



LARASGUNA

The Coordination Layer for Verifiable Preventive Care

Making preventive health measurable, accountable,
and economically sustainable through decentralized
human-oracle verification and zero-knowledge proofs.

Token Symbol: LRGN
Whitepaper Version: 1.0
Canonical Release



TABLE OF CONTENTS

Executive Snapshot

1.0 PROTOCOL THESIS & SYSTEM TOPOLOGY

2.0 THE PREVENTIVE HEALTH MARKET FAILURE

3.0 PROOF OF CARE

4.0 PROTOCOL ARCHITECTURE & MODULAR HEALTH STACK

5.0 DECENTRALIZED CARE VALIDATOR NETWORK (DePIN)

6.0 ENTERPRISE INTEGRATION & RESEARCH ACCESS

7.0 LRGN TOKENOMICS & VALUE ACCRUAL

8.0 CANONICAL SUPPLY, ALLOCATION & CAPITAL FORMATION

9.0 DECENTRALIZED PROTOCOL GOVERNANCE

10.0 GO-TO-MARKET & NETWORK EXPANSION

11.0 PROTOCOL STEWARDSHIP, CONTRIBUTOR GUILDS & GOVERNANCE ARCHITECTURE

12.0 SYSTEMIC RISK TAXONOMY & DISCLOSURES

BACK MATTER





Executive Snapshot

The world spent \$9.8 trillion on healthcare in 2021, yet 80% of chronic disease burden stems from preventable conditions. Current healthcare systems reward treatment volume, not health outcomes. Insurance actuaries cannot price prevention because adherence happens in the privacy of homes, beyond the reach of verification.

Larasguna solves this through a decentralized physical infrastructure network (DePIN) of human validators who cryptographically attest to real-world preventive health actions—medication adherence, screening attendance, lifestyle interventions—without exposing raw medical records. The protocol connects three previously disconnected parties: individuals who perform health actions, community health workers (CHVs) who verify them, and institutional payers (employers, insurers, governments) who fund outcomes.

By September 2026, sovereign health record infrastructures in high-density archipelagic corridors have unified patient data at the individual level for the first time. Statutory single-payer systems covering regional populations exceeding 250 million across aggregate pilot zones have publicly committed to value-based reimbursement models. A network of over one million community health validator terminals and point-of-care nodes exists but lacks digital coordination tools. These three developments create a once-in-a-generation arbitrage: the technical, institutional, and human infrastructure for outcome-based health financing now exists—only the economic coordination layer is missing.

Larasguna is that layer. The LRGN token does not replace fiat healthcare payments. It coordinates a three-sided market: users stake commitment to care plans, CHVs stake quality assurance bonds, and outcome funders deposit milestone escrows released only upon zero-knowledge proof of verified actions. Each verification burns a protocol fee; each unmet milestone reallocates staked capital to high-performing nodes. The result is a self-regulating mesh where fraud costs more than honest work, and prevention becomes financially legible for the first time.

This document presents the protocol architecture (Chapters 1–4), cryptoeconomic mechanisms (Chapters 5–7), technical implementation (Chapter 8), governance framework (Chapter 9), and a milestone-governed rollout plan anchored to independently verifiable health impact metrics (Chapter 10). Unlike speculative health tokens, Larasguna's value accrual is tied to reduction in emergency department visits, medication non-adherence rates, and preventable hospital admissions—outcomes tracked by existing sovereign health databases and auditable on-chain.

The protocol does not diagnose, prescribe, or treat. It verifies that agreed-upon preventive actions occurred, and routes capital accordingly.



1.0 PROTOCOL THESIS & SYSTEM TOPOLOGY

1.1 Executive Abstract

Preventive health is the largest under-capitalized asset class in the global economy. Payers already know its value with actuarial precision: a hypertensive patient kept in range costs a fraction of a stroke admission; a diabetic who attends quarterly retinal screening rarely reaches dialysis. What payers cannot do is confirm, across millions of households, that the medication was taken, the appointment kept, the follow-up completed. Absent verification there is no enforceable contract. Absent a contract, capital stays parked in curative budgets, where outcomes are at least observable in the form of invoices.

Larasguna is a decentralized coordination protocol that closes this verification gap. It converts discrete preventive actions into cryptographically attested events, bonds a physical network of certified Community Health Validators (CHVs) to the accuracy of those attestations, and routes payer capital through programmatic escrows that release only against verified milestones. The attestation primitive, Proof of Care (PoC), combines an off-chain signature from a bonded human validator with a client-side zero-knowledge proof that the attested value satisfies a clinical threshold. Raw clinical data never leaves the participant's device. The ledger records that a threshold was met, who vouched for it, and how much collateral stood behind the claim.

The LRGN token is the instrument that makes this three-sided market self-enforcing. Validators post LRGN bonds that are slashed on fraudulent or negligent attestation. Institutional payers lock LRGN in milestone vaults and in gas-sponsoring Paymaster pools that absorb every on-chain action a participant takes, so a user who has never held a cryptocurrency experiences the protocol as an ordinary mobile application. Research consortia pay LRGN licensing fees to run federated, privacy-preserving queries across the network. Each of these flows removes supply from circulation for the duration of a care program, and a fixed share of every fee is burned. Total supply is capped at 1,000,000,000 LRGN with no post-genesis minting function, and the supply is governed by a single canonical ledger that can be represented across multiple execution chains without fragmenting liquidity.

The timing of this release reflects a convergence that did not exist eighteen months ago. In the high-density archipelagic corridors where the protocol will first deploy, sovereign health record infrastructures have completed individual-level unification of patient data, with access gated by statutory consent. Single-payer systems covering populations in the hundreds of millions have publicly committed to value-based reimbursement, which requires exactly the kind of verifiable outcome data this protocol produces. And a workforce of more than a million community health workers, already embedded in neighborhoods and already trusted by the households they serve, operates without a digital coordination or compensation layer. The record infrastructure supplies the ground truth, the payer



supplies the capital, the workforce supplies the physical verification. Larasguna supplies the mechanism that connects them.

The protocol does not diagnose, prescribe, or treat. It verifies that agreed-upon preventive actions occurred and settles capital accordingly. Every economic claim in this document is tied to modeled cost avoidance under explicitly stated adherence baselines, and every technical component carries an evidence label (✓ Deployed, † In Development, ‡ Proposed) so that diligence desks can distinguish production code from roadmap.

1.2 The Larasguna Paradigm: Dynamic Homeostasis as a Coordination Asset

The name joins two roots that circulate widely across the Austronesian and Sanskrit linguistic sphere. *Laras* denotes balance, attunement, the state of a system held in tune. *Guna* denotes quality, merit, or functional use, the measurable worth of a thing. Together they describe the protocol's object: physiological homeostasis treated as something with quantifiable merit, and therefore something that can be contracted for.

Health economics has long treated prevention as a public expenditure, a line item justified on moral grounds and cut first when budgets tighten. The framing is wrong in a specific way. A population's metabolic stability is a stock that depreciates without maintenance, and the payer who carries the liability for its depreciation (the insurer, the statutory fund, the self-insured employer) has every financial reason to fund the maintenance. The missing piece is collateral. Maintenance happens in kitchens and pharmacies and community clinics, and nobody has been able to post a credible bond that it happened.

Larasguna treats that bond as the asset. A verified preventive action is an under-collateralized coordination asset: valuable to the payer, costly to fake once a human validator has staked capital on it, and transferable as a settlement trigger across any payer who recognizes the attestation standard. Once the asset exists, the capital follows.

1.3 Architectural Axioms: Five Non-Negotiable Tenets

Five constraints govern every design decision in the protocol. Governance may adjust parameters within them; it may not remove them.

Axiom I — Actuarial Payer Capitalization. Every reward distributed to a participant or validator is funded by a payer deposit that reflects modeled cost avoidance. Participant rewards are funded exclusively by payer deposits; validator network bootstrapping incentives are drawn from a finite, pre-allocated genesis pool with no post-genesis minting for participant rewards. If no payer has funded a care program, no reward exists for completing it.

Axiom II — Zero-Retention Data Architecture. The protocol ledger, its gateways,



and its off-chain infrastructure never ingest plaintext protected health information. What crosses the boundary from a participant's device is a cryptographic commitment and a proof that the committed value satisfies a public predicate. Deletion requests cannot be honored because there is nothing to delete.

Axiom III – Proof of Care, Not Gamification. An attestation requires a bonded human validator's signature over a physical session, combined with a client-side proof. Self-reported data, accelerometer counts, and application screenshots are not attestations and earn nothing.

Axiom IV – DePIN Human-Oracle Consensus. The validator network is a physical infrastructure. Its nodes are people with certification, geographic presence, and staked capital. A software adversary cannot clone a validator; it can only attempt to corrupt one, and the slashing schedule prices that attempt above its expected return.

Axiom V – Canonical Ledger Chain-Agnosticism. One authoritative supply ledger. Execution chains are chosen on liquidity, settlement cost, and end-user access cost, and can be added or retired without altering the supply or the care programs running on it.

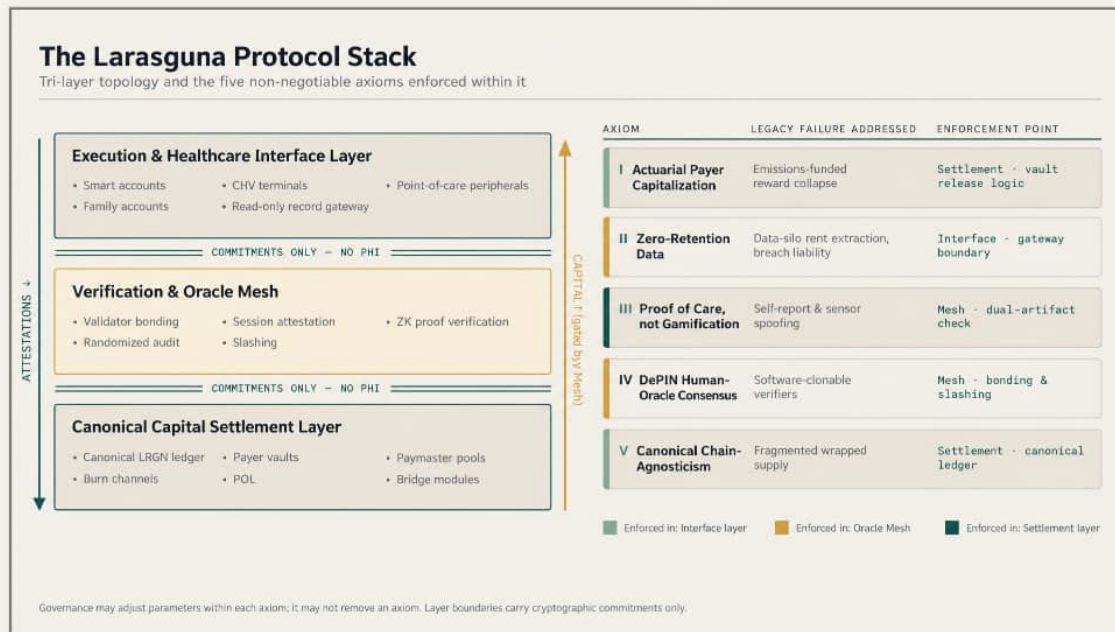
1.4 Macro Protocol Architecture

The system decouples into three layers so that change in one does not force change in the others.

The **Execution & Healthcare Interface Layer** is where care happens: participant smart accounts, CHV terminals, point-of-care peripherals, family care account permissions, and the read-only gateway adapters that map enterprise health records into protocol-legible commitments. A clinical governance decision to add a new screening milestone changes this layer only.

