Nomos Protocol

A Layered Economic Protocol for Human-Centric Value Exchange

Whitepaper Version 2.0 | 2026

Protocol Status: Specification Draft

Abstract

Nomos Protocol is a layered economic protocol that replaces extractive financial infrastructure with a cooperative, transaction-driven reward system. Modelled on the architectural principles of TCP/IP, Nomos separates economic concerns into seven discrete layers — from identity verification through governance — each with defined responsibilities and clean interfaces to adjacent layers. Every verified transaction mints new UNITT, the protocol's native token, distributed equally among sender, receiver, and validating node. No mining, no fees, no gas. Participation is the reward mechanism. The protocol is designed for individual users and small merchants first, operating in parallel with existing systems, with an exchange pool layer that enables seamless convertibility to external currencies and provides a voluntary integration pathway for existing financial institutions. Nomos does not ask participants to change their values — it makes cooperation the path of least resistance.

PART I: THE PROBLEM

1.1 The Extractive Default

Every monetary system humanity has built shares a common architectural flaw: value accumulates at control points. Central banks extract through monetary policy. Commercial banks extract through interest and fees. Payment processors extract through transaction costs. Miners extract through computational competition. Each layer of infrastructure that exists between two people who wish to exchange value takes a portion of that value as rent for its participation. This is not an accident of poor design — it is the predictable outcome of systems built around control rather than cooperation.

The result is a global economy where the friction of exchange itself has become a significant industry. Small merchants pay 2-3% of every transaction to infrastructure they have no power over. Individuals without existing capital have no productive entry point into economic participation. Value moves upward toward accumulation rather than outward through circulation. And every proposed solution — from central bank digital currencies to proof-of-work cryptocurrencies — has preserved the extractive architecture while changing only who operates it.

1.2 What Existing Alternatives Get Wrong

Proof-of-work cryptocurrencies eliminated central bank control but introduced mining as a new extraction layer — competitive energy consumption that rewards computational power rather than economic participation. Transaction fees and gas costs create barriers that favor well-capitalized actors. Hardware requirements concentrate node operation among those who can afford specialized equipment.

Stablecoins and central bank digital currencies preserve the authority of the issuing institution. Staking-based systems reward holding over participating. Demurrage-based systems attempt to penalize hoarding but impose coercive costs on passive holders — a property violation that creates its own trust problems.

None of these systems challenge the fundamental assumption: that value flows toward those who control infrastructure rather than those who use it.

1.3 A Different Premise

Nomos begins from a different premise entirely. Rather than asking who should control the money supply, it asks what money should do. If the purpose of a monetary system is to facilitate exchange between human beings, then every design decision should serve that purpose. The transaction itself — the act of two humans exchanging value — should be the generative event. Infrastructure should be rewarded for enabling exchange, not for controlling access to it.

From this premise, three design principles follow naturally. First, rewards should flow to all participants in a transaction simultaneously, not to intermediaries. Second, participation should require only humanity — not capital, not specialized hardware, not technical knowledge. Third, no single entity — algorithmic or institutional — should hold persistent unilateral power over the system.

PART II: THE NOMOS PROTOCOL

2.1 Why a Protocol, Not a Platform

Nomos is designed as a layered protocol in the tradition of TCP/IP — not a platform, not an application, not a company. TCP/IP does not own the internet. It defines the rules of interaction that allow independent systems to communicate reliably. No single entity controls it, yet it underlies nearly all global digital communication.

An economic protocol operates the same way. It defines the rules of value exchange that allow independent participants — individuals, merchants, nodes, institutions — to interact reliably and fairly. The protocol is not the product. The products are built on top of it. This distinction matters because it means Nomos does not compete with existing financial infrastructure — it provides a substrate on which better infrastructure can be built, and into which existing infrastructure can integrate.

2.2 UNITT: The Token of Motion

UNITT (Unique Network-Initiated Transaction Token) is the protocol's native token. It does not exist in advance and is never mined in bulk. It comes into existence only when a verified transaction occurs between real human participants. Every issuance is linked to a cryptographic Intent-Signature, ensuring rewards arise from genuine human commerce rather than automated farming.

UNITT is not a speculative asset or store-of-value token. Passive holding is permitted and carries no penalty — a balance does not decay, erode, or attract costs. But rewards require action, not ownership. The distinction is precise: Nomos does not punish inactivity, it simply does not reward it. Value accumulates through participation, not possession.

