WHITEPAPER

EDYN — Proof of Participation

A token whose supply is bound to verified life in a physical community

> **Draft for review — pre-launch.** EDYN is deployed and operating on a public **testnet**. There is no mainnet deployment, no token sale, and no offer to sell. Any future issuance is gated on an independent security audit and securities counsel review. Nothing in this document is an offer, a solicitation, or a promise of value, return, or appreciation.

1 Abstract

Bitcoin demonstrated that scarcity can be manufactured by mathematics: a fixed schedule, enforced by code no participant can override. EDYN applies that discipline to a different substrate. Its supply is fixed at 21,000,000 and released on an immutable calendar — but a unit is only ever created when a **specific act of participation in a physical residential community** has been publicly declared in advance, funded from a capped commitment, attested by an accountable operator, and either ratified by a randomly drawn jury of resident stakeholders or recorded on-chain as having passed without their review.

The design does not claim to solve the oracle problem. Someone must still observe whether the porch was swept. What it does claim — and what is verifiable by any stranger with a block explorer — is narrower and unusual: **the rules that convert attested facts into money are beyond the operator's reach.** The operator can be wrong about what happened. It cannot mint beyond the cap, mint outside the schedule, mint what it did not first publicly promise, mint what a jury withheld, mint while residents have pulled the emergency stop, freeze a holder's balance, or upgrade the contract underneath them.

2 The problem

Physical communities run on contribution that is economically invisible. Someone organizes the dinner, repairs the irrigation, welcomes the new family, notices the broken light. This labor is what makes a place worth living in, and it is systematically unrewarded — while the financial upside of a thriving community accrues to whoever owns the land.

Conventional answers fail in predictable ways. Loyalty points are unilateral corporate liabilities that can be inflated or revoked. Equity is illiquid, legally heavy, and unrelated to daily contribution. Existing community tokens are usually pre-mined and distributed by discretion, which means their scarcity is a marketing claim rather than a property of the system.

EDYN's premise is that a community's internal economy should have the same property a well-designed monetary system has: **the issuer cannot cheat, and everyone can check.**

3 Design principles

1. **Immutable core, adjustable periphery, free app layer.** The supply cap, era schedule, retarget mathematics, and anti-double-spend machinery are permanently unchangeable. Staking, lock terms, and quorum parameters sit behind a multisig and timelock. Verification methods, reward rates, and pool sizes remain ordinary business decisions.
2. **Declare before you pay.** Nothing can be compensated that was not publicly promised, with funds committed, before the work occurred.
3. **The residents adjudicate facts, not values.** Juries confirm *that things happened*. They never price the work; pricing is an operator function, disclosed and reviewable.
4. **Privacy is structural.** A residential ledger is a record of people's daily lives. Only fingerprints and aggregates reach the chain.
5. **Verifiable now, progressively decentralized.** Claims are limited to what is true today, with decentralization as published, gate-based milestones rather than aspiration.

4 The token

Symbol	EDYN
Decimals	8
Supply cap	21,000,000, enforced in an immutable contract
Standard	ERC-20, with EIP-2612 Permit and dormant ERC20Votes checkpoints
Owner	None — no owner function exists
Admin mint	None
Blacklist / freeze / seizure	None
Upgrade path	None — no proxy
Minter	A single immutable contract, fixed at construction

The token is deliberately inert: a "dumb token with smart periphery." Every novel behavior lives in separate contracts, so the asset itself has the smallest possible attack surface and no discretionary controls whatsoever.

For calibration: the two largest tokens in circulation, USDT and USDC, each retain the power to freeze and blacklist holders and to expand supply at the issuer's discretion; USDC additionally sits behind an upgradeable proxy. EDYN has none of these powers. This is a statement about the token layer only — the operator's real influence is described honestly in §9.

5 Emission

Calendar eras, halving every four years from genesis.

ERA	YEARS	BUDGET
1	0–4	10,500,000 (includes the 1,000,000 Inception carve)
2	4–8	5,250,000
3	8–12	2,625,000
4	12–16	1,312,500

Approximately 93.75% of supply is issued within sixteen years, exceeding 99% by roughly year twenty-eight — deliberately mirroring Bitcoin's trajectory.

Quarterly difficulty retarget. Within each era, the budget is divided into retarget windows. The mint rate per unit of participation is *window budget ÷ trailing participation volume*. A busy quarter therefore mints **less per act**, and a quiet one mints more, while the calendar total remains fixed. This is the direct analogue of Bitcoin's difficulty adjustment: **participation is priced; the schedule is not negotiable.** Unminted budget rolls forward; a burst ceiling prevents any single window from emitting more than twice its base allocation.

The Inception Tranche. Up to 1,000,000 EDYN (~4.8% of supply) is carved from Era 1 for real founding work — securing land, capitalizing the entity, shipping the platform, obtaining permits, assembling the founding cohort. These are not minted outright. Each founding act is declared with a cap, published in full, and passes through the same epoch and ratification machinery as any resident's contribution. The honest boundary: the provenance is real and public; the valuation is self-priced, and bounded by the hard carve.