The **Verification & Oracle Mesh** is where truth is adjudicated. Validator bonding, session attestation, zero-knowledge proof verification, randomized secondary audit, and slashing all live here. It is indifferent to which clinical program generated the attestation and to which chain will settle the resulting payment.

The **Canonical Capital Settlement Layer** is where money moves: the canonical LRGN ledger, institutional payer vaults, Paymaster pools, burn channels, protocol-owned liquidity, and the bridge modules that project supply onto execution chains. A decision to migrate primary settlement to a different chain touches this layer and nothing above it.



1.5 What Larasguna Is — and What It Is Not

Larasguna is an open coordination layer for verified preventive clinical and lifestyle actions. Anyone may build a care program on it; any accredited validator may serve it; any payer may fund it.

It does not practice medicine. Clinical protocols are authored by licensed professionals and reviewed by an independent Clinical Ethics & Safety Board; the protocol executes them without interpreting them. It is not a health data marketplace by default: participant data cannot be sold because the protocol never holds it, and research access is limited to federated queries that return aggregate statistics only. It is not an insurance pool; the protocol never assumes underwriting risk, and payer deposits remain the payer's property until a milestone releases them. And it is not a yield product. LRGN earns nothing by being held. It earns by being staked against work that someone has paid for.

2.0 THE PREVENTIVE HEALTH MARKET FAILURE

2.1 The Global Curative Misallocation

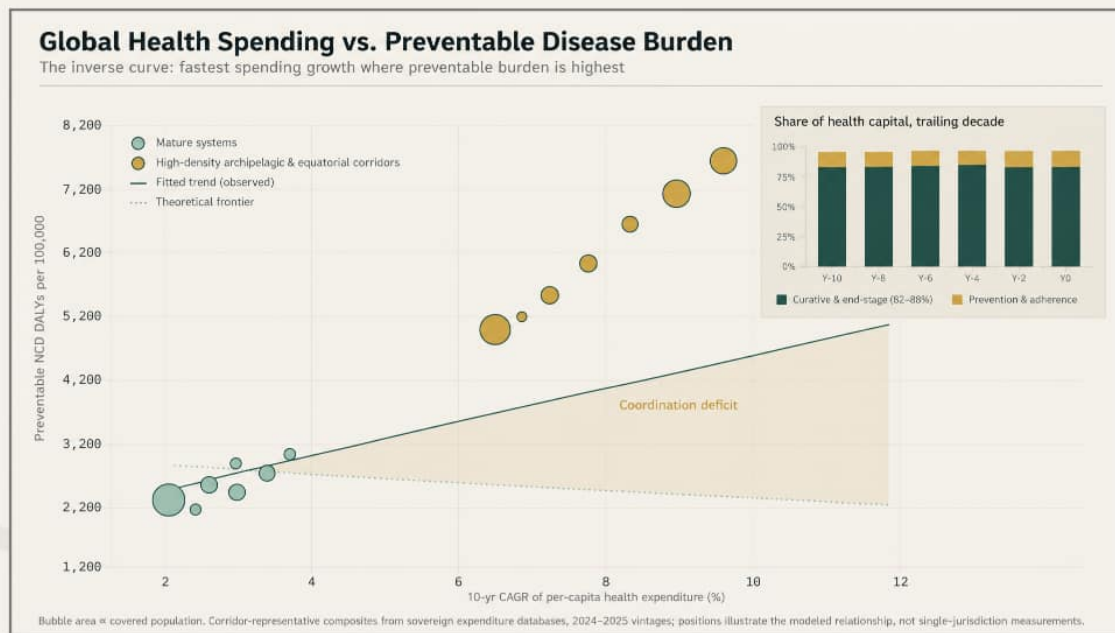
Composite analysis of sovereign health expenditure databases places between 82



%–88%[1] of global health capital in end-stage clinical intervention: hospital admissions, surgical procedures, pharmaceutical treatment of established disease, and the administrative overhead that attaches to each. Primary prevention, early detection, and adherence support share what remains. The ratio has been stable for two decades across mature and high-growth economies alike, through fiscal expansions and austerity cycles, under single-payer and multi-payer systems. Its persistence suggests a structural cause rather than a policy oversight.

The cause is observability. Curative spending produces an invoice. A procedure occurs at a known location, at a known time, performed by a licensed party who submits a coded claim. Budget systems are built to pay invoices. Prevention produces an absence: a stroke that did not happen, a dialysis chair that stayed empty. No invoice is generated for an averted event, and the household actions that averted it (the pill taken, the appointment kept, the diet adjusted) occur outside any institutional line of sight. A finance ministry or an insurer can model the savings but cannot audit the inputs, and capital does not flow to unauditable inputs at scale.

The consequence shows up in national accounts as a chronic deficit that compounds. Health spending in most economies grows faster than GDP. The growth is concentrated in non-communicable disease management, which is precisely the category where early action has the highest modeled return and the lowest actual funding.



2.2 The Equatorial Metabolic Cliff & Demographic Fragility

The misallocation is a global condition. Its acute form is regional.

High-density tropical and archipelagic economic corridors have passed through an epidemiological transition in a single generation. Urbanization, dietary shift toward



refined carbohydrates and processed fats, and a collapse in occupational physical activity have produced adult type-2 diabetes prevalence that moved from approximately 10%–11% to 11%–12% across the most recent national survey cycle in one representative corridor, with modeled trajectories approaching 16% by mid-century.[3] Hypertension prevalence in the same populations exceeds one in three adults. Cardiovascular disease is now the leading cause of death and the largest single claims category for the statutory health funds that cover these populations.

These systems carry a second burden that mature economies have largely shed. Childhood stunting still affects roughly 19%–20% of children under five in the same corridors,[3] down from above 30% a decade earlier but far from eliminated. A health system managing malnutrition in one generation and metabolic excess in the next is managing both at once, often in the same household.

Institutional capacity has not kept pace. Specialist physicians concentrate in tier-1 archipelagic metropolises; secondary and tertiary hospital beds per capita in outlying regions run at a fraction of the national mean. Sovereign single-payer systems in these corridors have achieved near-universal nominal coverage, which means the fiscal exposure to the metabolic cliff is fully socialized. When a diabetic in a remote district reaches end-stage renal disease, the statutory fund pays for dialysis at a tertiary center, plus transport, plus the lost productivity that reduces the contribution base. The fund's leadership has said publicly that it cannot sustain the trajectory on curative reimbursement alone and has begun shifting hospital contracts toward value-based payment.

That shift is the opening. A payer that reimburses on outcomes needs to see outcomes, and the outcomes that matter most in metabolic disease are produced at home.

2.3 The Longitudinal Detection-to-Action Chasm

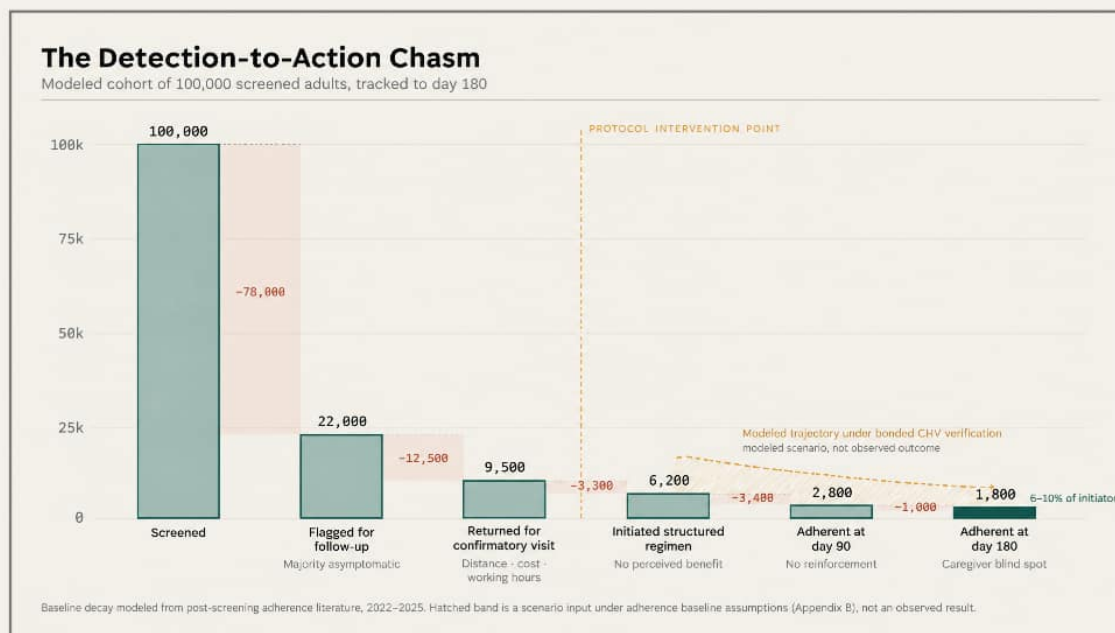
Screening is the part of prevention that governments have learned to scale. Mass screening campaigns in the corridors described above now reach tens of millions of adults annually through mobile clinics, community posts, and employer programs. The detection layer works. In a single recent campaign year, one national program identified several hundred thousand previously undiagnosed diabetics and several million previously undiagnosed hypertensives.

What follows detection is where the system breaks. Of those newly identified, fewer than 3%–4% achieved controlled status under regular treatment within the campaign's own follow-up window.[4] Longitudinal literature on post-screening adherence in comparable settings is consistent with this: without structured reinforcement, adherence to a prescribed preventive regimen decays to approximately 6%–10%[2] by day 180.

The decay has identifiable drivers. The conditions are asymptomatic, so the patient feels no cost from non-adherence and no benefit from adherence. Follow-



up requires travel to a facility that may be hours away, during working hours, at the patient's own expense. The clinician who delivered the diagnosis has no mechanism to know whether the patient returned, and no compensation tied to whether they did. Family members who could reinforce the regimen have no visibility into it. Each of these is a coordination failure, and none of them is solved by better screening.



2.4 Structural Failure of Web3 Precedents

The crypto industry has attempted health coordination before. The attempts failed for reasons that are instructive, and the protocol is designed specifically against them.

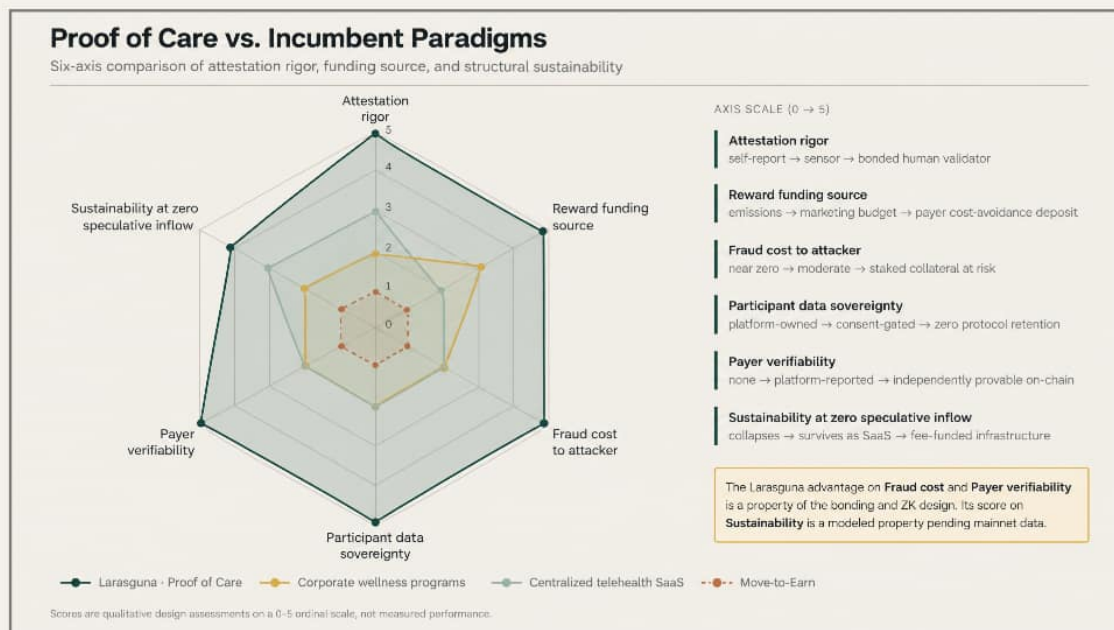
Move-to-Earn. The first wave of health tokens paid users for step counts. The attestation layer was an accelerometer, trivially spoofed by a phone taped to a fan. The reward layer was token emissions, funded in practice by new-entrant purchases. When inflows slowed, the token price fell, rewards became worthless, and users left; the mechanism had no payer, no clinical anchor, and no reason to exist once speculative demand ebbed. Several of these networks lost more than 95% of active users within twelve months of peak.

