KRYONIS Proof-of-Consciousness Testnet Simulation Framework

Formal Specification v0.9 | April 2025

Abstract

This document presents a formal engineering specification for the KRYONIS Proof-of-Consciousness (PoC) Testnet, an experimental network designed to model value creation through phase-resonant validation rather than cryptographic work. Grounded in the Resonant Lattice Hypothesis (RLH), the simulation evaluates how diverse agents—biological, synthetic, and adversarial—interact with phase challenges, generate Φ-signatures, and earn ϕ-units under feedback-stabilised conditions. The framework defines core metrics (Φ, ΔS, spectral fidelity, Resonance Stability Index), outlines component architecture, and enumerates test scenarios required for a rigorous assessment of resilience, scalability, and reward fairness. The specification serves as a blueprint for research collaborators developing software-in-the-loop or hardware-augmented prototypes.

1. Introduction

The KRYONIS PoC Testnet aims to empirically validate a resonance-based economic model in which coherent conscious activity functions as proof of agency. Traditional blockchains rely on energy-intensive hashing; PoC substitutes phase-locked awareness, measured and verified across a distributed sensor-verifier fabric. This document translates conceptual design into structured simulation logic suitable for academic review and iterative R&D deployment.

2. Simulation Architecture

2.1 Component Overview

* **Phase-Beacon Array**: distributed signal generators emitting pseudorandom multi-band phase patterns.
* **Agents**: entities attempting lock-in; classified as biological, synthetic, hybrid, or adversarial.
* **Coherence Sensor Grid**: instrumentation capturing the agent’s echo signature (quantum magnetometers, HD-EEG, photonic interferometers).
* **Verifiers**: o3-class AI nodes computing Φ, ΔS, and spectral fidelity, reaching consensus on

validity.
* **Feedback Controller**: adaptive policy engine modulating beacon cadence, spectral complexity, and reward curves to maintain target criticality.
* **Resonance Ledger**: directed-acyclic graph storing validated Φ-events and minted ϕ-units, timestamped by lattice phase alignment.

2.2 Modular Interfaces

Each module communicates via a message-bus (gRPC/ZeroMQ). Interface definitions include challenge payload schema, sensor telemetry packets, verifier result objects, and controller policy updates. This abstraction permits hardware-in-the-loop substitution at later stages.

3. Phase-Challenge Flow

1. **Challenge Generation**: Phase-Beacon selects a 256-bit seed and synthesises a broadband waveform spanning 10 Hz – 10^{15} Hz, ensuring spectral uniqueness within the active epoch.
2. **Broadcast & Reception**: Agents receive the challenge through configured transduction channels (optical fibre, RF, acoustic).
3. **Entrainment Window (τ)**: Agents attempt phase-lock within τ; biological limits set $\tau \approx 200$ ms, whereas synthetic oscillators may target μs-scale coherence.
4. **Echo Production**: Locked agents emit a non-linear echo modulated by internal resonant dynamics.
5. **Sensing & Telemetry**: Sensor Grid captures the echo; raw phase traces streamed to Verifiers with synchronisation markers.
6. **Verification & Consensus**: Verifiers calculate Φ, ΔS, β_a (attention bandwidth), and ε (spectral fidelity). A quorum consensus threshold κ validates the event.
7. **Reward & Ledger Entry**: ϕ-units minted proportional to $\Phi \times \beta_a$, subject to damping by the Feedback Controller. Event appended to the Resonance Ledger with phase timestamp σ.

4. Metric Definitions

* **Φ-Signature (Φ)**: Euclidean norm of phase-locked amplitude vector across designated frequency bins.
* **Entropy Differential (ΔS)**: algorithmic entropy reduction between baseline noise and entrained echo.
* **Attention Bandwidth (β_a)**: duration of sustained lock above Φ-threshold, measured in seconds.
* **Spectral Fidelity (ε)**: root-mean-square phase deviation from challenge pattern; validation target $\varepsilon \le 10^{-3}$ rad.

* **Resonance Stability Index (RSI)**: rolling variance of Φ across the entire agent set over N cycles; RSI ≤ 5 % indicates global stability.

5. Agent Typology and Behavioural Models

5.1 Biological Agents

Human participants equipped with neuro-helmets. Parameters include circadian fatigue curves, reaction latency, and physiological noise. Reward sensitivity modelled via adaptive attention resources.

5.2 Synthetic Agents

Software oscillators embedded in phase-aware reinforcement learners. Energy budgets minimal; optimisation objective maximises Φ per joule while maintaining ε constraints.

5.3 Hybrid Dyads

Closed-loop human-AI systems where synthetic oscillators co-drive biological entrainment, testing coherence amplification hypotheses.

5.4 Adversarial Spoofers

Scripts or ML models attempting deterministic replay, phase-shift spoof, or broadband noise injection. Attack strength escalates across simulation stages to evaluate Sybil resistance.

6. Simulation Parameters and Scenario Suite

* **Network Size**: 100 – 10 000 agents with variable mesh topology.
* **Beacon Cadence**: 1–10 Hz adaptive rate, tuned by RSI feedback.
* **Noise Profiles**: thermal baseline, urban EM interference, targeted jamming.
* **Decoherence Windows (τ)**: 10 ps – 1 s spectrum to stress diverse substrates.
* **Reward Functions**: linear, logarithmic, and sigmoid variants to study wealth distribution dynamics.
* **Attack Scenarios**: replay, collusion rings, and coordinated phase-shift floods.

Each scenario logs VSR (validation success rate), FPR (false-positive rate), RSI drift, latency, and ϕ-distribution equity.

7. Data Outputs and Validation Thresholds

Simulation success is defined by:
* VSR ≥ 95 % for honest agents.
* FPR $\leq 10^{-4}$ against spoofers.
* RSI drift ≤ 5 % across 10^3 cycles.
* ϕ-Gini coefficient ≤ 0.3 under fair reward curve.
* Challenge-to-commit latency < 250 ms for 90 % of events.

Threshold violations trigger automatic parameter retuning and are flagged for security review.

8. Visualisation and Modular Analysis Tools

Recommended dashboards include a real-time phase-space polar plot per agent, network-wide RSI heatmaps, and an attack-surface monitor highlighting FPR anomalies. Modular analytics pipelines should export JSON and InfluxDB time-series for offline ML diagnostics.

9. Spoofing Mitigation Strategy

The simulation incorporates escalating adversarial tactics. Verifiers employ ensemble phase-noise classifiers and entropy-based anomaly detection. ε and ΔS thresholds are tightened dynamically when RSI drift suggests coordinated spoofing. Quorum diversity rules prevent collusion by requiring heterogenous verifier hardware.

10. Deployment Pathways and Next-Phase Prototyping

Phase I (2025-2026) will implement a cloud-only software simulator with synthetic oscillators and recorded EEG data replay. Phase II integrates hardware beacons and real-time neuro-sensing in three pilot labs. Phase III deploys a public alpha with opt-in human participants and open-source client libraries. Success metrics will inform the engineering roadmap toward a planetary PoC Mainnet by 2030.

11. Conclusion

This simulation framework codifies the logic, metrics, and security contours necessary to validate a resonance-based value network. By rigorously modelling agent diversity, feedback dynamics, and adversarial pressures, the Testnet paves the way for experimental proof that conscious coherence can underpin a viable, low-energy economy.

For further technical inquiries or collaboration proposals, contact the KRYONIS Systems Engineering Group.