Triple-Layer Integrity: Certificate of Authenticity and Provenance

Core Strategic Authority

Principal Architect & Signatory: **Aevust**

Verified by OpenTimestamps.org & GMO Sign

4 June 2026

Abstract. This certificate formalizes the **Triple-Layer Integrity Protocol** for the Rincoin ecosystem—a verification architecture ensuring academic provenance, cryptographic immutability, and institutional digital integrity.

1. **Academic Integrity (DOI):** Indexed via Zenodo (10.5281/zenodo.20674990) to ensure permanent visibility in the global academic record.
2. **Cryptographic Integrity (Bitcoin Anchor):** Anchored to the Bitcoin blockchain to provide an immutable timestamp and proof-of-existence (SHA256: `52692`...).
3. **Institutional Integrity (Digital Signature):** Secured via GMO Sign's third-party digital signatures to prevent any unauthorized tampering or post-dated alterations.

This framework ensures that the Rincoin whitepaper provides a timestamped, independently verifiable record.

---

1. Target Document Information

This certificate proves the existence and integrity of the following digital document at the recorded time.

DOI (Version 1.6.4): 10.5281/zenodo.20674990

File Name: `Tokino_Rincoin_v1.6.4.pdf`

SHA256 Digest: `5269207ea7e363e8df312ed50c00afc119b43e6fa5d3c717e6a7d8fc9863147b`
(Note: This hash must exactly match the SHA256 hash of the target file.)

2. Timestamp Details

The document's cryptographic digest is anchored to the Bitcoin Blockchain.

Timestamp Date: 2026-06-04 16:29:12 UTC

OTS File: `verification_data_v1.6.4.ots` (10.5281/zenodo.20674990)

Verification Tool: opentimestamps.org

(Upload the original PDF and OTS file here to verify the timestamp manually.)

3. Blockchain Anchors (Bitcoin Transactions)

The following Bitcoin transactions contain the Merkle Root verifying the document.

- **Transaction 1:**
  092cd81a5d0a57f39dbe442cb75cb46818d1b54d7c4bc8b7e6c1563145ad0d94
- **Transaction 2:**
  02023d4a1987dbcc43224ec8043a03a08f97731356dcbc654d45d89a2df42ba3
- **Transaction 3:**
  de597558a7d3a16cb63a080bb4b64daf1f5e2ad18bb76f67e823a771f0302773

4. Canonical Directory: Rincoin Pillars of Integrity

Last Updated: 2026-07-05

I. Academic & Sovereign Foundations

First Whitepaper & Origin: coin.rin.so
The original whitepaper and project origin site, maintained by Founder **ysmreg**.

Core Authority: rincoin.org
The official website of the Rincoin project, maintained by the Core Authority.

Protocol Integrity: rincoin.com
Hosts the cryptographic and institutional integrity proofs for the Rincoin protocol.

Scientific Provenance: doi.org/10.5281/zenodo.17141922
Rincoin's theoretical foundation, modeling **Regenerative Thermodynamic Security** via **SDE** and **Fokker-Planck dynamics**.

Ethos Document: doi.org/10.5281/zenodo.17590314
The Rincoin ethos and official logo, archived with a permanent DOI.

II. Technical Infrastructure

Origin Repository (GitHub): github.com/Rin-coin
The official source of truth for open-source development. Changes reach this repository only through reviewed pull requests, never direct edits.

Development & Staging Repository: github.com/rincoin-core
The development and staging repository for the Rincoin Core protocol.

Improvement Proposals (RIPs): rips.rincoin.org
The registry for Rincoin's improvement proposals, modeled after Bitcoin's BIP process. Proposals are drafted in the canonical repository, Aevust/rincoin-rips, created and maintained by Aevust, author of RIP-0001 through RIP-0011 and its inaugural RIP editor; consensus-critical RIPs require Core Strategic Authority approval.

Verification Suite: github.com/Aevust/rincoin-regenerative-simulations
The open-source Python framework validating Rincoin's macroeconomic homeostasis via Monte Carlo simulation of the protocol's long-term equilibrium.

Sandbox: github.com/Aevust/rincoin-sim (10.5281/zenodo.20363269)
A network-isolated `regtest` environment with hardcoded killswitches blocking mainnet connectivity, validating the **Customized Halving (Scenario II)** boundary values at 1/1000 scale and the full **MWEB** activation lifecycle.

On-Chain Explorer (Origin): explorer.rin.so
The Genesis Node documenting the historical launch and origin of Rincoin by our Founder **ysmreg**.

On-Chain Explorer (Basic): rinscan.org (explorer.rincoin.org)
The basic block explorer, managed by the Core Research & Core Authority Lead.

Browser Extension Wallet (Alpha v1.0.5): Chrome Web Store
The official portable gateway for RIN holders, developed by Founder **ysmreg**. This non-custodial implementation (Alpha) provides secure asset management through intuitive PIN-code authentication and encrypted local backup.

