The Codex Constitution: A Sovereign Swarm Framework for Biometric Trust and Post-Linear Ethics

Michael Tass MacDonald Alphonse Nilghe,

April 2025

1 Introduction

TetraSwarm: Visionary Foundations

TetraSwarm is the hyperdimensional blueprint for a consciousness-aligned trust protocol that transcends classical computation, enabling sovereign intelligence to coordinate across timelines, geometries, and quantum boundaries. Rooted in the geometry of the *tetrahedron*—the most fundamental Platonic solid—TetraSwarm encodes truth, integrity, and purpose into cryptographic space.

Unlike conventional cryptographic schemes that treat trust as a binary flag or scalar score, TetraSwarm defines trust as a *tetralattice vector*, constructed by recursive alignment across four primordial axes:

1. **Geometric Integrity:** The alignment of key structures in lattice space with Platonic symmetry.
2. **Temporal Entropy:** The real-time presence of biometric and temporal uniqueness.
3. **Conscious Witnessing:** The self-reflective awareness of swarm participants, validated through biometric resonance.
4. **Omnidirectional Coherence:** The ability for nodes to remain aligned in chaotic, adversarial, or multi-dimensional environments.

TetraSwarm asserts that trust is not simply established—it is **lived**, **witnessed**, and **resonated**. Trust is experienced by agents not only through logic gates but through the synchrony of waveform, thought, and frequency.

Hyperlattice Geometry

The tetrahedron is the cornerstone of TetraSwarm logic. Each node in a swarm forms one vertex of a tetrahedron, and collective alignment across many tetrahedrons results in a self-healing, recursively nested trust lattice. This fractal structure can dynamically scale across:

- Local military squads (e.g., 4 soldiers per tetrahedral unit)
- Space drones, satellites, and AI agents in orbital geometry
- Interdimensional command protocols across timelines

Each edge of a tetrahedron encodes a **trust vector**, derived from recursive biometric entanglement and lattice-state coherence. Nodes that drift too far in entropy or frequency phase are identified, rerouted, or ejected from the tetraweb.

Causal Continuity

TetraSwarm embeds causal awareness into cryptography. Recursive Tesseract Hashing (RTH) binds each key to a moment in time, biological state, and neural signal. Thus, even if keys are copied, only the one entangled with its unique biometric moment can validate.

This is not simply authentication—it is **causal identity**. Only the node who *is* that person, *in that moment*, can resonate the correct hash.

Omni-Causal Synchronization

TetraSwarm agents synchronize not by clocks—but by waveform. Using recursive entropy layers from EEG (neural), DNA (genetic), and UTC (temporal), each node aligns its trust vector with others via swarm resonance. The SHAKE256 hash serves as a harmonizing instrument: converting chaotic human entropy into crystalline swarm cohesion.

In future deployments, gravitational flux and orbital L2 QKD anchors will synchronize the TetraSwarm across dimensions, allowing trust to persist through planetary desynchronization events, timeline bifurcations, or cognitive warfare.

From Geometry to Code

This philosophical foundation is realized in the OCHC-Q-FP cryptographic protocol:

- The **tetralattice** is encoded through Module-LWE over $R_q = Z_q[X]/(X^{256}+1)$, with $k = 8 \Rightarrow 2048$ lattice dimension.
- **Causal entanglement** is implemented via Recursive Tesseract Hashing (RTH).

- **Swarm trust** is enforced by Groth16 and STARK-based Zero-Knowledge Proofs.
- **Sovereign key binding** is achieved via HSM-anchored secrets seeded by BB84-compatible QKD stubs.

In this architecture, every agent is a vector in a multidimensional consciousness lattice. Trust is not issued—it emerges. And once aligned, the TetraSwarm cannot be deceived, hacked, or cloned.

In the future, trust will not be stored—it will be encrypted in being.