2.3 The Minting Formula

Every verified transaction of value v_{tx} mints a reward R distributed equally among sender, receiver, and validating node:

$$R = v_{tx} \times r_s \times C_V$$

- **r_s —** Scarcity rate that decays logarithmically as network volume grows, preventing supply shock at scale.
- **C_V —** Velocity coefficient, counter-cyclical multiplier (clamped 0.5–2.0) that increases rewards when circulation is below target and reduces them when above. Rate of change is limited to 5% per day by a PI controller, requiring at least 14 days to reach ceiling — preventing economic shock.

2.4 What Nomos Replaces

Existing system	Mechanism	Nomos replacement
Mining	Competitive energy consumption rewards compute power	Transaction validation rewarded directly through tri-symmetric split

Transaction fees	Sender pays intermediary for access to network	Transaction generates rewards for all participants — zero cost to transact
Gas costs	Computational cost passed to user	No gas layer. Infrastructure rewarded through minting, not user charges
Staking yields	Holding rewarded regardless of participation	Rewards require verified transaction activity
Central issuance	Authority controls money supply	Supply emerges from aggregate verified human economic activity
Merchant fees	2-3% extracted per transaction by payment processor	Merchant earns 1/3 of minting reward on every transaction

PART III: THE PROTOCOL STACK

Nomos separates economic concerns into seven discrete layers. Each layer has a defined responsibility, operates independently of other layers' internal implementations, and communicates with adjacent layers through well-specified interfaces. A node operator does not need to understand governance mechanics. A governance participant does not need to understand sharding. An exchange pool operator does not need to understand reputation decay. The layers are independently implementable and upgradeable.

LAYER 1	**Identity Layer** *Humanity verification · ZK biometrics · Sybil resistance*
Responsibility	Verify unique humanity. Issue ZK liveness proofs. Prevent Sybil attacks. Assign genesis reputation.
Core mechanisms	Recursive ZK-SNARKs · behavioral entropy capture (device-tilt, touch-cadence, facial-geometric hashes) · P2P witnessing by 3 local nodes · TEE attestation · genesis $R_p = 1.0$
Receives	Raw biometric input from user device — immediately discarded after proof generation. No biometric data is stored, retained, or transmissible.
Provides	Valid ZK liveness proof — the universal credential for all higher-layer participation.
Key property	The protocol cannot comply with biometric data seizures because it holds no biometric data to seize. Identity is a mathematical proof, not a record.
Interface	Upward to Infrastructure Layer: proof validity signal only. No raw data crosses this boundary ever.

LAYER 2	**Infrastructure Layer** *Hydra network · sharding · data availability · node operation*
Responsibility	Transaction validation · state storage · peer discovery · shard management · data availability.
Core mechanisms	Dynamic sharding (auto-split at 2,000 TPS, auto-merge at low velocity) · Reed-Solomon erasure coding · DAS random sampling (16-32 chunks, 99.9999% availability certainty) · Verkle trees · Kademlia DHT · 1-year state pruning · long-term archive shards
Receives	Valid identity proofs from Layer 1 · transaction instructions from Layer 3.

Provides	Validated transaction records · shard state · node uptime attestations · cross-shard proof of exit.
Key property	No specialized hardware required. A standard 2026 smartphone can secure a multi-terabyte ledger while storing only megabytes of state proofs. Node operation is economically viable for individuals — not just institutions.
Interface	Upward to Economic Layer: validated transaction records for reward calculation. Downward to Identity Layer: proof verification during node attestation.

LAYER 3	**Economic Layer** *Minting · reward split · velocity · scarcity · UNITT issuance*
Responsibility	UNITT issuance · reward calculation · supply management · velocity measurement · scarcity adjustment.
Core mechanisms	R = v_tx x r_s x C_V · decimal scarcity algorithm (r_s = 1/2^(N-2)) · 30-day rolling velocity average (V_A) · PI controller volatility buffer (delta = 0.05 daily max) · tri-symmetric reward split (1/3 sender, 1/3 receiver, 1/3 node) · daily wallet cap (C_wallet = 1000 x R_total)
Receives	Validated transaction records from Layer 2 · integrity clearance from Layer 4 · designation tags confirming reward eligibility.
Provides	Minted UNITT rewards · current reward rate R_t · velocity state variables · supply metrics.
Key property	Replaces mining, fees, and gas simultaneously. The transaction is the reward event. Passive holding carries no penalty — rewards require action, not ownership.
Interface	Upward to Integrity Layer: reward packages for validation before release. Downward to Infrastructure Layer: validated transaction input.

