, statutory reason code, and append-only correction lineage
7. Penalties, collateral forfeiture, or slashing	**Unilateral algorithmic adjudication prohibited**	Mandates evidentiary threshold, human compliance officer review, and appellate recourse
8. Final commercial dispute adjudication	Restricted to timeline and cryptographic hash reconciliation	Escalated to independent human arbitration or court of competent jurisdiction
9. Cross-organization or cross-border sensitive data sharing	Blocked by default (`DEFAULT_DENY`)	Requires explicit purpose-bound, time-limited secondary authorization by data owner
10. Core protocol upgrades & risk-policy mutations	**Instant unilateral or agentic activation prohibited**	Enforces `3-of-4` multi-jurisdictional multisig plus mandatory timelock (`eta`) disclosure

SECTION 03

Pillar II: MYRILUM LingheOS Wallet v5.1.0 Zero-Dependency Sovereign Client

3.1 Zero-Dependency Supply-Chain Immunity and Four-Runtime Isomorphic Sandbox

Historically, the most devastating losses across self-custodial digital-asset clients have stemmed not from mathematical breaks in elliptic-curve discrete logarithms, but from transitive software supply-chain poisoning inside bloated third-party package trees. Suppose a client application imports D external runtime packages (typically $D \in [400, 1200]$ in conventional web wallets) with arithmetic-mean per-release compromise probability $\bar{p}_{\text{dep}} = \frac{1}{D}\sum_{i=1}^{D} p_{\text{dep},i} = 10^{-4}$; by the elementary bound $1 - x \le e^{-x}$ $(x \in [0,1])$, aggregate supply-chain exposure satisfies the strict lower bound:

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

To reduce third-party runtime supply-chain risk mathematically to $P_{\text{compromise}}(0) \equiv 0$, `MYRILUM LingheOS Wallet v5.1.0` is constructed under strict clean-room engineering rules with `0` **external runtime or development** `npm` **dependencies**. Every cryptographic encoder, recursive ABI decoder, typed transaction serializer, bespoke SVG financial chart renderer, and zero-trust MCP dispatcher is implemented from first principles atop standard language primitives and native operating-system cryptographic interfaces, passing automated verification across all `60` functional and security obligations (`OBL-001` through `OBL-060`).

From a single canonical codebase, `LingheOS Wallet v5.1.0` compiles into **four isomorphic sandboxed client runtimes**: (i) zero-dependency standards-compliant Web browser single-page application (SPA); (ii) Chromium `Manifest V3` isolated-world browser extension (enforcing `all_frames: false` , strict origin-bound `postMessage` , and honest `isMetaMask = false` multi-provider discovery via `EIP-6963`); (iii) macOS native `WKWebView` desktop container; and (iv) iOS native `WKWebView` mobile container. The client natively supports `169` heterogeneous networks (spanning `Linghe Chain 88888` , EVM L1/L2 ecosystems, and `SLIP-0010 Ed25519` chains) with byte-identical deterministic behavior.

3.2 Account Abstraction Matrix (`EIP-7702` / `P-256` / `EIP-5792` / `ERC-7715`) and Pre-Sign Phishing Firewall

Designed for both institutional treasury governance and bounded autonomous-agent execution, `LingheOS Wallet v5.1.0` implements the complete modern smart-account standard stack behind a deterministic pre-sign security firewall (Figure 2):

- **Smart-Account Delegation, Passkeys & Benchmark-Primitive Paymaster Sponsorship (`OBL-002` , `OBL-049` , `OBL-055`)**: Supports `EIP-7702` type- `0x04` EOA code delegation (`0x05` authorization tuples) paired with `Osaka` `EIP-7951` `WebAuthn Passkey` signers (`SubjectPublicKeyInfo` / `SPKI` `P-256` public-key extraction and canonical low-s normalization), `EIP-5792` atomic call bundles (`wallet_getCapabilities` , `wallet_sendCalls` , `wallet_getCallsStatus` compiling $1 \dots 32$ calls into `ERC-7579` `0x01` batches), and `ERC-4337 v0.7` `PackedUserOperation` paymaster sponsorship (quoting non-circulating `LUSD` or `LHKD` benchmark-state units in sandbox evaluation with zero native gas-coin balance required, and compatible with independently authorized third-party settlement tokens in permitted jurisdictions).
- **Fine-Grained Bounded Session Permissions (`OBL-050` — `ERC-7715`)**: `grantErc7715Permissions` issues scoped `permissionsContext` tokens constrained along three hard axes: (i) explicit `contract-call-allowlist` target and selector bounds; (ii) cumulative periodic native or `ERC-20` atomic allowance caps; and (iii) mandatory maximum session lifetime $0 < t_{\text{exp}} - t_{\text{now}} \leq 30 \times 86,400 \text{ s}$ (`30` days), with instant single-call revocation.
- **Approval Health Auditor & Atomic `Permit2` Lockdown (`OBL-051`)**: Continuously audits `ERC-20` , `ERC-721` , `ERC-1155` , and canonical `Permit2` (`0x000000000022d473030f116ddee9f6b43ac78ba3`) allowances—flagging unlimited approvals ($\geq 2^{255}$), unverified spenders, collection-wide NFT operators, and dormant approvals exceeding `90` days—computing a `0-100` health score and compiling atomic `approve(spender, 0)` plus `Permit2.lockdown` revocation batches.
- **Pre-Sign Drainer & Address-Poisoning Firewall (`OBL-052` , `OBL-053`)**: Prior to any signature invocation, `simulateAndAuditSignRequest` executes four deterministic checks: (i) permanently hard-blocks legacy raw-digest `eth_sign` (risk score `100` , `BLOCK: RAW_ETH_SIGN_FORBIDDEN`); (ii) inspects `EIP-712` payloads to return `BLOCK` on unlimited + unverified `Permit` / `PermitSingle` / `PermitBatch` drainers and untrusted `EIP-7702 SetCode` delegations, while raising `WARN` for human review on scoped off-chain permits or `domain.chainId` anomalies; (iii) **Lookalike Address-Poisoning Interception**—if a recipient is absent from known recent counterparties yet matches both the first ≥ 3 hex characters (after `0x`) and last ≥ 4 hex characters of a historical counterparty while differing in interior bytes, the firewall returns `BLOCK: ADDRESS_POISONING_LOOKALIKE` (risk score `94`); and (iv) validates `EIP-4361` Sign-In with Ethereum (`SIWE`) origin-host binding with `ERC-6492` counterfactual signature wrapping.

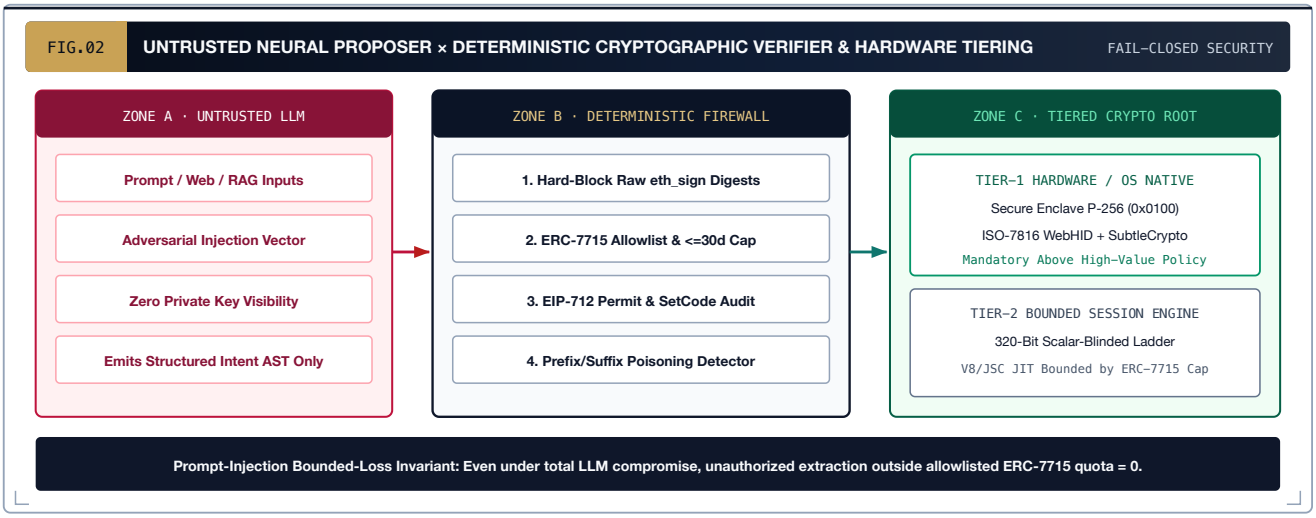


FIGURE 02 — Untrusted Neural Proposer × Deterministic Policy Firewall & Tiered Hardware Side-Channel Boundary

Note: Explicitly separates OS/silicon native cryptography (Tier-1) from V8/JSC JIT-hosted 320-bit scalar-blinded Montgomery session keys (Tier-2).