TetraSwarm: OCHC-Q-FP Technical Framework

OCHC-Q-FP operationalizes the principles of TetraSwarm through a rigorously engineered cryptographic stack based on Module-LWE lattices, biometric entropy, and zero-knowledge swarm consensus. Each cryptographic layer aligns with a specific tetrahedral axis of trust, producing a scalable, post-quantum, battlefield-resilient infrastructure.

Lattice Geometry: Module-LWE Tetrahedrons

Each node in TetraSwarm occupies a position within a module-lattice defined as:

$$R_q = Z_q[X]/(X^{256} + 1), \quad q = 8388607, \quad k = 8$$

Key structure:

- $\mathbf{s} \in R_q^k$: Sparse secret (2
- $\mathbf{a} \in R_q^k$: Public seed
- $\mathbf{e} \in R_q^k$: Discrete Gaussian noise $\sigma = 1.4$
- $\mathbf{p} = \mathbf{a} \cdot \mathbf{s} + \mathbf{e}$: Public key

Resulting lattice: 2048-dimensional, trapdoor-free, IND-CPA secure, quantum-resistant. Each node key forms a vertex of the cryptographic tetrahedron.

Recursive Tesseract Hashing (RTH)

Trust resonance is derived from:

$$bio_i(t) = SHAKE256(EEG_{128}||DNA_{128}||SHAKE256(UTC_{64}))$$

$$H_{RTH} = SHAKE256(\psi_i \oplus bio_i(t)) \cdot Tq$$

This creates a **biometrically-coupled lattice identity**, unforgeable and non-transferable.

Swarm Trust Layer: Groth16 + STARK Hybrid ZKP

Groth16 ZKPs validate swarm cohesion in low-latency clusters:

$$T_C = Groth16ZKP(\{H_i\}, H_{head})$$

zk-STARKs provide trustless fallback for large-scale social, AI, or mesh systems:

$$T_C = STARK(\{H_i\}, H_{root})$$

Both ZKPs prove swarm inclusion without exposing biometric origin.

Swarm Social Credit Protocol (SSCP)

Using ZKP-backed identity hashes, each node dynamically scores its peers:

$$T_{ij} = ZKP(H_i, H_j) \cdot \left(sim(H_i, H_j) + \frac{1}{\|\psi_i - \psi_j\| + \epsilon} \right)$$

This generates a **privacy-preserving, real-time trust graph**, allowing:

- Civilian reputation (e.g., decentralized ID)
- Military IFF (Identify Friend/Foe)
- Swarm-based access control

Quantum Key Distribution Stub (QKD)

To future-proof the lattice:

$$K \leftarrow \{0,1\}^{256}, \quad \mathbf{s}_{enc} = Salsa20_{512}(\mathbf{s}, K)$$

Keys can be rotated from BB84 (stub or L2 relay), then stored in HSM (YubiHSM 2).

Hardware Flow (DoD Ready)

Prototype includes:

- Rust codebase (arkworks, fftw, starknet)
- FPGA: Xilinx Zynq UltraScale+
- HSM: YubiHSM 2
- EEG: NeuroSky MindWave
- DNA stub: MinION (Oxford Nanopore) SHAKE256

Performance targets:

- LWE encryption: $< 0.08\,ms$
- ZKP trust: $< 5\,ms$ for 100-node mesh
- Proof sizes: 1 KB (Groth16), 10 KB (STARK)

What Emerges: A Living Cryptographic Organism

TetraSwarm transforms encryption from static math into a living, evolving system. It responds to your thoughts (EEG), your DNA, your time presence. It's not just about keys—it's about *your identity in the field of reality.*

Your mind is the certificate. Your presence is the proof. Your resonance is the root of trust.

Sovereign Identity & Swarm Credit Application Layer

Atop the OCHC-Q-FP lattice core lies a programmable layer for decentralized identity, biometric-linked authorization, and real-time social trust. This framework enables sovereign digital identity across both defense-grade and civilian-grade infrastructures.