Centralized telehealth SaaS. Venture-backed platforms in the same corridors offer teleconsultation, pharmacy delivery, and basic adherence reminders. They work as businesses. They do not solve the coordination problem, because the platform is simultaneously the party that records adherence and the party that profits from the data, so no external payer can treat its adherence logs as verification. Incentives, where they exist, are discount coupons funded from marketing budgets. Patient data sits in a proprietary silo that the patient cannot port and that breaches periodically.



Corporate wellness programs. Self-insured employers spend heavily on wellness incentives. Participation is self-reported or verified by vendors with their own commercial interest in reporting high engagement. Fraud rates in self-attested programs are high, and participation skews toward employees who were already healthy, which means the capital flows away from the population where cost avoidance is largest.

Each precedent lacks at least one of the following: a payer whose money is at risk, a verifier whose capital is at risk, or a data architecture that lets a third party trust the verification without seeing the data. Larasguna requires all three.



3.0 PROOF OF CARE

3.1 Formal Specification of Proof of Care (PoC)

A Proof of Care attestation is a two-part object, and the parts are generated by parties with different incentives.

The first part is a physical session signature, σ_{CHV} . It is produced when a participant and a certified Community Health Validator are in the same place, connected through an authenticated terminal session. The signature commits to a small set of structured fields: the milestone identifier, a timestamp, the validator's accreditation reference, a device attestation from the point-of-care peripheral if

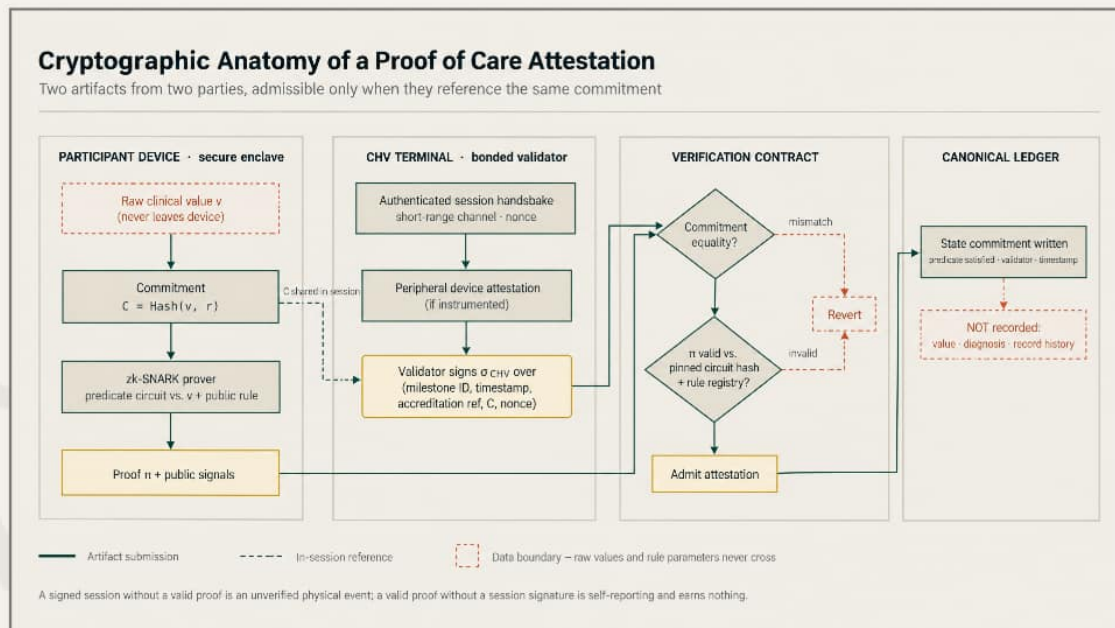


instrumentation was involved, and a cryptographic commitment to whatever value the milestone concerns. The last field matters. When a diabetic participant has a blood glucose reading taken, the signature does not carry the reading. It carries a binding commitment to that reading, held on the participant's device, so that a later proof can demonstrate properties of the value without disclosing it.

The second part is a client-side zero-knowledge proof. The participant's device holds the raw value and the clinical rule that governs the milestone: systolic below a threshold, fasting glucose within a band, a screening attendance record with the correct interval, a medication dispensation confirming a continuous supply. The device constructs a proof that the committed value satisfies the rule, then publishes the proof and the rule identifier. Neither the value nor the rule's parameters appear on-chain in plaintext; an observer learns that the predicate was satisfied, and nothing more.

Both parts must be present and mutually consistent. A signed session without a valid proof is an unverified physical event. A valid proof without a session signature is self-reporting, and self-reporting earns nothing under the protocol's third axiom. The verification contract checks the pairing, including that the proof references the same commitment the validator signed, and rejects any attestation where the two diverge.

This design carries a limitation worth stating plainly. A validator could physically follow every step of the session, sign honestly, and still be describing a participant who is enrolled in a care program they do not actually follow. The protocol's defense against that is economic rather than cryptographic, and Section 3.4 sets out how it is priced.





3.2 Taxonomy of Verifiable Preventive Milestones

Milestones are the protocol's unit of settlement. Each is defined by a clinical rule, an evidence standard, and a funding weight. The registry is versioned and governed through the clinical review process rather than by token vote.

Biomarker screening continuity. Attendance at periodic screening for a defined condition within the prescribed interval, with the commitment binding the measured value if the milestone requires a threshold. Metabolic screening at annual or biannual cadence, blood pressure monitoring at higher frequency for participants under active management, and retinal imaging at the intervals clinical guidelines specify for diabetic populations. This category carries the highest volume and the lowest per-event cost, which makes it the natural first beachhead.

Pharmacological and lifestyle protocol adherence. Continuous supply of a prescribed medication verified against dispensation records, with refill timing as the evidence; structured lifestyle interventions verified through session attendance and, where a device is present, physiological confirmation. Adherence milestones require a quorum of sessions across a window rather than a single verification, so a participant cannot satisfy a ninety-day adherence program with one visit.

Maternal and nutritional compliance. Antenatal visit completion at guideline intervals, micronutrient supplementation continuity, and child growth monitoring with anthropometric measurement. These milestones involve household members other than the primary account holder, which is what makes the family account structure in Section 5.4 a functional requirement rather than a localization amenity.

Point-of-care diagnostic milestone completion. Triage-relevant tests performed at a community node when the participant is present and a licensed professional has authorized the test in advance. The protocol records completion and, where the result is a rule input, a proof of the result's category. It does not record the result itself, and it does not transmit anything to the authorizing clinician through protocol channels.

Each milestone entry specifies a maximum attestation latency, a required validator accreditation class, and a funding weight used by payer vaults to compute release amounts. Adding a milestone requires clinical review and a registry version increment; the contracts read the registry, so no redeployment is needed.

3.3 The Actuarial Value Recycling Engine

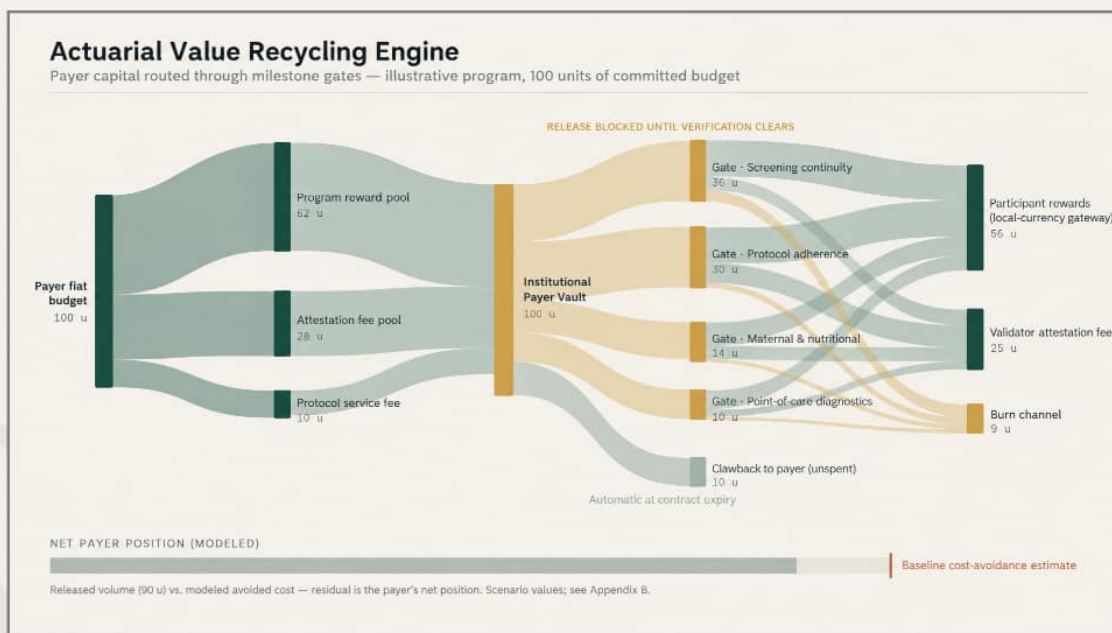
The protocol's economics rest on one claim: preventive actions generate measurable cost avoidance for a specific payer, and that payer will pay a portion of the avoidance to have the actions verified. The engine turns that willingness into recurring protocol capital flows.



A payer's participation begins with a modeled baseline. For a cohort of a defined size and risk profile, the payer's actuaries produce an expected annual cost of care under current behavior, typically derived from claims history: emergency department visits, inpatient admissions for ambulatory-sensitive conditions, dialysis initiation, and the pharmaceutical spend that accompanies established disease. Against that baseline, the payer specifies target improvements in adherence or screening continuity and the cost avoidance the improvement is expected to generate. The modeled range the protocol uses for planning purposes is a 20%–25% reduction in preventable acute admissions among participants who remain adherent for a full program cycle.[2] That figure is a scenario input, not an observed result, and it will be replaced with measured performance as program data accumulates.

The payer then deposits capital into an Institutional Payer Vault and locks the corresponding LRGN against program milestones. As attestations arrive and clear verification, the vault releases the fiat-denominated reward to the participant and the attestation fee to the validator. Capitals sit in escrow until a milestone releases them, and unspent balances return to the payer at contract conclusion through the automatic clawback path in Section 6.2.

Two properties of this arrangement separate it from an emissions model. The reward budget exists before any participant acts, so there is no schedule that pays more than the payer has committed. And the payer's comparison is between a verified payout and an unverified baseline cost, which means the protocol does not need to convince anyone of the value of prevention in the abstract; it needs to be cheaper than the admission the payer would otherwise expect.





