W3CR-WP-2026-06 | Division VII & VIII | Computational Law, Zero-PII Automata & Systemic Stability | Published 2026/11/23

Enshrined Computational Law: Kernel TIP-403 Automata, Zero-PII Travel Rule Envelopes, and Merkle Proof-of-Reserve

Institutional Attribution (COPE): Web3 Capital Research - Divisions VII & VIII
Computational Law & Systemic Stability Working Group

ACM Reproducibility Badges: Artifacts Available | Artifacts Functional | Results Reproduced

ABSTRACT

Public settlement ledgers confront a fundamental trilemma between statutory non-circumvention, personal data protection, and continuous solvency verifiability: application-layer ERC-20 blacklists are routinely bypassed via wrapper contracts or cross-chain solvers, naive Travel Rule logging leaks personally identifiable information (PII) onto immutable ledgers, and cached Proof-of-Reserve (PoR) dashboards mask upstream insolvency faults. Building on deontic logic, we compile multi-jurisdictional compliance invariants directly into kernel-enshrined state automata. First, the Rust-level TIP-403 Policy Registry enforces O(1) authorization across all six balance-mutating pathways, proving zero regulated balance mutation for restricted addresses. Second, a dual-track FATF Recommendation 16 engine combines 24-hour sliding anti-structuring windows (HK$7,800.00 single / US$5,000.00 cumulative) and POSIX 0600 atomic write-ahead persistence with salted Keccak-256 commitments achieving zero on-chain PII bytes (I(PII; pi) = 0). Third, domain-separated LINGHE_CAP656_HQLA_V1 sorted binary Merkle trees, Euclidean floor contraction within the [7.7500, 7.8500] corridor, and fail-closed HTTP 503 telemetry guarantee zero false-positive solvency reporting.

FORMAL THEOREM - Theorem 6.1 (Complete Sanctions Non-Circumvention, Zero-PII Mutual Information & Fail-Closed Solvency)

Let S_h denote the restricted address set in kernel precompile TIP-403 (0x403c...0000) at block height h, let pi denote on-chain Travel Rule and KYB commitments anchored in 0x8800...0001 and 0x8004...0001 under high-entropy 256-bit off-chain VASP salts in the Random Oracle Model, and let R_Merkle be the sorted binary Merkle root over domain-separated leaves ell_i = Keccak256('LINGHE_CAP656_HQLA_V1' || symbol_i || bic_i || mask_i || val_i || days_i). Then: (1) across every valid state transition (direct transfer, 0x76 batch, session spend, enshrined CLOB, ERC-7683 omnichain fill, and BN254 ZK withdrawal), any u in S_h satisfies Delta Bal_reg(u) === 0; (2) on-chain plaintext PII storage is 0 bytes with mutual information I(PII; pi) = 0 up to 2^-256 preimage bound, while POSIX 0600 atomic rename preserves exact 24h anti-structuring state across arbitrary crashes; and (3) Euclidean corridor swaps over [77500, 78500] satisfy f_HKD->USD(f_USD->HKD(x)) <= x and fail-closed telemetry yields Pr[rho_hat_t >= 100% | not Healthy_t] === 0 (HTTP 503).

FALSIFIABLE EMPIRICAL BENCHMARK METRICS

[LINGHE_CAP656_HQLA_V1] Domain-Separated Merkle PoR - O(log N) sorted binary inclusion verifying 101.20% LHKD & 100.50% LUSD synthetic vectors
[0 B (I(PII; pi) = 0)] On-Chain Plaintext PII Bytes - Salted Keccak-256 commitments over HK$7,800.00 / 24h windows + POSIX 0600 atomic WAL
[HTTP 503 -> 0.00%] Upstream-Loss Solvency Gate - 2,500 ms AbortController + no-store

telemetry zeroing stale PoR gauges upon fault
[[7.7500, 7.8500]] Synthetic Corridor Bounds - Bytecode-locked [77500, 78500]
Euclidean floor contraction preventing rounding drains

1. PROBLEM FORMULATION & SYSTEM MODEL

Translating statutory financial and data-protection mandates - formalized since von Wright (1951) as deontic modalities of obligation, permission, and prohibition - into distributed state machines exposes three architectural vulnerabilities. First, perimeter-only Solidity token blacklists are trivially circumvented when restricted entities wrap tokens into secondary vaults or instruct clean cross-chain solvers to deliver funds to fresh destination addresses. Second, storing plaintext originator or beneficiary attributes on-chain to satisfy FATF Recommendation 16 irreversibly violates data minimization and erasure principles under Singapore PDPA 2012, Hong Kong Cap. 486 PDPO, and EU GDPR. Third, solvency dashboards that serve cached ratios during RPC timeouts create dangerous false-positive assurance during Diamond-Dybvig (1983) liquidity stress.

We model a regulated settlement state machine in which synthetic, non-circulating benchmark units (LHKD and LUSD , strictly satisfying S_token === 0 and r_holder === 0 with zero retail bank deposits or issued liabilities) transition exclusively through kernel-enshrined compliance, corridor, and Merkle Proof-of-Reserve predicates.