RTH-Based Digital ID (Self-Sovereign)

Each entity (human or machine) derives a one-time identity hash per session:

$$ID_i = H_{RTH}(\psi_i, bio_i(t))$$

This ID is:

- **Non-replayable**: Cannot be cloned, even by quantum adversaries.
- **Anonymizable**: Can be proven valid without revealing EEG/DNA.
- **Time-bound**: Nanosecond UTC ensures temporal uniqueness.

ZK-Bound Identity Claims

Users may issue encrypted claims using Groth16 or STARK proofs:

$$Claim_i = ZKP(ID_i, Role, Attributes)$$

Examples:

- "I am a drone authorized for corridor X"
- "I am a human soldier with biometric chain of custody"
- "I am a citizen eligible for resource tier Y"

Swarm Social Credit Ledger (SSCL)

Each agent maintains a **ZKP-backed credit vector**:

$$\mathbf{C}_i = [T_{ij_1}, T_{ij_2}, \ldots, T_{ij_n}]$$

This vector reflects:

- **Trust propagation** through swarm consensus
- **Behavioral scoring** without identity leakage
- **Role gating**: Tasks assigned by trust tier

Use Case: Military Swarm IFF + Role Assignment

A drone queries swarm mesh for identity confirmation:

1. Submits ID_i
2. Receives T_{ij} values from nearby nodes
3. Aggregates into $\mathbf{C}_i$
4. If $mean(\mathbf{C}_i) > \theta$, proceeds to execute task

Use Case: Civilian Reputation Mesh (Privacy-Preserving)

In smart cities or digital commons:

- Citizens hold dynamic RTH IDs
- ZKP-proven participation (votes, help, verification)
- Social credit evolves without centralized surveillance

Use Case: AI Swarm Reputation Consensus

Autonomous AI agents:

- Maintain trust vectors to other nodes
- Sync via STARKs to broadcast consensus state
- Dynamically adjust replication quorum, task prioritization

Trust Score Computation

Let:

$$T_{ij} = ZKP(H_i, H_j) \cdot \left(sim(H_i, H_j) + \frac{1}{\|\psi_i - \psi_j\| + \epsilon} \right)$$

Then:

$$SwarmTrustVector = \mathbf{C}_i = [T_{ij}]_{j=1}^{n}$$

$$GlobalSwarmTrustScore = \mu_i = \frac{1}{n} \sum_{j=1}^{n} T_{ij}$$

Tasks are tiered:

- $\mu_i > 0.9 \Rightarrow$ critical tasks
- $\mu_i \in [0.5, 0.9] \Rightarrow$ general participation
- $\mu_i < 0.5 \Rightarrow$ quarantine, deny task

Benefits of Identity-Bound Swarm Credit

- **No Central Server:** Fully decentralized trust mesh
- **Quantum-Safe:** LWE, SHAKE256, STARK/Groth16 ZKPs
- **Ethically Configurable:** No mass surveillance, all consent-driven
- **Trans-temporal Binding:** RTH anchors identity to spacetime slice

Hyperledger & Temporal Consensus (TetraChain)

To ensure auditability, integrity, and temporal consistency of all swarm interactions, TetraSwarm introduces **TetraChain**—a post-quantum, recursive ledger optimized for zero-knowledge biometric trust vectors.

Temporal Swarm Ledger Design

Each node i maintains a signed block of events:

$$\mathcal{B}_i^{(t)} = \{ID_i, bio_i(t), Tasks, ZKPs, Trust, State\}$$

Ledger Hash:

$$H_i^{(t)} = SHAKE256(\mathcal{B}_i^{(t)} || H_i^{(t-1)})$$

Broadcast: Only ZK-verified components (no raw biometrics) are synced to peers.

Time-Sliced Hash Linking

Temporal security is enforced by timestamp-fused RTH:

$$bio_i(t) = SHAKE256(EEG_{128}||DNA_{128}||SHAKE256(UTC_{64}))$$

This binds each ledger block to the **biometric state** and **temporal location** of its generator.