6 From act to coin

```
declare → claim → attest → daily batch → epoch opens → jury → mint
```

Declare. A sponsor publishes an act on-chain: a content hash, a reward cap, a community. The commitment is escrowed in the same transaction. An unfunded promise cannot exist, and a retroactively invented one cannot pay.

Claim. Participants signal completion with their own signatures.

Attest. The operator, in the role of *judge*, attests which specific people performed the act. Naming payees individually is the control against free-riding on group work.

Batch. Attestations are aggregated into a single Merkle root per community per day (see §8).

Epoch. Time is divided into fixed calendar periods. Once a period completes, **anyone** may open it for ratification — the operator has no special authority here and cannot delay it.

Jury. The contract draws nine residents at random from those staked in that community. The draw is flat: **one residency, one ticket, never weighted by holdings.** Jurors review a set assembled from a materiality threshold, a random sample, and any resident-raised flags. A supermajority ratifies. A dissenting juror must name the specific items they doubt and give a reason; those items alone are withheld while the rest of the epoch proceeds. If the jury does not act, the epoch finalizes as `PASSED_UNCHALLENGED` — a distinct, permanently visible state — and still mints, because residents' earnings must not be hostage to other residents' inattention.

Appeal. Withheld items go to a fresh panel of twenty-one, drawn excluding the original jury. A majority restores; otherwise the withholding stands permanently.

Mint. A serial mints only when it presents a valid Merkle proof against a finalized epoch, carries an unused nullifier, falls within its declared act's remaining commitment, fits the

current window budget, and the circuit breaker is not engaged. Redemption is member-initiated — conversion happens only when the earner chooses, never on a schedule imposed on them. (The tax treatment of conversion is a question for counsel and is not characterized here.)

7 Resident authority

The jury is the routine check: drawn at random, flat by design, adjudicating occurrence rather than worth.

The circuit breaker is the emergency one. Any staked resident may flag an open epoch. When flags reach **10% of all staked wallets**, the contract halts issuance protocol-wide. The operator has no override; issuance resumes only by the verdict of an oversized jury. The adjustable ceiling on this threshold is itself capped, so governance may tune the valve but can never disable it.

Guardian review. Operational keys can be compromised. A guardian (a multisig) may instantly strip operational roles or pause periphery contracts — but this power is *purely subtractive*: the contract offers no way to grant a role, move funds, or change a parameter. A stolen guardian key is a denial of service against the operator, never a theft. Every such action opens a review episode that a resident jury can **reverse**, and the reversal executes automatically on their verdict.

The guardian carries two further incident tools, both subtractive and both jury-answerable. A **mint pause** halts all conversion protocol-wide, free of charge, and expires on its own after five days — epochs, votes, and appeals keep running; only conversion stops. A **serial veto** permanently voids specifically named serials, and it is *bonded*: the guardian posts 0.1% of the Merkle-proven vetoed value (capped at 100 EDYN; both figures timelock-adjustable inside immutable corridors, so the deterrent can never be zeroed nor the tool priced out of reach) in the same transaction. If a supermajority of the review jury overrules the veto, the serials are restored — finally, they can never be re-vetoed — and the bond is frozen forever at an unreachable address: being overruled by the town costs the operator real value, on the public record. If the jury upholds the veto or declines to act, the veto stands permanently and the bond returns. Vetoed value is never redistributed and the bond is never burned; total supply is unaffected.

Two staking tiers. Residency staking is admin-approved and agreement-specific — economically a deposit on a home — and is the sole source of jury eligibility and breaker

weight. Open staking is permissionless and confers **no** governance power at all. This asymmetry is the sybil firewall: acquiring tokens never acquires a vote on whether work occurred.

8 Privacy

A residential participation ledger is a record of people's daily lives, and a blockchain has no delete key. Three commitments, adopted before the first batch was ever posted:

1. **Batching.** Resident claims and attestations never appear individually on-chain. They are committed inside one daily Merkle root per community.
2. **Timestamp coarsening.** Roots post on a fixed clock, so the chain asserts only that events occurred within a window — not the rhythm of anyone's day.
3. **Amount bucketing.** Public metadata carries totals; per-person splits exist solely inside hashed leaves.

Everything remains **derivable**: the operator retains all preimages, so any root, balance, or split can be reconstructed for audit, escrow, or dispute — and any participant can prove their own inclusion. Corporate declarations remain individually public, because a funded promise has no personal privacy interest and its visibility is the entire point.

9 What the operator controls, stated plainly

Elysium determines what happened and what it was worth. Verification methods, reward rates, and pool sizes are ordinary business decisions, changeable at will, exactly as the internal points ledger already is. Elysium declares acts, attests completions, approves residency staking, issues lock tranches, and runs day-to-day operations.

