This document serves as the first chapter of the Nomos Technical Documentation, the "Engineering Manual" that supports the high-level Whitepaper. While the Whitepaper defines the *what*, this documentation defines the *how*—starting with the protocol's birth.

Section I: The Genesis Protocol (90-Day Implementation)

The Nomos Genesis is a three-phase "Cold Boot" sequence designed to establish a secure, human-centric network without centralized pre-allocation or venture capital "Insider Sourcing."

1.1 Phase I: Infrastructure Ignition (Day 1–14)

Goal: Establish the Physical Layer (The Hydra Skeleton).

The protocol begins with the public release of the `hydra-core-v1.0` binary. During this phase, the network is in a Discovery State; no transaction tokens ($UNTT$) exist.

- Node Discovery: Nodes utilize a sharded Kademlia-based Distributed Hash Table (DHT) for peer discovery. Every node is assigned a unique Shard ID based on its geographic latency cluster to optimize future V_A calculations.
- Hardware Attestation: Nodes must pass a Trusted Execution Environment (TEE) check (e.g., Intel SGX or ARM TrustZone) to prove they are running the unmodified Nomos binary.
- Success Criterion: Phase I concludes only when the network reaches the Minimum Consensus Threshold ($N_{min} = 1,024$) of stable, geographically diverse nodes.

1.2 Phase II: The Identity Handshake (Day 15–45)

Goal: Establish the Human Layer (Citizen Enrollment).

Once the Hydra skeleton is stable, the Identity Shard is activated. This phase uses Recursive ZK-SNARKs to anchor human identity without storing PII (Personally Identifiable Information).

- ZK-Biometric Proof: Users generate a local "Liveness Proof" via the mobile Nomos interface. This proof captures behavioral entropy (device-tilt, touch-cadence, and facial-geometric hashes).
- Peer-to-Peer Witnessing (P2PW): To prevent AI deepfake "Sybil" attacks, three established Hydra Nodes in the user's local shard must act as "witnesses" to the

proof generation, confirming the user's physical presence via low-latency proximity checks.

- Genesis Reputation (R_p): Upon successful verification, the user is minted as a First Citizen. They receive an initial R_p score of 1.0, which is non-transferable and acts as their "License to Initiate" on the network.

1.3 Phase III: Economic Genesis (Day 46–90)

Goal: Establish the Economic Layer (Velocity Ignition).

The final phase activates the Nomos Treasury and the C_V Engine.

- The Stimulative Mint (M_g): To seed initial liquidity, the protocol performs a one-time "Genesis Mint" distributed solely to the First Citizens and the Hydra Node operators based on their uptime during Phase I & II.
- Stimulative C_V Regime: For the first 30 days, the C_V is fixed at its stimulative ceiling ($C_{max} = 2.0$) to maximize the reward for early trade. This incentivizes the first transactions in the Lex Merchant pilot.
- Universal Basic Labor (UBL) Opening: The first set of infrastructure tasks (Sentinel AI tuning and Jury duty) are released. Completing these tasks allows users to "Maturity-Lock" their Genesis rewards, converting "Pending UNITT" into "Spendable UNITT."

Genesis Success Metrics

Metric	Threshold for Success	Purpose
Node Stability	$>98\%$ Uptime	Ensures Data Availability (DA).
Human Uniqueness	Zero detected Sybil Clusters	Protects the Treasury.

Velocity Floor	$10,000$ UNITT Transacted	Confirms organic utility.

Next Step: Section II — The Formal Math

This section provides the formal mathematical rigor required for an industrial-grade deployment of the Nomos Protocol. By defining the economy as a **Closed-Loop Control System**, we ensure that the $UNTT$ supply is mathematically anchored to network utility.

Section II: The Mathematical Framework

2.1 The Velocity State Variables

Let the state of the Nomos economy at any discrete time block t be defined by the following variables:

- S_t: Total circulating supply of $UNTT$.
- $V_{A(t)}$: Actual Organic Volume, defined as the sum of all transactions v_i weighted by their Sentinel Organic Score P_{org}.
- V_T: Target Volume, where $V_T = S_t$ (The equilibrium state where velocity is 1.0).