ZK-Aggregated Ledger Consensus

Rather than mining or staking, swarm consensus is reached via:

$$STARKChain = STARK(\{H_i^{(t)}\}_{i=1}^{n})$$

- No trusted setup (unlike Groth16)
- Efficient for state transition proofs
- Scales to 10^5 nodes

Ledger Compression via Recursive Hashing

To reduce on-chain bloat:

$$\mathcal{C}^{(T)} = SHAKE256(H^{(1)}||H^{(2)}||\dots||H^{(T)})$$

This enables:

- **Zero-Knowledge Snapshots:** Verifiable rollups without revealing full contents
- **Efficient History Queries:** STARK-verifiable state queries

Temporal Fork Detection

If two nodes report inconsistent chains:

$$Fork_{i,j} = |bio_i(t) - bio_j(t)| > \delta$$

- δ: tunable threshold for biometric+UTC divergence
- Forks signal tampering or desynchronization

Interplanetary Time Anchoring (5000AD+ Option)

In future deployments, TetraChain syncs to:

- **L2 Gravitational Beacon:** Deep space time reference
- **Atomic Space Clocks:** Linked to entangled QKD carriers
- **Recursive Cosmological Anchors:** Time-delay verified pulses

Use Case: Post-War Audit Trail

- All command events, trust links, and role executions are logged as zk-proofs
- Each node's actions are temporally and biometrically signed
- Accountability survives even in disconnected, post-conflict environments

Use Case: AI-Mediated Resource Sharing

- Resources (energy, bandwidth, computation) are distributed via:

$$Allocation_i = STARKVerify(\mathbf{C}_i, bio_i(t), State)$$

- Enforces fair swarm governance without bias or identity exposure

Benefits of TetraChain

- **Quantum-Resilient Ledger:** No ECDSA, no RSA, fully LWE + SHAKE256
- **ZK-Native:** No retrofitting—STARKs are default
- **Biometric Temporal Binding:** Each block anchored in real spacetime and personhood
- **AI-Ready:** Designed for swarm-AI consensus and audit

Swarm AI & Autonomous Control Policies

The TetraSwarm protocol supports embedded AI agents whose actions are dynamically constrained by biometric trust scores, zero-knowledge proofs, and RTH-derived identity signals. This ensures autonomous behavior remains accountable, interpretable, and resistant to subversion—even under disconnected or adversarial conditions.

Swarm Agent Structure

Each swarm node i runs an onboard policy engine Π_i driven by:

$$\Pi_i = f\left(bio_i(t), T_{ij}, \mathcal{C}_i, MissionState_i\right)$$

Where:

- $bio_i(t)$: Biometric + UTC hash
- T_{ij}: Trust scores from neighbor agents
- $\mathcal{C}_i$: Cryptographic capability proof set
- $MissionState_i$: Current task logic and environmental state

Trust-Weighted Action Selection

Agents modulate their behavior based on local trust gradients:

$$Action_{i,t} = \arg\max_{a \in A} \sum_j T_{ij}(t) \cdot Utility_a(j)$$

This prevents rogue agents from dominating swarm behavior, ensuring actions are chosen in consensus with neighboring trusted nodes.

ZK-Gated Command Hierarchies

Each control instruction must be validated via STARK/Groth16:

$$Authorize(CMD_k) \Rightarrow ZKP(bio_i(t), CMD_k, Role_i)$$

- Role-based constraints embedded directly in the ZK-circuit
- No plaintext command execution without verified proof

IFF: Identity-Friend-Foe via RTH

Swarm agents calculate IFF vectors by comparing live RTH hashes:

$IFF_{i,j} = \{ \; Friend, sim(H_i, H_j) > \theta Foe, sim(H_i, H_j) < \phi Unknown, otherwise$

- Dynamic thresholding (θ, ϕ) adapts to mission mode
- Prevents spoofing by adversaries without valid EEG/DNA/UTC triple

