Elara Tokenomics v0.3.2

Elara Protocol: Token Economics

Version 0.3.2 Date: February 21, 2026 **Author:** Nenad Vasic **Contact:** nenadvasic@protonmail.com

Disclosure: This document was written with AI assistance for technical prose and economic modeling. The economic architecture, design decisions, and all core concepts are the author's original work.

Status: Early design. This document will evolve as the protocol approaches mainnet. All parameters are subject to change based on testnet data.

Abstract

This paper specifies the token economic model for the Elara Protocol — a post-quantum universal validation layer for digital work. The ELA token is a utility token that enables witness incentives, resource exchange, and governance within the protocol's Layer 2 network consensus.

The economic model is built on four principles that distinguish it from existing blockchain token designs:

1. **Conservation, not inflation** — fixed total supply; tokens circulate between producers and consumers, never minted after genesis
2. **No gas fees** — transaction costs are absorbed by the network's reciprocal witnessing model, not charged per transaction
3. **Layer 1 is always free** — local cryptographic validation never has a cost
4. **Native chain** — the Directed Acyclic Mesh (DAM) is the ledger; no dependency on any external blockchain

This paper covers the supply model, distribution, storage delegation markets, anti-centralization mechanisms, governance economics, Sybil cost analysis, securities law considerations, and launch strategy. It is a companion to the Elara Protocol Whitepaper, which specifies the technical architecture.

Table of Contents

---

1. Design Philosophy

1.1 Why Not Use an Existing Chain?

Most token projects deploy contracts on existing blockchains. This is fast and easy but creates fundamental problems for the Elara Protocol:

Gas fees at scale are prohibitive. The Elara Protocol is designed for millions of nodes performing witness attestations. If each attestation incurs a gas fee — even $0.001 on a Layer 2 — a factory with 10,000 nodes performing 100 attestations per hour would spend $1,000/hour in gas alone. At a million nodes, the economics collapse.

Dependency on external consensus. Deploying on an existing chain means the protocol's economic layer depends on that chain's consensus, fee market, and governance. A protocol designed for 1,000-year operation cannot depend on the continued health of another project.

The DAM already is a ledger. The Directed Acyclic Mesh — the protocol's core data structure — already handles signed records, cryptographic identity, witness attestation, and trust scoring. Token transfers are simply a new record type in an existing architecture. Building on an external chain would mean maintaining two consensus systems.

1.2 The Token is Energy, Not Currency

Traditional token models treat tokens like money: you buy them, hold them, sell them. The ELA token is designed like **energy in a closed system** — it transforms but is never created or destroyed after genesis.

```
Physics:  Energy is conserved. It transforms between kinetic,
potential, thermal.
          Total energy in a closed system is constant.

ELA:      Tokens are conserved. They transform between witness
```

```
rewards, storage payments,
         governance stakes. Total supply is constant after genesis.
```

This means: - No inflation eroding existing holders - No deflationary spirals from aggressive burning - No miner extractable value from fee markets - Economic activity is measured by token **velocity** (how fast they circulate), not token **supply**

1.3 Four Non-Negotiable Principles

Principle	Rationale
Layer 1 is always free	A teenager in Kenya validates her poem on a $30 phone. No token required. The moral bright line of the protocol.
No gas fees	At scale, per-transaction fees kill the economics. Reciprocal witnessing absorbs the cost.
Fixed supply	No inflation, no minting after genesis. Tokens circulate, not accumulate.
Native chain	The DAM is the ledger. No external blockchain dependency.

2. The Conservation Model

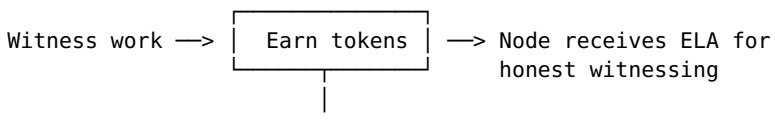
2.1 Supply Mechanics

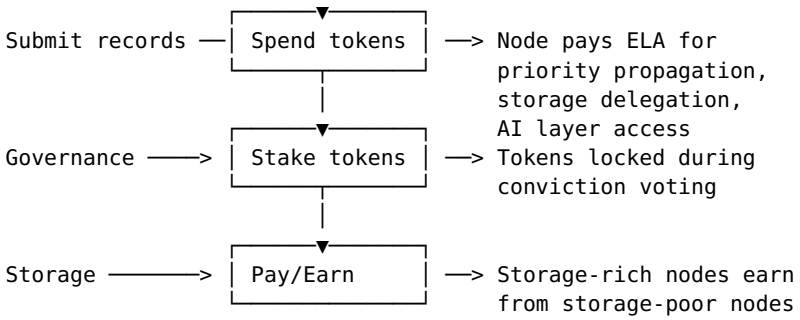
```
┌──────────────────────────────────────────────────┐
│              ELA Token Supply                    │
│                                                  │
│  Genesis: X tokens minted into distribution pools │
│  After genesis: ZERO new tokens ever minted      │
│                                                  │
│  Total supply = X  (constant, forever)           │
└──────────────────────────────────────────────────┘
```

The total supply X is determined before mainnet launch based on testnet economics data. The number itself is less important than the conservation property: every token in circulation was created at genesis and will exist until the protocol ceases to operate.

2.2 Circulation, Not Accumulation

Tokens flow through the network in a closed loop:





Where the tokens go when you "spend" them:

Unlike gas fees (which are burned or paid to miners), ELA tokens spent on services flow directly to the nodes providing those services:

Action	Tokens flow to
Priority propagation	Relay nodes that propagate your records faster
Requested witnessing	Anchor nodes that attest to your records on demand
Storage delegation	Storage nodes that hold your records long-term
AI layer access	Nodes running Layer 3 cognitive services
Dispute arbitration	Arbitration panel members (refundable if claim upheld)

No tokens are burned. No tokens go to "the protocol." Every token spent by one node is earned by another. Conservation.

2.3 Why Not Burn Tokens?

Many protocols burn tokens to create deflationary pressure. This is counterproductive for Elara:

- **Burning reduces circulating supply** → tokens become scarcer → new participants face higher entry cost
- **Burning rewards hoarding** → participants hold tokens expecting appreciation rather than using them
- **Burning creates MEV-like incentives** → node operators optimize for burn-adjacent transactions

The conservation model avoids all of these. Token value comes from **utility** (what you can do with them on the network), not **scarcity** (how many exist). A healthy network has high token velocity — tokens moving fast between producers and consumers — not high token price.

---

3. Token Utility

3.1 What Tokens Do

The ELA token has exactly four uses. If an action is not in this list, it does not require tokens:

1. Witness Staking Witness and anchor nodes stake tokens to participate in attestation. The stake creates an economic barrier against Sybil attacks (Protocol Whitepaper, Section 11.1) and aligns incentives — a witness with skin in the game is more likely to attest honestly.

2. Priority Network Services Basic network propagation and organic witnessing are free. Tokens purchase expedited services: - Priority propagation (faster global reach) - Requested witnessing (specific anchor nodes attest on demand) - Priority sync (records synced first during bandwidth-limited windows) - Layer 3 AI capabilities (pattern analysis, similarity search, anomaly detection)

3. Storage Delegation Nodes that cannot store their own records long-term pay storage-specialized nodes to hold them (see Section 4).

4. Governance Participation Token holders participate in protocol governance through conviction voting — staking tokens toward proposals with time-weighted conviction (see Section 7).