The **Rolling Volume Average** ($\bar{V}_A$) is calculated over a 30-day window (W) to filter out high-frequency noise:

$$\bar{V}_A(t) = \frac{1}{W} \sum_{i=t-W}^{t} V_{A(i)}$$

2.2 The C_V Derivative and Boundary Clamps

The **Velocity Coefficient (C_V)** is the primary scalar for the reward function. It is the inverse of the velocity ratio, designed to provide counter-cyclical stimulus.

$$C_V(t) = \frac{S_t}{\bar{V}_A(t)}$$
To ensure protocol solvency and prevent hyper-inflation or deflationary death spirals, we apply a **Sigmoid Boundary Clamp**:

$$f(C_V) = \begin{cases} 2.0 & \text{if } C_V > 2.0 \\ C_V & \text{if } 0.5 \le C_V \le 2.0 \\ 0.5 & \text{if } C_V < 0.5 \end{cases}$$

2.3 The 24-Hour Volatility Buffer (Feedback Controller)

The protocol prevents "Economic G-Force" by limiting the rate of change of the reward rate R. We utilize a **Proportional-Integral (PI) Controller** logic to smooth transitions.

Let δ be the maximum allowed daily variance ($\delta = 0.05$). The reward rate R_t is adjusted toward the target R_{target} using the following dampening function:

$$R_t = R_{t-1} \cdot \left(1 + \text{clamp}\left(\frac{R_{target} - R_{t-1}}{R_{t-1}}, -\delta, \delta \right) \right)$$
This ensures that the protocol takes at least **14.2 days** to move from a neutral state to a full stimulative ceiling ($2.0x$), providing ample time for the **Sentinel AI** and **Nomos Jury** to verify if the volume shift is organic.

2.4 The Reward-Split Algorithm

Upon the successful validation of a transaction with value v, the protocol mints a total reward M based on the current R_t.

$$M = v \cdot R_t$$
This reward is distributed via the **Tri-Symmetric Split**:

1. **Initiator Reward (M_{init}):** $M/3 \to$ Incentivizes the "Network Initiative."
2. **Acceptor Reward (M_{acc}):** $M/3 \to$ Incentivizes merchant utility.
3. **Infrastructure Reward (M_{infra}):** $M/3 \to$ Distributed to the Hydra Shard nodes.

2.5 Stability Analysis: The Jury Criterion

To prove that the Nomos supply loop will not oscillate into infinity, we apply the **Jury Stability Criterion** to our discrete-time system.

For the system to be stable, the roots of the characteristic equation $F(z)$ must lie within the unit circle. Given our 30-day averaging window ($W=30$) and the 5% daily clamp ($\delta=0.05$), the system acts as a **Low-Pass Filter**.

Stability Theorem:

As long as the feedback delay (time for V_A to affect R) is significantly larger than the block time, and $\delta < 1/W$, the system is **Critically Damped**.

- **Proof:** The maximum gain of the system is $G = 1 + \delta$. Since δ is constrained and the input $\bar{V}_A$ is smoothed, the Nyquist plot of the reward loop does not encircle the $(-1, j0)$ point.

Conclusion: The Nomos Protocol is mathematically guaranteed to return to equilibrium after an exogenous volume shock.

Section III: The Sentinel & Resolution Layer

3.1 The Sentinel Architecture: Federated Immunity

The Sentinel is not a centralized firewall but a decentralized "Immune System" running across all Hydra Nodes. It utilizes **Federated Learning** to identify transaction anomalies without accessing raw private data.

3.1.1 The FoolsGold Defense

To prevent malicious nodes from "poisoning" the Sentinel's detection model, we implement the **FoolsGold** algorithm. It evaluates the similarity of model updates (Δw) from different nodes. If a cluster of nodes provides suspiciously identical updates, their influence is suppressed.