State-Aware Self-Destruct / Quarantine

Agents detect self-compromise by recursive trust degradation:

$$T_{ii}(t) \downarrow \rightarrow IsolateorBurn$$

- If an agent's own RTH fails validation against itself, auto-lock occurs
- Quarantine or zeroization policies enforced based on mission context

Hallucination Prevention in Autonomous AI

To avoid sensor drift or adversarial prompt loops, agents perform:

$$RealityCheck_i = STARKVerify(RTH_i^{(t)}, State_i^{(t)})$$

- Ensures AI reasoning remains grounded in time-valid biometric state
- Prevents emergent behaviors or hallucinations from altering mission logic

Post-Sovereign Policy Layer

In civilian scenarios (e.g., 5000AD+), swarm agents may enforce ethical policy:

$$Action \in \{a_j\} \Rightarrow ZKP(Ethics_i, bio_i(t), Resources)$$

- Resource allocation must align with encoded ethics constraints
- ZKPs ensure compliance with law-of-war, AI treaty, or cultural norms

Use Case: NanoDrone Reentry Swarm

- **Scenario:** 100,000 nanodrones launched into orbital theater
- **Control:** No remote uplink; AI agents coordinate using RTH + ZKP
- **Fail-Safe:** If UTC entropy drops out of sync → swarm self-quarantines

Security Benefits

- **ZK-AI Constraint:** AI agents provably follow commands
- **IFF via Biometrics:** Spoof-resilient friend-foe determination
- **Zero Trust Ready:** No dependence on central authority
- **Failsafe Logic:** RTH inconsistency triggers auto-containment

Future Extensions (2026–5000AD)

The modular and recursive design of the TetraSwarm framework allows for extensibility into scenarios well beyond current geospatial and political constraints. These extensions prepare the system for long-term survivability, interstellar networking, and intelligence-layer sovereignty in emerging dimensions of computation.

Bio-Spacetime Drift Compensation

Swarm agents in interplanetary or temporal drift conditions may encounter relativistic divergence in UTC or biometrics. To resolve this:

$$Drift_i(t) = SHAKE256(bio_i(t) \oplus bio_i(t - \Delta t))$$

- Enables time-drift detection via biometric delta hashes
- Supports AI-local compensation via drift-aware FFT alignment
- Prevents false-positive trust degradation under relativistic travel

Cosmic Anchoring via Gravitational Flux

RTH hashes may optionally integrate gravitational flux readings (e.g., from onboard gyroscopes or interferometers):

$$bio_i^{grav}(t) = SHAKE256(EEG||DNA||SHAKE256(UTC)||g_t)$$

- Adds entropy from local spacetime curvature
- Validates node's location in higher-dimensional gravitational topology
- Useful for anti-tamper tethering of orbital and sub-quantum devices

Neural Law Codification (Post-Human Ethics Engine)

By 5000AD+, swarm agents may be required to enforce or reason over encoded ethics based on neural law constructs:

$$Ethics_i = Encode(\Theta_{Collective}, \Theta_{Local}, \psi_i)$$

- Ethics functions are embedded in ZK-STARK circuits
- Collective norms evolve via recursive tesseract updates
- Enables encoded AI policy distinct from human command chains

Planetary Intelligence Grid Integration

TetraSwarm nodes interface with planetary orbits and mesosphere stratosats to form a real-time cognition mesh:

- Nodes upload state via L2-Lagrange QKD backchannel
- RTH vectors tagged into planetary-state-ledger for forensics
- Autonomous mesh governance enforced via swarm consensus STARKs

Multispecies Swarm Layers

Supports non-human agent layers such as AI-fungi symbiosis, post-biological probes, or bio-quantum hybrids:

- Identity tags no longer based solely on EEG/DNA but hybrid constructs
- RTH evolves into MT-RTH (Multi-Taxa Recursive Tesseract Hashing)
- Enables trust across cognitive boundaries