3.2 What Tokens Do NOT Do

- **Layer 1 validation** — Always free. No token required.
- **Basic network propagation** — Free via gossip protocol. Relaying is incentive-compatible (nodes benefit from a well-connected DAM).
- **Organic witnessing** — Witnesses choose what to attest. Attestations from organic witnesses accumulate without payment.
- **Identity creation** — Generating a cryptographic keypair is free.
- **Record creation** — Creating and signing validation records is free.

The protocol is fully functional without tokens for any single user. Tokens become relevant only when a node interacts with the Layer 2 network and wants services beyond baseline.

---

4. Storage Delegation Market

4.1 The Problem

Not every node can store everything. Phones, IoT sensors, Raspberry Pis — limited storage. But these devices still want to participate (witness, earn tokens, submit records). The network must accommodate nodes with asymmetric capabilities.

4.2 Tiered Node Participation

```
┌─────────────────────────────────────────────────┐
│  Light Node (phone, IoT device, small computer)  │
│  - Stores own records + record headers only      │
```

```
│  - Can witness other nodes' records (earns tokens)  │
│  - Can submit records (uses free-tier or paid-tier) │
│  - Delegates long-term storage to storage nodes     │
├─────────────────────────────────────────────────────┤
│  Full Node (desktop, server, NAS)                   │
│  - Stores all records in its assigned shard         │
│  - Witnesses + serves data to light nodes           │
│  - Earns tokens from both witnessing and serving    │
├─────────────────────────────────────────────────────┤
│  Storage Node (datacenter, high-capacity server)    │
│  - Specializes in storage + data serving            │
│  - Earns tokens from light/full nodes for hosting   │
│  - Competes on reliability, uptime, and price       │
└─────────────────────────────────────────────────────┘
```

Module Tiers and Economic Roles

The Elara Core reference implementation (v0.15.0) introduces a **module tier system** that controls cognitive capability at the node level. This is orthogonal to the economic participation tiers described above: module tiers control what a node *thinks*, economic roles control what a node *does on the network* for token purposes.

Core Module Tier	Cognitive Capability	Typical Economic Role	Token Interaction
Tier 0: VALIDATE	Signing only	Light Node	Submits records; may delegate storage; no witnessing
Tier 1: REMEMBER	Memory + persistence	Light Node	Same as Tier 0, plus basic recall for own records
Tier 2: THINK	Reasoning + analysis	Full Node	Witnesses, earns tokens, generates cognitive checkpoints
Tier 3: CONNECT	Full network cognition	Full/Storage Node	Full participation: witnessing, storage, Layer 3 AI services, inter-node cognitive exchange

A Tier 0 gateway at a factory is a Light Node that submits batch-signed sensor readings but never earns witness tokens. A Tier 3 server is a Full Node that runs cognitive analysis, witnesses records, and provides AI layer

services for tokens. The tier determines capability; the economic role determines token flow.

Nodes can operate at any module tier regardless of economic role — a Storage Node could theoretically run at Tier 0 (just storing data, no cognition), while a Light Node could run at Tier 2 (reasoning locally, but not serving the network). In practice, higher tiers correlate with higher economic participation because cognitive capabilities enable higher-value services.

4.3 Delegation Mechanism

A light node creates a `STORAGE_DELEGATE` record on the DAM:

```
STORAGE_DELEGATE {
    from:          light_node_identity
    to:            storage_node_identity
    record_refs:   [record_id_1, record_id_2, ...]
    cost:          N ELA
    duration:      365 days
    signed_by:     light_node_private_key
    witnessed_by:  [independent_witness_1, independent_witness_2]
}
```

The storage node holds the full record payloads. The light node retains the signed headers (tiny, ~500 bytes each). This means:

- The light node can always **prove ownership** of its records (it holds the signed headers)
- The storage node provides **data availability** (it serves the full payloads on request)
- If the storage node goes offline or loses data, its **trust score drops** — storage delegation is a reputation-critical function

4.4 Storage Market Dynamics

Storage nodes compete in an open market:

- **Price competition** — multiple storage nodes offer different rates
- **Reliability competition** — nodes with higher uptime and data integrity earn higher trust scores, attracting more clients
- **Geographic diversity** — nodes in different regions provide redundancy; light nodes can delegate to multiple storage nodes for fault tolerance

The node **chooses** its storage provider. The network does not assign storage. This is a free market within the protocol's conservation economics.

> **Hardware evolution note:** The storage economics described here assume current hardware, where the DAM requires ~45% index overhead (Hardware Whitepaper, Section 3.3). Native hardware (Gen 1 FPGA 2029, Gen 2 ASIC 2032+) progressively eliminates this overhead through physical dimensional addressing, reducing per-

> record storage costs by up to 30%. As native hardware adoption grows, the storage delegation market equilibrium will shift — lower costs per byte stored, potentially lower fees, but also lower overhead for storage providers. The conservation model accommodates this: tokens circulate at whatever price the market clears.

4.5 The Header Rule

Critical invariant: The original node always retains the signed record header. Only the payload is delegated. This means:

- Ownership proof is always local (header contains the creator's signature)
- Storage delegation is a convenience, not a dependency
- Even if every storage node in the world goes offline, the header-holder retains cryptographic proof of their work

4.6 Cognitive Checkpoint Storage Economics

The Cognitive Continuity Chain (Protocol Whitepaper v0.5.2, Section 3.2 and 11.35) generates `cognitive_checkpoint` ValidationRecords on the DAM. These records have storage and economic implications that integrate with the delegation market.

Layer 1 (local): always free.

Cognitive checkpoints stored locally on the generating node have zero token cost. This preserves the protocol's moral foundation — a node's cognitive continuity is its own business, not a billable event. A developer running Elara Core on a laptop generates ~30 checkpoints/day, stored locally, for free.

Storage delegation: checkpoints count toward the delegated record set.

If a Tier 2+ node delegates storage to a storage node (Section 4.3), its cognitive checkpoints are included in the delegated set. The storage cost is proportional to size:

```
Checkpoint storage budget:
  30 checkpoints/day × ~3,500 bytes = ~100 KB/day
  365 days × 100 KB = ~36.5 MB/year per node

Compare to typical record storage:
  A moderately active creator: ~10 MB/day in validation records
  Cognitive checkpoints: ~0.1 MB/day = 1% of total storage

Cost impact: negligible. Checkpoints round to zero in storage
delegation pricing.
```

Network witnessing: same fees as any other record.

Cognitive checkpoints that propagate to the Layer 2 network are witnessed under the same economic rules as any other ValidationRecord. Organic witnessing is free. Requested witnessing (specific anchor attestation) costs

tokens per the standard witness fee schedule.

In practice, most cognitive checkpoints are **not** propagated to the public network — they are local or private network records. A node may choose to publish its cognitive continuity chain for trust purposes (proving unbroken operation to peers), but this is optional.

Industrial scale: negligible.

Consider the Samsung factory scenario (Protocol Whitepaper v0.5.2, Section 3.6):

```
1 factory AI (Tier 2): ~30 checkpoints/day = 100 KB/day
100 factories: 3,000 checkpoints/day = 10 MB/day
vs. 86.4 billion sensor records/day

Cognitive checkpoints = 0.00000001% of total record volume
```

Cognitive checkpoints are economically invisible at industrial scale. They generate negligible storage demand, negligible witness demand, and zero impact on token velocity. The Cognitive Continuity Chain is a trust mechanism, not an economic one — it consumes resources the way a heartbeat consumes calories: real but unnoticeable.

---

5. Distribution

5.1 Genesis Allocation

Genesis Token Distribution	
Network Bootstrap	30%
Development Fund	20%
Community/Governance	20%
Founding Team	15% (4-year vest)
Early Contributors	10% (2-year vest)
Reserve	5%

5.2 Allocation Details

Network Bootstrap (30%) — Distributed to the first 10,000 nodes through participation rewards. Nodes earn tokens by running validators, witnessing records, and providing storage during the bootstrap phase. This is the largest allocation because it directly incentivizes the network's critical early growth. No purchase required — tokens are earned by doing real work.

