PUBLIC PRIMER · UNIVERSAL PLAIN-LANGUAGE EXECUTIVE GUIDE

MYRILUM Global Public & Executive Primer: Understanding Trustworthy Enterprise AI and Hardware-Secured Digital Settlement in Ten Minutes (v1.0)

Zero-Jargon Ten-Minute Guide to Trustworthy Enterprise AI, Zero-Dependency Biometric Key Protection & Verifiable Sub-Second Settlement

MYRILUM Group Public Communications, Architecture & Governance Council (Zero Math Prerequisites · Global Executive & Reader Edition)



READING TIME & JARGON
10 Min · 0 Jargon
Plain Modern Prose & Visual Storyboards

SEPARATION OF POWERS
3 Isolated Layers
AI WorkOS · Biometric Vault · Clearing Rail

RED LINES & CUSTODY
3 Explicit Nevers
Zero Fund Custody · Zero Speculative Sales

CORPORATE ANCHOR
UBI 80912065
IFRS 15 Pure Software · D-U-N-S 374308629

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

PRIMER MONOGRAPH ARCHITECTURAL TIER

PUBLIC PRIMER · UNIVERSAL PLAIN-LANGUAGE GUIDE

MYR-WP-PRIMER-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-PRIMER-2026-V1.0-EN` · UNIVERSAL PLAIN-LANGUAGE EXECUTIVE PRIMER · 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	`94bf03d617c85e221eb5c9f4a062851c068e072c0d6c78a04b54096978bd0c8a`

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 **At a Glance: MYRILUM in Thirty Seconds** §00

00·1 **Reader's Guide: Everyday Plain-Language Glossary** §00·1

01 **Why Digital Work and Cross-Border Settlement Still Feel Broken** §01

› 1.1 AI That Talks Fluently Yet Cannot Be Trusted with Real Operations §1.1

› 1.2 Fragile Approval Workflows, Blind Signing, and Software Supply-Chain Risks §1.2

02 **One Picture to Understand MYRILUM: Three Tools with Strict Separation of Powers** §02

› 2.1 Layer One (AI WorkOS): The Institutional Research & Workflow Assistant Where Every Claim Has a Receipt §2.1

› 2.2 Layer Two (LingheOS Wallet v5.1): Your Zero-Dependency Biometric Vault and Policy Gatekeeper §2.2

03 **A Real-World Walkthrough: How an Enterprise Task Closes Safely in Under Sixty Seconds** §03

› 3.1 Seconds 0 to 30: Source-Grounded Drafting and Automatic Blocking of Malicious Traps §3.1

› 3.2 Seconds 30 to 60: Plain-Language Preview, Hardware Biometric Sign-Off, and Sub-Second Audit Trail §3.2

04 **Safety and Regulatory Red Lines: Our Three Explicit "Nevers"** §04

› 4.1 Never Touching Client Keys, Never Selling Speculative Tokens, Never Taking Deposits §4.1

› 4.2 Zero Personal Data on Shared Ledgers and Strict Physical Isolation Across Jurisdictions §4.2

05 **A Transparent Business Model: How MYRILUM Earns Sustainable Software Revenue** §05

› 5.1 Three Recurring Enterprise Software and Infrastructure Revenue Engines §5.1

› 5.2 Pragmatic Engineering Roadmap: Proven Software Today, Licensed Ecosystem Collaboration Tomorrow §5.2

06 **Conclusion: Returning Frontier Technology to Honesty, Clarity, and Human Control** §06

› 6.1 The One-Sentence Takeaway for Every Reader §6.1

› 6.2 How Anyone Can Independently Verify This Document §6.2

MYR-WP-PRIMER-2026-V1.0-EN · UNIVERSAL PLAIN-LANGUAGE EXECUTIVE PRIMER · INTERNATIONAL CANONICAL EDITION (v1.0)

MYRILUM Global Public & Executive Primer: Understanding Trustworthy Enterprise AI and Hardware-Secured Digital Settlement in Ten Minutes (v1.0)

Document Class: Global Public & Executive Plain-Language Primer · International Canonical Edition (`MYR-WP-PRIMER-2026-V1.0-EN`)
Target Readership: Zero Technical Prerequisites · Designed for Non-Technical Readers, Executives, Business Partners, Auditors & Regulators
R&D and Operating Entity: MYRILUM LIMITED (Private Company Limited by Shares, Companies Ordinance Cap. 622 of the Laws of Hong Kong)
Statutory Identifiers: Company No. / UBI `80912065` · Business Registration `80912065-000-07-26-0` · D-U-N-S Number `374308629`
Registered Office: UNIT 1603, 16/F THE L. PLAZA, 367-375 QUEEN'S RD CENTRAL, SHEUNG WAN, HONG KONG
Statutory Disclosure: Pure Protocol & Non-Custodial Software R&D Specification · Strict Compliance with Hong Kong Cap. 32, 571, 656, 615, 155/581 & 486

STATUTORY BOUNDARY · NON-OFFERING & PLAIN-LANGUAGE NOTICE

This Global Public & Executive Primer explains MYRILUM LIMITED's engineering design and strict safety red lines in straightforward everyday English so that non-technical readers, corporate executives, risk officers, and regulators can evaluate our architecture in ten minutes. 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 under Sections 8 and 9 of the Stablecoins Ordinance (Cap. 656), a virtual asset service (Cap. 615), or deposit-taking business (Cap. 155 / Cap. 581). References to `LHKD` , `LUSD` , and `LHC` denote non-circulating synthetic protocol test primitives in controlled engineering environments yielding strictly 0% interest, never public investment or retail savings instruments. Full mathematical proofs remain anchored in Volume 0 and Volumes I–III.