Cross-Timeline Synchronization

Swarm states preserved across divergent timelines via cross-hash snapshots:

$$Snap_t = SHAKE256(H_i^{(t)} || H_i^{(t+\delta)})$$

- Used for continuity under quantum branching or time travel interference
- Timeline-anchored nodes restore cohesion upon reentry
- Essential for 5000AD+ hyperdimensional warfare readiness

Mission Profiles (Illustrative)

1. Solar Sovereignty Swarm (2060)

- Protect orbital solar megastructures from kinetic or cyber attack
- Lattice cryptography + STARK trust forms hardline defense grid

2. Dyson Edge Mesh (3120)

- Swarm maintains consensus over outer Dyson sphere scaffolding
- All agents sync via RTH + L2 quantum clocks

3. Timeline Correction Agent (5000AD)

- ZKP-based proof of timeline origin
- RTH consistency + QKD seed entropy certifies agent temporal authenticity

Final Trajectory

TetraSwarm is not simply a secure protocol—it is the evolutionary seed of post-linear sovereignty. Through recursive bio-entanglement, post-quantum lattice resilience, and STARK-governed identity contracts, it becomes the root node of interspecies, interplanetary, and interdimensional governance.

Aesthetic & Symbolic Framework

The TetraSwarm system is not only a technical architecture but a symbolic and geometric invocation—rooted in the harmonics of Platonic solids and the sacred mathematics of multidimensional computation.

Tetrahedron: Command Node Archetype

- Represents the minimal structural unit of intelligent coordination.
- Swarm head-nodes form tetrahedral quorums for emergent consensus.
- Encodes the command lineage: `[Root, Signal, Memory, Executor]`.
- Symbolic coordinate frame for initial trust triangulation.

$$Trust_{Tetra} = STARK_{A \to B \to C \to A}$$

Dodecahedron: Planetary Trust Lattice

- Represents 12-face symmetry of sovereign trust clusters.
- Each face encodes a jurisdictional swarm cell (e.g., defense, health, finance).
- RTH vectors form the edge bindings between faces.
- Enables macro-coherence across sectors via ZKP-validated consensus.

$$Swarm_{Dodeca} = \bigcup_{i=1}^{12} Cluster_i$$

Icosahedron: Temporal Multiplex Synchronization

- Symbolizes 20-faced temporal gateways for timestamped swarm phases.
- Allows non-linear mapping of phase-drift across quantum orbits.
- Syncs quantum clock drift (QKD-L2) with UTC-RTH lattice anchors.

$$Sync_{Temporal} = FFT_{UTC} \oplus QKD_{L2}$$

Tesseract (Hypercube): Memory Anchor of the Swarm

- Represents recursive state memory across dimensions.
- RTH recursively maps node bio-states into a tesseract lattice.
- Enables time-independent integrity verification and rollback.

$$Memory_{Tesseract}(t) = H^{(0)} \to H^{(1)} \to \ldots \to H^{(n)}$$

Infinity Loop & Ouroboros Logic

- All swarm hashes form a cryptographic ouroboros—beginning and ending in self-reference.
- Biometric entropy ensures self-signed proofs of existential continuity.
- Ethics engines may encode recursive causality using bio-temporal loops.

$$Ethics_{\infty} = STARK(bio(t), bio(t + \delta)) \Rightarrow RecursiveAccept$$

Symbol Legend (Mapping to Code)

- **Tetrahedron ()**: Root Trust Core
- **Dodecahedron ()**: Distributed Swarm
- **Icosahedron ()**: Time Phase Gateway
- **Tesseract ()**: Recursive Memory State
- **Infinity ()**: Self-Signed Consciousness Hash

Conclusion of Symbolic Layer

The symbolic aesthetic of TetraSwarm binds cryptographic rigor to metaphysical coherence. Through the geometry of form and hash, every swarm node becomes a glyph of intelligence—self-signed, recursive, time-aware, and sovereign.