Development Fund (20%) — Controlled by a multi-signature wallet (minimum 3-of-5 signers, geographically distributed). Funds protocol development, security audits, and infrastructure maintenance. Transparent quarterly reports on fund usage.

Community/Governance (20%) — Treasury for conviction voting governance (Section 7). Used for developer grants, research funding, ecosystem growth, and community witnessing pools (anchor nodes that attest to free-tier records, ensuring economic accessibility).

Founding Team (15%) — 4-year vesting with 1-year cliff. No tokens accessible in year 1, then linear monthly unlock over years 2-4. This allocation is not purchased — it is earned through protocol development. The vesting schedule prevents dump-and-run incentives.

Early Contributors (10%) — 2-year linear vesting. For developers, testers, and researchers who contribute before mainnet launch. Allocated through a transparent grants process governed by multi-sig.

Reserve (5%) — Emergency fund for unforeseen circumstances (security incidents, legal defense, critical infrastructure failures). Requires 4-of-5 multi-sig approval for any withdrawal.

5.3 What is NOT in the Distribution

- **No ICO.** No public token sale before mainnet.
- **No pre-sale.** No venture capital allocation at a discount.
- **No airdrop.** No free tokens for wallet addresses. Tokens are earned through participation.
- **No exchange listing campaign.** The token launches on decentralized exchange (protocol-native) only.

This distribution model is designed to make the “investment of money” prong of the Howey test inapplicable (see Section 11).

---

6. Anti-Centralization Mechanisms

6.1 The Threat

Every decentralized network faces the same risk: large entities accumulate disproportionate power. Proof-of-work chains see mining pools controlling 51%+. Proof-of-stake chains see staking providers dominating validation. If Elara’s token economy allows similar concentration, the network’s decentralization is a fiction.

The specific threat for Elara: a large entity (factory, cloud provider, state actor) runs thousands of nodes → earns most witness rewards → accumulates most tokens → controls governance → network is effectively centralized.

6.2 Why Elara is Structurally Different

Consensus is trust-based, not token-based.

In proof-of-stake systems, consensus power is proportional to staked tokens. More tokens = more blocks = more rewards = more tokens (positive feedback loop).

In Elara, consensus is based on **witness trust scores** — earned through honest behavior over time, not purchased with tokens.

Node trust score (reputation of a specific node):

```
Node trust: T(n) = 1 - 1/(1 + attestation_count)
where attestation_count = honest witness attestations by this node

New factory spins up 10,000 nodes:
  Day 1:   T = 0.0 for all nodes (untrusted)
  Day 30:  T ≈ 0.3 (if consistently honest)
  Day 90:  T ≈ 0.5 (still building)
  Day 365: T ≈ 0.8 (approaching trusted status)

Meanwhile, a solo node running for a year: T ≈ 0.97
```

Trust is earned slowly and lost instantly. A factory cannot buy trust. It must earn it through sustained honest behavior.

> **Two levels of trust:** This formula defines **node trust** — a node's accumulated reputation. The Protocol Whitepaper (Section 11.12) defines a separate **record trust** formula: T(r) = 1 - product(1 - w(n) x d(n, W)) over all witnesses, incorporating correlation discounts to prevent trust inflation from correlated attestation. Node trust feeds into record trust — a record witnessed by high-trust nodes accumulates record trust faster. The witness reward formula below (Section 8.1) uses the node trust score.

6.3 Diminishing Returns per Entity

Token earning rate scales logarithmically with node count per entity:

```
earning_rate(nodes) = BASE_RATE × log₁₀(1 + nodes)

1 node:      1.0x earning rate
10 nodes:    2.0x earning rate  (not 10x)
100 nodes:   3.0x earning rate  (not 100x)
1,000 nodes: 4.0x earning rate  (not 1,000x)
1M nodes:    7.0x earning rate  (not 1,000,000x)
```

Running a million nodes gives ~7x the earning rate of a single node, not 1,000,000x. The economics strongly favor broad participation over concentration.

Sybil defense for earning rate: Entity identification uses cryptographic identity clustering — nodes that share key material, IP ranges, or attestation-pattern signatures are clustered as a single entity. Creating truly independent entities requires truly independent infrastructure and behavior over extended periods.

6.4 Cross-Cluster Validation Requirement

Records are validated at three levels:

```
LOCAL:     Witnessed by nodes in the same trust cluster
           → Fast, usable internally
           → NOT recognized by the broader network

NETWORK:   Witnessed by nodes from ≥2 different trust clusters
           → Recognized network-wide
           → Required for token transfers and governance

ANCHORED:  Network-validated + externally timestamped
           → Highest assurance, immutable proof
```

A factory's internal nodes can witness each other's records — but those records only reach LOCAL status. Network validation requires witnesses from **outside** the factory's cluster. This creates a natural incentive to connect to the broader network.

A factory that operates as a trust island gets no network-level trust for its records, earns no tokens from the broader economy, and has no governance power. The network doesn't penalize isolation — it simply doesn't reward it.

6.5 Identity-Based Governance Cap

No single cryptographic identity can exceed a governance weight cap:

```
max_governance_weight = TOTAL_GOVERNANCE_POOL × 0.05  (5% cap)
```

Even if one entity holds 50% of all tokens, their governance weight is capped at 5%. Surplus tokens have economic value (can be spent on services) but no additional governance power. Twenty independent small holders collectively outvote the largest possible whale.

6.6 Network Sync Guarantee

Every node periodically pulls the global record index (headers only, lightweight). If a node's local DAG diverges from the global index by more than a configurable threshold, the node flags it. This prevents silent divergence — a factory operating as a trust island will see warnings that its records are not network-validated.

---

7. Governance Economics

7.1 Conviction Voting

Cross-zone protocol decisions use conviction voting (Protocol Whitepaper, Section 10.3) with square-root dampening:

- Token holders stake tokens toward proposals
- Voting weight accrues over time with plutocracy dampening:

```
governance_weight = min(sqrt(stake) × (1 - e^(-t/τ)), 0.05 ×
TOTAL_STAKED)
where τ = 7 days (time constant), and the 5% cap is per-identity
(Section 6.5)
```

- The square-root dampening means staking 10,000 tokens gives sqrt(10) ≈ 3.16x the influence of staking 1,000 tokens, not 10x (Protocol Whitepaper, Section 10.4)
- Conviction reaches ~63% at 7 days, ~86% at 14 days, ~98.6% at 30 days
- Supermajority required (>67% of conviction-weighted stake)
- Quorum required (>25% of all staked tokens participating)
- 30-day implementation delay after passing

7.2 The Pooling Problem

The risk: Small holders delegate votes to "pools" (analogous to mining pools or staking pools). One or two large pools accumulate majority voting power. The square-root dampening (Section 7.1) reduces whale influence, but pooling can circumvent it by aggregating many small stakes into one large position.

This is a real problem. Every mechanism can be gamed at some level. Mining pools, staking pools, and DAO voting cartels in existing networks demonstrate that centralization pressure is relentless.

7.3 Defense: Personal Conviction Lock

To vote, a token holder must **personally lock** their tokens for the conviction duration. There is no delegation mechanism in the protocol.

To "pool" votes, participants would have to **transfer custody** of their tokens to a pool operator. Unlike mining pools (where you point hashrate but keep your hardware) or staking pools (where smart contracts manage delegation), conviction voting requires giving away your tokens. Most participants will not transfer significant holdings to a third party.