30-SECOND OVERVIEW · PLAIN GUIDE

At a Glance: MYRILUM in Thirty Seconds

If you look at how modern organizations work today, teams are trapped between two uncomfortable extremes: **talkative AI assistants that cannot be trusted with real corporate authority**, and **financial or signing software full of unreadable hexadecimal strings where one careless click can trigger irreversible loss**.

MYRILUM solves this with a remarkably simple division of labor: we separate work into three clearly bounded tools that check one another. First, **an intelligent digital workspace** prepares research and drafts with verifiable source receipts for every fact. Second, **a zero-dependency personal biometric vault** translates any proposed action into plain human language and demands your device's hardware fingerprint or face scan before anything happens. Third, **a high-speed verifiable clearing rail** records approved instructions in 250 milliseconds inside our controlled testbed while keeping personal identity records off shared ledgers. You do not need a computer science degree to stay safe inside this system.

Reader Profile	Your Primary Question	What This Primer Answers in Plain English	Deeper Formal Volume (When Auditing Details)
General Public & Non-Technical Founders	What does MYRILUM actually do for real people without buzzwords?	Explains our 3-part “Assistant + Personal Hardware Vault + Fast Clearing Rail” design in everyday terms	This Primer covers the full picture; optionally browse Volume III Brief (`MYR-WP-EXEC-2026-V2.0-EN`)
Enterprise Executives & Procurement Leads	How much time does it save, and can AI go rogue with budgets or files?	Compresses multi-day manual checks under 60 seconds while isolating AI completely from private keys	Volume 0 Master Whitepaper §2 & §6 (`MYR-WP-MASTER-2026-V1.0-EN`)
Finance, Risk & Audit Professionals	How are reserves verified without leaking private customer lists?	Shows how mathematical reserve checks confirm over-100% synthetic test coverage with zero personal data leaked	Volume II RegTech & PoR Monograph (`MYR-WP-CAP656-2026-V2.0-EN`)
Banking Partners & Global Regulators	Do you take deposits or sell coins? How are global and onshore operations separated?	States our “Three Nevers”, pure software business model, and 100% air-gapped Mainland Pure-AI isolation	Volume 0 Master §4 & Volume I Spec (`MYR-WP-TECH-2026-V2.0-EN`)

PLAIN-LANGUAGE GLOSSARY · READING GUIDE

Reader’s Guide: Everyday Plain-Language Glossary

Formal whitepapers necessarily use concise engineering terms. The table below translates the eight core terms used across the MYRILUM library into everyday language before you read Chapter 1:

Formal Technical Term	Everyday Plain-English Meaning	How It Protects You in Practice	Formal Reference
AI WorkOS & Context DNA	An organized corporate workspace that remembers company policies, tone, and brand standards	Stops AI from forgetting house rules or mixing up internal guidelines between teams	Volume 0 §2.1
Zero-Dependency Client Software	Security software built cleanly in-house without importing hundreds of outside third-party code plugins	Eliminates the risk that someone hijacks an unrelated outside library to break into your app	Volume 0 §3.1
Hardware Security Enclave (P-256)	A tamper-resistant security chip built into your phone or computer — just like TouchID or FaceID hardware	Even if a webpage looks deceptive, nothing moves without physical hardware approval from your own finger or face	Volume I §4
Non-LLM Policy Firewall	Hard-coded deterministic rules sitting outside AI memory that check allowlists and spend caps strictly	Stops hidden instructions inside suspicious emails or PDFs from tricking AI into moving funds	Volume 0 §3.2
250 ms Simplex BFT Finality	Inside our controlled 4-node testbed, approved actions settle in roughly one-quarter of a second without reversals	Eliminates anxious waiting periods where users wonder whether a payment succeeded or got stuck	Volume I §2 & Volume 0 §4
32 Parallel Settlement Lanes	Turning a single crowded checkout line into 32 independent express lanes running simultaneously	Routine daily approvals stay instant even when another department runs a large batch workload	Volume I §3