THEOREM 3.1 — Prompt-Injection Bounded-Loss Invariant

Suppose the cognitive plane $\mathcal{W}_{\text{os}}$ suffers arbitrary adversarial compromise via indirect prompt injection at time t, emitting an arbitrary sequence of malicious calls $\{m_1, \dots, m_r\}$ against the `14` Zero-Trust MCP endpoints of $\mathcal{K}_{\text{wallet}}$. Let $\pi = (\mathcal{A}_{\text{allow}}, \mathcal{I}_{\text{allow}}, Q_{\text{cap}}, t_{\text{exp}})$ be a well-formed least-privilege session policy provisioned exclusively via human step-up authorization such that: (i) MCP handlers prepare unsigned policy drafts only and cannot self-activate or escalate live signing authority; (ii) $\mathcal{I}_{\text{allow}} \neq \varnothing$ permits only recipient-bound selectors with empty-calldata native transfers disabled and zero standing unlimited router approvals (paired with `OBL-058` rolling 24-hour on-chain spend cap Q_{daily} across at most $K_{\text{win}} = \lceil (t_{\text{exp}} - t_0)/86400 \rceil \leq 30$ windows); and (iii) autonomous signing halts fail-closed whenever `OBL-052` evaluates $\Gamma_{\text{fw}}(m_j) \neq \text{SAFE}$ (blocking both `BLOCK` and `WARN` verdicts), with sponsored execution fees bounded by F_{gas}. Under standard `EUF-CMA` security (parameter λ) of the underlying signature curve, mnemonic exfiltration probability is identically zero and total session extraction satisfies:

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

PROOF

By construction of the Zero-Trust MCP dispatcher (`OBL-008` , `OBL-060`), all `14` tool handlers execute in an unprivileged routing scope devoid of mnemonic or raw-scalar export bindings (`wallet_grant_erc7715_permission` constructs unactivated policy descriptors only). For every candidate call m_j, `validateExecutionAgainstErc7715` evaluates pure deterministic set-membership and integer predicates: if $\text{to}(m_j) \notin \mathcal{A}_{\text{allow}}$, empty calldata is supplied, $\text{sel}(m_j) \notin \mathcal{I}_{\text{allow}}$, $t \geq t_{\text{exp}}$, or $u_{\text{used}} + \text{val}(m_j) > Q_{\text{cap}}$, execution aborts fail-closed (`allowed = false`). Attempts to bypass transfer caps via raw digests or off-chain `Permit` payloads yield `BLOCK` or `WARN` under `OBL-052` ($\Gamma_{\text{fw}}(m_j) \neq \text{SAFE}$), halting autonomous signing, while `OBL-058` enforces Q_{daily} on-chain. Up to negligible `EUF-CMA` forgery probability $\text{negl}(\lambda)$, no out-of-policy transition can execute.

Q.E.D. ■

3.3 Shamir $\text{GF}(2^8)$ Threshold Secret Sharing and 48-Hour Timelocked Guardian Recovery

To resolve the classic self-custody dilemma between catastrophic single-seed loss and single-backup theft, `LinghеOS Wallet v5.1.0` combines information-theoretic offline secret splitting with timelocked on-chain modular recovery:

1. **Shamir k-of-n Threshold Backup over $\mathrm{GF}(2^8)$ (`OBL-057`)**: Operating over the Rijndael finite field $\mathrm{GF}(2^8) = \mathbb{F}_2[\zeta]/(\zeta^8 + \zeta^4 + \zeta^3 + \zeta + 1)$ (`0x11b`), each secret byte s_l of secret $S \in \mathbb{B}^L$ $(1 \le L \le 256)$ is embedded as the constant term of a random polynomial $f_l(x) = s_l \oplus \bigoplus_{d=1}^{k-1} (a_{l,d} \otimes x^d)$ of **degree at most** $k-1$ with independently sampled coefficients $(a_{l,1}, \ldots, a_{l,k-1}) \xleftarrow{\$} \mathrm{GF}(2^8)^{k-1}$ (where $\otimes$ denotes field multiplication), evaluated at distinct non-zero coordinates $x_i = i \in \{1, \ldots, n\}$ to emit n share strings carrying `32` -bit `SHA-256` transport integrity checksums ($2 \le k \le n \le 16$). After screening accidental corruption via checksums, any k distinct shares reconstruct s_l at $x = 0$ via Lagrange interpolation (followed by public-key commitment verification against active share tampering):

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

Any coalition holding fewer than k shares gains strictly zero Shannon information regarding S.

2. **On-Chain `ERC-7579` + `ERC-7201` 48-Hour Timelocked Guardian Recovery & Daily Spend Caps (`OBL-058`)**: Utilizing collision-free `ERC-7201` namespaced storage with zero developer or administrative backdoors (`owner` is exclusively the smart account itself), k-of-n guardian recovery proposals enforce a mandatory minimum timelock $\Delta_{\text{rec}} \ge 48$ hours. Throughout this `48` -hour window, an active account owner retains unilateral fail-closed veto power via `cancelRecovery()` , neutralizing guardian collusion, alongside per-token rolling 24-hour spending caps (`DailySpendCapExceeded`) and `OBL-056` `FIFO` / `HIFO` `SHA-256` -sealed audit tax reporting.

Table 3.1 summarizes the complete `60` -obligation (`OBL-001` through `OBL-060`) specification matrix and all `14` Zero-Trust MCP tools.

Obligation Range	Core Cryptographic & Client Security Subsystem	Public Standards / Enforced Invariants	Zero-Trust MCP Tool Bindings (14 Total)
`OBL-001` – `003`	Multi-chain key core, Passkey & cold hardware signer	`BIP-39/32` , `SLIP-0010` , `EIP-7702` , `P-256` , `ISO-7816` `WebHID`	`wallet_get_status` , `wallet_get_portfolio`
`OBL-004` – `008`	Recursive ABI decoding, intent AST & omnichain `x402`	`EIP-137` , `ERC-4626` , `ERC-7579` , `x402` , `TIP-403` , `BN254`	`wallet_decode_calldata` , `wallet_compile_intent` , `wallet_verify_session_policy` , `wallet_quote_dex` , `wallet_x402_mcp_challenge` , `wallet_check_tip403_compliance` , `wallet_omnichain_x402_invoke` , `wallet_zk_light_client_bridge`
`OBL-009` – `048`	`169` -chain isomorphic registry, vault & client foundation	`AES-256-GCM` , `PBKDF2-SHA256` (600k iter), `EIP-6963` , tri-mode geofence	Read-only exposure via `wallet_get_status` , `wallet_get_portfolio` & `wallet_quote_dex`
`OBL-049` – `050`	Atomic call batching & scoped periodic session grants	`EIP-5792` (1–32 atomic calls), `ERC-7715` ($\le$ 30-day cap)	`wallet_build_eip5792_batch` , `wallet_grant_erc7715_permission`
`OBL-051` – `053`	Approval health revoker, pre-sign firewall & SIWE	`Permit2 lockdown` , `EIP-712` anti-poisoning, `EIP-4361` , `ERC-6492`	`wallet_audit_approvals_and_revoke` , `wallet_simulate_sign_firewall`
`OBL-054` – `060`	Gasless intents, paymaster, tax, recovery & local gateway	`ERC-7683` , `ERC-4337 v0.7` , `FIFO/HIFO SHA-256` , `Shamir GF(2^8)` , `48h` guardian	Isomorphically embedded in Security Center & `64 KB` bounded local Zero-Trust gateway

SECTION 04

Pillar III: MYRILUM Linghe Chain (`ChainID 88888`) Sub-Second Parallel Settlement State Machine

4.1 `Commonware Simplex BFT` Single-Slot Finality and Type-`0x76` 2D-Nonce Parallel EVM

Anchoring the settlement layer of the Trinity Stack, `MYRILUM Linghe Chain` (`ChainID = 88888` / `0x15b38`; immutable Genesis Block-0 `SHA-256`: `96208e9900b218935143be3024d2602566a86d61caa906d42399f35b83afd991`) is engineered for deterministic machine micropayments and regulated Real-Time Gross Settlement (`RTGS`).