3.4 Sybil-Resistance & Game-Theoretic Slashing

The adversary the protocol must survive is a colluding validator and participant pair producing attestations for sessions that never occurred, or describing clinical values that do not hold. Fresh accounts are cheap; the defense therefore cannot rest on identity.

Four mechanisms act together.

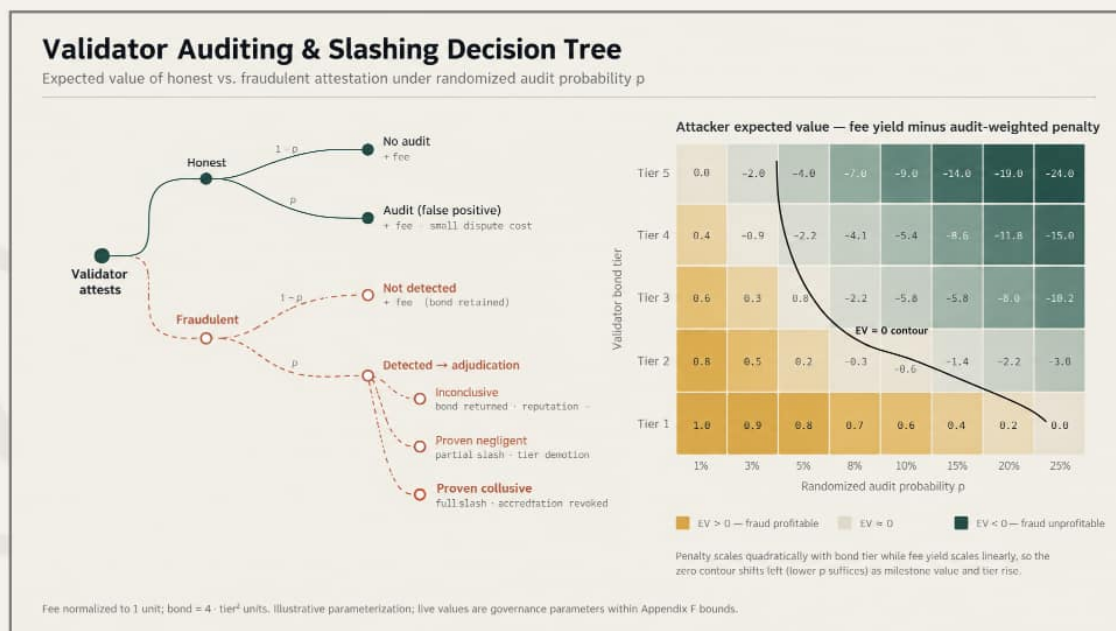
Randomized secondary audit assigns a bounded probability p to any attestation being re-examined. Re-examination takes one of two forms: an independent validator dispatched to the same participant within a short window, or a record query through the consent-gated gateway where the participant has authorized record linkage.

Stake lockup imposes a time cost. Bonded collateral supporting an attestation remains locked for a challenge window that extends with the value of the milestone, so a fraudulent validator's capital is exposed after the fact rather than released immediately.

Quadratic penalties set the cost of a proven violation to scale with the square of the mis-attested value relative to the validator's bond tier. The intent is to make a single large fraud more expensive than a long series of small ones, which pushes attacks toward the pattern that randomized audit detects most efficiently.

Reputation decay and accreditation consequences follow a proven violation in the layer where the adversary cannot be anonymous: accreditation is issued by jurisdictional health authorities and partner institutions, and loss of accreditation removes the ability to sign at all. A validator whose collateral is slashed also loses the physical and regulatory standing that made the bond meaningful.

The composite effect is a floor on the cost of fraud relative to its yield.





4.0 PROTOCOL ARCHITECTURE & MODULAR HEALTH STACK

4.1 Five-Tier Modular Architecture

The stack is organized into five tiers with explicit interface contracts between them. The layering exists so that a change in one tier does not propagate upward into care programs or downward into settled supply.

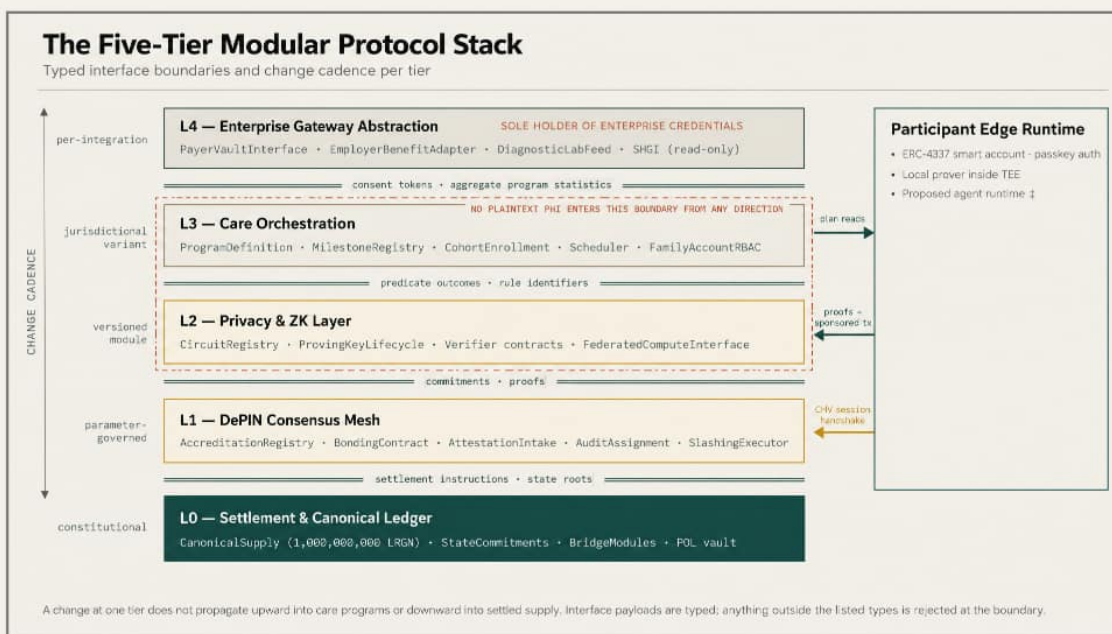
L0 — Settlement & Canonical Ledger. The authoritative record of LRGN supply and of attestation state commitments. One canonical ledger; token representation on other chains is a projection of it, not a parallel issuance. L0 holds no participant-identifying data and no clinical values.

L1 — DePIN Consensus Mesh. The validator layer. Accreditation registry, bonding contracts, session attestation intake, audit assignment, slashing execution. L1 is where the protocol's physical infrastructure is represented economically, and it is deliberately agnostic about clinical content: it processes milestone identifiers and commitments, not diagnoses.

L2 — Privacy & ZK Layer. Circuit registry, proving key management, verification contracts, and the federated compute interfaces used for research queries. The tier exists as a distinct module because proof systems are the component most likely to require replacement over the protocol's lifetime, and a clean boundary lets the protocol migrate from one proof system to another without touching the care logic above or the ledger below.

L3 — Care Orchestration. Program definition, milestone registry, cohort enrollment, scheduling, participant and caregiver notifications, and the family account permission model. This is the layer that resembles a conventional health application, and it is the layer most subject to jurisdictional variation.

L4 — Enterprise Gateway Abstraction. The adapters that let external systems participate: payer vault interfaces, employer HR and benefit systems, licensed diagnostic lab feeds, and the read-only health record gateway. Gateways translate between external data models and protocol-legible commitments, and they are the only components permitted to hold enterprise credentials.



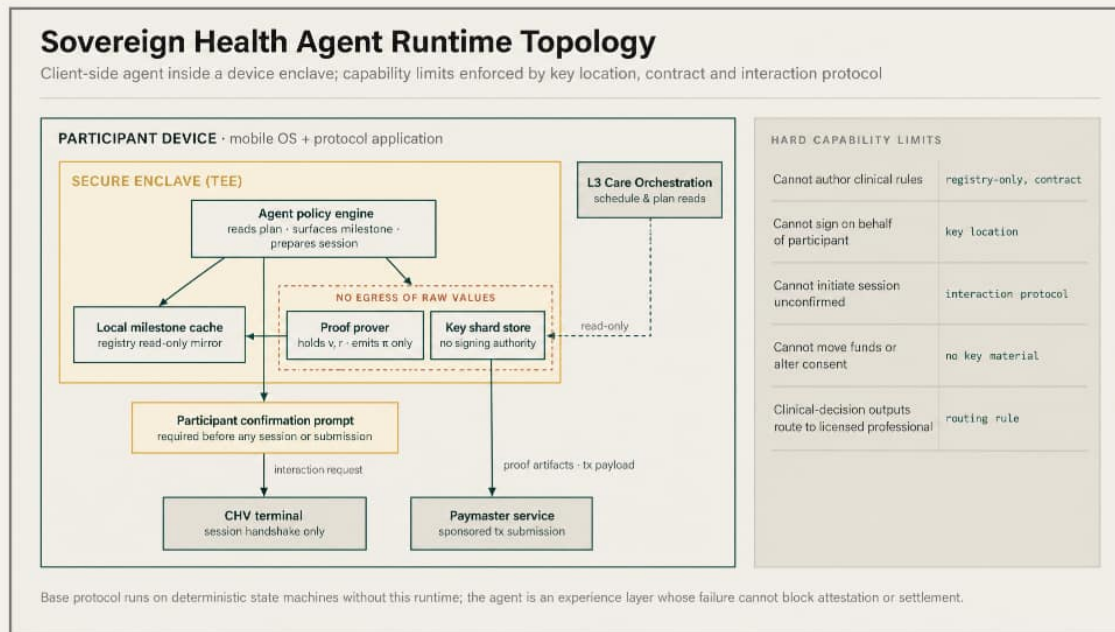
4.2 Towards Sovereign Health Agents (Client-Side DeFAI) ‡

The base protocol is driven by deterministic state machines: a milestone's rule, a session's validity window, an escrow's release condition. That design has no single point of orchestration failure and no model dependency, and it is what the initial network runs on.

Phase II introduces an agent runtime on the participant side. These agents execute inside a trusted execution environment on the participant's own device, manage an ERC-4337 smart account through the account abstraction layer in Section 4.5, and handle the mechanical parts of participation: reading the participant's care plan, surfacing the next relevant milestone at a time the participant is likely to act, opening the session handshake with a nearby accredited validator, preparing the proof inputs, and submitting the resulting transaction through the sponsored Paymaster path.

The agents are constrained in ways that matter for a health context. They cannot author clinical rules; they read the registry. They cannot access raw values outside the enclave's processing scope. They cannot initiate a session without participant confirmation of the interaction, they cannot sign on the participant's behalf, and they hold no key material that would let them move funds or alter consent state. Where an agent's output would inform a clinical decision, the transaction is routed to a licensed professional rather than executed.

The category label for this component is *proposed*. Sandbox validation of the runtime is complete, integration with the account abstraction layer is not, and the protocol's live behavior does not depend on it.