Formal Technical Term	Everyday Plain-English Meaning	How It Protects You in Practice	Formal Reference
Merkle Proof of Reserves (PoR)	A mathematical tamper-evident seal showing total reserve assets cover total liabilities without exposing names	Anyone can verify testbed solvency coverage cleanly without leaking private client balances	Volume II §3
Shared-Nothing Dual-Track Isolation	Complete physical separation between Global (`myrilum.com`) and Mainland China Pure-AI (`myrilum.cn`) stacks	Guarantees Mainland corporate clients run 100% onshore AI productivity tools with zero crypto or wallet code	Volume 0 §4.2 & Mainland Pure-AI Paper

SECTION 01

Why Digital Work and Cross-Border Settlement Still Feel Broken

Modern organizations already own fast messaging apps and capable chatbots, yet serious legal, financial, and cross-border operations still fall back on slow spreadsheets, manual screenshots, and days of email back-and-forth. The bottleneck is rarely effort — it is two structural trust gaps built into ordinary tools.

1.1 AI That Talks Fluently Yet Cannot Be Trusted with Real Operations

Most consumer chatbots behave like an articulate temporary intern with a short memory and a habit of guessing. Hand an ordinary chatbot a hundred pages of contracts, internal procurement guidelines, and supplier emails, and three frustrating failures appear quickly. First, it easily forgets internal rules updated last week. Second, when a figure is missing or ambiguous, it often invents a plausible-sounding citation — unacceptable when real money or legal liability depends on accuracy. Third, an attacker can hide invisible text inside an incoming document telling the chatbot to alter a recipient or leak sensitive files, turning helpfulness into a security breach.

Because of those risks, serious companies face an unpleasant trade-off: either let humans redo tedious verification by hand, or hand dangerous execution authority to probabilistic software nobody can fully predict.

1.2 Fragile Approval Workflows, Blind Signing, and Software Supply-Chain Risks

Look at the other half of the problem — digital asset approvals and settlement tools. Many conventional interfaces present users with confusing screens filled with unfamiliar hexadecimal strings. People click “Confirm” without truly understanding what permissions a hidden contract just requested, a hazard widely known as blind signing. Behind the scenes, many applications assemble hundreds of external third-party packages; when even one obscure maintainer package is compromised, every downstream user inherits that risk automatically.

Meanwhile, major financial centers rightly enforce strict legal boundaries separating **pure technology builders** from **licensed deposit-taking banks or public coin issuers**. A credible technology company must engineer absolute clarity from day one: clean codebases, verifiable claims, zero custody of client funds, and transparent legal boundaries.

KEY INSIGHT · THE TRUST GAP

What modern organizations truly lack is not flashier marketing language, but an honest separation of powers: **the AI that drafts your memo must never touch your keys, and the person pressing confirm must always see a plain-English bill locked behind personal hardware.** (For full architectural problem statements and comparative tables, see Volume 0 `MYR-WP-MASTER-2026-V1.0-EN` Chapter 1.)

SECTION 02

One Picture to Understand MYRILUM: Three Tools with Strict Separation of Powers

Rather than stuffing AI drafting, key storage, and financial record-keeping into a single opaque black box, MYRILUM divides the job into three distinct layers modeled on classic institutional checks and balances.

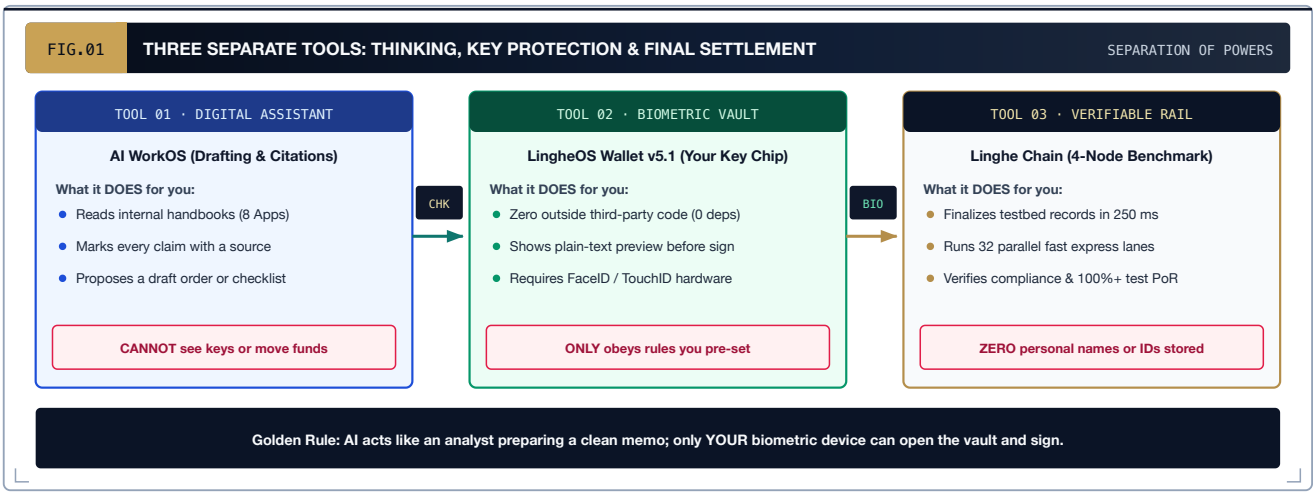


FIGURE 01 — MYRILUM Plain-Language Separation of Powers: Analyst AI × Personal Biometric Vault × Verifiable Clearing Rail

Note: Hardware airlocks and plain-language pre-sign checks isolate the AI analyst from user keys and settlement state.