Consensus is driven by `Commonware Simplex BFT` across a four-node benchmark committee (`HK-HKMA`, `SG-MAS`, `JP-FSA`, `CH-FINMA`; $N_{\text{val}} = 4, f = 1, q = 3$) registered in kernel precompile `0xccccccccc0000000000000000000000000000000` — **Non-Endorsement Disclaimer: these four identifiers are strictly synthetic regional latency and compliance simulation profile tags operated solely by `MYRILUM LIMITED` inside isolated benchmark testbed infrastructure; they denote zero affiliation, node operation, licensing, supervision, or endorsement by the Hong Kong Monetary Authority (HKMA), Monetary Authority of Singapore (MAS), Financial Services Agency of Japan (JFSA), or Swiss Financial Market Supervisory Authority (FINMA)**. Via single-hop all-to-all notarization broadcast and local-timeout dummy skip certificates, the protocol attains irreversible single-slot deterministic finality within $\Delta_{\text{slot}} = 250$ ms ($P_{\text{reorg}} \equiv 0$; Recovery Point Objective $\text{RPO} = 0$).

State execution runs on a customized modular Rust `Paradigm Reth` engine configured with a per-slot computational ceiling $G_{\max} = 3,000,000,000$ Gas ($\Theta_{\text{gas}} = 1.2 \times 10^{10}$ Gas/s). To eliminate 1D sequential-nonce head-of-line stalling across multi-threaded institutional treasuries, `Linghe Chain` enshrines **EIP-2718 type-`0x76` unsigned two-dimensional nonces** $(k, \nu) \in \mathbb{U}_{192} \times \mathbb{U}_{64}$ at `0x4e4f4e4345000000000000000000000000000000`: channel $k = 0$ preserves legacy sequential compatibility, while the default active account lane pool $\mathcal{K}_{32} = \{1, \ldots, 32\} \subset \mathbb{U}_{192}$ exposes $K = 32$ independent lock-free settlement lanes per account. By the `Pollaczek–Khinchine` queueing identity, partitioning an arrival stream λ across K orthogonal lanes reduces per-lane queueing utilization from $\varrho_1 = \lambda/\mu_1$ to $\varrho_K = \lambda/(K\mu_1)$, collapsing steady-state mean queueing wait super-linearly:

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

Paired with `TIP Fee Manager` (`0xfeec0000000000000000000000000000000000000`) and domain-separated `0x78` fee-payer sponsorship, autonomous agents settle gas directly in enshrined fiat-referenced benchmark primitives without holding volatile native tokens. On the controlled `ChainID 88888` benchmark testbed, `20/20` concurrent `0x76` micropayment transactions from a single treasury reach deterministic finality in `~1,004 ms` with zero nonce collisions and zero queue stalls.

4.2 Kernel-Enshrined RegTech (`TIP-403`), Linked-Rate Corridor, and Binary Merkle Solvency Proofs

Rather than relying on bypassable application-layer wrappers, `Linghe Chain` enshrines regulatory compliance invariants directly inside Genesis state space and Rust execution-kernel boundaries:

1. **Orthogonal Genesis Ledger Primitives, Zero Inflation & Zero-Yield Invariant**: Genesis Block-0 isolates the consensus staking accounting unit (`LHC`, `0x20c0000000000000000000000000000000000000`, carrying **zero inflationary staking rewards, zero retail delegation pooling, and zero corporate buyback-and-burn commitments**) from non-circulating 6-decimal deterministic benchmark reference states `LUSD` (`0x20c0000000000000000000000000000000000001`) and `LHKD` (`0x20c0000000000000000000000000000000000002`) carrying EIP-3541 `"0xef"` kernel dispatch sentinels and enforcing zero holder yield ($r_{\text{holder}}(t) \equiv 0$).
2. **Sub-Microsecond `TIP-403` Screening & Sliding-Window Travel Rule Envelopes**: Every value transfer invokes kernel precompile `0x403c0000000000000000000000000000000000000`, guaranteeing non-circumvention across arbitrary `CALL` / `DELEGATECALL` composition depths, while transfers meeting the single-transfer threshold (US$1,000.00 /

HK$7,800.00) or 24-hour anti-structuring rolling window (US$5,000.00 / HK$39,000.00) require a Zero-PII `FATF Recommendation 16` cryptographic VASP envelope digest.

3. **Binary Merkle Solvency & HKMA Linked-Rate Corridor Invariants**: The Compliance Reserve Vault (`0x8800000000000000000000000000000000000001`) verifies `LINGHE_CAP656_HQLA_V1` domain-separated custodian Merkle trees. **Explicit Synthetic Test-Vector Disclosure**: within the isolated benchmark testbed, the Genesis `LHKD` test vector (`HK$78,936,000.00` reference HQLA state against `HK$78,000,000.00` liability state, `101.20%` arithmetic coverage, Merkle root `0xa3e5fd1ee51db26128c49f848bc4eb6d71443fbfee51a40b9159832a21beae6e`) and `LUSD` test vector (`US$10,050,000.00` reference HQLA state against `US$10,000,000.00` liability state, `100.50%` arithmetic coverage, Merkle root `0x5c3f82332fbffc0be49434232a9a97e2bf2c797423aa3fde4afd19b2c264f410`) **are 100% synthetic deterministic cryptographic test vectors (`0` real bank deposits, `0` custodial fiat assets, and `0` issued monetary liabilities)** engineered to verify smart-contract arithmetic invariants; simultaneously, the Omnichain Settler (`0x8900000000000000000000000000000000000001`) locks conversions inside the statutory HKMA Linked Exchange Rate band (with $\rho_t := +\infty$ whenever $L_t = 0$):

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

4.3 Dual-Curve Cryptographic Roots (`EIP-7951 P-256` + `BN254 Groth16`) and Omnichain Settlement Customs

To bridge silicon confidential compute with external multi-chain liquidity, `Linghe Chain` unifies two elliptic-curve proof systems across precompiles and Genesis system contracts (benchmark comparison in Figure 3; canonical SSOT address registry in Table 4.1):

- **Two-Phase Silicon TEE Attestation & `ERC-8004` Bilateral Service Clearing**: Enclave settlement follows a strict two-phase cryptographic separation—**(Phase A: Enclave Quote Registration)** the Hardware Attestation Verifier (`0x8900000000000000000000000000000000000003`) invokes `Osaka EIP-7951` (`0x0000000000000000000000000000000000000100`), reinforced by post-genesis `LingheSovereignSecurityGuardV5` enforcing strict low-s canonicalization $0 < s \leq \lfloor n_{\mathrm{P256}}/2 \rfloor$, to verify silicon root quotes (e.g., NVIDIA H100 / AWS Nitro) and bind an attested enclave `runtimeSigner` ; **(Phase B: Per-Task Escrow Clearing)** the Validation Escrow (`0x8004000000000000000000000000000000000003`) verifies `runtimeSigner` authorization over `outputHash` , releasing deterministic bilateral fee-for-service splits across `ERC-8004` Identity and Reputation registries (`0x8004000000000000000000000000000000000001` – `0x8004000000000000000000000000000000000002`).
- `ERC-7683` **Bidirectional Customs &** `BN254 Groth16` **Light-Client Bridge**: The ZK Light-Client Bridge (`0x8900000000000000000000000000000000000002`) invokes pairing precompile `0x0000000000000000000000000000000000000008` at a verified cost of `815,381 gas` (`0.027%` of a single slot), achieving `~936 ms` end-to-end gasless cross-chain `x402` fulfillment across six external EVM networks plus Solana.



FIGURE 03 — Empirical Settlement Finality, 20-Lane Concurrent Burst Throughput & Global Rail Log10 Comparison

Note: Horizontal bar lengths map strictly to Log10(ms) across 6 orders of magnitude (100 ms to 100,000,000 ms) on the controlled ChainID 88888 benchmark testbed.