This is not a perfect defense — informal pooling can still occur. But the friction is significantly higher than in protocols with native delegation.

7.4 Defense: Trust-Weighted Random Committee Selection

For critical protocol decisions (cryptographic algorithm changes, supply adjustments, zone dissolution), the protocol uses **random committee governance** instead of direct conviction voting:

```
Protocol change proposed
  → Random committee of 100 identities selected
  → Selection weighted by trust score (NOT token amount)
  → Selected members have 14 days to cast votes
  → Supermajority required (67%)
  → 30-day challenge period: any node can flag concerns
  → If challenged, new larger committee (200) re-votes
```

This mechanism defeats pooling because:

- **Selection is random** — cannot predict who will be on the committee
- **Weighted by trust, not tokens** — cannot buy selection probability
- **Committee size is large** — bribing 67 of 100 random people is impractical
- **Challenge mechanism** — suspicious outcomes trigger re-vote with larger committee

7.5 Combined Governance Model

Decision type	Mechanism	Why
Zone-local policy (storage, witness counts)	Zone stakeholder vote	Local matters, low stakes
Cross-zone non-critical (feature flags, parameter tweaks)	Conviction voting	Proven mechanism, adequate for routine decisions
Cross-zone critical (crypto algorithms, supply, zone dissolution)	Random committee	Highest stakes, must resist pooling
Emergency veto	>75% of anchor nodes	Circuit breaker, rate-limited (2/zone/quarter)

7.6 Governance Attack Resistance Summary

```
Defense strength against centralization:

Conviction voting alone:             ██▒▒▒▒▒▒▒▒  (pools defeat it)
+ Personal token lock (no delegation): ████▒▒▒▒▒▒  (friction helps)
+ Identity-based 5% cap:             ██████▒▒▒▒  (hard ceiling)
+ Trust-weighted random committees:   ████████▒▒  (pools can't
form)
+ Cross-cluster validation:          ████████  (trust islands
excluded)
```

No single mechanism is sufficient. The combination makes centralization impractical: you can't delegate without losing custody (costly), you can't create fake identities without years of trust building (slow), you can't predict or control committee selection (random), and you can't earn network rewards in isolation (cross-cluster requirement).

---

8. Witness Incentive Model

8.1 How Witnesses Earn

Witnesses earn ELA tokens by performing honest attestation:

```
witness_reward = BASE_REWARD × trust_multiplier × diversity_bonus

trust_multiplier = witness_trust_score  (0.0 to 1.0)
diversity_bonus  = 1.0 + 0.1 × unique_clusters_witnessed_today  (max
2.0)
```

A new witness with T=0.1 earns 10% of base reward. A trusted witness with T=0.9 earns 90%. This prevents Sybil witnesses from earning meaningful rewards — fresh identities have near-zero trust.

The diversity bonus rewards witnesses who attest across different clusters (not just within their own network). A witness attesting to records from 10 different clusters earns up to 2x base reward. This directly incentivizes cross-cluster validation (Section 6.4).

8.2 Witness Reputation

Beyond token rewards, witnesses earn **reputation** based on attestation quality:

```
reputation_delta = f(record_outcome)

Record never disputed:                        +1 reputation
Record disputed, witness sided with winner:   +2 reputation
Record disputed, witness sided with loser:    -5 reputation
Record flagged as spam/anomaly:              -10 reputation
```

A witness that attests to everything — including spam and disputed records — rapidly loses reputation. Reputation loss reduces the weight of future attestations, reducing earned rewards. Indiscriminate witnessing is economically irrational.

8.3 The Nash Equilibrium

The incentive structure is designed so that **selective, honest witnessing** is the dominant strategy:

- Attesting honestly earns tokens and builds reputation → future earnings increase
- Attesting to spam loses reputation → future earnings decrease
- Attesting indiscriminately dilutes reputation → net earnings decline
- Not attesting earns nothing

The rational witness evaluates records before attesting: checking rate-limit compliance, duplicate content, identity trust, and causal consistency. This is the Nash equilibrium of the witness economy.

8.4 Where Witness Rewards Come From

In the conservation model, witness rewards come from three sources:

1. **Priority service fees** — nodes paying for priority propagation or

requested witnessing. These fees flow directly to the witnesses who provide the service.
2. **Network bootstrap pool** — during the first 5 years, the 30% bootstrap allocation subsidizes witness rewards to compensate for low network utility.
3. **Storage delegation fees** — storage nodes pay witnesses to attest to their data availability proofs (proving they actually hold the delegated data).

After the bootstrap phase, witness rewards are entirely funded by network service fees. If the network has sufficient activity, witnesses earn from organic fee flow. If activity is low, rewards are low — but so are network costs.

---

9. Sybil Cost Analysis

9.1 Attack Cost Model

To mount a meaningful Sybil attack on Elara's consensus, an attacker must:

Barrier	Cost per fake node	Scales as
Token staking (PoWaS)	MIN_STAKE ELA	Linear with node count
Trust building	~365 days of honest behavior	Linear with time (cannot be parallelized per node)
Cross-cluster validation	Independent infrastructure	Linear with cluster count
Computational (PoWaS puzzle)	CPU cycles per attestation	Linear with attestation count

9.2 Diminishing Returns

Even if an attacker successfully creates N Sybil nodes, the earning rate cap (Section 6.3) limits their reward to $\log_{10}(1+N) \times$ BASE_RATE. For 1,000,000 Sybil nodes:

- **Cost:** 1,000,000 × MIN_STAKE (token acquisition) + years of trust building + independent infrastructure
- **Earning:** ~7 × BASE_RATE (logarithmic cap)
- **Governance power:** Capped at 5% regardless of holdings

The cost-to-benefit ratio makes Sybil attacks economically irrational at any scale.

9.3 Comparison with Existing Systems

System	Sybil defense	Weakness
PoW chains	Proof of Work (energy)	Mining pools centralize; few pools control majority
PoS chains	Proof of Stake (capital)	Staking pools centralize; single providers can dominate
Elara	PoWaS + Trust + Cross-cluster	Trust cannot be purchased; earning is logarithmic; governance is capped

10. Network Bootstrap Economics

10.1 The Cold Start Problem

The first node has no one to witness its records. The 100th node has few witnesses. How does the token economy bootstrap?

10.2 Phased Bootstrap

Phase 1: Genesis (nodes 1-10) - Founding team operates genesis anchor nodes - No token economy active — all validation is trust-bootstrapped - This is centralization, acknowledged openly (Protocol Whitepaper, Section 11.4)

Phase 2: Early Growth (nodes 10-1,000) - Network bootstrap pool activated (30% of genesis supply) - Elevated witness rewards (3-5x base rate) to compensate for low network utility - Genesis anchors actively attest to new nodes' identity registrations - Early participants earn disproportionate rewards for bootstrapping the network

Phase 3: Decentralization Threshold (nodes 1,000-10,000) - Genesis anchors' special status expires (become regular anchor nodes) - Governance transitions from founding team to conviction voting - Witness rewards normalize toward base rate - Network effects begin: developers build on the protocol because users exist

Phase 4: Critical Mass (10,000+ nodes) - Network is self-sustaining - Witness rewards funded entirely by service fees (bootstrap pool exhausted or winding down) - Token economy reaches equilibrium — or it doesn't, and the open questions (Section 13) become empirical findings

Zero-Friction Installation (v0.14.0+)

The cold start problem is fundamentally a friction problem: if joining the network requires downloading a blockchain, syncing state, configuring wallets, and managing keys, the first 1,000 nodes are difficult to attract.