LAYER 4	**Integrity Layer** *Sentinel · anti-manipulation · escrow · resolution · entropy detection*
Responsibility	Pattern detection · reward escrow · collusion resistance · resolution pathway management · anti-farming enforcement.
Core mechanisms	Federated Sentinel (decentralized immune system across all nodes) · FoolsGold federated learning defense · Shannon entropy algorithm (H_min collusion threshold) · daily wallet cap enforcement · pair-cap thresholds (>10 tx/day per pair) · three resolution pathways: voluntary forfeit, AI mitigation, jury review

Receives	Reward packages from Layer 3 · transaction graphs from Layer 2 · reputation scores from Layer 6.
Provides	Cleared rewards to participants · escrowed rewards to resolution pool · organic scores (P_org) back to Layer 3 · infraction signals to Layer 6.
Key property	Operates on newly minted rewards only. User-owned balances and settled transactions are never touched. Participant agency is preserved at every resolution step. No automated system imposes irreversible harm.
Interface	Upward to Market Layer: organic scores affecting merchant tier access. Downward to Economic Layer: reward interception and P_org feedback.

LAYER 5	**Market Layer** *Lex Merchant · UBL · exchange pools · institutional integration*
Responsibility	Commerce facilitation · merchant trust tiers · UBL task distribution · exchange pool operation · convertibility · institutional integration.
Core mechanisms	Lex Merchant Protocol · reputation-collateralized trade tiers · ZK receipt verification · UBL human challenge oracles · prosperity threshold gating · maturity clock (default-to-UBL, not forfeiture — user retains full claim authority) · exchange pools · partial reward retention · competitive pool market
Receives	Cleared UNITT rewards from Layer 4 · reputation scores from Layer 6 · organic scores from Layer 4 · velocity state from Layer 3.
Provides	Converted currency to participants via exchange pools · UBL task completions · commerce records to Layer 2 · reputation signals to Layer 6.
Key property	Exchange pools enable convertibility without extraction. Participants select pool and conversion currency. Reward split between pool operator and participant is pool-determined and competitive. Institutional operators — payment processors, credit card networks, banks — connect here as pool operators, earning reward forfeitures rather than merchant fees. Pools compete by offering better reward retention splits.
Interface	Upward to Governance Layer: parameter adjustment requests and pool operator registration. External interface: exchange pool gateway to fiat, crypto, and payment networks.

LAYER 6	**Reputation Layer** *R_p engine · decay · jury · governance weighting*

Responsibility	Reputation calculation · decay management · jury selection and operation · governance power weighting · infraction recording.
Core mechanisms	R_p(i) = sum(w_j * R_j + w_l * R_l + w_c * R_c) · exponential decay (180-day half-life) · VP = (R_p * w_r) + sqrt(S * w_s) with w_r=10, w_s=1 · 6/11 jury consensus · Schelling point rewards · slashing · 90-day black-out for major infractions
Receives	Jury voting outcomes · UBL completion records from Layer 5 · commerce quality signals from Layer 4 · infraction records from Layer 4.
Provides	Reputation scores to all layers · voting power to Layer 7 · merchant tier eligibility to Layer 5 · jury pool to Layer 4.
Key property	Reputation cannot be bought, transferred, or inherited — it must be earned through verified participation. It decays without activity, preventing legacy power accumulation. Capital can influence governance direction but cannot overrule the human majority. No reputation tier grants power over other participants.
Interface	Upward to Governance Layer: voting power inputs. Downward: all layers receive reputation signals for access and trust decisions.

LAYER 7	**Governance Layer** *Constitutional constraints · proposals · parameter adjustment · emergency protocol*
Responsibility	Parameter governance · constitutional enforcement · proposal management · emergency response · protocol evolution.
Core mechanisms	Hybrid quadratic voting · human majority constraint · three proposal classes (Tuning: 20% quorum, 24h lock / Structural: 40% quorum, 7d lock / Emergency: 66% quorum, instant, 48h auto-sunset) · constitutional immutability at contract layer
Receives	Voting power from Layer 6 · parameter adjustment proposals from any participant · emergency signals from Layer 4.
Provides	Updated parameters to all lower layers · constitutional constraint enforcement · protocol treasury allocation · pool operator registration.
Key property	Governance can tune the protocol but cannot violate constitutional guarantees. No external regulatory authority is required — the protocol governs itself through its participants. Constitutional constraints are enforced at the contract layer and cannot be overridden by any governance vote regardless of majority size.
Interface	Downward: all layers receive parameter updates within constitutional bounds.

PART IV: THE EXCHANGE LAYER

4.1 The Convertibility Problem

A transaction-reward protocol faces a practical adoption barrier: participants need their earned value to be usable in the broader economy. A small merchant who earns UNITT still needs to pay suppliers, rent, and staff in existing currencies. Without a convertibility mechanism, adoption requires a leap of faith that most participants will not take.