Architectural Layer	Subsystem & Protocol Semantics	Canonical Genesis SSOT Address
Native Ledger Primitives	`LHC` (Zero-Inflation Staking Unit) / `LUSD` / `LHKD` (Non-Circulating Synthetic Benchmark States)	`0x20c0000000000000000000000000000000000000` – `0x20c0000000000000000000000000000000000002`
Cryptographic Precompiles	`BN254` Curve Add/Mul/Pairing (`Groth16`) & `Osaka EIP-7951` `P-256` Verify	`0x0000000000000000000000000000000000000006` – `0x0000000000000000000000000000000000000008`, `0x0000000000000000000000000000000000000100`
Rust Execution Kernel	`TIP-403` Gate, `2D Nonce`, Account Keychain, Validators, Multi-Primitive Fee Manager & Sandbox Reference Central Limit Order Book (CLOB)	`0x403c000000000000000000000000000000000000`, `0x4e4f4e4345000000000000000000000000000000`, `0xaaaaaaaa0000000000000000000000000000000000`, `0xcccccccc0000000000000000000000000000000000`, `0xfeec000000000000000000000000000000000000`, `0xdec0000000000000000000000000000000000000`
Sovereign Agent Economy	`ERC-8004` Identity, Payment-Weighted Reputation, Fee-for-Service Escrow & Session Manager	`0x8004000000000000000000000000000000000001` – `0x8004000000000000000000000000000000000003`, `0x8402000000000000000000000000000000000001`
RegTech & Omnichain Customs	`Cap. 656` Reserve Vault, `ERC-7683` Settler, `ZK` Bridge, `P-256` Verifier, `3-of-4` Multisig & `Permit2`	`0x8800000000000000000000000000000000000001`, `0x8900000000000000000000000000000000000001` – `0x8900000000000000000000000000000000000004`, `0x000000000022d473030f116ddee9f6b43ac78ba3`

SECTION 05

Cross-Stack Causal Co-Design: From Enterprise Cognition to Sub-Second Verifiable Settlement

5.1 Seven-Stage End-to-End Deterministic State-Transition Pipeline and Compositional Invariance

When all three pillars operate in concert, an institutional workflow—such as an analyst swarm in `AI WorkOS` procuring external confidential model inference to synthesize a board research report while settling compute service fees atomically—progresses through seven deterministic causal stages carrying a unique idempotent tracing identifier $\kappa_j \in \mathbb{B}^{16}$ (`correlationId`):

1. **Stage I (Bounded Cognitive Planning)**: `SessionTurnEngine` loads tenant τ `Context DNA` , pre-reserves compute quota, and emits a structured, key-free intent AST $\mathcal{I}_{\mathrm{AST}}$ tagged with κ_j .
2. **Stage II (Zero-Trust MCP Challenge Handshake)**: Upon receiving an `HTTP 402` machine-payment challenge from a compute provider, `WorkOS` forwards the challenge and $\mathcal{I}_{\mathrm{AST}}$ across the `64 KB` bounded local transport to `LingheOS Wallet v5.1.0` via `wallet_x402_mcp_challenge` .
3. **Stage III (Non-LLM Policy & Anti-Phishing Verification)**: The client executes `OBL-052` pre-sign firewall inspection (rejecting blind hashes, lookalike poisoning, and unbounded `Permit` approvals), `OBL-050` `ERC-7715` allowance verification Π_{7715} , and `wallet_check_tip403_compliance` preflight screening.
4. **Stage IV (Parallel Lane Allocation & Envelope Signing)**: Upon passing all predicates, the client selects an idle 2D-nonce lane $k \in \mathcal{K}_{32}$ and signs a type- `0x76` fiat-referenced benchmark-primitive-sponsored transaction (or gasless `ERC-7683` cross-chain order).
5. **Stage V (250 ms Kernel Compliance & Single-Slot Finality)**: `Linghe Chain` verifies `TIP-403` sanctions clearance, linked-rate corridor bounds, and parallel state transitions within one `250 ms` slot, emitting an irreversible `Simplex BFT` finality certificate over $\mathcal{R}(\sigma')$.
6. **Stage VI (Two-Phase Hardware-Attested Inference & Service Clearing)**: The compute enclave (whose silicon root quote registered `runtimeSigner` via `0x8900000000000000000000000000000000000003` and low-s `P-256` precompile `0x0000000000000000000000000000000000000100`) verifies payment finality, executes inference inside silicon TEE, and submits `runtimeSigner` -authenticated `outputHash` authorization to `0x8004000000000000000000000000000000000000` for atomic clearing.
7. **Stage VII (Provenance Deliverable Synthesis & Idempotent Dual-Ledger Archival)**: `WorkOS` compiles the `JCS` -canonicalized `SHA-256` -sealed deliverable h_{art} and idempotently commits a sequenced `AuditEvent` keyed by κ_j binding h_{art} to the L1 transaction digest and finalized state root $\mathcal{R}(\sigma')$.

Let $\mathbf{\Omega} = \mathcal{S}_{\mathrm{os}} \times \mathbf{\Sigma} \times \mathcal{M}_{\mathrm{pipe}}$ denote the cross-stack product state space, where $\mathcal{M}_{\mathrm{pipe}}$ represents bounded inter-stage message envelopes carrying κ_j. Lifting each stage operator to a total endomorphism on $\mathbf{\Omega}$, the end-to-end composite transition operator $\Psi_{\mathrm{E2E}} : \mathbf{\Omega} \times \mathcal{U} \to \mathbf{\Omega}$ is strictly type-sound:

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

THEOREM 5.1 — Fail-Closed Prefix Safety and Idempotent Audit Convergence

For every cross-stack task invocation u_j initiated under tenant τ with unique tracing key κ_j, the lifted transition $\omega_{j+1} = (S_{j+1}, \sigma', m_{j+1}) = \Psi_{\mathrm{E2E}}(\omega_j, u_j)$ guarantees: (i) **Fail-Closed Prefix Safety**—a non-trivial on-chain value transfer $\sigma \to \sigma'$ occurs if and only if cognitive quota/schema bounds, client `ERC-7715` / `OBL-052` security predicates, and kernel `TIP-403` plus solvency invariants ($L_{t'} > 0 \Longrightarrow \rho_{t'} \geq 1.0000$) all hold; and (ii) `correlationId` - **Idempotent Audit Convergence**—once Stage V attains single-slot finality ($P_{\mathrm{reorg}} \equiv 0$), even under arbitrary network drops or process restarts across Stages VI–VII, deterministic replay keyed by (τ, κ_j) converges without duplicate settlement to a unique monotonically sequenced `AuditEvent` $e^* \in S_{j+1}$ cryptographically binding deliverable digest h_{art} to $\mathcal{R}(\sigma')$.

PROOF

i. On the product space $\mathbf{\Omega}$, every lifted stage operator acts as the identity on aborted envelopes $m = \perp$: if $\hat{\delta}_{\mathrm{turn}}$ rejects schema or quota constraints, it emits $(S_j', \sigma, \perp)$ and subsequent stages preserve $\sigma' = \sigma$; if $\hat{\Upsilon}_{\mathrm{MCP}}$ rejects policy or phishing predicates, no valid elliptic-curve signature is emitted and $\sigma' = \sigma$; if $\hat{\Upsilon}_{\mathrm{L1}}$ encounters a `TIP-403` hit or solvency breach, the Rust kernel reverts state atomically. (ii) Once `Simplex BFT` aggregates a `3-of-4` finality certificate, $\mathcal{R}(\sigma')$ is permanent; if a crash occurs prior to Stage VII archival, recovery queries finalized receipt state by (τ, κ_j) and invokes idempotent `appendAuditEvent`, which by Invariant 2.1's monotonic sequence and deduplication locks commits exactly one event binding $(h_{\mathrm{art}}, \mathcal{R}(\sigma'))$ without re-spending consumed 2D nonce (k, ν).

Q.E.D. ■

5.2 Machine-Native Micropayments (`x402`) and Bilateral Fee-for-Service Arithmetic Clearing

Across specialized skill orchestration and confidential inference execution, the Validation Escrow predeploy (`0x8004000000000000000000000000000000000003`) executes a **per-invocation bilateral commercial fee-for-service split** bounded by $\beta_{\mathrm{bps}} \in \{0, \ldots, 5000\}$—**involving zero pooled investor funds, zero fractionalized profit-sharing units, zero passive yield, and `0%` `MYRILUM LIMITED` protocol rake**. For any escrowed atomic service fee $V \in \mathbb{N}_+$ (6-decimal precision), the contract enforces exact integer floor division and remainder conservation:

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

Under the canonical benchmark parameter $\beta_{\mathrm{bps}} = 2,000$ (`20%` `skillAuthor` IP licensing fee, `80%` `agentPayee` compute execution fee), arithmetic conservation eliminates fractional dust lockups across arbitrary payment amounts, while conditioning settlement and `ERC-8004` fulfillment reputation on two-phase `0x0000000000000000000000000000000000000100` `P-256` enclave registration (`0x8900000000000000000000000000000000000003`) and `runtimeSigner` verification renders Sybil wash-trading economically unprofitable.

SECTION 06

Formal Trust Assumptions, Cryptographic Runtime Boundaries, and Hot-Spot Contention Degradation

Scientific integrity requires stating exact trust premises, microarchitectural boundaries, and worst-case degradation envelopes up front. This section addresses the primary scrutiny vectors of applied cryptographers, distributed-systems researchers, and adversarial red teams.