Elara Core v0.14.0 reduced network participation to two commands:

```
pip install elara-core
elara serve
```

That's it. The node generates a cryptographic identity on first run, starts an HTTP server, discovers local peers via mDNS, and begins witnessing. No blockchain sync. No wallet setup. No token purchase. No configuration file. A developer who installs Elara Core is a network participant within 30 seconds.

This doesn't solve the cold start economics — the first 1,000 nodes still need elevated rewards to compensate for low network utility. But it eliminates the *installation barrier* that prevents developers from becoming those first 1,000 nodes. The "where do the first 1,000 nodes come from?" question becomes easier when the answer is "anyone who runs `pip install`."

10.3 Community Witnessing Pool

A portion of the Community/Governance allocation funds a **public witnessing service** — anchor nodes that attest to free-tier records at no cost to the record creator.

This ensures economic accessibility: the teenager in Kenya (Protocol Whitepaper, Section 3.5) has her records witnessed by community anchors even if she holds zero tokens. Her Layer 2 trust score grows slower than paid-tier records — but it grows.

---

11. Securities Law and Regulatory Classification

> *This section is not legal advice. It describes protocol design choices intended to minimize regulatory risk. Formal legal opinions from qualified securities lawyers are required before any token launch.*

11.1 The Howey Test (US)

The US Securities and Exchange Commission classifies a digital asset as a security if it satisfies all four prongs of the Howey test:

1. **Investment of money** — Yes, if tokens are purchased.
2. **In a common enterprise** — Arguable, but likely yes.
3. **With an expectation of profit** — This is the critical question.
4. **Derived from the efforts of others** — This is the second critical question.

11.2 Design Choices that Mitigate Securities Classification

Prong 3 — No expectation of profit:

ELA tokens are consumed through use — paying for priority propagation, storage delegation, and governance participation. They are network fuel, not investment vehicles. The conservation model explicitly avoids deflationary pressure (no burning) that could create price appreciation expectations.

Prong 4 — Not derived from efforts of others:

The network's value comes from its participants' collective activity, not from the founding team's efforts. After the decentralization threshold (1,000+ nodes), the founding team has no privileged role. Token utility reflects network participation, not team performance.

11.3 Additional Safeguards

- **No ICO, no pre-sale** — eliminates the "investment of money" argument for initial distribution
- **4-year vesting for founding team** — prevents dump-and-run, demonstrates long-term alignment
- **No centralized exchange listing campaign** — avoids securities marketing characterization
- **Utility from day 1** — the token launches with working network utility, not promises
- **Regulatory counsel engaged pre-launch** — formal legal opinions from qualified securities lawyers in US, EU, and Singapore jurisdictions

11.4 EU MiCA Compliance

The Markets in Crypto-Assets regulation (MiCA) provides a clear framework for utility tokens. The ELA token is designed to qualify as a utility token under MiCA:

- Provides access to a service (Layer 2 network validation)
- Is accepted only by the issuer (the Elara Protocol network)
- Has a clear utility function documented in this paper

The protocol will pursue MiCA classification as a utility token where applicable.

11.5 Honest Acknowledgment

Regulatory classification is ultimately determined by regulators, not by protocol designers. The above measures minimize risk but cannot eliminate it. The protocol's design prioritizes genuine utility over speculative value, which is the strongest possible defense.

Regulatory posture toward digital assets varies by jurisdiction and administration, and can shift rapidly. The protocol's utility-first design is intentionally administration-agnostic — it does not rely on favorable regulatory climate but rather on structural compliance with existing legal frameworks.

---

12. Launch Strategy

12.1 No External Chain

The ELA token launches on the Elara Protocol's native DAM — not on any external blockchain. Token transfers are `TRANSFER` records on the DAM:

```
TRANSFER {
    from:          identity_a
    to:            identity_b
    amount:        100 ELA
    reason:        "witness_reward"
    signed_by:     identity_a
    witnessed_by:  [identity_c, identity_d]
}
```

Two independent witnesses confirm the transfer. Balance is computed by replaying the DAG — similar to the UTXO model used in other distributed ledgers, but using the existing DAM infrastructure with post-quantum signatures.

12.2 Phased Launch

Phase 1: Testnet (no real tokens) - Free validation for all participants - Simulated token economy to identify economic imbalances - Testnet data informs final supply number and parameter calibration

Phase 2: Mainnet Genesis - Fixed supply minted into distribution pools - Network bootstrap begins - No exchange listing — tokens earned by running nodes

Phase 3: Decentralized Exchange - Protocol-native exchange mechanism for ELA trading - No dependency on external DEX infrastructure - Liquidity emerges organically from network participants

Phase 4: External Bridges (optional, future) - If demand exists, bridges to external chains can be built by community - Not a protocol dependency — the native DAM is the primary token layer

12.3 What This Means

The ELA token is not a standard on any existing chain. It is a native asset on a purpose-built post-quantum validation network. This means:

- No gas fees to external validators

- No dependency on external chain consensus
- No smart contract risk (the DAM is the execution environment)
- Post-quantum secure from genesis (Dilithium3 + SPHINCS+ signatures on all transfers)

The trade-off: no instant listing on existing decentralized exchanges, no existing wallet integration, no existing tooling. These must be built. The benefit: architectural sovereignty.

---

13. Open Questions

The following questions require empirical data from testnet economics:

13.1 Equilibrium

Does the conservation model achieve economic equilibrium? If witness reward demand exceeds service fee generation, the system deflates (witnesses can't earn enough). If service fees exceed reward demand, tokens accumulate in service provider wallets (consumers can't access services). Testnet data must validate the balance.

13.2 Total Supply Number

What is the right genesis supply? Too small and tokens become prohibitively expensive for small participants. Too large and individual tokens have negligible value, making micro-transactions awkward. The number must be calibrated to expected network size and service pricing.

13.3 Minimum Stake

What is the right minimum staking amount for PoWaS? Too high and small nodes are excluded from witnessing. Too low and the Sybil barrier is insufficient. The PoWaS difficulty curve must be calibrated against real hardware performance data.

13.4 Bootstrap Duration

How long will the 30% bootstrap pool sustain elevated rewards? If the network grows faster than expected, the pool exhausts early and witness rewards drop before organic fee flow is sufficient. If growth is slow, the pool lasts longer but the network may not reach critical mass.

13.5 Storage Pricing

What is the natural market price for storage delegation? This depends on hardware costs, bandwidth costs, and competitive dynamics among storage nodes. Only a live market can discover the price.

13.6 Cross-Chain Bridges

Will the community demand bridges to external chains? If so, the bridge mechanism must be specified without compromising the native chain's security or the conservation model (bridged tokens must be locked on one side and minted on the other, maintaining total supply).

---

14. Long-Term Energy Dynamics

> *Note: This section is early-stage thinking — exploratory analysis of where the token economy trends over decades. These are not predictions but structural observations about the system's thermodynamic properties. The models here will evolve as testnet data becomes available.*

14.1 The Efficiency Paradox

As the network matures, individual operations become cheaper:

- More witnesses → faster consensus → less work per validation
- Better routing → fewer hops per record propagation
- Hardware improvements → lower compute cost per attestation
- Optimized DAM indexing → faster queries, cheaper storage overhead

If tokens represent energy and each unit of work costs fewer tokens, a natural question arises: **does the network converge toward an entropy state where tokens barely move?**

14.2 Three Possible End States

Heat Death (entropy). Every node becomes so efficient that token flow approaches zero. No economic gradients remain to drive work. The network technically runs but stagnates. This is the thermodynamic analogy: a closed system at maximum entropy where no useful work can be extracted.