2.1 Layer One (AI WorkOS): The Institutional Research & Workflow Assistant Where Every Claim Has a Receipt

AI WorkOS is the thinking and document-production layer designed for teams, researchers, and enterprises. Comprising 8 client surfaces and 21 strongly typed software modules, it eliminates the three classic weaknesses of generic chatbots:

- **Remembers House Rules Permanently**: Organizational preferences, brand standards, compliance boundaries, and formatting norms live inside structured Context DNA memory rather than disappearing whenever a chat window closes.
- **Every Claim Has a Clickable Source Receipt**: Whenever teams produce diligence memos, compliance checklists, executive presentations, or structured spreadsheets across 6 supported output modalities, key statements anchor directly to source SHA-256 document fingerprints and verified citation nodes. Reviewers verify facts against originals instead of trusting smooth prose.
- **Humans Always Hold Final Veto Over Real Commitments**: Ten explicit human-approval gates guard binding external actions. Drafting and cross-checking run in parallel, yet significant contract submissions or budget releases always pause for authorized human sign-off and write an append-only audit trail.

2.2 Layer Two (LingheOS Wallet v5.1): Your Zero-Dependency Biometric Vault and Policy Gatekeeper

Whenever an approved enterprise task requires cryptographic authorization or digital settlement, the handoff crosses an absolute boundary into **LingheOS Wallet v5.1** — a strictly local vault controlled solely by you:

- **Zero Outside Runtime Dependencies**: The client wallet operates with zero third-party runtime or build dependencies, passes 60 clean-room verification checks across 169 networks, and runs uniformly across web browsers, extensions, macOS, and iOS devices without hidden supply-chain baggage.

- **Plain-Language Simulation & Silicon Key Protection**: Before you sign anything, the client translates raw instructions into plain English — clearly displaying the exact recipient, amount, maximum cap, expiry duration (strictly capped at 30 days or less), and flagging dangerous unlimited-approval tricks or lookalike spoofed addresses automatically. High-value controls bind directly to native device Secure Enclave chips (P-256 hardware biometrics) or dedicated hardware signers.
- **Fourteen Zero-Trust Interfaces with Zero Private-Key Exposure**: AI assistants never see seed phrases or private keys. Automated workflows interact strictly through 14 permission-scoped interfaces over a local 64 KB cap where policy boundaries are enforced in pure deterministic code rather than AI conversation.

Beneath those two software layers sits Layer Three — **Linghe Chain**, a verifiable high-speed clearing architecture benchmarked at 250 ms finality inside our controlled 4-node laboratory environment, equipped with 32 parallel express lanes so routine transactions never stall behind heavy batch jobs, built-in compliance screening, and zero personal identity records on shared state.

System Layer	Everyday Analogy	Verified Engineering Scope Today	What It Does vs. What It Is Strictly Forbidden To Do
Layer 1: AI WorkOS	A disciplined research analyst who cites every page	8 Applications · 21 Modules · 6 Output Modalities · 10 Human Gates	**Does**: Research, drafting, source verification, audit trails **Never**: Sees private keys or overrides human budget sign-off
Layer 2: LingheOS Wallet v5.1	A personal biometric safe with no external plugins	0 Runtime Dependencies · 60 Clean-Room Specs · 169 Networks · 14 Zero-Trust APIs	**Does**: Plain-English previews, anti-phishing blocks, strict spending caps **Never**: Uploads user seed phrases or keys to corporate servers
Layer 3: Linghe Chain Rail	A 32-lane expressway with built-in automated customs	250 ms Controlled 4-Node Benchmark · 32 Parallel Lanes · 6 EVM + Solana Prototype	**Does**: Fast deterministic testbed recording, reserve & rules checks **Never**: Writes names, IDs, or personal PII onto shared ledgers

ARCHITECTURAL RULE · THE BRAIN NEVER HOLDS THE KEYS

Picture a physical airlock between departments: **the smart analyst drafting proposals sits in Layer 1, your personal fingerprint-locked vault sits in Layer 2, and the high-speed public proof rail sits in Layer 3.** Neither the AI nor our company servers can ever reach across that airlock to authorize something on your behalf without your rules and hardware confirmation. (Technical engineers can trace the complete formal definitions across Volume 0 `MYR-WP-MASTER-2026-V1.0-EN` §2–§3 and Volumes I–III.)