6.1 Four-Region `3-of-4` BFT Fiber-Geometry Assumptions and Mandatory Timelock Governance Bounds

All empirical `Linghe Chain` latency measurements ($\Delta_{\text{slot}} = 250$ ms finality and `~936 ms` omnichain fulfillment) rest upon two explicit formal assumptions:

1. **Controlled Four-Node Committee, Fiber-Optic Quorum Geometry & Non-Collusion Premise**: The benchmark topology comprises $N_{\text{val}} = 4$ validator nodes distributed across Hong Kong, Singapore, Tokyo, and Zurich ($f = \lfloor (N_{\text{val}} - 1)/3 \rfloor = 1$, quorum $q = 2f + 1 = 3$). **Safety** (zero conflicting finalized blocks) holds unconditionally under arbitrary asynchronous network partitions provided at most $f = 1$ validator exhibits Byzantine fault or collusion; **Liveness & Fiber Geometry** hold post-Global Stabilization Time (`GST`) under Dwork-Lynch-Stockmeyer partial synchrony: because quorum requires $q = 3$ of 4 validators, the three Asia-Pacific nodes (`HK` – `SG` – `JP`, interconnected at ≤ 35 ms one-way fiber latency) close three-step `Simplex BFT` notarization and finality comfortably within $\Delta_{\text{slot}} = 250$ ms under an honest APAC leader while the Zurich node (`~85–95 ms` one-way) replicates asynchronously; when leader rotation selects Zurich or encounters a single faulty leader, deterministic local-timeout dummy skip certificates bound worst-case slot progression to ≤ 500 ms. Scaling $N_{\text{val}} \gg 4$ in future permissioned or federated expansions introduces $O(N_{\text{val}}^2)$ all-to-all message overhead requiring threshold signature aggregation (e.g., BLS) and updated empirical disclosure.
2. **Dual-Layer Genesis Multisig & Post-Genesis Timelock Governance Bounds**: While Genesis Block-0 initializes the foundational `3-of-4` multisig at `0x8900000000000000000000000000000000000004`, post-genesis `LingheSovereignSecurityGuardV5` wraps critical protocol parameter transitions inside an enforced on-chain queued timelock satisfying $\text{eta} = t_{\text{queue}} + \Delta_{\min}$ ($\Delta_{\min} \in (0, 30\ \text{days}]$), eliminating instantaneous single-admin mutation and guaranteeing non-custodial users an auditable advance-warning and exit window prior to rule activation.

6.2 Tiered Side-Channel Defense: Silicon Hardware Roots (`Tier-1`) vs. Managed JIT Runtime Boundaries (`Tier-2`)

In applied cryptography, claiming unconditional microarchitectural constant-time execution inside a managed JavaScript virtual machine contradicts modern Just-In-Time (JIT) compiler internals. `MYRILUM LingheOS Wallet v5.1.0` therefore enforces an explicit **Two-Tier Cryptographic Side-Channel Boundary**:

- **Tier-1: Silicon Hardware Enclaves & OS Native Constant-Time Core (`Tier-1 Hardware / OS Native Root`)**:
  - Vault master-key derivation and encryption-at-rest delegate exclusively to host OS/browser native C++ and assembly `WebCrypto SubtleCrypto` implementations (`PBKDF2-HMAC-SHA256` at `600,000` iterations and non-extractable `AES-256-GCM`);
  - **Mandatory Institutional Hardware-Only Policy**: High-value institutional treasuries and policy approvals bind directly to silicon hardware roots—specifically non-extractable Apple `Secure Enclave` `NIST P-256` WebAuthn Passkeys verified on-chain via `0x0000000000000000000000000000000000000100`, or air-gapped hardware cold signers driven over `64`-byte framed `ISO-7816 WebHID` Application Protocol Data Units (`APDUs`)—**with software signing fallback strictly disabled**, ensuring master private scalars never enter general-purpose host RAM.
- **Tier-2: Bounded Session 320-Bit Scalar-Blinded Montgomery Ladder Plane (`Tier-2 Scalar-Blinded Montgomery Ladder Session Plane`)**:
  - For high-frequency micro-allowance `x402` session signing, the zero-dependency elliptic-curve engine applies **62-bit CSPRNG multiplicative scalar blinding** $k' = (k \bmod n) + (3 \cdot 2^{62} + r_{62}) \cdot n$ ($r_{62} \leftarrow_{\$} \{0, \ldots, 2^{62} - 1\}$, fixing exact bit-length $\lfloor \log_2 k' \rfloor + 1 = 320$) executed across a fixed 320-step balanced-stride Montgomery ladder over `secp256k1` and `secp256r1`;
  - **Explicit Affine Inversion & JIT Runtime Boundary Disclosure**: Because affine point addition invokes extended-Euclidean modular inversion (`modInv`) and V8/JavaScriptCore represent native `BigInt` operands using variable-length limb arrays subject to dynamic JIT tiering and garbage-collection (`GC`) scheduling, pure managed-language arithmetic cannot claim microarchitectural cache-timing invariance against co-resident CPU

L1/LLC adversaries (e.g., Prime+Probe). Consequently, architectural policy restricts `Tier-2` strictly to revocable short-lived `ERC-7715` session keys capped by micro-allowances and target allowlists, mandating `Tier-1` hardware step-up authentication for institutional treasury transfers, allowlist mutations, or guardian configuration.

6.3 Parallel Execution Degradation Under Hot-Spot Write Contention and Deterministic Serial Fallback

While 32-lane type-`0x76` 2D nonces eliminate **sender-side** mempool queueing, multi-core EVM execution speedup remains physically bounded by **target storage-slot write contention** (for example, concurrent orders targeting the identical top-of-book slot on the sandbox reference orderbook `0xdec0000000000000000000000000000000000000`).

Let a `250 ms` slot contain m ordered transactions, let $\alpha = G_{\text{serial}}/G_{\text{slot}} \in [0,1]$ denote the fraction of computational gas exhibiting overlapping read/write or write/write storage dependencies requiring causal serialization, and let $\delta_{\text{occ}}(\alpha) \geq 0$ denote the normalized Optimistic Concurrency Control (`OCC`) conflict-detection and re-execution scheduling overhead. By the generalized Amdahl–Brent serialization bound across K execution lanes, effective parallel state-transition speedup $S(\alpha, K)$ satisfies:

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

Under orthogonal agentic `x402` micropayments and sharded escrow settlements ($\alpha \approx 0, \delta_{\text{occ}} \approx 0$), execution approaches full $K = 32$-lane concurrency. Conversely, under extreme single-contract hot-spot contention ($\alpha \to 1$), scheduling **degrades deterministically to canonical in-block topological serial execution**, while EIP-1559 dynamic base-fee congestion control and per-lane execution-time budgets bound per-slot execution strictly within the `250 ms` consensus slot budget without livelock or state-root divergence.

Table 6.1 summarizes explicit non-claims and mandatory fail-closed Kill Criteria across the stack.

Audit Dimension	Explicit Boundary Disclosure (Non-Claims)	Mandatory Fail-Closed Kill Criterion
Off-Chain Reserves & Oracles	On-chain Merkle roots prove structural accounting consistency and $\geq 100\%$ arithmetic coverage (benchmark values are synthetic test vectors), not bank-vault audits.	Any breach of $\rho_t \geq 100.00\%$ or corridor $[7.7500, 7.8500]$ in licensed deployment halts minting and cross-chain settlement immediately in bytecode.
Autonomous Agent Authority	Foundation models are treated as untrusted, prompt-injectable proposers devoid of legal personhood.	Any code path enabling unapproved, uncapped, or unlogged AI fund movement triggers immediate feature suspension.
Client Cryptographic Runtime	Explicitly separates `Tier-1` silicon/OS native primitives from `Tier-2` 320-bit scalar-blinded JIT session keys.	Institutional high-value vaults are strictly prohibited from enabling software fallback or bypassing `Tier-1` hardware step-up verification.
Commercial Unit Economics	Corporate unit gross profit must remain strictly positive purely from software, policy licensing, and SLA fees.	Any product line requiring token emission subsidies or promised investment returns to remain viable is terminated.

SECTION 07

Multi-Jurisdictional Regulatory Engineering and Shared-Nothing Dual-Hemisphere Isolation

7.1 Hong Kong Statutory Compliance Matrix (Cap. 622, 32, 571, 656, 615, 155/581 & 486) and Non-Issuer Safe Harbor

Headquartered in the Hong Kong Special Administrative Region, MYRILUM LIMITED maps statutory ordinances directly into enforceable architectural boundaries (Table 7.1), maintaining a clean pure-technology R&D safe harbor.