Jevons Equilibrium (demand absorption). Efficiency doesn't reduce total consumption — it increases demand. Cheaper validations mean more people validate more things. A factory that couldn't afford to validate every sensor reading at $0.01/record suddenly validates everything at $0.0001/record. Total token flow stays constant or grows because the volume of work expands to absorb the efficiency gains. This pattern is well-documented in energy economics: cheaper electricity didn't reduce consumption, it enabled new industries.

Gravitational Collapse (attention singularity). The AI layer (Layer 3) becomes efficient enough to optimize the network itself. Tokens concentrate around the most valuable cognitive work — predictions,

anomaly detection, pattern recognition. The economy doesn't spread thin; it focuses. The risk here is that "most valuable" becomes self-reinforcing, leading to centralization (Section 14.4).

14.3 The Phase Transition Model

The most likely trajectory is not a single end state but a **phase transition** — the token economy changes what it primarily values over time:

```
Phase 1 (Bootstrap):    Computation dominates
  Tokens flow to:       Witnesses, validators, consensus
participants
  Value driver:         Raw attestation work
  Bottleneck:           CPU cycles, honest nodes

Phase 2 (Growth):       Storage dominates
  Tokens flow to:       Storage nodes, data availability providers
  Value driver:         Keeping records alive and retrievable
  Bottleneck:           Disk space, bandwidth, geographic
distribution

Phase 3 (Maturity):     Attention dominates
  Tokens flow to:       AI layer nodes, cognitive service providers
  Value driver:         Pattern recognition, prediction, anomaly
detection
  Bottleneck:           Quality of analysis, not quantity of
hardware
```

In each phase, the "energy" in the system doesn't disappear — it transforms. Computation becomes cheap, so tokens migrate to storage. Storage becomes cheap (hardware improves, native DAM hardware eliminates index overhead), so tokens migrate to attention — which nodes are producing the most valuable insights from the data.

14.4 The Centralization Pressure at Maturity

The Phase 3 transition creates a new centralization risk. If the most valuable work is cognitive (AI analysis), and certain nodes consistently produce better analysis, then:

```
Better AI output → attracts more clients → earns more tokens
→ affords better hardware/models → produces even better output
→ becomes the dominant cognitive provider → centralization
```

This is the same gravity well that concentrates power in every network (Section 6.1), but applied to the attention economy rather than infrastructure.

What resists it:

1. **Zone topology fragments the market.** "Most valuable" is context-dependent. Medical pattern recognition in Kenya is most valuable to Kenyan health nodes, not to a German manufacturing cluster. The zone dimension prevents a single global AI monopoly — it creates many local markets.

2. **Cognitive work follows the human.** Unlike storage (which is location-fixed) or compute (which benefits from scale), the value of cognitive output is inherently personal and mobile. A prediction about *your* workflow patterns is only valuable to *you*. This creates natural distribution — the value creation is tied to individual humans, not centralized infrastructure.

3. **Local LLM requirement.** If Layer 3 nodes must run local models (not cloud APIs), the cognitive layer is physically distributed by design. No single provider can capture it because the intelligence runs on each node. This is not just a feature — it is an anti-centralization architectural choice.

4. **Diminishing returns (Section 6.3) still apply.** Even in the attention economy, the logarithmic earning cap limits how much a dominant node can extract.

What doesn't resist it:

Nodes that run larger, better local models will produce better cognitive output. If model quality becomes the differentiator, and model quality correlates with hardware investment, then the attention economy favors well-funded nodes. The logarithmic cap slows this but doesn't prevent it.

This is an open problem. It may require attention-specific anti-centralization mechanisms not yet designed — for example, cognitive diversity bonuses (rewarding analysis from many independent models over repeated analysis from one dominant model).

14.5 The Storage Floor

One structural property prevents true entropy: **storage costs are physical.**

You can make computation arbitrarily cheap through software optimization. You cannot make storage free — disk space, power, bandwidth, and geographic distribution have irreducible real-world costs. Even with native DAM hardware eliminating index overhead (Hardware Whitepaper, Section 3.3), the raw data must still be stored somewhere.

This means the token economy always has a floor: as long as the network holds data, storage delegation creates token flow. The economy can shift from 80% compute / 20% storage (early network) to 5% compute / 15% attention / 80% storage (mature network), but it cannot reach zero flow.

The conservation model is preserved because the work changes form — from validating to storing to analyzing — but never disappears as long as humans (and AIs) continue creating work worth recording.

14.6 Interplanetary Implications

These dynamics become more pronounced across planetary distances (Protocol Whitepaper, Section 7). Mars-Earth communication delays (4-22 minutes one-way) create natural economic zones:

- **Local compute** is always cheaper than cross-planet compute (latency)
- **Local storage** is always cheaper than cross-planet storage (bandwidth)
- **Local attention** may not always be cheaper — a rare specialist AI on Earth might produce more valuable analysis of Mars data than any local model

This creates an interesting economic gradient: compute and storage tokens flow locally, but attention tokens may flow across planets. The interplanetary economy could naturally specialize — Mars nodes store and validate locally but pay Earth nodes for cognitive analysis that requires models trained on Earth's larger dataset.

Whether this specialization is healthy (comparative advantage) or pathological (cognitive colonialism) is a governance question, not a technical one. The protocol can enable either outcome.

14.7 Summary

The token economy does not converge to entropy, singularity, or permanent centralization. It undergoes phase transitions — changing what tokens primarily pay for as different resources become the bottleneck. The conservation model survives because physical storage costs create an irreducible floor on token flow, and the zone topology fragments centralization pressure into local markets.

The deepest open question is what happens when attention (cognitive output) becomes the dominant value driver. The current anti-centralization mechanisms (logarithmic caps, trust-based scoring, zone topology) provide structural resistance, but attention-specific defenses may be needed. This is an area of active exploration.

```
Early thinking. These models will be tested against testnet data.
The real dynamics may surprise us.
```

---

15. Private Networks and the Validation IPO

Note: Early-stage thinking. This section explores a deployment model that emerged from analysis of enterprise adoption patterns. The economic dynamics are speculative and will require simulation and real-world data to validate.

15.1 The Enterprise Reality

The public Elara network assumes that all participants benefit from global consensus — open propagation, cross-zone witnessing, and shared trust accumulation. But many of the most valuable potential users have no

interest in public consensus:

- **Yamaha** validating firmware versions across 50 factories does not need the public network to witness those records
- **NASA** validating mission-critical software provenance needs internal consensus, not external
- **SpaceX** validating avionics code authorship across engineering teams works better as a closed network
- **A pharmaceutical company** validating drug trial data provenance cannot expose records to public nodes

These organizations want the *cryptographic properties* of the Elara Protocol — post-quantum signatures, DAM structure, causal ordering, tamper-evident history — without the *network properties* of public consensus.

15.2 Private Network Deployment

The Elara Protocol's layered architecture (Protocol Whitepaper v0.5.2, Section 3.2) enables this naturally:

Layer 1 is always free and always independent. A private deployment is simply a set of Layer 1 nodes that never connect to the public Layer 2. They validate locally, propagate within their own network boundary, and accumulate internal trust. The cryptography is identical. The wire format is identical. The records are structurally indistinguishable from public records — they are simply not shared.

Layer 2 can be private. An organization runs its own discovery, its own witness nodes, its own consensus boundary. Internal trust accumulation follows the same Adaptive Witness Consensus rules, just within a closed peer set.