2. FORMAL CONSTRUCTION & MATHEMATICAL PROOF

Our formal construction unifies three decidable cryptographic automata:

- Kernel TIP-403 Complete State-Space Non-Circumvention: Enshrined Rust precompile 0x403c...0000 gates all six balance-mutating pathways - direct transfers, type- 0x76 parallel batches, SessionKeyManager spends, enshrined CLOB matching (0xdec0...0000), ERC-7683 dual-party origin/recipient screening, and BN254 Groth16 bridge releases - in [Formal Mathematical Expression] memory lookups, ensuring [Formal Mathematical Expression] for every restricted address [Formal Mathematical Expression] .

- Zero-PII Travel Rule & Crash-Idempotent Anti-Structuring: Transfers reaching US$1,000.00 (HK$7,800.00) singly or US$5,000.00 across a unified 24-hour sliding window [Formal Mathematical Expression] require an off-chain TLS 1.3 VASP envelope (halting with RFC 7725 HTTP 451 otherwise). Only salted 32-byte Keccak-256 digests are anchored on-chain (0 B plaintext PII, [Formal Mathematical Expression]), while synchronous POSIX 0600 temp-file write-ahead rename prevents restart-based structuring evasion.

- Domain-Separated Merkle PoR & Corridor Contraction: Reserve tranches hash under "LINGHE_CAP656_HQLA_V1" (Merkle, 1987) into lexicographically sorted binary trees verified on-chain against 0x8800...0001 . Bytecode-clamped corridor conversions over [Formal Mathematical Expression] ([7.7500, 7.8500]) enforce truncating division [Formal Mathematical Expression] , while telemetry probes bounded by 2,500 ms force exported coverage to 0.00% and return HTTP 503 upon any upstream fault.

3. EMPIRICAL EVALUATION & REFERENCE IMPLEMENTATION VERIFICATION

Independent verification against the synthetic genesis state vectors on ChainID 88888 reproduced exact four-leaf sorted Merkle roots for both non-circulating benchmark primitives: 0xa3e5fd1ee51db26128c49f848bc4eb6d71443fbfee51a40b9159832a21beae6e (101.20% modeled coverage, 24.12-day WAM, 54.39% 0-day cash tranche) for LHKD , and 0x5c3f82332fbffc0be49434232a9a97e2bf2c797423aa3fde4afd19b2c264f410 (100.50% modeled coverage, 25.47-day WAM) for LUSD .

Across adversarial compliance tests, all six wrapper/CLOB/omnichain sanctions-bypass

vectors reverted deterministically, multi-tx sub-threshold smurfing sequences summing to HK$7,800.00+ across process restarts triggered HTTP 451 with 0 bytes of plaintext PII written on-chain, out-of-band corridor mutations reverted with OUTSIDE_HKMA_BAND , and simulated upstream RPC severance transitioned health endpoints immediately to HTTP 503 with 0.00% reported ratio.

4. VERIFICATION PROVENANCE & COMPETING INTERESTS DISCLOSURE

COPE Authorship & Verification Provenance: Prepared and audited by the Divisions VII & VIII Working Group of Web3 Capital Research under Principal Investigator sign-off with zero invented personal names. Every leaf digest, sorted Merkle proof, corridor bound, and fail-closed telemetry transition is reproducible offline via W3AI-Bench v1.0 conformance vectors.

Statutory Safe Harbor & Competing Interests Disclosure: Published open-access (CC-BY-4.0) from the Republic of Singapore under Singapore SFA 2001, FAA 2001, PSA 2019, and PDPA 2012 safe harbors and EU AI Act Regulation (EU) 2024/1689 Article 2(6) & 2(8) exemptions. Neither Web3 Capital Research nor reference implementation author MYRILUM LIMITED (HK UBI 80912065 ; Hong Kong Cap. 615 non-VATP and Cap. 656 non-issuer R&D posture, https://myrilum.org/research and https://myrilum.io/) issues fiat-referenced tokens, accepts deposits, or solicits public funds; LHKD and LUSD denote strictly non-circulating synthetic test vectors.

VERIFIED REFERENCES

[MERKLE-1987] R. C. Merkle (1987). "A Digital Signature Based on a Conventional Encryption Function." Advances in Cryptology - CRYPTO '87, Lecture Notes in Computer Science, Vol. 293, pp. 369-378. https://doi.org/10.1007/3-540-48184-2_32

[DIAMOND-DYBVIG-1983] D. W. Diamond and P. H. Dybvig (1983). "Bank Runs, Deposit Insurance, and Liquidity." Journal of Political Economy, Vol. 91, No. 3, pp. 401-419. https://doi.org/10.1086/261155

[VON-WRIGHT-1951] G. H. von Wright (1951). "Deontic Logic." Mind, Vol. 60, No. 237, pp. 1-15. https://doi.org/10.1093/mind/LX.237.1

[RFC7725-451] T. Bray (2016). "An HTTP Status Code to Report Legal Obstacles (RFC 7725: 451 Unavailable For Legal Reasons)." IETF Request for Comments (RFC 7725). https://www.rfc-editor.org/rfc/rfc7725

[EU-AI-ACT-2024] European Parliament and Council of the European Union (2024). "Regulation (EU) 2024/1689 Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act), Article 2(6) & 2(8)." Official Journal of the European Union, OJ L, 2024/1689. https://eur-lex.europa.eu/eli/reg/2024/1689/oj

[SG-SFA-PSA-STATUTES] Parliament of Singapore (2020). "Securities and Futures Act 2001 (2020 Revised Edition) and Payment Services Act 2019 (2020 Revised Edition)." Singapore Statutes Online, Attorney-General's Chambers of Singapore. https://sso.agc.gov.sg/Act/SFA2001