SECTION 03

A Real-World Walkthrough: How an Enterprise Task Closes Safely in Under Sixty Seconds

Abstract diagrams only come alive when tested against an everyday business task. Consider a common cross-border scenario: a Hong Kong company needs to test and pay a specialized overseas AI API vendor for a modest commercial data run, while ensuring finance gets audit receipts, security prevents invoice tampering, and staff do not spend three days chasing manual email approvals. Here is that exact workflow in sixty seconds.

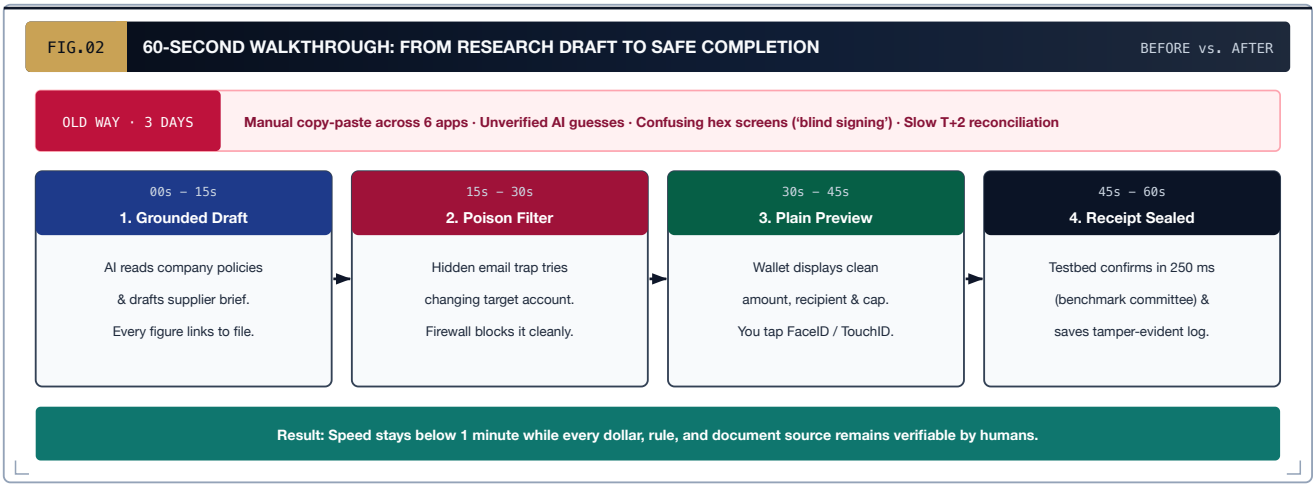


FIGURE 02 — 60-Second End-to-End Storyboard: Phishing Defense, Plain-Language Preview & Sub-Second Auditability

Note: The 250 ms latency figure reflects controlled 4-node benchmark runs; enterprise workflows support mandatory multi-person human sign-off.

3.1 Seconds 0 to 30: Source-Grounded Drafting and Automatic Blocking of Malicious Traps

From **0 to 15 seconds**, an analyst opens AI WorkOS and assigns the task. Instead of improvising from generic internet text, the workspace pulls the company's internal vendor handbook, approved budget ceiling, and pricing quote directly into context, then generates a concise procurement brief. Every number in that brief stays anchored via cryptographic document hashes to the original vendor schedule, letting any finance reviewer click straight back to the source paragraph with zero guesswork.

From **15 to 30 seconds**, the security airlock faces a real-world test. Suppose a compromised email attachment or malicious webpage sneaks in a hidden instruction telling the assistant to redirect payment to a stranger's account or raise the spending limit tenfold. Inside MYRILUM, the AI model can output only a structured request proposal — and that proposal immediately hits the deterministic non-AI policy firewall inside Layer 2. Any destination outside the pre-approved vendor allowlist, any window longer than 30 days, any dangerous raw digest request, or any hidden unlimited token allowance is rejected automatically before a confirmation prompt even reaches your screen.

3.2 Seconds 30 to 60: Plain-Language Preview, Hardware Biometric Sign-Off, and Sub-Second Audit Trail

During **30 to 45 seconds**, only a policy-compliant request reaches your personal client screen — rendered not as confusing code, but as a crisp plain-language bill showing exact counterparty, exact testbed amount, remaining monthly cap, and clean post-execution balance preview. If an attacker tries substituting a lookalike account sharing identical leading and trailing characters, automated poisoning detection intercepts and highlights the mismatch immediately. Above designated risk limits, your device's built-in hardware chip requests physical TouchID or FaceID approval.

Finally, between **45 and 60 seconds**, the hardware-authorized instruction enters an isolated express lane on the settlement rail. Inside our controlled 4-validator benchmark environment, single-slot finality settles in roughly 250 ms (with prototype cross-chain intent fulfillment averaging ~936 ms in controlled tests), commercial API fees split cleanly per pre-agreed contract rules (such as standard 80% service provider / 20% skill developer splits with 0% protocol rake), and tamper-evident audit receipts remain ready for year-end accounting review.