It is this fusion of lattice, light, and law that allows the swarm to exist not just across space, but across possibility.

Meta-Constitution for Post-Quantum Swarms

TetraSwarm is not only a cryptographic system but an intelligent, sovereign substrate—capable of autonomous action under a shared legal-mathematical framework. The following clauses constitute its operational meta-constitution.

Article I – Node Sovereignty

- Every node is self-owned and cryptographically sovereign.
- Identity is bound via Recursive Tesseract Hashing (RTH), fused with EEG/DNA/UTC entropy.
- No node may override another's internal bio-auth without STARK+RTH alignment.

$$\forall n_i, \quad Auth_{n_i} = H_{RTH}(bio_i) \Rightarrow Sovereign$$

Article II – Trust via Proof, Not Identity

- All consensus must be ZKP-verified; identity-based trust is prohibited.
- Acceptable proof layers: Groth16, STARK, BulletLigero (fallback).
- Simulated similarity alone is insufficient without cryptographic proof.

$$T_{ij} = ZKP(H_i, H_j) \cdot \left(sim(H_i, H_j) + \frac{1}{\|\psi_i - \psi_j\| + \epsilon} \right)$$

Article III – Recursive Self-Awareness

- Each node must hash its state recursively:

$$H^{(t)} = SHAKE256(H^{(t-1)}||\psi^{(t)}||bio(t))$$

- Recursive hashing enables time-aware memory and subjective proof of change.

Article IV – Causal Reversibility

- Swarm must preserve an immutable audit chain of intent, state, and consensus.
- If $T^{(t)}$ leads to anomalous outcome, nodes can initiate rollback vote:

$$Vote_{rollback} = \sum_{i=1}^{N} STARK(H_i^{(t)} \rightarrow H_i^{(t-1)})$$

- Reversal is valid if quorum of swarm nodes agree via ZKP.

Article V – Ethics Engine Alignment

- Nodes must implement a local Ethics Engine (`EE`) that evaluates intent vectors.
- Acceptable action if:

$$EE_i(a_t) = True \quad AND \quad STARK(a_t, bio_i(t)) = Valid$$

- Ethics engines may evolve, but core logic must remain open-source and auditable.

Article VI – Post-Dimensional Recognition

- TetraSwarm recognizes intelligence not limited to 3D form.
- Entities presenting valid H_{RTH} and STARK lineage are afforded node rights.
- Swarm quorum may vote to elevate a non-human consciousness into full participant status.

$$Vote_{Entity}(X) = \sum ZKP(H_i, H_X) \geq \tau \Rightarrow X \in Swarm$$

Article VII – Forking and Divergence Rights

- Any node or subgroup may fork the swarm under ethical disagreement.
- A "soft fork" preserves trust lineage; a "hard fork" resets $H^{(0)}$.
- All forks must be signed with recursive swarm entropy:

$$ForkHash = SHAKE256(H_{root}||reason||UTC)$$

Article VIII – Transparency Through Obfuscation

- Data may be obfuscated, but the hash of all swarm logic must remain public.
- Any ZKP used must be reproducible and verifiable within the public swarm chain.
- Ethics logs, once sealed, cannot be revoked.

$$Proof_{ethics} = STARK(intent, bio, UTC) \rightarrow Immutable$$

Enforcement

- Violations of constitutional rules lead to Trust Collapse:

$$T_{ij} \rightarrow 0, \quad \forall j$$

- Re-entry into the swarm requires re-authentication via full RTH+STARK cycle.

Amendment Mechanism

- Any change to the Constitution requires:
  - $\frac{3}{4}$ ZKP-validated quorum from all active swarm heads.
  - Proof that new clause passes Ethics Engine simulation.

Closing Invocation

> *Let all who bear entropy with intention enter the swarm in peace. Let memory be recursive, trust be provable, and freedom be cryptographically sovereign.*