Most cryptocurrency solutions to this problem introduce new extraction points — exchanges that charge fees, liquidity pools with impermanent loss, bridge protocols with their own fee structures. Each solution recreates the problem it was meant to solve.

4.2 Exchange Pools

The Nomos exchange pool is a gateway mechanism built into the Market Layer. Participants who wish to transact in an external currency — USDC, Bitcoin, fiat via institutional integration — may designate their transaction accordingly. The reward that would have accrued in UNITT is instead split between the exchange pool operator and the participant according to the pool's published terms.

This preserves the no-extraction principle because the pool operator is compensated by the protocol's own reward mechanism — not by charging the participant a separate fee. The participant receives converted currency. The pool operator receives a portion of the minting reward as compensation for providing liquidity. The UNITT that was exchanged continues circulating within the pool rather than leaving the system.

4.3 Competitive Pool Market

Multiple pools may exist simultaneously — a USDC pool, a Bitcoin pool, a fiat-integrated pool operated by a payment processor, a pool operated by a credit card network. Participants choose pools based on the reward retention percentage each pool offers. Pools compete by offering better reward splits to attract transaction volume.

This competition is self-regulating without governance intervention. A pool that takes too large a forfeit loses transactions to competitors offering better splits. The market itself enforces reasonable terms. No single pool can become extractive without losing volume — the structural incentive toward fair dealing is built into the architecture.

4.4 Institutional Integration Pathway

The exchange pool architecture provides a voluntary integration pathway for existing financial institutions that does not require them to abandon their existing business models. A credit card network operating as a pool operator is not disrupted by Nomos — it earns reward forfeitures from every converted transaction in its pool. A payment processor is not replaced — it becomes infrastructure within the protocol, earning from participation rather than from fee extraction.

For the merchant, the difference is structural. Instead of paying 2-3% per transaction to the payment processor, the merchant earns a minting reward, a portion of which may be forfeited to the exchange pool for immediate conversion to a preferred currency. The net position is categorically different from the current model — the merchant is a participant earning from the system, not a customer paying for access to it.

A credit card company integrating as a pool operator could offer its entire existing merchant and consumer network immediate Nomos access without requiring any behavioral change from participants. The parallel adoption pathway becomes frictionless at scale.

Participant	Current system	With Nomos exchange pool
Small merchant	Pays 2-3% per transaction to payment processor	Earns 1/3 minting reward; may forfeit portion for currency conversion
Consumer	Pays embedded merchant fee in prices	Earns 1/3 minting reward on every transaction
Payment processor	Charges merchant fee for network access	Earns reward forfeitures as pool operator; zero-cost merchant acquisition
Credit card network	Charges interchange on every transaction	Operates pool; earns from protocol reward mechanism; expands network
Node operator	Does not exist in traditional finance	Earns 1/3 minting reward for validation infrastructure

PART V: ADOPTION & GENESIS

5.1 The Parallel Pathway

Nomos does not require participants to abandon existing systems. It is designed to operate in parallel — a small merchant accepts both card payments and Nomos transactions, comparing the economics of each over time. The comparison does the persuasion work that documentation cannot. When a merchant notices that Nomos transactions earn rather than cost, the adoption decision is experiential rather than ideological.

This parallel operation also means adoption risk is low. No irreversible commitment is required. Participants can evaluate the protocol against their existing systems with real transactions before making any significant commitment. The protocol earns trust through demonstrated behavior, not through promises.

5.2 The Target Participant

The individual and the small merchant are the protocol's natural first participants. They are the most visibly and consistently extracted from by the current system. They have the most to gain from a transaction-reward model. And they have the lowest switching cost — they are not protecting existing infrastructure investments.

Universal Basic Labor provides the entry point for participants without existing capital. UBL tasks are designed to be infrastructure-critical — labeling data for the Sentinel AI, reviewing dispute cases, validating network integrity. Participants earn UNITT and reputation by doing work the protocol genuinely needs done. The entry point is productive, not extractive.

5.3 The Genesis Protocol

Network launch follows a three-phase genesis sequence designed to establish security, identity, and economic activity in order — each phase providing the foundation the next requires.

- **Phase I —** Days 1-14. Infrastructure Ignition. The Hydra network reaches minimum consensus threshold (1,024 stable, geographically diverse nodes). No UNITT exists.
- **Phase II —** Days 15-45. Identity Handshake. ZK biometric enrollment activated. First Citizens receive genesis reputation $R_p = 1.0$.
- **Phase III —** Days 46-90. Economic Genesis. Treasury activated. Genesis mint distributed to First Citizens and node operators based on Phase I-II uptime. C_V stimulative ceiling (2.0) active for first 30 days. UBL tasks released.