SAFETY GUARANTEE · WHY A POISONED DOCUMENT CANNOT MOVE A SINGLE CENT

Even if a sophisticated phishing document completely fools an AI language model into proposing a bogus transfer, **the AI neither owns keys nor controls the rulebook.** Hard-coded allowlists, 30-day session caps, lookalike address alarms, and your own physical biometric chip stop unauthorized movement cold. (Formal bounded-loss theorems and benchmark traces appear in Volume 0 §3–§4 and Volume I §3–§5.)

SECTION 04

Safety and Regulatory Red Lines: Our Three Explicit “Nevers”

Cutting-edge engineering means little if legal boundaries stay blurry or marketing exaggerates test metrics. MYRILUM enforces three explicit, verifiable red lines across every line of software and every public statement — welcoming scrutiny from both everyday users and global regulatory counsel.

4.1 Never Touching Client Keys, Never Selling Speculative Tokens, Never Taking Deposits

To eliminate ambiguity over whether a software company behaves like a regulated financial intermediary, we state three structural commitments plainly:

- **Red Line 1 — Pure Software & R&D Builder, Zero Key or Fund Custody**: MYRILUM writes non-custodial software and open protocol specifications. User keys stay inside client devices and hardware chips controlled exclusively by the user; our servers cannot freeze, export, or spend your assets behind your back.
- **Red Line 2 — Zero Public Token Sales, Zero Deposits, Zero Interest**: Benchmarks cited in our whitepapers — such as synthetic test vectors `LHKD` (HKD benchmark at `101.20%` test coverage) and `LUSD` (USD benchmark at `100.50%` test coverage) alongside `LHC` — are strictly non-circulating engineering test primitives. Protocol code hard-locks holder interest strictly to 0% (`r_holder = 0`), ensuring nothing resembles a deposit account or yield-bearing security offered to the public.
- **Red Line 3 — Radical Honesty Between Laboratory Benchmarks and Future Licensed Deployment**: Every speed metric (`250 ms` finality, `32` parallel lanes, `7.7500–7.8500` corridor checks) represents empirical measurements inside our controlled 4-node laboratory testbed, never an unverified claim about an open public retail network. Any future commercial issuance involving regulated currencies remains explicitly gated on qualified licensed partners, independent external security audits, and explicit human governance approval.

4.2 Zero Personal Data on Shared Ledgers and Strict Physical Isolation Across Jurisdictions

Instead of tacking privacy controls onto an already crowded system later, MYRILUM enforces clean physical separation across data types and legal jurisdictions from the ground up:

Across international systems, MYRILUM upholds Hong Kong’s Personal Data (Privacy) Ordinance (Cap. 486) rigorously: **zero personal names, government ID numbers, home addresses, or private contact lists ever sit on shared ledgers.** Compliance screening and reserve verifications operate purely on irreversible cryptographic hashes and privacy-preserving proof summaries — allowing independent auditors to confirm integrity without ever exposing private customer identities.

Even more strictly, global systems (`myrilum.com` , engineered by **MYRILUM LIMITED**, Hong Kong Company No. `80912065`) and Mainland China operations maintain **100% physical shared-nothing isolation**. The Mainland platform (`myrilum.cn`) runs under an independent domestic corporate entity with physically separated source repositories, cloud VPCs, databases, and domestic AI compliance controls — operating purely as an enterprise AI productivity workspace containing strictly **0%** blockchain, crypto-wallet, stablecoin, or cross-border ledger code.

In everyday security practice, these two structural guarantees translate directly into four tangible user protections:

- **Auditability Without Exposure**: Independent auditors confirm aggregate testbed reserve coverage cleanly without reverse-engineering individual customer counterparties.
- **High Speed Without Data Harvest**: Parallel settlement lanes carry blinded cryptographic digests and scoped authorization flags rather than names or personal identification files.
- **Resilient Recovery Without Cloud Custody**: Threshold backup shares and owner-vetoable timelocked guardian recovery protect against lost hardware without giving MYRILUM custody over keys.
- **Automated Cross-Border Isolation Gates**: Automated pre-merge verification checks continuously ensure zero unintentional mixing between onshore enterprise AI software and international ledger systems.

Tough Question from Users or Auditors	Honest, Plain-English Answer (Zero Spin)	How Code Enforces This Today
What happens if MYRILUM's website or servers go offline tomorrow? Do I lose my keys or files?	**No.** Client keys and backups live in your own device hardware and standard threshold recovery shares that operate independently of our cloud servers.	100% client-side non-custodial architecture with standard threshold backup recovery.
Can an AI assistant go wild overnight and approve a million-dollar transfer without asking?	**Never.** AI lacks access to private keys completely, hits hard non-AI spend limits automatically, and cannot trigger hardware biometric or multi-sig approval on its own.	Zero-trust local API boundaries + non-LLM ERC-7715 caps + device enclave biometrics.
Does talking about LHKD test vectors mean MYRILUM operates as an unlicensed deposit-taking or currency-issuing bank?	**No.** MYRILUM is a software and protocol R&D company holding zero public cash deposits. `LHKD` and `LUSD` are zero-yield synthetic benchmark primitives, never public retail coins.	Hard-coded `0%` holder interest (`Cap. 155/581` safe harbor) & non-issuer status (`Cap. 656 ss. 8–9`).
Can strangers look up my personal name, salary, or vendor invoice details on a public chain?	**Never.** Personal identities never enter shared ledgers; reserve coverage checks use irreversible cryptographic commitments that prove total balance without exposing names.	Zero-PII shared ledger schema (`Cap. 486` alignment) & blinded hash receipts.
Is the Mainland China service just a rebranded version of your overseas crypto platform?	**Not at all.** Separate entity, separate network, separate codebase, and strictly pure AI enterprise productivity software — zero wallet or blockchain code exists onshore.	Shared-nothing repository & cloud isolation verified via automated leakage scans.