Two roles are held on-chain and named: a **judge** key that declares and attests, and a **registrar** key that binds verified identity to residency staking. They are separate keys for blast-radius isolation, though one company holds both. The registrar is relinquishable only by its holder — it encodes a legal-entity function (leases, identity verification, fair-housing obligations) that a jury cannot assume, be liable for, or be audited on. Its powers are enumerated in code, its every action is a public event, and succession is a single transaction.

Elysium **cannot**: exceed the cap; alter the schedule or retarget mathematics; mint without a finalized epoch root and a valid proof; mint beyond a declared commitment; reuse a serial; exceed a window budget; freeze, seize, or blacklist any holder's tokens; upgrade the token; override the circuit breaker; or refuse a jury verdict.

10 Demand

EDYN's utility is internal to the community rather than speculative:

- **Stake-to-reside** — residency requires locked EDYN for its duration, transferable to an approved incoming resident as a membership deed.
- **Restricted tranches** — sold with per-case terms, non-transferable, spendable on dues: *lock in tomorrow's cost of living at today's dollars.*
- **A holdings-gated privilege ladder** — priority, amenities, and purchase allowances.
- **Participation weight amplification** for residents with a stake in the town.
- **Spend-to-replenish covenants** that keep circulation alive rather than rewarding hoarding.

Every value sink is denominated in EDYN. Gas is an operating expense paid by Elysium; residents never encounter it.

11 Governance

STRATUM	RUNS ON	CHANGE RULE
Immutable core	Chain	No one, ever, including Elysium
Periphery	Chain, multisig + timelock	14-day standard lane; 48-hour emergency lane; a subtractive, jury-reversible guardian lane
App layer	Operator database	Freely

Resident veto over periphery upgrades is a **published future milestone, not a present feature**. The reasoning is deliberate: this ratchet turns one way. Granting residents that power later is a milestone; withdrawing it later would be a betrayal.

12 Current status and honest limitations

EDYN is deployed and operating on **Base Sepolia**, a public test network. As of this draft, the following have been executed and are independently verifiable on a public block explorer: the founding ledger declared and minted under a capped commitment; an epoch ratified by a nine-juror panel with votes relayed on residents' behalf; an epoch that passed unchallenged with a seated jury that did not vote; a carve-out in which one dissenting juror withheld two specific acts while the remainder of the epoch minted; a twenty-one-juror appeal panel drawn with zero overlap with the original jury; a redemption routing part of the proceeds into a real multi-year lock; and sixteen distinct attack paths — forged proofs, double-mints, undeclared acts, unauthorized staking — rejected by the contracts.

The contracts carry 107 automated tests including invariant suites, and have been through four independent adversarial review passes which together confirmed forty-five distinct issues, four of them critical. All were fixed, with regression tests, and the dispositions are published. The fourth pass reviewed the guardian incident tools (the mint pause and the bonded serial veto) and the treasury-funded vesting rework; its five confirmed defects — among them a stale pause verdict that could cancel a newer active pause, and a revocation path that could have drawn on other grants' escrow — were fixed before the suite was redeployed. Beyond the test suite, a fourteen-stage verification battery re-deploys the entire protocol from scratch and drives every contingency live — the golden path, the guardian lane, the mint pause, the veto with both jury outcomes, the circuit breaker, and the keeper — and it runs green end to end.

Limitations, without hedging:

- The code is **pre-audit**. An independent security audit is a prerequisite, not a formality.
- **No mainnet deployment, no sale, no price.** Any future issuance is gated on counsel.
- **The oracle problem is unsolved here.** A trusted party still reports what happened in the physical world. The protocol constrains what that report can *cost*, not whether it is true.

- **Layer-2 reality:** transaction ordering is currently operated by a single company; Ethereum provides settlement finality, with fraud proofs and a force-inclusion escape path.
- **Randomness:** jury selection currently derives from committed block hashes. A verifiable random function consumer is built and ready, but is not yet the live source.
- **The testnet cohort is simulated.** The staked residencies exercising the protocol on testnet are a test cohort, and their wallet keys are custodial stand-ins operated for the demonstration; production uses device-held keys (Secure Enclave / passkeys).
- **Scale is unproven.** The jury workload model — a materiality floor, a small random sample, parallel panels — is designed so a resident serves roughly once a year. It has been exercised at a scale of dozens, not thousands.

13 What would falsify this design

Stated plainly, because a paper that cannot be wrong is not worth reading:

- If juries systematically fail to participate, `PASSED_UNCHALLENGED` becomes the norm and ratification is theater — visible in public telemetry, and a reason to revisit incentives.
- If the operator's pricing discretion is exercised unfairly, no on-chain mechanism corrects it; the check is disclosure, the activity-log review, and residents' freedom to stop contributing.
- If residency staking concentrates in few hands, the flat jury draw weakens even though it is not stake-weighted.
- If the community never reaches a size where a 10% breaker threshold is meaningful, the emergency stop protects less than it appears to.

Each of these is measurable, and the metrics that would reveal them — participation rates, coverage ratio, unreviewed-epoch frequency — are published every epoch by design.