Hong Kong Ordinance	Statutory Regulatory Perimeter	Architectural Safe-Harbor & Technical Enforcement
Cap. 622 **Companies Ordinance** & Cap. 310 **Business Registration**	Corporate legal personality, statutory registered name, and commercial registry disclosure.	MYRILUM LIMITED is incorporated under its sole statutory English corporate name pursuant to Cap. 622 s. 899(1) (UBI: 80912065 , BR: 80912065-000-07-26-0 , D-U-N-S: 374308629).
Cap. 32 **Companies (Winding Up and Miscellaneous Provisions) Ordinance (CWUMPO) &** Cap. 571 **Securities and Futures Ordinance**	Prohibits unauthorized public prospectuses, offers of securities or futures contracts, collective investment schemes (CIS), Part III Automated Trading Services (ATS), and Type 4/9 investment advice or asset management.	Pure computer-science specification; zero public fundraising, zero futures/derivatives issuance, zero profit-pooling, zero order-matching brokerage, and zero investment solicitation.
Cap. 656 **Stablecoins Ordinance** (Sections 8 & 9)	Prohibits unlicensed issuance of specified stablecoins in HK or active marketing to the HK public.	MYRILUM LIMITED acts solely as **non-issuer Protocol & Software R&D Author**; LHKD / LUSD are non-circulating synthetic benchmark states, and fiat adapters are open client interfaces for independent licensed institutions.
Cap. 615 **Anti-Money Laundering and Counter-Terrorist Financing Ordinance (AMLO Part 5B s. 53ZRD)**	Regulates Virtual Asset Trading Platforms (VATP) custody/matching and enforces FATF Rec. 16 Travel Rule compliance.	100% client-side self-custodial software (zero client key/asset custody, zero centralized order matching, zero brokerage fee—non-VATP); protocol enshrines TIP-403 screening and 24h anti-structuring hash envelopes.
Cap. 155 **Banking Ordinance** & Cap. 581 **Deposit Protection**	Prohibits non-authorized institutions from taking interest-bearing deposits or repayable public funds.	Accepts zero public funds; state-machine bytecode permanently locks zero holder interest $r_{\text{holder}}(t) \equiv 0$.
Cap. 486 **Personal Data (Privacy) Ordinance**	Mandates data minimization, purpose limitation, and cross-border personal-data protection.	All on-chain states and proofs enforce **Zero Individual PII** (anchoring irreversible 32-byte digests only).

7.2 International Regulatory Alignment (Howey , MiCA , BCBS SCO60 & App Store Rules) and Tri-Mode Geofencing

Across international jurisdictions and mobile distribution ecosystems, the stack enforces deterministic compliance adaptation:

- **U.S.** Howey **Structural Disjunction, EU** MiCA **&** BCBS SCO60 **Technical Alignment**: Enterprise customers pay fixed contractual SaaS and infrastructure fees for software utility while LHC carries zero inflationary staking pooling or profit buybacks, LUSD / LHKD lock zero yield ($r_{\text{holder}} \equiv 0$), and ERC-8004 executes per-invocation bilateral commercial fee-for-service splits (0% MYRILUM rake), structurally negating common-enterprise and expectation-of-

profit prongs under investment-contract doctrines. Reserve proof data schemas maintain technical compatibility with `BCBS SCO60` prudential exposure standards and EU `MiCA` reserve-attestation formats (`MYRILUM LIMITED` conducts zero `MiCA` Art. 16 asset-referenced token or Art. 48 e-money token public offer in the EEA).

- **Tri-Mode Client Jurisdictional Geofencing & Apple App Store Alignment (`OBL-005`)**: `LingheOS Wallet v5.1.0` enforces three deterministic runtime compliance profiles: (i) `GLOBAL_PRO` —exposes advanced analytics and non-custodial signing tools exclusively in permitted institutional jurisdictions; (ii) `HK_RETAIL_STRICT` —automatically suppresses unlicensed leveraged derivatives, yield vaults, and event-contract interfaces for Hong Kong retail contexts; and (iii) `APP_STORE_SAFE` —complies strictly with **Apple App Store Review Guidelines `3.1.1` (In-App Purchase—never using `x402` or crypto assets to unlock digital app features or SaaS subscriptions inside mobile binaries), `3.1.5(i)-(v)` (Cryptocurrencies: Wallets, Transactions, Exchanges, ICOs/Derivatives, and Cryptocurrency Apps), and `5.3` (Gaming, Gambling, and Lotteries)**, maintaining pure non-custodial utility devoid of unlicensed fiat ramps, custodial exchanges, or digital-purchase bypasses.

7.3 Physically Air-Gapped Mainland China Pure-AI Enterprise Architecture (`myrilum.cn`)

To satisfy strict cross-border data-residency and financial-regulatory boundaries, the architecture enforces a **100% Physical Shared-Nothing Air-Gap** between the international sovereign R&D stack (`MYRILUM LIMITED` · `myrilum.com`) and the Mainland China Pure-AI Enterprise WorkOS (`myrilum.cn`, PRC MIIT ICP Filing `2026055724-1`) (Figure 4):

1. **Independent Onshore Legal Entity & Four-Plane Physical Separation**: The Mainland portal `myrilum.cn` is independently operated by the onshore PRC legal entity `Beijing Linghe Agentic Technology Co., Ltd.` (Unified Social Credit Code: `91110108MAERKJRC8R`), contracting and invoicing purely in onshore corporate RMB with statutory VAT invoices. Its codebase, domestic cloud VPCs, encrypted databases, and KMS key spaces are physically isolated; compiled artifacts contain `0%` **blockchain client code, smart-contract ABIs, cryptographic wallets, mnemonic generators, `x402` settlement modules, or cross-chain bridges**.
2. **Domestic Statutory & Dual AI-Labeling Compliance**: The Mainland edition adheres to the PRC *Cybersecurity Law*, *Data Security Law*, *Personal Information Protection Law (`PIPL`)*, and *Interim Measures for the Management of Generative Artificial Intelligence Services*. `100%` of enterprise documents, `Context DNA`, and audit logs reside encrypted inside Mainland China data centers; inference routes to PRC-region compliant model endpoints guarded by `providerNotice` transparency gates (with provincial CAC generative-AI launch filing staged under Gate `G8`); where an enterprise tenant optionally enables federated SSO, cross-border identity verification strictly follows `PIPL` Articles 38–39 separate consent and security-assessment rules (`100%` domestic intranet closure in Private Edition); and all synthesized deliverables enforce mandatory **explicit plus metadata-implicit AI content labeling under PRC national standard `GB 45438-2025`**.

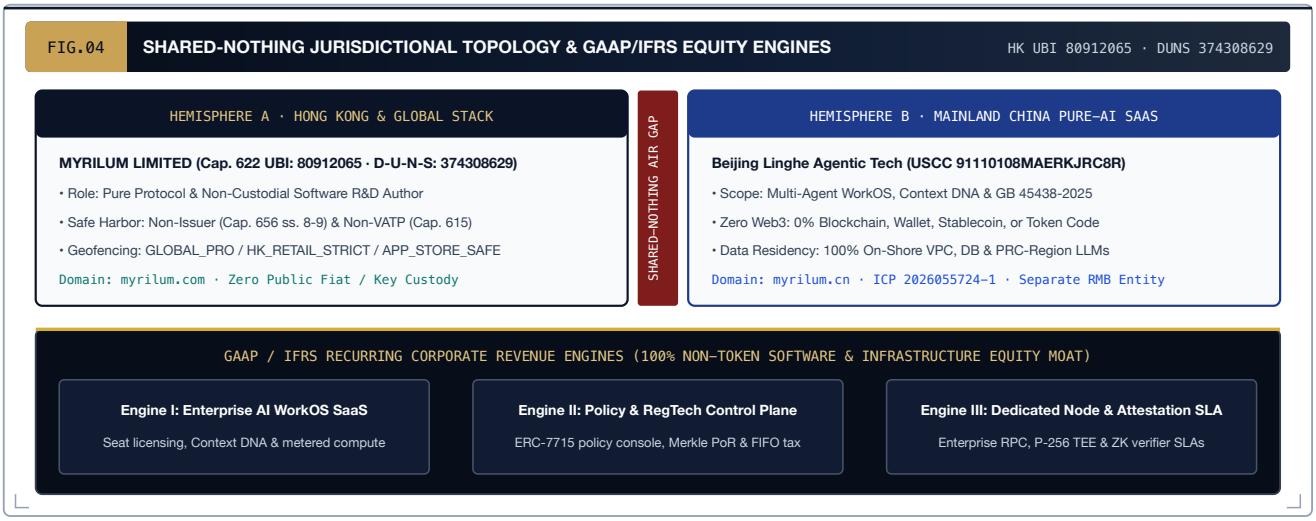


FIGURE 04 — Shared-Nothing Dual-Hemisphere Regulatory Topology & Three GAAP/IFRS Corporate Equity Revenue Engines

Note: Global and Mainland stacks enforce 100% physical shared-nothing isolation across codebases, VPCs, databases, and key spaces.