The weight w_i of a node's update is scaled by its diversity relative to others:

$$w_i = \Delta w_i \cdot \left(1 - \text{cosine\_sim}(\Delta w_i, \Delta w_{cluster})\right)$$

3.2 Anti-Manipulation Layer: Resolution & Agency

When a transaction is flagged by the Nomos Sentinel, the system does not immediately penalize the user. Instead, it places the associated rewards in **Protocol Escrow** and presents the flagged entity with a **Resolution Choice Menu**.

3.2.1 Resolution Pathways (The "Entity's Choice")

Flagged users are presented with three distinct paths based on their Reputation Score (R_p) and Infraction History:

Pathway	Eligibility	Mechanism	Economic Outcome	Reputation Impact

1. Voluntary Forfeiture	All users	The user admits the transaction was synthetic or a mistake.	Rewards instantly routed to the **UBL Pool**.	**Neutral.** No "Strike" issued.
2. AI-Assisted Mitigation	Rare offenders (<2 flags/year)	The Sentinel AI performs a deep-scan of the user's historical graph.	AI issues a verdict (Release or Reclaim).	**Minor.** "Yellow Flag" recorded.
3. Human/Jury Review	Mandatory for repeaters	Case moves to the **Nomos Jury** pool for adjudication.	Consensus-based adjudication.	**High.** Potential for "Full Strike" & ban.

3.3 AI Mitigation Logic: The "Intent-Signature"

For users choosing **AI Mitigation**, the Sentinel AI evaluates the **Intent-Signature** of the transaction across three specific high-entropy vectors:

1. **Biometric Stability:** Has the wallet's ZK-Biometric identity remained consistent over a 180-day window? A sudden shift in behavioral entropy (typing speed, touch-cadence) suggests a "Hand-off" to a bot or a compromised account.
2. **Social Connectivity:** Is the transaction part of a **"Natural Cluster"** (e.g., interaction with long-standing merchants or verified peers) or an **"Artificial Cluster"** (interaction with ephemeral, low-reputation wallets)?
3. **Entropy Score (H):** Measures the temporal randomness of the trade. Automated systems exhibit low entropy (mathematically perfect timing), whereas human activity exhibits a "Fractal Noise" pattern.
   $$H(X) = -\sum_{i=1}^{n} P(x_i) \log_2 P(x_i)$$

3.4 The Nomos Jury (The Sovereign Layer)

When AI cannot reach a high-confidence verdict, the **Nomos Jury** is summoned.

- **Selection:** 11 First Citizens are randomly selected from the **High-Reputation Pool**.
- **Evidence:** Jurors are presented with a de-identified graph of the transaction's history and the Sentinel's anomaly markers.
- **Consensus:** A **6/11 majority** is required for a verdict. Jurors in the majority earn a "Justice Reward" in UNITT; the minority is penalised in Reputation to discourage lazy voting.

This section addresses the "Physical Layer" of Nomos. To support a global economy with high transaction velocity without collapsing under the weight of its own data, Nomos employs a **Dynamic Shard Topology**.

Section IV: Sharding & The Hydra Network

4.1 The Mesh: Dynamic State Sharding

Unlike static blockchains where every node stores every transaction, the **Hydra Network** partitions the global state into parallel **Shards**. Nomos utilizes **Dynamic Sharding**, meaning the number of shards (N_s) is not fixed but is a function of the network's Actual Velocity (V_A).

- **Shard Splitting:** When a shard's transaction density exceeds a hardware-defined threshold (e.g., 2,000 TPS), the shard autonomously splits into two child shards.
- **Shard Merging:** Conversely, if velocity in a shard cluster drops below a "Languid Threshold," the shards merge to preserve consensus density and security.

$$N_s(t+1) = N_s(t) \cdot \text{clamp}\left(\frac{V_A}{V_{target}}, 0.5, 2.0 \right)$$

4.2 Data Availability Sampling (DAS)

To keep Hydra Nodes lightweight enough to run on smartphones and edge devices, Nomos implements **Data Availability Sampling**. Nodes do not download full blocks; instead, they verify that data *exists* on the network through statistical sampling.