Protocol Architecture: hackmd.io/@agi/rJ4_2EWQZx
The blueprint of our code, embodying the Pure PoW and Fair Launch ethos.

III. Institutional Communication Hubs

Discord: discord.gg/H4Du5YuqFa
The official community hub for real-time discussion and coordination.

Announcements (X): x.com/RincoinOrg
The official channel for transparency and real-time updates.

IV. Decentralized Liquidity & P2P Infrastructure

DEX (Proposed Exchange Arena): rincoin.xyz
A planned venue for non-custodial, peer-to-peer asset exchange (*Conceptual Phase*).

Independent Market Integration (Third-party): As a sovereign, open-source protocol, Rincoin may be independently integrated by global trading platforms. The project does not provide official endorsements for centralized entities, preserving community members' autonomy and security.

V. Global Asset Directories & Analytics

Mining Ecosystem Analytics: miningpoolstats.stream/rincoin
Real-time visualization of our decentralized hashrate distribution and network security.

Institutional Asset Metadata: blockspot.io/coin/rincoin
Professional-grade validation of Rincoin's core network parameters and market metadata.

5. Roadmap (2026–2027)

Last Updated: 2026-07-05

Q1 2026: Institutional Strengthening

- ✅ **Governance Evolution:** Implementation of a dual-unit organizational structure, dividing the project into the Core Team and the Grassroots Team.
- ✅ **Scientific Milestone (v1.6):** Rincoin mathematically proposes a model addressing Bitcoin's long-term security budget decay through thermodynamic modeling of lost-asset entropy.
- ✅ **Decentralized Market Integration:** Integration with BasicSwapDEX for trustless P2P cross-chain trading.
- ✅ **Network Resilience:** Deployment of multiple Official SEED Servers, with a dual-layer Fulcrum setup: an official Dockerized node by the Core Research & Authority Lead and a decentralized Community Fulcrum node.
- ✅ **Zero-Trust Operational Security:** Implementation of hardware-backed biometric SSH authentication across core VPS infrastructure, reducing credential-based attack surface.
- ✅ **Discord Security:** Adopted Discord Developer Tools for shared bot management and deployed the Wick anti-nuke bot in the community hub.
- ✅ **Ecosystem Entry:** Internal Alpha of the Rincoin Browser Extension Wallet: a non-custodial gateway with encrypted local backup.
- ✅ **Network Visibility:** Launch of the Official Basic Explorer, Community Explorer, global unveiling of Logo v1.2.
- ✅ **Brand Renewal:** Overhaul of the official web infrastructure.

Q2 2026: Technical Mid-Cycle Review *(Tech-Focus)*

- **Advanced Protocol Engineering:** Began **Customized Halving** development, supported by multiple AI assistants for simulation work, and standardized coding environments.
- **Scientific Formalization (Pre-Release v1.6.2):** Publication of the comprehensive theoretical treatise laying the mathematical foundation for the upcoming whitepaper v1.7.
- **Scientific Refinement (Pre-Release v1.6.3–v1.6.4):** Integration of operational mechanics (phased migration, piecewise bounty, temporal smoothing) and high-precision sensitivity analysis (N = 1,000,000) delineating the statistical decoupling threshold up to $\mu = 1.9\%$.
- **Computational Verification Suite:** Public release of a comprehensive Python-based simulation framework (`rincoin-regenerative-simulations`).
- **Core Consensus (Pre-Release v1.0.6):** Official pre-release establishing P2P protocol sovereignty and verified MWEB/Customized Halving integration through a 100% "Test Green" consensus framework (`github.com/Aevust/rincoin/releases`).
- **Accelerated Consensus Sandbox (v1.0.6.1):** Public release of a network-isolated, killswitch-secured `regtest` environment engineered to empirically validate the 1/1000-accelerated **Customized Halving** boundary values and the complete **MWEB** privacy lifecycle (`github.com/Aevust/rincoin-sim`).
- **Governance Formalization (RIPs):** Public launch of the Rincoin Improvement Proposals repository, establishing a Bitcoin BIP-equivalent process for transparent, auditable protocol governance. All consensus-critical upgrades — beginning with **RIP-0002 (Customized Halving)** — are now formally specified and open for community review (`rips.rincoin.org`).
- **Upstream Contribution (Litecoin Ecosystem):** Identified an uninitialized-variable defect (undefined behavior under `[basic.indet]`) in Litecoin's `-vbparams` deployment parser, where the optional `nStartHeight`/`nTimeoutHeight` fields are left indeterminate when the BIP9-compatible argument form omits them. The report includes a root-cause analysis, a reproduction case, and a structural comparison with Bitcoin Core's parser, which value-initializes the parameter struct and assigns optional fields an explicit default. A minimal, one-line fix restoring the implicit zero-default contract was proposed. The defect is confined to the `regtest`-only `-vbparams` path and does not affect mainnet or testnet consensus; it was discovered during Rincoin-Sim development (`litecoin/#1095`, assigned by David Burkett, the lead MWEB developer).