SECTION 08

Corporate Equity Monetization, GAAP/IFRS Cash-Flow Engines, and Unit Economics

8.1 Pure Software Equity Value Capture and `IAS 7` Cash-Flow Reconciliation Without Token Subsidies

Under institutional equity valuation standards (including Wall Street institutional underwriting and Hong Kong Stock Exchange Chapter `18C` Specialist Technology criteria), sustainable enterprise value requires recurring, auditable fiat cash flows independent of inflationary token emissions. `MYRILUM LIMITED` enforces a **Pure Corporate Equity Value-Capture & Separate-Entity Accounting Axiom**: international software licensing and infrastructure SLA revenues accrue to `MYRILUM LIMITED` in Hong Kong, whereas Mainland China pure-AI enterprise software revenues are contracted, taxed, and accounted for independently by `Beijing Linghe Agentic Technology Co., Ltd.` onshore with zero unapproved cross-border capital commingling and zero token emission subsidies ($S_{\text{token}} \equiv 0$).

For M_{ent} enterprise and institutional clients over accounting period T, let $R_{\text{sub},\,i}$ denote recurring seat and platform subscription revenue, $R_{\text{meter},\,i}$ denote principal-fulfilled metered multi-agent orchestration and verification SLA overages, and $C_{\text{cogs},\,i}$ denote direct cloud and model-inference fulfillment cost. In strict accordance with *IAS 7 / ASC 230 (Statement of Cash Flows)*, per-customer Gross Profit (GP_i), corporate Operating Cash Flow (OCF_{corp}), and corporate Free Cash Flow (FCF_{corp}) satisfy a strictly positive unit gross-profit constraint and exact cash-flow reconciliation (where C_{opex} denotes R&D and SG&A operating expenses, T_{tax} cash corporate taxes, D_{da} non-cash depreciation and amortization, ΔNWC net working-capital change including deferred-revenue contract liabilities, and CapEx capital expenditures):

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

Through `QuotaEntitlementMeter` pre-turn cost reservation and context-prefix caching inside `@myrilum/linghe-harness-core`, every principal-fulfilled inference and verification call locks in strictly positive unit gross profit ($\text{GP}_i > 0$) prior to execution.

8.2 Three Recurring Fiat Revenue Engines and `IFRS 15` / `ASC 606` Revenue Recognition

Table 8.1 details the three recurring corporate cash-flow engines structured under *IFRS 15* / *ASC 606* five-step performance-obligation bifurcation, Standalone Selling Price (`SSP`) allocation, and Principal-versus-Agent (`IFRS 15.B34–B38`) rules.

Corporate Revenue Engine	Target Institutional Buyer Profile	Standardized Pricing Primitives & Open-Core Boundary	`IFRS 15` / `ASC 606` Recognition & Margin Profile
Engine I: Enterprise AI WorkOS SaaS & Private Deployment	Multinational corporations, financial research/legal desks, consulting firms, and large organizations.	Annual Contract Value (`ACV / ARR`) + `Context DNA` repository tiers + prepaid multi-agent compute packs + air-gapped/private VPC licensing & Post-Contract Support (`PCS`).	Cloud SaaS (`Right to Access` , `IFRS 15.35`) recognized ratably over contract term; on-premises private deployments bifurcated by `SSP` into point-in-time functional IP license (`Right to Use` , `IFRS 15.B58`) and ratable `PCS` ; prepaid compute recorded as **Contract Liabilities** and recognized **Gross** upon consumption solely where `MYRILUM` acts as principal (`IFRS 15.B34–B38` , excluding BYOK or client-side peer-to-peer `x402` pass-throughs).
Engine II: Institutional Policy Control Plane & RegTech Commercial Suite	Family offices, licensed asset managers, payment/stablecoin applicants, and corporate treasuries.	**Open-Core Model**: base self-custodial client wallet remains free/open; commercial enterprise editions license multi-seat RBAC `ERC-7715` policy consoles, `TIP-403` /Travel Rule gateways, Merkle Proof-of-Reserve (`PoR`) verifiers, HSM connectors, and `FIFO/HIFO` tax audit modules.	Pure non-custodial enterprise software licensing and support (`100%` zero balance-sheet custody risk; `> 85%` target steady-state software gross margin `[ARCHITECTURAL_SPEC]`).
Engine III: Multi-Chain High-Throughput RPC & Attestation Infrastructure SLAs	Quantitative desks, confidential GPU clouds, cross-chain market makers, and fintech rails.	Immediate commercialization spans dedicated low-latency RPC clusters across `169` external networks, batch `P-256` TEE attestation verification SLAs, and archival audit streams; regulated settlement-node commercialization remains gated on `G9` licensing (`[ROADMAP_GATED]`).	Recognized ratably over contracted SLA service periods (`IFRS 15.35(a)`), net of variable-consideration reserves for SLA uptime credits (`IFRS 15.50–56`).

SECTION 09

Master Whitepaper Suite Lineage, Version Reconciliation, and Cryptographic Attestation Index

9.1 Four-Volume Global Monograph Hierarchy and Client Specification Reconciliation (`v5.0 -> v5.1.0`)

With the completion of this Group Master Whitepaper (`Volume 0`), the MYRILUM technical literature forms a unified, `1:1` structurally symmetric bilingual **Four-Volume Global Sovereign Suite (`8` Overseas Editions) plus a Physically Isolated Mainland Pure-AI Monograph** (Table 9.1):

- **Volume 0 (`Master Suite` · This Monograph)**: Establishes the overarching Sovereign Trinity Architecture (`AI WorkOS` × `LingheOS Wallet v5.1.0` × `Linghe Chain 88888`), product-space cross-stack causal proofs, microarchitectural side-channel and fiber-quorum boundaries, Shared-Nothing jurisdictional governance, and `IFRS 15` / `IAS 7` corporate equity economics.
- **Volume I (`Protocol Yellow Paper`)**: Derives the complete six-tuple state space, five-phase transaction execution semantics, `Simplex BFT` safety/liveness proofs, and dual-curve (`BN254` / `P-256`) cryptographic algebra of `Linghe Chain` .
- **Volume II (`Enshrined RegTech & Merkle PoR Specification`)**: Formalizes `Cap. 656` Schedule 2 solvency coverage invariants, the `[7.7500, 7.8500]` linked-rate corridor, and kernel `TIP-403` / `FATF Rec. 16` compliance state machines.
- **Volume III (`Architecture & Empirical Benchmark Monograph`)**: Provides a concise executive monograph and logarithmic latency benchmark synthesis for institutional decision-makers.

VERSION & STATUTORY NOMENCLATURE RECONCILIATION NOTICE — `v5.0 -> v5.1.0` & Frozen Digest Preservation

1. **Client Capability Lineage**: Volumes I, II, and III (`v2.0` frozen editions) were compiled against the `v5.0` client audit baseline referencing `48` client capabilities and `10` Zero-Trust MCP tools. Subsequent to their publication freeze—and without modifying the immutable `Linghe Chain` Genesis Block-0 `SHA-256` (`96208e9900b218935143be3024d2602566a86d61caa906d42399f35b83afd991`) or the frozen cryptographic digests of Volumes I–III— `MYRILUM LIMITED` completed the backward-compatible clean-room upgrade to `MYRILUM LingheOS Wallet v5.1.0` , expanding verified capabilities from `48` to `60` (`OBL-049` through `OBL-060`) and Zero-Trust MCP tools from `10` to `14` (Table 3.1).
2. **Statutory Registered Corporate Name Precision**: Pursuant to Hong Kong `Cap. 622` s. 899(1), `MYRILUM LIMITED` (`UBI: 80912065`) is registered with the Hong Kong Companies Registry solely under its English corporate name; parenthetical localized Chinese entity renderings appearing in frozen `v2.0` Chinese sub-volumes I–III served purely as informal descriptive translations and remain byte-frozen solely to preserve their anchored `SHA-256` digests. Across the entire suite, `MYRILUM LIMITED` governs as the sole statutory corporate identifier.