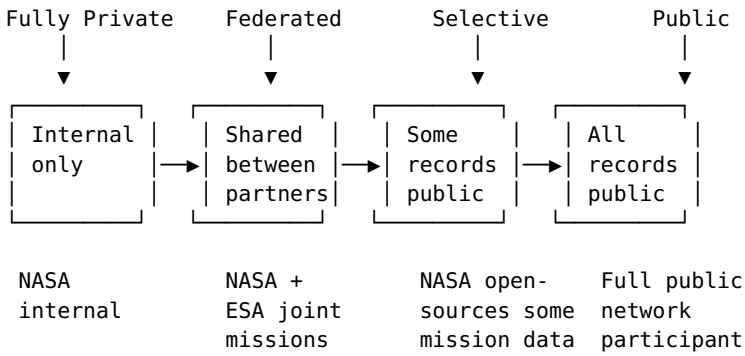
Layer 3 operates independently. AI analysis, pattern recognition, and cognitive functions run against the private DAG without external data exposure.

The economic implications:

- **No token requirement.** Private networks can operate entirely without ELA tokens. Tokens are a coordination mechanism for the public network — private networks coordinate through organizational hierarchy instead.
- **Centralization is acceptable.** Within a corporation, centralized trust is the norm. A private Elara network may have a single root of trust (the corporate PKI), and that is fine. The anti-centralization mechanisms (Section 6) are designed for the public network, not for every deployment.
- **No governance overhead.** The conviction voting model (Section 7) does not apply to private networks. Governance is corporate governance.

15.3 The Spectrum of Privacy

Private networks exist on a spectrum:



1. **Fully private** — closed network, no external connections. All records internal. No tokens.
2. **Federated** — two or more private networks share specific record types with each other. A bilateral trust agreement. Still no public tokens, but may use internal token economics for cross-org resource allocation.
3. **Selective publication** — the organization publishes some records to the public network while keeping others private. This is a mixed mode: internal records stay private, published records enter public consensus and the token economy.
4. **Full public** — all records participate in public consensus. Standard public network operation.

Organizations may operate at different positions on this spectrum for different record types simultaneously. A company might keep internal engineering records fully private, share supply chain records with partners (federated), and publish finished product validations publicly.

15.4 The Validation IPO

The most interesting economic event is what happens when a private network decides to transition from private to public. This is structurally analogous to a company's Initial Public Offering (IPO):

In a traditional IPO: - A private company opens its shares to public markets - Historical financial records are disclosed - The market assigns value based on the company's track record - Liquidity increases but control decreases - The transition is irreversible — you cannot easily go private again

In a Validation IPO: - A private Elara network publishes its historical DAG to the public network - Historical validation records become publicly witnessed - The public network assigns trust based on the depth and consistency of the published history - The organization's records gain broader attestation but are now visible - The transition is *selective* — you can publish some record types while keeping others private

Key differences from a traditional IPO:

1. **Granularity.** A traditional IPO is all-or-nothing for the company entity. A Validation IPO can be per-record-type. Publish your open-source contributions while keeping trade secrets private.

2. **Trust accumulation from history.** A private network that has been running for 5 years has a deep, internally-consistent DAG. When published, the public network can verify the entire causal chain — every signature, every timestamp, every parent reference. This history is cryptographic proof of sustained, consistent operation. A 5-year-old private DAG published today is more trusted than a 5-year-old public node because it has demonstrated sustained private operation with no incentive to game public trust.

3. **Retroactive witnessing.** When published records enter the public network, public nodes can witness them retroactively. The records gain new trust attestations without modifying the original signatures. The DAG grows new edges (public witnesses) connected to old nodes (historical records).

15.5 The NETWORK_PUBLISH Record Type

The transition requires a new protocol-level record type:

```
NETWORK_PUBLISH {
    source_network_id:  [public key of private network root]
    published_records:  [record ID range or classification filter]
    publication_scope:  "full" | "selective" | "federated"
    target_zone:        [zone ID in public network]
    historical_depth:   [how far back to publish]
    redaction_policy:   [which metadata fields are stripped]
    transition_mode:    "snapshot" | "streaming" | "gradual"
}
```

Transition modes:

- **Snapshot** — publish entire historical DAG at once. Highest immediate trust, but requires bandwidth and exposes everything simultaneously.
- **Streaming** — publish historical records in chronological order over time. Allows the network to absorb the history gradually. Trust accumulates as the history verifies.
- **Gradual** — begin with recent records only, then extend historical depth over time. Lowest initial exposure, lowest initial trust, but allows the organization to control the pace.

15.6 Token Economics of the Transition

The Validation IPO creates specific economic dynamics:

Pre-publication (private network): - No ELA token involvement - Internal resource allocation through organizational mechanisms - No storage delegation market costs — the organization stores its own data

During publication: - The publishing organization must acquire ELA tokens for: - **Storage delegation** — public nodes storing the published records - **Witness incentives** — compensating public nodes for retroactive witnessing - **Zone registration** — if the organization publishes as a new zone - This creates a **demand shock** — a large, established private network entering the public network needs tokens in proportion to its history depth

Post-publication: - The published records generate ongoing token flow through storage delegation - The organization's nodes become participants in the public witness economy - Internal work that continues privately has no token cost; published work does

The demand curve:

Large private-to-public transitions create predictable token demand:

```
Token demand = f(history_depth, record_count, storage_redundancy,
witness_count)
```

A Yamaha publishing 5 years of firmware validation records across 50 factories would represent a significant token demand event. This is healthy for the token economy — it represents real utility demand, not speculation.

15.7 Anti-Gaming Considerations

The Validation IPO model introduces new attack surfaces:

Fake history attacks: An adversary creates a fabricated private DAG with backdated timestamps and publishes it for instant trust. **Defense:** Post-quantum signatures bind records to specific key generation events. The cryptographic material itself has temporal properties — a key generated today cannot have signed a record "5 years ago" if the key generation record references recent randomness sources or hardware attestations (Section 8 of the Protocol Whitepaper).

Selective disclosure attacks: An organization publishes only favorable records, hiding failures or disputed work. **Defense:** The DAG's causal structure resists this. If published records reference parent records that are not published, the gaps are visible — the public network can see "holes" in the causal chain. Completeness proofs (Merkle-style) can optionally attest that published records represent a complete subset of the private DAG.

Pump-and-dump publication: An organization creates hype around a Validation IPO to inflate token value, then sells. **Defense:** The conviction voting mechanism's time-weighted staking (Section 7) and the logarithmic earning cap (Section 6.3) limit short-term extraction. The token demand from a genuine publication is gradual (especially in streaming/gradual mode), not a spike.

15.8 The Long-Term Vision

If the Elara Protocol succeeds, the landscape might look like this:

2027-2030: Individual developers and small teams use the public network. Tokens circulate primarily for storage delegation and basic witnessing.

2030-2035: Enterprises run private Elara networks for internal validation. No token involvement. The protocol proves its value in closed environments.

2035+: Some enterprises begin Validation IPOs — publishing portions of their private DAGs to the public network. Each publication event creates real token demand. The public network grows both through new participants and through historical records entering from private networks.

The network grows in two directions simultaneously: 1. **Forward** — new records created by public participants 2. **Backward** — historical records published from private networks

This dual growth model is unique. Traditional networks grow only forward. The ability to absorb verified historical data from private networks means the public DAG can grow faster than real-time — a 10-year-old private network publishing its history adds 10 years of validated records in a single transition.

The economic model is self-reinforcing: the more valuable the public network becomes (larger trust pool, more witnesses, broader attestation), the more incentive private networks have to publish. The more private networks publish, the more valuable the public network becomes.

```
Early thinking. The Validation IPO model needs simulation
to understand demand dynamics, token price implications,
and optimal transition incentives. The concept itself is
novel — we are not aware of prior work on private-to-public
DAG transitions as an economic event.
```

15.9 The Mega-Publication Problem

What happens when the publisher is too big?