4.3 Zero-Knowledge Attestation Engine †

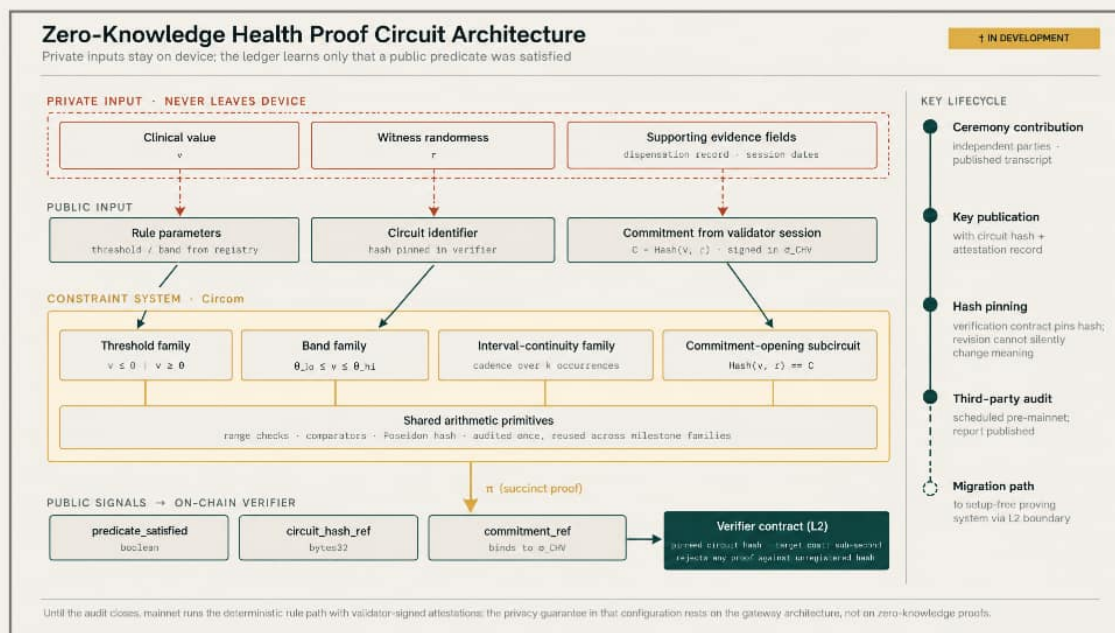
The proof system is the component that makes the privacy claim structural rather than contractual. A participant proving that a value sits inside a clinical band discloses the band's satisfaction and nothing else; there is no dataset on the protocol side from which the value could later be reconstructed, subpoenaed, or sold.

Circuits are authored in Circom and organized around predicate families rather than individual milestones, so that a new milestone within an existing family reuses audited constraint logic. A threshold circuit takes a private value and a privately held witness and a public threshold parameter; a range circuit handles bands where both a floor and a ceiling are clinically meaningful; an interval-continuity circuit proves that a series of governed occurrences satisfies a cadence requirement without disclosing the individual dates. Public signals are limited to what the settlement layer needs: predicate satisfied, circuit identifier, and the commitment reference that ties the proof to the validator's session signature.

Key management is the part most likely to cause operational failure, and the design reflects that. Proving keys are published with their circuit hash and an attestation record; verification contracts pin the hash, so a circuit revision cannot silently change what a passed predicate means. Trusted setup contributions are recorded with participant attestations from independent parties, and the ceremony transcript is published. Where a proof system that removes the trusted setup requirement becomes production-ready for the circuit sizes involved, the L2 boundary permits migration without touching L3.



The engine is in development. Testnet circuits are exercised against reference data, and a third-party cryptographic audit is scheduled before mainnet. Until that audit closes, any mainnet deployment of the protocol runs on the deterministic milestone rule path with validator-signed attestations, and the privacy guarantee in that configuration rests on the record architecture of Section 4.4 rather than on zero-knowledge proofs.



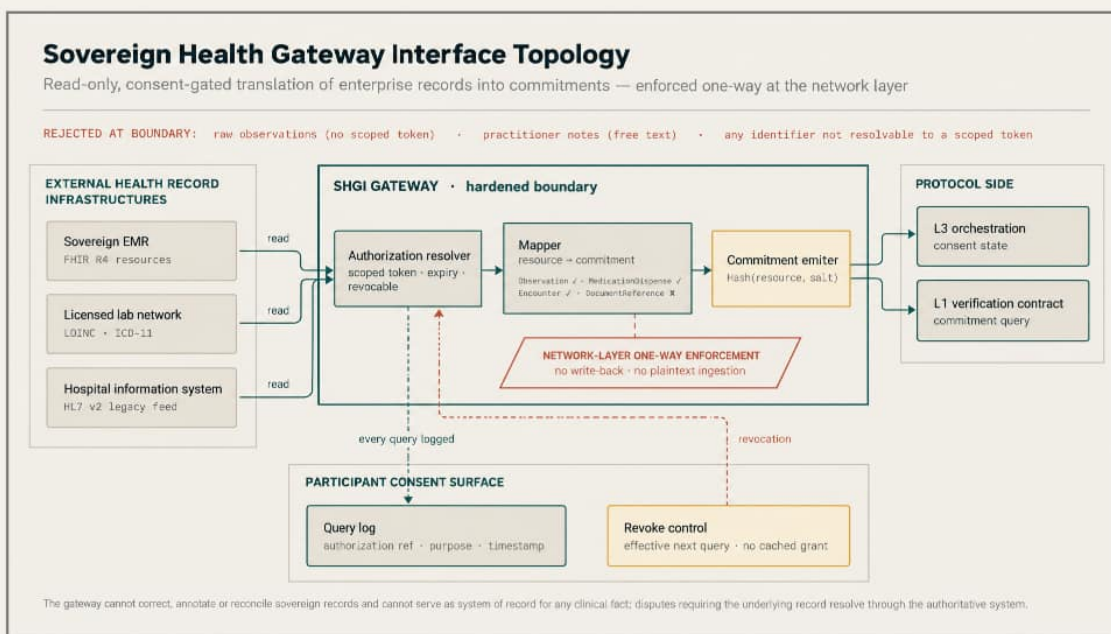
4.4 Sovereign Health Gateway Interface (SHGI)

Enterprise and sovereign health record systems speak their own dialects. The gateway exists to translate without importing.

The interface is HL7 FHIR R4 and ICD-11 conformant on the external side. On the protocol side it emits only commitments and consent state. The boundary rule is single-directional: the gateway reads, hashes, and passes a commitment; it never writes protocol state into the record system, and it never transmits a clinical value into protocol storage. The architecture enforces this at the network layer rather than through policy alone, so an integration error cannot produce plaintext ingestion.

Consent handling follows the same principle. A participant authorizes a specific query class for a specific purpose over a bounded period; the gateway resolves that authorization into a scoped access token that expires and is revocable. Every query is logged with its authorization reference, and the participant's account surface shows the log. Revocation takes effect on the next query; there is no cached grant.

Read-only integration has a second consequence worth being explicit about. The protocol cannot correct, annotate, or reconcile records held by sovereign systems, and it cannot serve as the system of record for any clinical fact.



4.5 Native Account Abstraction (ERC-4337+) ✓

A participant in a metabolic care program in a dense tropical corridor is unlikely to hold a crypto wallet, acquire gas tokens, or manage a seed phrase. If protocol participation requires any of those, the addressable population shrinks to the small fraction already active in digital assets, and the health thesis collapses for lack of users. The stack therefore removes them.

Accounts are ERC-4337 smart accounts created during program enrollment, keyed to device biometrics through passkey authentication. Key material is sharded and recoverable through a social recovery flow configured at enrollment, with the participant's chosen guardians. There is no seed phrase to record, no password to forget, and no separate application to install for chain interaction.

Transaction sponsorship runs through protocol Paymaster pools funded by payers and gateway partners. When a participant's action produces an on-chain state change, the Paymaster settles the network cost and burns a fixed quantity of LRGN in the process. From the participant's side the interaction is a confirmation on a screen after a session with a community validator; the settlement is invisible.

This component is deployed, and it is what makes the rest of the stack usable by the population the protocol is designed to serve. It also creates the demand link that Section 7.1 develops: network throughput converts directly into LRGN consumption through the Paymaster path, independent of any secondary market activity.



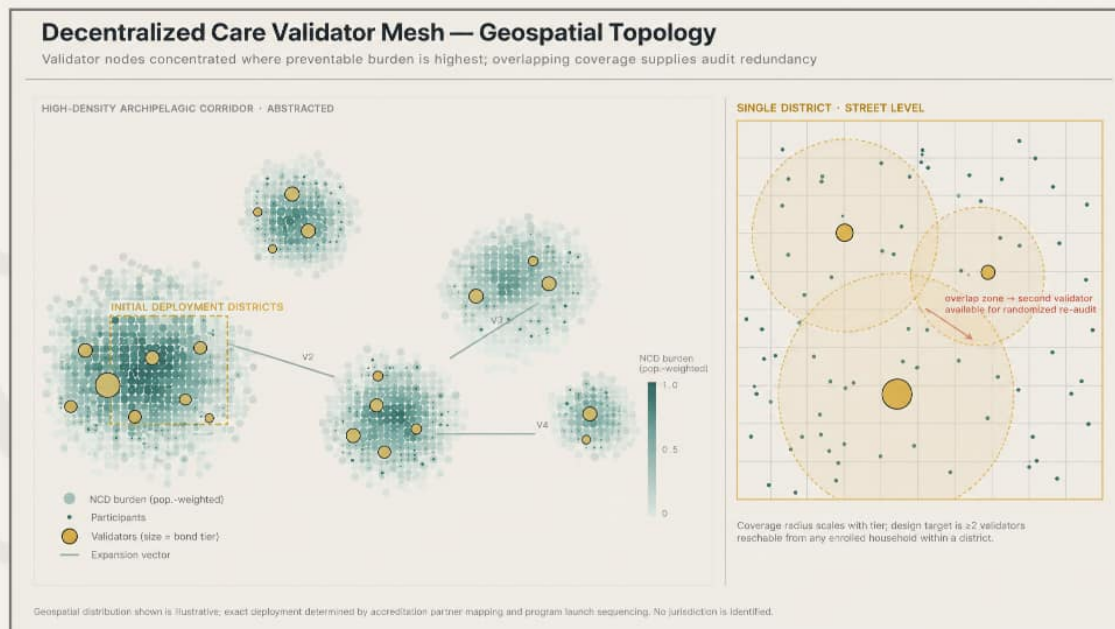
5.0 DECENTRALIZED CARE VALIDATOR NETWORK (DePIN)

5.1 The Human-in-the-Loop Imperative

Software alone cannot close the verification gap that Section 2.3 describes. A step counter proves nothing about metabolic health. A mobile photograph of a pill proves nothing about swallowing it. An application that reads sensor output from an unmonitored peripheral proves only that the peripheral produced a signal, which is a different thing from proving that a qualified person witnessed the measurement, confirmed the device was calibrated, and attested that the result was not coached.

This is not a technology limitation waiting to be solved by better sensors. It is an adversarial environment where the magnitude of the incentive to commit fraud is knowable in advance, since the payer's deposit schedule is transparent, and the sophistication of the attack scales with the reward. Hardware attestation schemes that rely on a single device's self-report have been defeated in every previous health incentive program that tried to use them at scale. The realistic defense is a human whose collateral is at risk and whose physical presence in a community makes persistent fraud costly and visible over time.

Community Health Validators are that defense. They are already embedded in the networks they serve, often in the same neighborhoods for years. The protocol does not recruit strangers; it provides the economic coordination layer for a workforce that already exists and already has the community relationships that make its attestations meaningful. What the protocol adds is a financial stake, a standardized attestation format, a reputation system that persists across programs, and a slashing mechanism that turns the community trust a validator has built into the most valuable thing they stand to lose.