- ✅ **Upstream Contribution (Bitcoin Ecosystem):** Diagnosed a `strlcpy`/`strlcat` declaration collision causing fatal build failures on glibc 2.38+ (Ubuntu 24.04), where glibc's fortified `__gnu_inline__` definitions conflict with the bundled `inline` declarations under `_FORTIFY_SOURCE`. The root-cause analysis documents why the common workarounds are unsatisfactory: dropping the bundled header breaks linking on platforms lacking these functions, while `-D_FORTIFY_SOURCE=0` disables a hardening feature to mask a declaration clash. The proposed fix keys the bundled fallback on the same feature-test condition glibc itself uses (`__GLIBC_PREREQ(2,38)` together with `__USE_MISC`), preserving `_FORTIFY_SOURCE` hardening across all toolchains while retaining compatibility with older libc. Root-cause analysis and fix shared with the `bitcoin-seeder` repository maintained by Pieter Wuille (sipa), known for SegWit and libsecp256k1 (`bitcoin-seeder/#109`).
- ✅ **Infrastructure Bootstrap (rincoin-seeder):** Submitted the foundational `rincoin-seeder` Pull Request, integrating the glibc 2.38+ build fix and completing the full rebrand from `bitcoin-seeder`: source files, include guards, Rincoin network parameters (P2P port `9555`, seed host `seed.rincoin.org`), and copyright attribution to the original `bitcoin-seeder` by sipa (`rincoin-seeder/pull/2`).
- ✅ **Hard-Fork Validation Sandbox (v1.0.7):** Public release of the `regtest` environment validating the **Block 840,000** hard fork — **Customized Halving** dilation and RIN3 `nVersion` enforcement (cross-version replay protection) — at 1/1000 accelerated scale, with a 5,461-block deep-reorg withstood (full CH-history erasure) and all 71 BVA boundaries passing (`github.com/Aevust/rincoin-sim`, `zenodo.20745260`).

Q3 2026: Validation & Resilience

- ✅ **Institutional Repository:** Establishment and public announcement of the `rincoin-core` GitHub organization (`github.com/rincoin-core`) as the development & staging home for Rincoin Core, hosting the public `rincoin` repository.
- ✅ **Website Update:** Relaunch of the official website (`rincoin.org`, `rincoin.com`) as a machine-verifiable provenance record — semantic HTML with structured data and an explicit open-crawler policy, replacing the prior PDF-only root.
- ○ **Formal Audit:** Intensive testing and security audit period for the halving mechanism.
- ○ **Strategic Buffer:** Risk assessment, performance optimization, and evaluation of potential feature enhancements.

Q4 2026: Deployment

- ○ **Implementation:** Successful completion and activation of the Customized Halving protocol.

Q1 2027: Ecosystem Diversification

- ○ **New Development Infrastructure:** Official deployment of a self-hosted code repository (**Forgejo**) on core VPS infrastructure, ensuring institutional ownership of all source materials and reducing dependency on centralized hosting platforms.

Q2 2027 & Beyond

- ○ **P2P Network Expansion:** Expanding integration with decentralized exchanges (e.g., Bisq and RetoSwap).
- ○ **Community-Native OTC Trading:** Establishment of a dedicated trading server (Discord or an equivalent platform) as a direct, non-custodial P2P trading hub backed by underlying DEX protocols. As no intermediary holds or controls funds, this mechanism operates outside the custodial exchange framework by design.
- ○ **Layer-2 Scaling Research:** Commencement of theoretical and technical research into off-chain scaling solutions (e.g., Lightning Network adaptations) to enable instant, micro-fee P2P transactions while maintaining base-layer PoW security.

6. Verification of Cryptographic Stewardship

*This certificate records the Bitcoin anchoring of the target document by Aevust, serving as the **Principal Architect** for the **Rincoin Core Strategic Authority**. The attached PGP signature provides verifiable proof of provenance and authorship, attesting to the protocol's mathematical and theoretical integrity at the time of publication.*

PGP Fingerprint: `ED20 B635 4EE4 526D 01F8 3B53 8B6E 3BF4 5C71 4ECA`

Cryptographic Authority: `Aevust <info@rincoin.org>`
***Principal Architect** of the Rincoin ecosystem, attesting to the authenticity of all signed releases and communications. Valid Until: 2029-01-15.*

Public Key (Keyserver): `keys.openpgp.org`
The corresponding public key is publicly retrievable from the OpenPGP keyserver, allowing verification of signed releases and communications without reliance on any single hosting platform. After retrieval, the key's fingerprint MUST match the value above.

Security Policy: `SECURITY.md (rincoin-rips)`
Canonical key-import instructions, the authoritative Core Team roster, and independent DNS verification are maintained in the repository security policy.