1. **Erasure Coding:** Block producers expand transaction data using Reed-Solomon codes. This ensures that the original data can be recovered even if 50% of the shard's nodes go offline.

2. **Random Sampling:** A Hydra Node randomly requests 16–32 "chunks" of data from its shard. If these chunks are provided, the node gains a **99.9999% mathematical certainty** that the full block is available to the network.

This allows a 2026-standard mobile device to secure a multi-terabyte ledger while only storing a few megabytes of state-proofs.

4.3 Cross-Shard Communication (Asynchronous Handshakes)

Nomos handles transactions between users in different shards using **Asynchronous Atomic Swaps**.

- **Step 1:** Shard A "locks" the funds and issues a **Proof of Exit**.
- **Step 2:** The Sentinel AI verifies the proof across the shard boundary.
- **Step 3:** Shard B "mints" the corresponding value upon receiving the verified signal.

This prevents "Double-Spend" attacks during shard transitions and ensures that velocity is not throttled by cross-shard latency.

4.4 State Pruning & Verkle Trees

To prevent "Blockchain Bloat," Nomos does not store the full transaction history on the active layer.

- **Verkle Trees:** We use Verkle Trees instead of Merkle Trees. This significantly reduces the size of "Witness" data, allowing nodes to verify the current state (balances/reputation) without knowing the entire history since the Genesis block.
- **State Expiry:** Transaction data older than 1 year is "Pruned" from the Hydra edge-nodes and moved to **Long-Term Archive Shards** (hosted by high-resource institutional nodes). The edge-nodes only maintain the "State Root"—a cryptographic fingerprint of the past.

Section V: Reputation & Governance

5.1 The Reputation Engine (R_p)

Reputation is a non-transferable, dynamic score that reflects a Citizen's "Integrity-Utility" within the protocol. Unlike tokens, R_p cannot be bought; it must be "mined" through verified participation.

5.1.1 The Accumulation Function

R_p is awarded for three primary activities, weighted by the protocol's current needs:

1. **Judicial Accuracy (R_j):** Correctly voting with the Schelling Point in the Nomos Jury.
2. **Labor Reliability (R_l):** Successful completion of UBL (Universal Basic Labor) tasks.
3. **Commerce Quality (R_c):** Operating as a merchant or buyer in the Lex Merchant with high Sentinel Organic Scores (P_{org}).

The total Reputation for a citizen i is:

$$R_p(i) = \sum (w_j R_j + w_l R_l + w_c R_c)$$

5.2 Entropy & Decay (The Anti-Stagnation Law)

To satisfy **Article V, Clause 2** of the Constitution, reputation is subject to **Temporal Decay**. This ensures that "Legacy Power" cannot dominate the protocol.

The current reputation $R_p(t)$ at time t is calculated using an exponential decay function:

$$R_p(t) = R_p(0) \cdot e^{-\lambda t}$$
Where:

- $R_p(0)$ is the reputation at the last active contribution.
- t is the time elapsed since that contribution.
- λ is the **Decay Constant** (initially set to a half-life of 180 days).

Logic: If a high-authority juror stops participating, their voting power naturally evaporates, allowing new, active citizens to rise in influence.

5.3 Governance Mechanics: Voting Power (VP)

Nomos utilizes a **Hybrid Quadratic Governance** model. This prevents "Sybil" attacks by requiring reputation while allowing stakeholders to signal their "Skin in the Game."

The Voting Power (VP) for any proposal is defined as:

$$VP = (R_p \cdot w_r) + \sqrt{S \cdot w_s}$$
Where:

- R_p: The citizen's current Reputation.
- S: The amount of $UNTT$ staked for the vote.
- w_r, w_s: Protocol weights (Initially $w_r = 10, w_s = 1$).

The "Innate Human" Constraint: A proposal cannot pass without a simple majority of **Unique Human IDs** (First Citizens), regardless of the total VP deployed. This ensures that capital (S) can influence the *direction* of the protocol but cannot *overrule* the human collective.