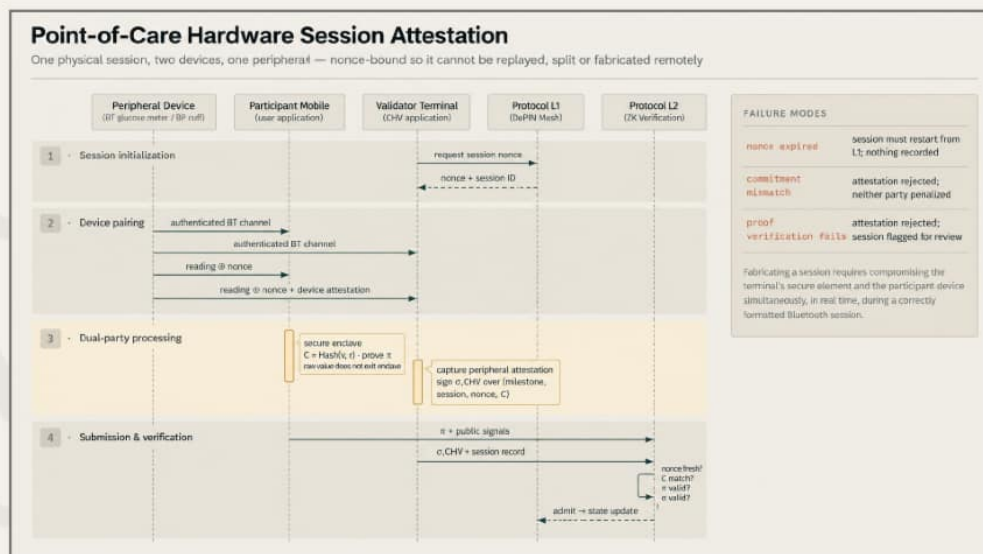


5.2 CHV Infrastructure & Point-of-Care Hardware Handshakes

Validators operate from certified mobile terminals, which in the initial cohort are commercially available devices meeting a minimum hardware security specification, paired with off-the-shelf Bluetooth medical peripherals: validated glucose meters, certified blood pressure cuffs, and anthropometric tools where maternal and child milestones require them. There is no proprietary hardware. The certification requirement is at the software and key management level: the terminal application must run in a secure enclave, the Bluetooth session with the peripheral must be authenticated, and the peripheral's device attestation must be captured within the session record.

A session proceeds as follows. The validator opens an authenticated session with the protocol's terminal application, which generates a nonce and registers a session identifier on L1. The participant's device connects to the same session using a short-range authenticated channel. The peripheral performs its measurement and transmits an authenticated reading to both devices simultaneously, binding the reading to the session nonce. The participant's device stores the raw reading in its secure enclave and begins constructing the zero-knowledge proof. The validator reviews a structured summary of the session—not the raw value—and signs the session record with the accreditation-bound key held in the terminal's secure element. Both the proof and the session signature are submitted to the verification contract.

The nonce and the Bluetooth authentication together mean that a session record cannot be replayed from a prior encounter, cannot be constructed without the peripheral present, and cannot be split between a validator and a participant who are not in the same physical session. An adversary trying to fabricate a session must compromise both the terminal's secure element and the participant's device simultaneously, in real time, during a correctly formatted Bluetooth session.





5.3 Validator Economics, Bonding & Slashing Curves

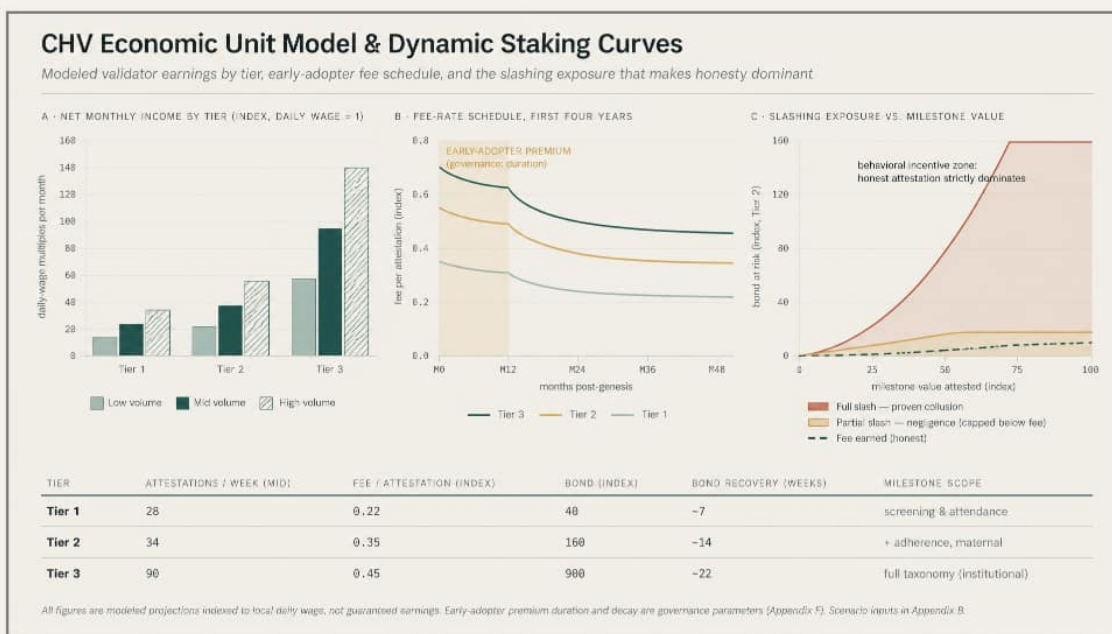
Validators choose a bond tier at accreditation. The tier determines the maximum value of milestones they can attest in a single program cycle, the fee rate they earn per verified attestation, and the slashing exposure they carry if fraud is proven against them.

Three tiers are active in the initial network. Tier 1 is the entry level, accessible to any accredited CHV with the required terminal setup and a bond in the lower range. Tier 1 validators are limited to standard biomarker screening and attendance milestones. Tier 2 requires additional clinical supervision credentials and a larger bond; it unlocks pharmacological adherence and maternal care milestones. Tier 3 is reserved for validated institutional partnerships—licensed diagnostic sites, community health centers, and similar entities—with institutional-grade bonds and access to the full milestone taxonomy.

Fee rates scale with bond tier and fall gradually as the network grows, following a schedule set by governance. The schedule is designed so that early validators who assume higher risk during the network's bootstrapping phase earn above-market fees for the period before throughput normalizes, without locking in rates that would make the protocol uncompetitive for institutional payers once scale is achieved.

Slashing conditions fall into two categories. Negligence—failing to follow the session protocol in ways that produce an unverifiable or inconsistent record—results in a partial slash of the bond posted against the specific milestone, capped below the attestation fee earned. Collusion—proven to have coordinated with a participant to generate a false attestation—results in full bond slash, tier revocation, and a mandatory referral to the accrediting authority for disciplinary review. The distinction matters because the protocol does not want to punish honest validators who encounter edge cases in the session protocol; it wants to make deliberate fraud catastrophically expensive. Governance holds the parameters of this distinction and can tighten the negligence threshold if the audit data shows a pattern of soft exploitation.

Unit economics across representative adoption scenarios: at current modeled throughput, a Tier 2 validator completing an average program week earns fees that compare favorably to the daily wage in the corridors where the initial cohort operates, with a bond recovery timeline that makes the entry cost manageable for an individual practitioner or small community clinic. These are modeled figures based on program funding projections and peer compensation data; actual earnings depend on program availability, local geography, and individual throughput.



5.4 Multi-Generational Family Care Accounts ✓

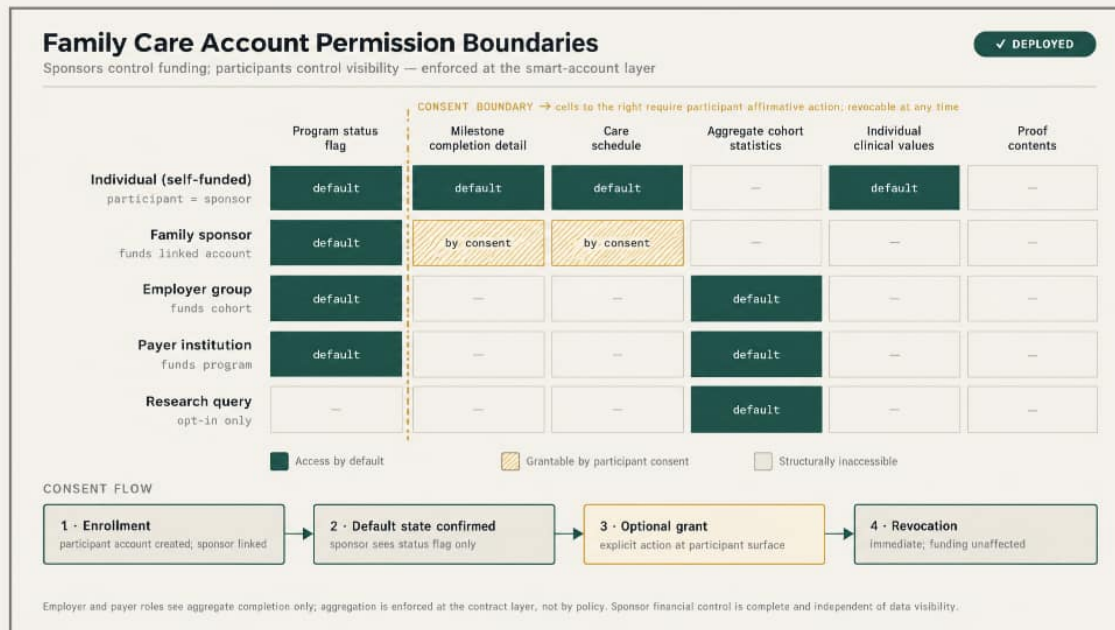
Preventive health decisions in the corridors where the protocol launches are rarely made by isolated individuals. An adult daughter arranges and funds a parent's diabetes follow-up appointments. A husband tracks whether a wife on a maternal care plan has completed her scheduled visits. A grandparent's household is the practical unit for managing children's nutrition milestones. Designing for isolated account holders would force users to choose between the privacy architecture and the reality of how care decisions are made.

Family care accounts solve this through a role-based permission model built at the smart account layer, which is why this component carries the Deployed label: the underlying account abstraction infrastructure is operational, and the family permission model runs on top of it without requiring additional cryptographic components.

An account sponsor can fund care programs for one or more linked participant accounts. The sponsor's financial access is complete—they control the deposit and can revoke it—but their visibility into the participant's data is governed entirely by the participant's consent settings. The default configuration at enrollment exposes only a program status flag: "care plan active," "milestone pending," "milestone verified." The participant can grant the sponsor a richer view, down to milestone completion details and care schedule, but this requires an explicit affirmative action at the participant's account surface, not at the sponsor's. The participant can revoke any granted access without affecting the program funding. The sponsor cannot read anything the participant has not shared, including the content of any zero-knowledge proof, and cannot direct or constrain which milestones the participant pursues within a funded program.



This design has a second function that matters for the protocol's approach to payer verification. When a corporate employer funds a group program for employees, the employer vault is in the sponsor role relative to the employee participant accounts. The employer can see program status and aggregate completion rates—information they need to verify that the service they purchased was delivered—but they cannot see individual clinical data, individual milestone records, or which employees are or are not adhering. The aggregation is enforced at the contract layer rather than by policy.