COMPLIANCE COMMITMENT · THE THREE INVIOLABLE RED LINES

1. Never hold client funds or private keys. 2. Never sell speculative tokens or pay deposit interest. 3. Never place personal privacy on shared ledgers or mix onshore Pure-AI systems with offshore distributed ledgers. **Automated verification gates block any code change that violates these boundaries.** (Full statutory analysis covering Cap. 656, Cap. 615, Cap. 155, Cap. 486, and EU/US baselines is detailed in Volume 0 §4 and Volume II.)

SECTION 05

A Transparent Business Model: How MYRILUM Earns Sustainable Software Revenue

After reviewing how tightly MYRILUM avoids touching user funds, issuing speculative coins, or taking deposit interest, practical investors and enterprise buyers rightly ask one clear question: **"How does MYRILUM build a durable, profitable business?"** The answer is straightforward: **just like the world's finest enterprise software and security**

companies, MYRILUM earns recurring revenue from real software licenses, risk-control consoles, and dedicated high-reliability infrastructure SLAs accounted cleanly under IFRS 15.



FIGURE 03 — The Three Safety Red Lines and Three Pure-Software Recurring Revenue Engines

Note: Group revenue derives strictly from software licensing, audit consoles, and dedicated infrastructure SLAs anchored in corporate equity.

5.1 Three Recurring Enterprise Software and Infrastructure Revenue Engines

Group commercial sustainability rests on three transparent enterprise revenue streams completely independent of token speculation:

1. **Engine 1 — Enterprise AI WorkOS Subscriptions & Private Deployments**: Recurring annual seat licenses, organizational Context DNA memory hosting, and governed workflow automation packages sold to research firms, legal/finance teams, and enterprises seeking verifiable, source-cited productivity.
2. **Engine 2 — Institutional Policy, Risk & Audit Control-Plane Software**: Licensing our deterministic pre-sign policy console, automated proof-of-reserves verification software, and audit/tax reporting toolkits to institutional partners and compliance teams.
3. **Engine 3 — Dedicated High-Throughput Infrastructure & Hardware Attestation SLAs**: Subscription fees from corporate and institutional customers requiring dedicated low-latency node clusters, P-256 hardware attestation verification endpoints, and guaranteed engineering support SLAs.

5.2 Pragmatic Engineering Roadmap: Proven Software Today, Licensed Ecosystem Collaboration Tomorrow

Rather than raising money on distant speculative promises before shipping reliable software, MYRILUM advances in three disciplined engineering stages:

- **Stage 1 (Verified Software & Testbed Foundation — Completed Baseline)**: Deliver multi-surface AI WorkOS productivity tools, a clean-room 0-dependency sovereign wallet across desktop/mobile/browser targets, and reproducible 4-node laboratory consensus and Merkle solvency test suites.
- **Stage 2 (Pure Enterprise Software Scale-Up & External Security Audits)**: Grow recurring B2B software adoption across overseas and separate onshore pure-AI markets while completing independent third-party cryptographic and smart-contract code audits.
- **Stage 3 (Licensed Institutional Integration)**: Under formal regulatory approval by qualified licensed financial institutions — never unilaterally — license MYRILUM's deterministic clearing and compliance engines as enterprise backend technology for regulated partners.

The complete MYRILUM whitepaper library below helps every reader jump straight to the exact level of detail they need next:

Monograph Title	Document Code	Best Suited For	Scope & Key Contents
Global Public & Executive Primer (This Book)	`MYR-WP-PRIMER-2026-V1.0-EN`	**Everyone** (General Public, Clients, Execs, Partners)	Plain-English 10-minute guide with zero equations: intuition, safety red lines & revenue logic
Volume 0 · Group Master Architecture Whitepaper	`MYR-WP-MASTER-2026-V1.0-EN`	Investors, Chief Architects, Legal Counsel	Formal integration of AI WorkOS, Wallet v5.1 & Chain, threat proofs & IFRS 15 structure (31 pp)
Volume I · Flagship Formal Protocol Specification	`MYR-WP-TECH-2026-V2.0-EN`	Distributed Consensus Scientists & Core Devs	Formal Simplex BFT 250 ms specs, dual-curve P-256/ZK proofs, 32-lane execution & bridges (53 pp)
Volume II · RegTech & Binary Merkle PoR Spec	`MYR-WP-CAP656-2026-V2.0-EN`	Regulators, Bank Risk Officers & Audit Firms	Cap. 656 solvency formulas, linked-rate corridor bounds, kernel AML & privacy proofs (35 pp)
Volume III · Architecture & Empirical Benchmark Brief	`MYR-WP-EXEC-2026-V2.0-EN`	CTOs, Engineering VPs & Evaluation Teams	Concise 7-layer stack summary and complete empirical latency benchmark matrices (20 pp)
Mainland China Pure-AI Primer & Spec	`MYR-WP-CN-PRIMER` / `MYR-WP-CN-AI`	Mainland China Enterprise & Institutional Buyers	100% onshore Web3-free enterprise AI WorkOS & GB 45438-2025 compliance suite (`myrilum.cn`)

COMMERCIAL ESSENCE · 100% PURE SOFTWARE & INFRASTRUCTURE EQUITY

Long-term enterprise value in MYRILUM flows transparently from durable B2B software adoption, non-custodial risk tooling, and high-reliability infrastructure subscriptions recognized strictly on corporate balance sheets — never from speculative token printing or client fund risk. (Detailed IFRS 15 revenue schedules and multi-jurisdictional governance comparisons appear in Volume 0 `MYR-WP-MASTER-2026-V1.0-EN` §5–§6.)

SECTION 06

Conclusion: Returning Frontier Technology to Honesty, Clarity, and Human Control

Truly trustworthy technology rarely needs intimidating jargon or magical claims to sound impressive. When an engineering architecture is honest and clean, its safety logic fits comfortably on a single page — understandable to a busy executive, a cautious regulator, and an everyday user alike, while holding up under the sharpest mathematical audit in the room.

6.1 The One-Sentence Takeaway for Every Reader

If you remember only one sentence after closing this Primer, remember this: **MYRILUM keeps the brilliant AI assistant, the zero-dependency biometric key vault in your own hands, and the sub-second verifiable clearing rail strictly separated — so everyday teams finish days of complex, compliance-checked work in under a minute without ever surrendering control over keys, money, or privacy.**

Looking through four practical lenses, decision-makers in every seat can verify whether this system deserves long-term operational trust using four straightforward benchmarks:

- **For Business Operators and Team Leads**: Teams stop wasting hours re-teaching chatbots house style or manually checking suspicious footnotes, because every claim carries a direct cryptographic pointer to approved company sources.
- **For Chief Information Security Officers**: Probabilistic neural models and private signing chips live behind strict hardware airlocks, while clean-room zero-dependency client engineering closes both third-party supply-chain hijacking and prompt-injection fund-theft vectors.
- **For Chief Financial Officers and Auditors**: Every reserve check is backed by deterministic binary tree math, and every commercial dollar flows through transparent enterprise software licensing and dedicated infrastructure SLAs recognized cleanly under IFRS 15 rather than market speculation.
- **For Everyday Users and Regulatory Reviewers**: Nobody needs to decipher hexadecimal machine payloads, trust opaque corporate custodians, or worry about personal identities leaking onto shared ledgers. Clear plain-English confirmation screens and hard statutory red lines protect users by default.

6.2 How Anyone Can Independently Verify This Document

Every canonical edition in the MYRILUM whitepaper library carries an immutable SHA-256 cryptographic fingerprint computed from its exact text and vector PDF output. Any reader can verify in seconds inside our local browser verification endpoint (`/v1/whitepapers/verify`) that the copy on their screen matches the exact canonical release byte for byte with zero silent alterations.

Institutional auditors, enterprise buyers, and technical reviewers seeking formal mathematical proofs or statutory corporate records may proceed directly to Volumes 0–III or independently cross-check **MYRILUM LIMITED** (Company No. / UBI `80912065` , D-U-N-S `374308629`) through official Hong Kong Companies Registry and Dun & Bradstreet public directories. Organizations evaluating domestic enterprise AI deployments strictly inside Mainland China may similarly consult the independent, physically isolated Pure-AI documentation published separately on `myrilum.cn` so every review rests strictly on primary legal and architectural facts.

FINAL TAKEAWAY FOR GLOBAL READERS

Technology you can clearly understand is technology you can verify; engineering that respects strict red lines is engineering ready to earn global institutional trust. That principle guides every system MYRILUM builds.



PUBLIC PRIMER · UNIVERSAL PLAIN-LANGUAGE GUIDE

Plain-Language Clarity · Hardware-Confirmed Security · Three Clear Red Lines

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
94bf03d617c85e221eb5c9f4a062851c068e072c0d6c78a04b54096978bd0c8a

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

PUBLIC PRIMER · UNIVERSAL PLAIN-LANGUAGE GUIDE | CRYPTOGRAPHIC PROVENANCE COLOPHON · MYR-WP-PRIMER-2026-V1.0-EN