5.4 Proposal Classes & Thresholds

Not all changes are equal. Nomos categorizes proposals to balance agility with security:

Class	Scope	Quorum	Time-Lock
Tuning	Parameter adjustments (e.g., C_V clamps, δ).	20%	24 Hours
Structural	New modules, shard upgrades, or UBL tasks.	40%	7 Days
Emergency	Security patches or "Flash-Freeze" actions.	66%	Instant*

**Emergency actions "Auto-Sunset" after 48 hours unless ratified by a Structural vote.*

5.5 Slashing & The "Black-Out" Period

Malicious behavior results in the immediate destruction of R_p.

- **Minor Infraction:** (e.g., lazy jury voting) results in a 10% R_p reduction.
- **Major Infraction:** (e.g., proven wash-trading or collusion) results in a **Full Strike**. The citizen's R_p is set to zero, and they enter a 90-day "Black-Out" period during which they cannot earn rewards or participate in governance.

This final section defines the interface between the protocol and the real-world economy. By establishing a guaranteed labor market and a reputation-driven trade layer, Nomos ensures that the **UNITT** transitions from a medium of exchange to a foundational store of "Work-Energy."

Section VI: Market Layer & Recirculatory Infrastructure

6.1 The Lex Merchant Protocol (LMP)

The LMP is the service-level agreement (SLA) layer for the Nomos economy. It translates **Reputation (R_p)** into transactional efficiency.

6.1.1 Reputation-Collateralized Trade

Unlike legacy systems that require high escrow fees, Nomos uses the **Reputation Buffer**.

- **Tier 1 (High R_p):** Merchants with $R_p > 25$ can execute "Optimistic Releases." The protocol acts as a temporary guarantor.
- **Tier 2 (New/Low R_p):** Merchants must utilize the **Standard Escrow Handshake**, where $UNTT$ is locked until a ZK-Receipt of delivery is cryptographically verified by the buyer's wallet.

6.2 Velocity Multipliers (V_m) & Circularity

To discourage "Siloed Wealth," the protocol incentivizes **Multi-Point Circulation**.

- **The Chain-Bonus:** If a $UNTT$ travels through ≥ 3 unique high-reputation merchants within a 72-hour window, the reward multiplier V_m increases by **1.1x** for that specific chain.
- **Logic:** This encourages local supply chains (e.g., Farmer $\to$ Baker $\to$ Citizen) over simple one-to-one recycling.

6.3 Universal Basic Labor (UBL) Technical Logic

UBL is implemented as a **Targeted Recirculatory Sink**. It is the "lowest energy state" of the Nomos economy, ensuring that idle capital from Section 2.7 (Maturity Clock) is always put to work.

6.3.1 The Prosperity Threshold (T_p) Enforcement

Eligibility is enforced via the **Threshold Gatekeeper** in the smart contract.

$$Eligibility(i) = \begin{cases} 1 & \text{if } Balance(i) < T_p \\ 0 & \text{if } Balance(i) \ge T_p \end{cases}$$

- **Adjustability:** T_p is a "soft parameter" tuned by the **Elastic Velocity Stimulus** logic. If global velocity (V_A) is high, T_p may contract to prevent inflation.

6.3.2 Human Challenge Oracles (HCOs)

The UBL tasks are generated as **Human Challenge Oracles**. These are tasks designed to be:

1. **Computationally Hard to Fake:** Requires human cognitive nuance (e.g., sentiment analysis of Lex Merchant disputes).
2. **Infrastructure-Critical:** Every task performed strengthens the network (e.g., decentralized data labeling for the Sentinel AI).

6.4 Recirculation Flow (The Maturity Clock Sink)

Unclaimed rewards from the Maturity Clock (Day 45+) are automatically re-minted into the **UBL Reward Pool**.

- **Step 1:** The Maturity_Monitor identifies stale rewards.
- **Step 2:** The private key of the original earner is stripped of "Claim Authority."
- **Step 3:** The value is committed to the UBL_Treasury as a "Bounty" for HCO tasks.
- **Step 4:** A new citizen completes the work and "re-activates" the $UNTT$ into the circulating supply.