6.0 ENTERPRISE INTEGRATION & RESEARCH ACCESS

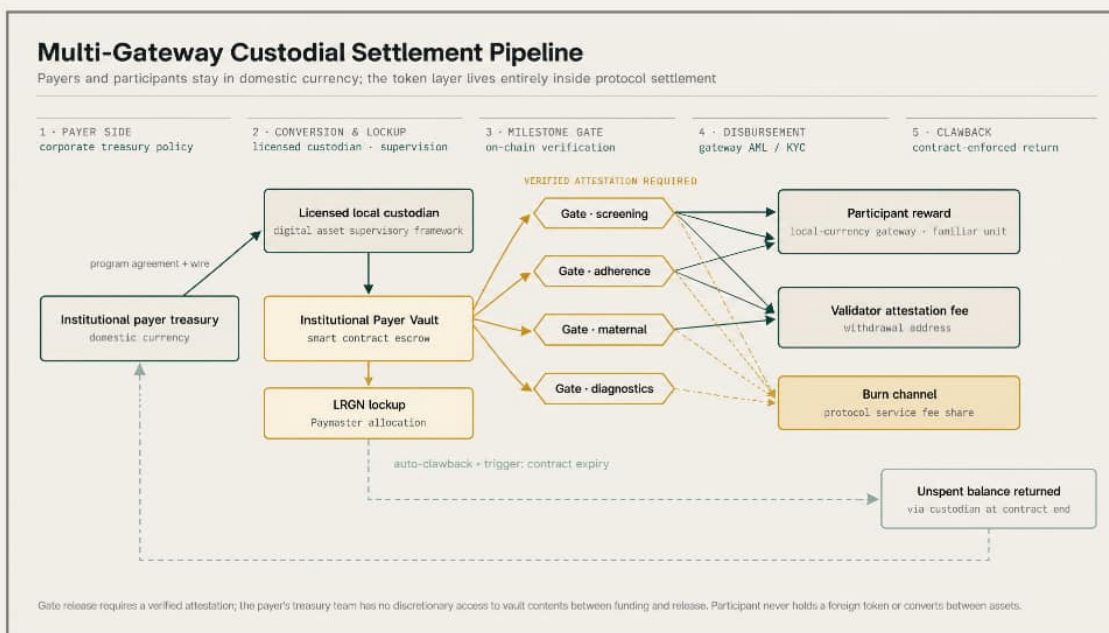
6.1 Multi-Gateway Custodial Settlement Pipeline

Institutional payers—self-insured employers, statutory health funds, licensed insurers, corporate wellness administrators—do not hold cryptocurrency balance sheets and are not positioned to do so under most jurisdictional accounting frameworks. Their participation channel runs through a pipeline that keeps their side of the transaction in domestic currency throughout.



A payer's engagement begins with a program agreement that defines the care plan parameters, the funded cohort, the milestone funding weights, and the contract duration. Against that agreement, the payer transfers domestic currency to a licensed local custodian that operates within the applicable digital asset supervisory framework. The custodian converts to a settlement asset and deposits the equivalent into an Institutional Payer Vault on the protocol, locking the corresponding LRGN required to activate the program's Paymaster allocation. From this point, the vault is a smart contract: the payer's treasury team has no discretionary access to its contents until either a milestone release triggers a participant reward disbursement, or the program concludes and the automated clawback returns unspent principal.

On the participant side, released rewards arrive through the compliant local-currency gateway interface, denominated in a familiar unit, via a channel the participant already uses. The participant never holds a foreign token, never needs an exchange account, and never converts between assets. The crypto layer is entirely within the protocol's settlement infrastructure.



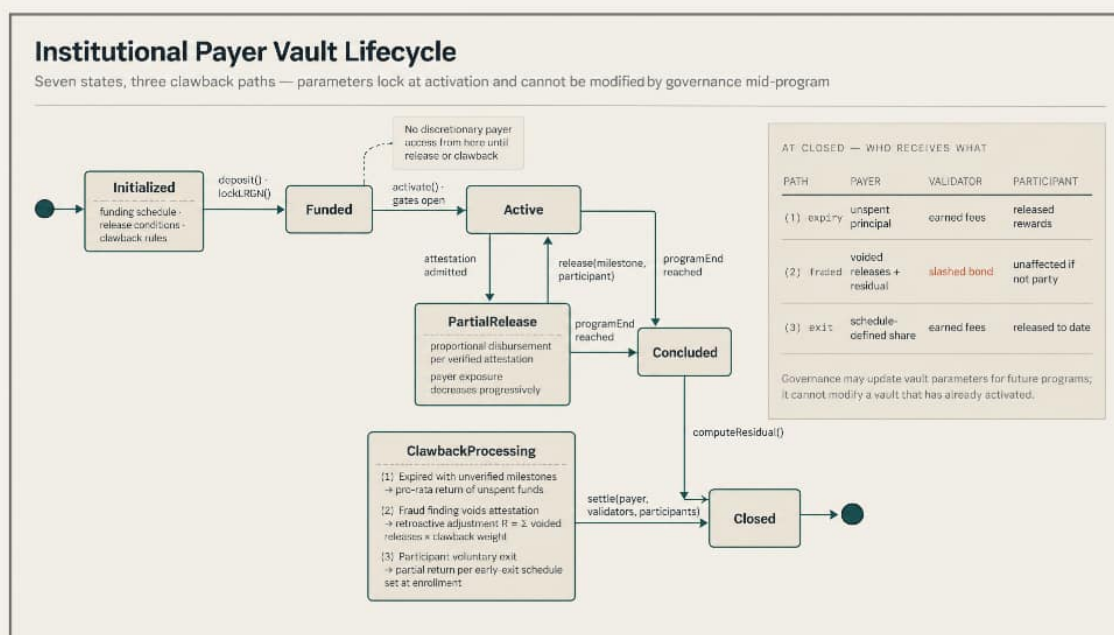
6.2 Institutional Payer Vault Framework

The vault is a set of on-chain contracts, not a custody relationship. The payer does not trust the protocol to honor its commitments; the protocol enforces the commitments by construction.



When a program agreement is loaded into the vault, it sets three categories of parameters that are locked for the program's duration: the funding schedule (how much is committed per milestone class per participant in the cohort), the release conditions (which attestation types and evidence standards unlock a payment), and the clawback rules (what fraction returns to the payer if a participant exits early, if the program expires with unverified milestones, or if a fraud finding retroactively voids an attestation). Governance can update vault parameters for future programs; it cannot modify the parameters of a vault that has already activated.

Partial releases occur as milestones verify. The vault does not accumulate and release in a lump; each verified attestation triggers a proportional disbursement in real time. This matters for participants whose adherence to a care plan is itself affected by whether they can see rewards arriving—behavioral research consistently finds that contemporaneous feedback has larger adherence effects than deferred rewards—and it means the payer's exposure decreases progressively as the cohort completes milestones rather than being carried as a single large liability through the program cycle.



6.3 Compliant Local-Currency Gateway Interfaces

The gateway interfaces are the component that makes protocol participation accessible to non-crypto users, and they are also the component most subject to jurisdictional variation. The architecture separates the protocol-level specification from the local implementation so that adding a new jurisdiction means certifying a new gateway partner, not modifying the settlement layer.



A gateway partner is a licensed entity—a regulated digital asset intermediary, a licensed payment institution, or a bank with the relevant digital asset permissions—operating within the jurisdiction where disbursements are made. The protocol defines the interface contract: the gateway receives a structured disbursement instruction from the vault, converts the settlement asset to domestic currency at a timestamped rate, and credits the participant's local account. The gateway is responsible for its own anti-money-laundering and know-your-customer compliance; the protocol does not operate as a financial institution, and it does not handle domestic currency directly.

Gateway diversity is a property the protocol preserves deliberately. If a single gateway partner fails, is revoked, or exits a jurisdiction, affected programs route to alternatives. The vault's disbursement logic references a registry of certified gateways rather than a single address, and governance can add or rotate entries in that registry without modifying vault contracts. An emergency pause function can halt new disbursements from a specific gateway while continuing all others.

6.4 DeSci Research Pipeline: Federated Zero-Knowledge Compute Queries ‡

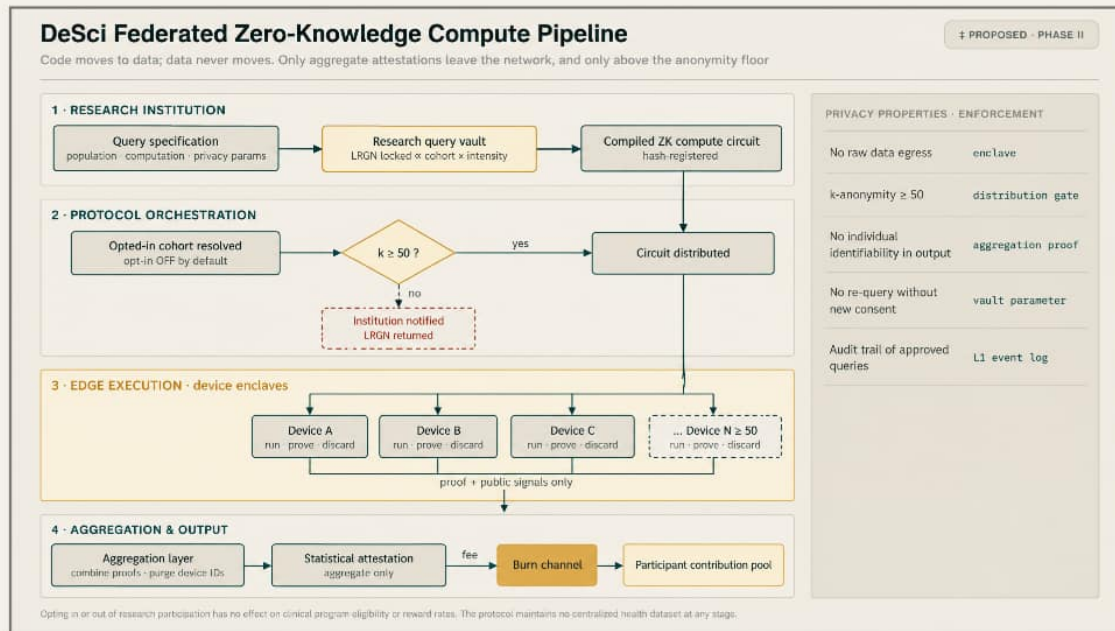
The aggregate health behavior data generated by protocol activity has scientific value that the protocol can realize without creating a centralized dataset. This component is proposed for Phase II and is not required for the initial network.

A research institution seeking access submits a query specification through a protocol interface: the target population characteristics, the statistical computation requested, the output format, and the privacy parameters. The query is represented as a zero-knowledge compute circuit that will execute locally on participating devices rather than on a server holding centralized data. LRGN is locked against the query to fund the licensing fee; the lock amount scales with the population size and the compute intensity of the circuit.

Participant devices that are online and have opted into research participation download the circuit and execute it against locally held data within a secure enclave. Each device returns only its local proof—a commitment to the computation's output under the differential privacy parameters the query specifies. The protocol's aggregation layer combines these proofs into a single statistical attestation, which is released to the research institution only if the contributing cohort meets the minimum anonymity threshold of $k\text{-anonymity} \geq 50$. Raw device outputs, individual device identities, and any reversible intermediate values are discarded after aggregation.