Volume & Jurisdictional Scope	Canonical Document Reference (`DocCode`)	Language	Architectural Scope & Cryptographic Provenance Status
Volume 0 (Group Master)	`MYR-WP-MASTER-2026-V1.0-ZH` / `EN`	Simplified ZH (Global) / EN	Sovereign Trinity Stack, formal threat boundaries, jurisdictional isolation & equity model (anchored in `WHITEPAPER_PUBLICATION_INDEX.json`).

Volume & Jurisdictional Scope	Canonical Document Reference (`DocCode`)	Language	Architectural Scope & Cryptographic Provenance Status
Volume I (Protocol Yellow Paper)	`MYR-WP-TECH-2026-V2.0-ZH` / `EN`	Simplified ZH (Global) / EN	`Simplex BFT` 250 ms consensus, `0x76` 2D parallel EVM, `BN254` & `P-256` formal proofs (Frozen SHA-256).
Volume II (RegTech & PoR Spec)	`MYR-WP-CAP656-2026-V2.0-ZH` / `EN`	Simplified ZH (Global) / EN	`Cap. 656` solvency invariants, `[7.7500, 7.8500]` corridor & kernel `TIP-403` specification (Frozen SHA-256).
Volume III (Benchmark Monograph)	`MYR-WP-EXEC-2026-V2.0-ZH` / `EN`	Simplified ZH (Global) / EN	Concise sub-second state-machine architecture & `~936 ms` omnichain log10 benchmarks (Frozen SHA-256).
Mainland China Pure-AI Edition	`MYR-WP-CN-AI-2026-V1.0-ZH`	Simplified ZH (Onshore)	Physically isolated pure-AI enterprise WorkOS whitepaper published by `Beijing Linghe Agentic Technology Co., Ltd.` for `myrilum.cn` (`ICP 2026055724-1`).

9.2 Stage-Gated Engineering Roadmap (`G0–G9`) and Reproducible Cryptographic Verification Protocol

MYRILUM replaces speculative marketing timelines with a deterministic ten-stage release gate (`G0–G9` , Table 9.2). External auditors, institutional counterparties, and academic reviewers can independently recompute the `SHA-256` digests of all eight overseas Markdown master sources and rendered PDF monographs against `WHITEPAPER_PUBLICATION_INDEX.json` , `LingheSovereignSecurityGuardV5.latestWhitepaperAnchor()` , and the deterministic verification endpoint `/v1/whitepapers/verify` .

Release Gate Stage	Deterministic Engineering, Security & Legal Entry Invariant	Verified Objective Status
`G0–G2` **Scope, Claims & SSOT**	Cross-repo truth ledger anchored; 100% of claims classified by maturity with counter-assumptions disclosed.	**ACHIEVED (** `VERIFIED` **)**
`G3–G5` **Prototype, Accountability & Security**	`WorkOS` 21 packages, `Wallet v5.1.0` 60 zero-dep specs & `Chain 88888` controlled testbed verified; 10-row `Human Gate` active.	**ACHIEVED (** `VERIFIED` **)**
`G6–G7` **Unit Economics & Isolation**	Three token-free `IFRS 15` revenue engines formalized; HK vs. Mainland `Shared-Nothing` isolation verified.	**ACHIEVED (** `VERIFIED` **)**
`G8` **External Audit & Channel KYC**	Apple Developer Program Organization enrollment (`D-U-N-S 374308629`) verification, third-party penetration audit & legal opinions.	**ACTIVE (** `IN_REVIEW` **)**
`G9` **Commercial Scale Sign-Off**	Phased institutional production activation upon satisfying target-jurisdiction licensing/filings and founder Human Gate sign-off.	**LOCKED (** `GATED` **)**

APPENDIX A

Normative Standards and Academic References

1. Dwork, C., Lynch, N., & Stockmeyer, L. (1988). Consensus in the Presence of Partial Synchrony. *Journal of the ACM*, 35(2), 288–323.
2. Chan, B. Y., & Pass, R. (2023). Simplex Consensus: A Simple and Fast Consensus Protocol. *Cryptology ePrint Archive*, Paper 2023/463.
3. Shamir, A. (1979). How to Share a Secret. *Communications of the ACM*, 22(11), 612–613.
4. Groth, J. (2016). On the Size of Pairing-Based Non-Interactive Arguments. *Advances in Cryptology — EUROCRYPT 2016*, LNCS 9666, 305–326.
5. Montgomery, P. L. (1987). Speeding the Pollard and Elliptic Curve Methods of Factorization. *Mathematics of Computation*, 48(177), 243–264.
6. National Institute of Standards and Technology (NIST). (2023). *Digital Signature Standard (DSS)*, FIPS PUB 186-5 (`secp256r1` / `Ed25519`).
7. Ethereum Foundation & Open Web Standards. *EIP-712: Typed Structured Data Hashing and Signing*; *EIP-2718: Typed Transaction Envelope*; *EIP-4337: Account Abstraction Using Alt Mempool v0.7*; *EIP-4361: Sign-In with Ethereum*; *EIP-5792: Wallet Call API v2.0*; *ERC-6492: Signature Validation for Predeploy Contracts*; *EIP-6963: Multi Injected Provider Discovery*; *ERC-7579: Minimal Modular Smart Accounts*; *ERC-7683: Cross Chain Intents*; *EIP-7702: Set EOA Account Code*; *ERC-7715: Grant Permissions from Wallets*; *EIP-7951: Precompile for secp256r1 Curve Support*; *ERC-8004 (Draft): Trustless Agents*; *HTTP 402 / x402 Machine Payment Protocol*.
8. Laws of Hong Kong. *Companies Ordinance* (`Cap. 622`); *Companies (Winding Up and Miscellaneous Provisions) Ordinance* (`Cap. 32`); *Personal Data (Privacy) Ordinance* (`Cap. 486`).
9. Laws of Hong Kong. *Securities and Futures Ordinance* (`Cap. 571`); *Anti-Money Laundering and Counter-Terrorist Financing Ordinance* (`Cap. 615`); *Banking Ordinance* (`Cap. 155`).
10. Laws of Hong Kong. *Stablecoins Ordinance* (`Cap. 656`), Sections 8, 9 & Schedule 2.
11. Hong Kong Monetary Authority (HKMA). *Linked Exchange Rate System Operational Mechanism* (`7.7500–7.8500 HKD/USD` Convertibility Undertakings).
12. Financial Action Task Force (FATF). *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers* (`Recommendation 16` Travel Rule).
13. Basel Committee on Banking Supervision (BCBS). *Prudential Treatment of Cryptoasset Exposures* (`SCO60`).
14. European Parliament and Council. *Regulation (EU) 2023/1114 on Markets in Crypto-Assets (`MiCA`)*.
15. International Accounting Standards Board (IASB) & Financial Accounting Standards Board (FASB). *IFRS 15 / ASC 606: Revenue from Contracts with Customers*; *IAS 7 / ASC 230: Statement of Cash Flows*.
16. Greshake, K., et al. (2023). Not What You've Signed Up For: Compromising Real-World LLM-Integrated Applications with Indirect Prompt Injection. *Proceedings of the 16th ACM Workshop on Artificial Intelligence and Security (AISec)*.
17. Pollaczek, F. (1930). Über eine Aufgabe der Wahrscheinlichkeitstheorie. *Mathematische Zeitschrift*, 32(1), 64–100.
18. Amdahl, G. M. (1967). Validity of the Single Processor Approach to Achieving Large Scale Computing Capabilities. *AFIPS Conference Proceedings*, 30, 483–485.

PUBLICATION IMPRINT & CRYPTOGRAPHIC SEAL

MYR-WP-MASTER-2026-V1.0-EN



VOL. 0 · GROUP MASTER ARCHITECTURE & GOVERNANCE WHITEPAPER

Sub-Second Deterministic Finality · Binary Merkle Solvency Proofs · Enshrined RegTech

CRYPTOGRAPHIC VERIFICATION & R&D ENTITY COLOPHON

FROZEN SSOT · v1.0

PROTOCOL R&D AUTHOR
MYRILUM LIMITED (HK Cap. 622 Body Corporate)

CORPORATE & BR REGISTRY
CR/UBI: 80912065 · BR: 80912065-000-07-26-0

SOVEREIGN NETWORK
ChainID: 88888 (0x15b38)

ON-CHAIN GUARD
LingheSovereignSecurityGuardV5.
latestWhitepaperAnchor()

GENESIS SHA-256
96208e9900b218935143be3024d2602566a86d61caa906d42399f35b83afd991

MARKDOWN MASTER SHA-256
522691a5113f695ad527669f22b8894e84737ff15e2496d9eea119252b8b3389

VERIFICATION ENDPOINT
/v1/whitepapers/verify

STATUTORY REGISTERED OFFICE
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