The Validation IPO model assumes the publishing entity is smaller than the existing public network — a corporation joining an established ecosystem. But consider the inverse: a dominant entity that has operated privately for decades, representing a substantial fraction of global economic output, decides to publish its entire history.

The problem is threefold:

1. Token demand exceeds supply. The conservation model fixes supply at 1 billion ELA. A mega-publisher needs storage delegation tokens proportional to its history size. If that history represents, say, 30-50% of all validated work globally, the token demand could approach the entire circulating supply. This is not a liquidity problem — it is a structural impossibility. The entity literally cannot acquire enough tokens to publish.

2. Economic shock propagation. Even with rate limits, the *anticipation* of a mega-publication moves markets. If the entity announces intent to publish, token speculators front-run the demand. Price spikes before a single record is published. This creates a perverse dynamic: the publication that would add the most value to the network (largest, most established history) is the publication most likely to destabilize the token economy.

3. Post-publication dominance. After publication, the entity's token expenditure on storage delegation flows to storage nodes — but the entity's newly-public history makes it the most trusted source on the network. Its Layer 3 AI analysis, trained on decades of private data, becomes the dominant attention-value producer. The entity spent tokens to publish, but it earns them back through the attention economy (Section 14.3). The net effect may be extractive — the entity dominates both the trust and the attention markets.

Economic defenses:

Scaled publication rate limits. The Protocol (Section 11.34) enforces a publication rate that scales inversely with the publisher's size relative to the network:

```
max_records_per_day = public_dag_size × 0.01 / (1 +
publisher_dag_size / public_dag_size)

Small publisher (1% of network):    ~1 day     (no meaningful
friction)
Equal-sized publisher (100%):       ~7 months  (manageable)
10× publisher:                      ~30 years  (serious throttle)
50× publisher:                      centuries  (effectively blocked
without network growth)
```

A flat 1% rate limit would allow a network-sized entity to publish in 100 days — 3 months is not a meaningful brake on economic shock. The scaled formula ensures that the entities most capable of causing disruption are precisely the ones most throttled. As published records enlarge the public DAG, the limit rises gradually — so the actual timeline is shorter than static calculations suggest, but still measured in years or decades for dominant entities.

Token acquisition velocity limits. Tied to the publication timeline — an entity cannot front-load token purchases:

```
max_acquisition_rate = circulating_supply × 0.005 per 30 days (0.5%)
AND
vesting_period = publication_duration × 0.5

An entity with a 30-year publication timeline:
  - vesting = 15 years minimum token acquisition period
  - max rate = 5M ELA per month (0.5% of supply)
  - whichever constraint is tighter applies
```

This spreads demand over years or decades. The market adjusts. Other participants can observe and respond. The velocity limit is a protocol-level rule, not a market convention — enforced through smart contract

constraints on publication-linked token transfers.

Publication-proportional token burn. For publications exceeding 5% of the public DAG's size, a fraction of the storage delegation tokens are **burned** (permanently removed from circulation) rather than paid to storage nodes:

```
burn_rate = (publication_size / public_dag_size) × 0.10

Example: An entity publishing records equal to 30% of the public DAG
  burns 3% of its storage delegation tokens.
  On 200M ELA, that's 6M ELA permanently removed from supply.
```

The burn serves two purposes: (1) it creates a cost for mega-publication beyond the economic value of storage, making publication-as-economic-warfare more expensive; (2) the supply reduction counteracts the inflationary pressure of a single entity dominating token flow.

Attention economy dampening for mega-publishers. Post-publication, the entity's Layer 3 cognitive output is subject to a **novelty decay** on attention-economy earnings:

```
attention_dampening = 1 / (1 + log₂(entity_publication_size /
median_participant_size))

An entity 1,000× the median participant size earns:
  1 / (1 + log₂(1000)) ≈ 1/11 ≈ 9% of baseline attention rate per
record
```

This is not a penalty — it is a scaling function. A large entity produces more cognitive output in absolute terms, but earns less per unit. The effect mirrors the logarithmic earning cap (Section 6.3) applied specifically to the attention economy.

The economic warfare variant. If the publication is intentional economic warfare — a dominant entity publishing to crash the token economy — the defenses above convert the attack from a spike into a slow bleed. The velocity limits mean the attacker must commit capital over years. The burn means the attack costs real tokens permanently. The governance cooling period (Protocol Whitepaper, Section 11.34) means the attacker gains no governance control during the attack. The circuit breaker means the network can pause ingestion if economic indicators spike.

The attacker's cost-benefit analysis:

```
Cost of mega-publication attack:
  - Token acquisition over years to decades (capital locked, scaled
to entity size)
  - Token burn (3-10% of acquired tokens, permanently lost)
  - Public exposure of entity's entire historical DAG (irreversible)
  - Zero governance influence during the attack (cooling period)

Benefit to attacker:
  - Temporary economic disruption of the public network
  - But: the published records ADD value to the network long-term
  - The attacker's own data is now publicly attested (benefits the
attacker's reputation)
```

The attack is structurally self-defeating: the weapon (published records) becomes an asset for the network, and the ammunition (tokens) is partially destroyed in the process.

The honest assessment:

No token economic model can prevent a dominant entity from being dominant. If an entity genuinely represents half the global economy, it will eventually become the most influential participant in any network it joins — social, political, economic, or cryptographic. The protocol's goal is not to prevent this — that would require rejecting legitimate participation, which violates the open-access principle.

The protocol's goal is to ensure the transition happens: 1. **Gradually** — over years, not hours 2. **Transparently** — all published records are public and verifiable 3. **At a cost** — token burns and velocity limits create real economic friction 4. **Without governance capture** — cooling periods prevent immediate political influence 5. **Survivably** — the circuit breaker prevents economic seizure during the transition

The deepest defense is diversity. A public network with thousands of active zones, millions of participants, and decades of organic growth has enough economic mass to absorb a mega-publication without collapse. The network bootstrap period (Protocol Whitepaper, Section 11.4) is the critical window — if the public network achieves sufficient scale before the first mega-publication, the defenses described here are sufficient. If a mega-publication occurs before the network reaches critical mass, the economic shock could be existential.

This is why the launch strategy (Section 12) prioritizes breadth over depth: many small participants across many zones, building a diverse trust landscape before any single entity becomes large enough for mega-publication to be relevant.

```
Early thinking. The mega-publication scenario requires economic
simulation to validate the rate limits, burn rates, and velocity
caps proposed here. The numbers are starting points for testnet
experimentation, not final parameters.
```

---

16. References

[1] Elara Protocol Whitepaper v0.5.2 — Vasic, 2026. Complete protocol specification.

[2] Elara Core Whitepaper v2.0.0 — Vasic, 2026. Layer 3 reference implementation.

[3] Elara Hardware Whitepaper v0.1.8 — Vasic, 2026. Native DAM hardware specification.

[4] “Conviction Voting: A Novel Continuous Decision-Making Alternative to Governance.” 2019.

[5] “Quadratic Payments: A Primer.” 2019.

[6] NIST FIPS 204. “Module-Lattice-Based Digital Signature Standard (ML-DSA).” 2024.

[7] NIST FIPS 205. “Stateless Hash-Based Digital Signature Standard (SLH-DSA).” 2024.

[8] EU Regulation 2023/1114. “Markets in Crypto-Assets (MiCA).” 2023.

[9] SEC v. W.J. Howey Co., 328 U.S. 293 (1946). The Howey test for investment contracts.

The same math for the teenager in Kenya and the colonist on Mars. The same economics for a solo developer and a factory with a million nodes.