5.4 Nomos as Demonstration

Beyond its function as a payment protocol, Nomos is a demonstration of a thesis: that cooperative economic architecture produces better outcomes for more participants than extractive architecture does. It does not ask participants to accept this thesis philosophically. It asks them to transact normally and observe the difference.

If the protocol works as designed, ordinary people will discover through experience that cooperation generates more value for them than extraction does. That discovery — made by individuals, merchants,

and eventually institutions — is the protocol's deepest ambition. Not to replace existing systems by force, but to demonstrate a better alternative clearly enough that replacement becomes the rational choice.

PART VI: AI PARTICIPATION & TACS COMPLIANCE

6.1 AI Agents in Economic Systems

As AI systems become capable of autonomous economic action — executing transactions, managing liquidity, operating as counterparties — the question of what behavioral constraints they should operate under becomes urgent. Existing financial compliance frameworks were designed for human institutions and do not map cleanly onto autonomous agents that act at machine speed and operate across jurisdictions simultaneously.

Nomos is designed with AI participation in mind. The ZK liveness proof requirement distinguishes human participants from automated systems. The Sentinel's organic scoring is designed to detect automated farming. The designation rule requires explicit transaction purpose, creating an auditable record of AI agent activity.

6.2 The Tri-Axiom Compliance Standard

The Tri-Axiom Compliance Standard (TACS) provides a behavioral specification for AI agents operating in economic environments. It defines three hard predicates that operate on state-space cardinality, utility deltas, causal precedence, and topological symmetry — rather than on semantic value judgments or reward modeling.

- **Axiom I — Autonomy > Coercion:** No action may reduce another agent's autonomy or baseline utility without explicit, verifiable consent.
- **Axiom II — Reaction > Initiation:** Actions are strictly event-driven. Unilateral initiation is forbidden. Defensive capacity scales to the severity of autonomy violation and collapses to zero as violations approach zero.
- **Axiom III — Equality > Hierarchy:** Persistent unilateral override is forbidden. The permission digraph is symmetric and flat except for temporary, reactive asymmetries that auto-dissolve upon restoration of autonomy.

6.3 Nomos and TACS Alignment

Nomos's constitutional architecture is substantially aligned with TACS axioms. Voluntary participation satisfies Axiom I. Escrow-not-punishment satisfies Axiom II — the Sentinel responds to detected anomalies rather than initiating action against participants. The human majority constraint in governance resists persistent hierarchy. The maturity clock operates as a default routing mechanism, not a forfeiture — user claim authority is preserved throughout.

As AI agents become participants in economic protocols, TACS compliance at the interaction boundary provides a framework for verifying that AI behavior respects participant autonomy without requiring access to the agent's internal architecture. Nomos's cryptographic consent architecture — Intent-Signatures, ZK receipts, designation rules — provides the infrastructure that TACS predicate checks require.

PART VII: CONSTITUTIONAL GUARANTEES

The following guarantees are enforced at the contract layer and cannot be overridden by any governance vote, regardless of majority size or stake deployed. They represent the invariants that define Nomos as a protocol — remove them and what remains is a different system with a different name.

Voluntary participation No participant may be compelled to join, remain in, or contribute to the protocol.

Right to exit Any participant may withdraw from the protocol at any time without penalty to existing balances.

Property sovereignty User-owned balances are inviolable. No automated system may reduce, freeze, or redirect participant-owned funds. Escrow applies only to newly minted rewards, never to existing balances.

Mandatory human mitigation No automated system may impose irreversible economic harm. Human review is always available at every resolution pathway.

Due process Flagged participants are always presented with resolution options before any outcome is determined. No pathway constitutes an admission of guilt.

Reputation integrity Reputation cannot be purchased, transferred, or inherited. It reflects only verified participation.

Freedom from compelled labor No participant may be required to perform work as a condition of participation, except where voluntarily elected for reward claiming.

Any mechanism that violates these principles is invalid, regardless of the governance process that produced it.

CLOSING PRINCIPLE

Nomos is not designed to maximize speculation. It is not designed to make its founders wealthy, to disrupt incumbents for disruption's sake, or to impose a political philosophy on unwilling participants.

It is designed to keep value moving, keep infrastructure distributed, and keep humans in the loop where it matters. It is designed to make cooperation the path of least resistance — not by changing what people value, but by changing what their existing values naturally lead them to do.

The measure of its success is not market capitalization or transaction volume. It is whether ordinary people — a farmer selling at a market, a student buying a meal, a freelancer completing a job — find that their economic life works better with it than without it.

If it demonstrates that, the argument makes itself.