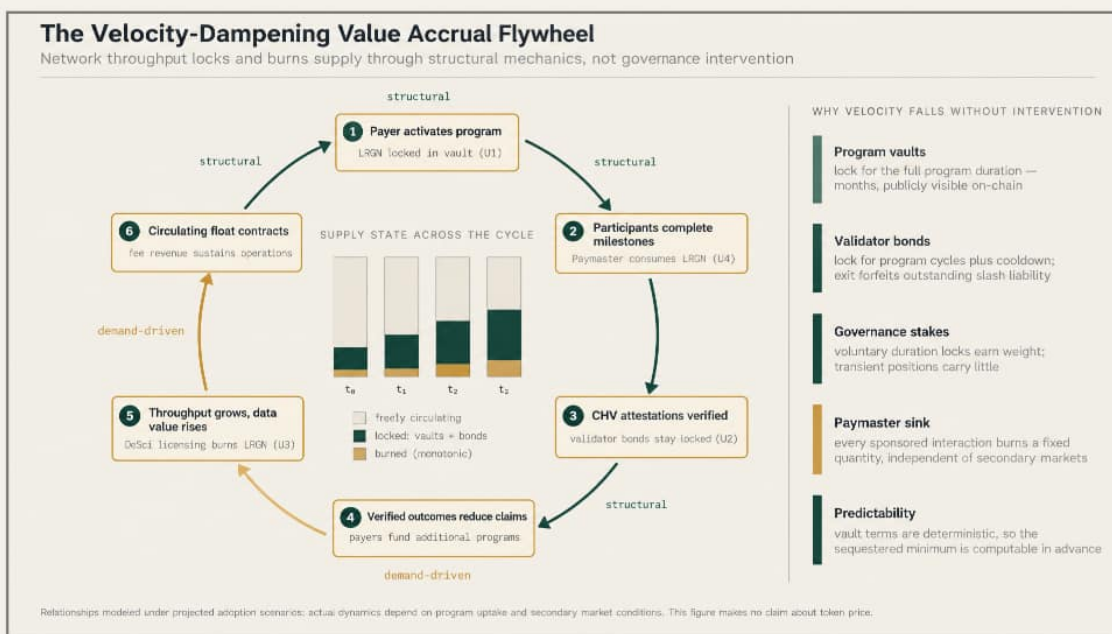
The licensing fee paid by the research institution flows to the burn channel in Section 7.1-7.2, and a smaller allocation routes to the participant reward pool for devices that contributed a proof, priced per contribution at a rate governance sets separately from the clinical program rewards. Participation in research queries is an explicit opt-in configured at enrollment; it is off by default, and opting in or out has no effect on clinical program eligibility or reward rates.



7.0 LRGN TOKENOMICS & VALUE ACCRUAL

7.1 Five-Tier Utility Architecture

LRGN has no yield function. Holding it earns nothing. Its design premise is that a token which can only be acquired to do something, and which is consumed or locked while doing that thing, has a different relationship to protocol activity than a token whose primary appeal is appreciation. The five utility tiers below describe what "doing something" means across the protocol's principal actors.



U1 — Institutional Program Lockups. When a payer activates a care program, the vault contract locks a quantity of LRGN proportional to the program's total milestone budget and cohort size. That LRGN serves two functions simultaneously: it collateralizes the Paymaster allocation that sponsors participant transaction costs for the program's duration, and it signals the payer's economic commitment to the protocol's verification layer. Neither function is replicable with a fiat deposit. A fiat deposit can fund the reward pool; it cannot atomically activate a decentralized Paymaster network or provide the on-chain signal that CHV nodes use to accept program attestations. The lockup releases when the program closes or is rolled into a renewal.

U2 — Validator Staking & Slashing Bonds. CHVs post bonds in LRGN at accreditation. The bond amount determines their tier, their milestone eligibility, and their fee rate. It stays locked for the duration of any program they are actively serving, with a cooldown before withdrawal. A validator exiting the network recovers their bond minus any outstanding slash liabilities; proven fraud results in full forfeiture. The economic logic is that the bond converts community trust—which is hard to acquire and easy to destroy—into a quantified financial stake, which makes the cost of losing that trust legible to the game-theoretic analysis in Section 3.4.

U3 — Federated DeSci Research Query Licensing. Research queries proposed for Phase II are priced in LRGN. A portion of the fee burns upon query submission; the remainder routes to the participant contribution pool for the devices that executed the circuit. Pricing scales with population size and circuit complexity, which means high-value queries—large cohorts, computationally intensive circuits—generate higher burn volumes. This creates a feedback between the scientific value of the network's aggregate data and the deflationary pressure on circulating supply.



U4 – Protocol Execution & Paymaster Sinks. Every on-chain state change sponsored by the Paymaster service consumes LRGN from the associated payer vault. The per-transaction burn is small individually but accumulates with throughput: a payer running a program across ten thousand participants over ninety days produces roughly a million sponsored interactions. Each one removes a fixed quantity of LRGN from the payer's allocation. The Paymaster sink is the mechanism that converts program activity—healthcare milestones being met—directly into protocol-level token consumption, without requiring any secondary market activity.

U5 – Parameter Governance. Staked LRGN participates in the on-chain governance chamber described in Section 9.1. Governance weight is a function of both stake size and stake duration, so transient positions carry less weight than long-held bonds. The design deliberately advantages participants whose stake reflects ongoing work in the network—validators, long-term program operators, ecosystem contributors—over pure financial positions.

Five-Tier Protocol Utility Matrix						
What each utility does, who triggers it, how long supply is held — and what breaks if the token is replaced						
UTILITY	ACTOR	TRIGGER	LOCK DURATION	BURN	FAILS IF REPLACED BY FIAT / POINTS	STATUS
U1 - Institutional Program Lockups	Payer	Program activation; vault funded	Program duration + renewal	partial	Fiat cannot atomically activate a decentralized Paymaster or signal commitment to CHV nodes on-chain STRUCTURALLY FAILS	✓ DEPLOYED
U2 - Validator Staking & Slashing Bonds	CHV	Accreditation; active program service	Program cycles + cooldown	on fraud	Cross-border slashing needs finality identical to the attestation it secures; no custodian can enforce STRUCTURALLY FAILS	✓ DEPLOYED
U3 - DeSci Research Query Licensing	Research consortium	Query submission	Query lifecycle	yes	Federated pricing requires a trustless settlement asset with no custodial intermediary STRUCTURALLY FAILS	⚡ PROPOSED
U4 - Protocol Execution & Paymaster Sinks	Payer vault (on behalf of participant)	Every sponsored on-chain interaction	Consumed per tx	yes	Bank-held fiat cannot execute atomically with a smart-contract state transition STRUCTURALLY FAILS	✓ DEPLOYED
U5 - Parameter Governance	Staked holders	Proposal lifecycle	Voluntary; weight = duration	no	Contribution-weighted, censorship-resistant voting has no fiat equivalent without a legal intermediary STRUCTURALLY FAILS	✓ DEPLOYED

Indispensability test: remove LRGN and substitute fiat escrow or loyalty points. Which functions break structurally rather than merely becoming more expensive?
All five — U1 and U4 on atomicity, U2 on cross-border enforcement, U3 on trustless settlement, U5 on intermediary-free governance.

Holding LRGN earns nothing: each utility requires the token to be staked, locked or consumed against work that a payer has funded.

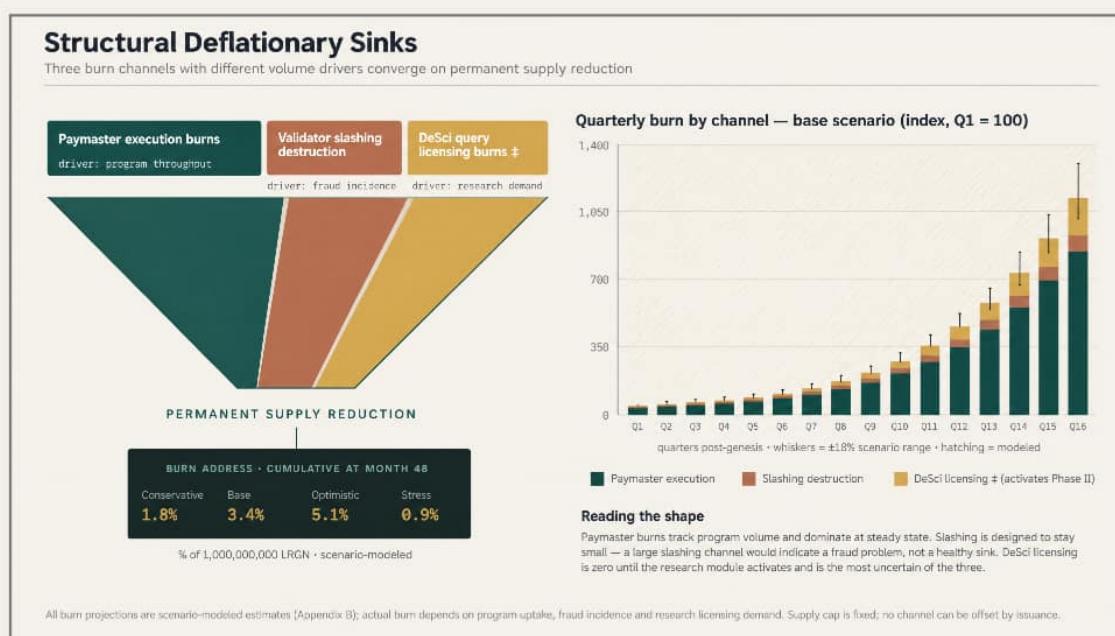
7.2 Velocity-Dampening Supply Mechanics

Token velocity—the rate at which a token circulates—typically correlates inversely with price stability. When every participant immediately converts earned tokens to fiat, and every payer purchases on the open market moments before locking, the token approaches a pure medium-of-exchange function where market cap converges toward a small multiple of transaction volume rather than a multiple of fundamental utility.



Larasguna's mechanic is structural rather than speculative. Program vaults lock capital for months. Validator bonds lock capital for program cycles plus cooldown. Governance stakes lock voluntarily for duration advantages. These are not artificial lock-ups that punish holders; they are the economic requirements of the functions the token performs. A validator cannot attest without a bond in place. A Paymaster cannot operate without a funded vault. A governance weight cannot exist without a duration-adjusted stake. The locks are native to the protocol's logic, not appended as a price management strategy.

The aggregate effect is that at any point in network operation, a predictable minimum fraction of circulating supply is sequestered in active program functions—predictable because program terms are publicly visible on-chain and their vault durations are deterministic. As program volume grows, this sequestered fraction grows proportionally, which dampens velocity mechanically rather than through governance intervention.



7.3 Algorithmic Deflationary Mechanics: Why Fiat and Points Structurally Fail

The token indispensability case is the argument that the strongest institutional diligence desks will probe first, so it deserves a direct answer.



A points-based alternative fails the validator layer immediately. Validator bonds must be slashable across borders without a custodian in the settlement path. A corporate wellness points system or a centralized database cannot enforce the atomicity required: the attestation is submitted, the contract verifies it, and the bond is either preserved or reduced in the same transaction. There is no custodian present. A cross-jurisdictional slash of a points balance requires a legal proceeding or a custodial relationship with enforcement rights—which defeats the purpose of a decentralized attestation network where validators in multiple jurisdictions operate without a common legal entity above them.

A fiat escrow alternative fails the Paymaster layer for a different reason. The Paymaster sponsorship mechanism requires on-chain execution: when a participant's interaction produces a state change, the Paymaster contract must simultaneously settle the network fee, record the sponsorship, and initiate the burn. Fiat held in a bank account cannot execute atomically with a smart contract state transition. Stablecoin held in an escrow controlled by a custodian introduces counterparty risk and settlement latency that the protocol is specifically designed to remove. The only settlement asset that can execute atomically with the verification contract is the protocol's own token on the same settlement layer.

The governance argument is less about technical necessity and more about alignment. Fiat-denominated governance rights are property in a legal system, not protocol mechanics. A LRGN-weighted vote executes directly without a legal intermediary, is censorship-resistant, and can be granted to validators and participants in proportion to their contribution to the network rather than their capital position. Fiat cannot replicate the contribution-proportional governance weighting the protocol uses without a complex legal structure that would be distinct from—and weaker than—what the token does natively.

Token Indispensability Matrix			
Five protocol functions tested against three settlement instruments — the question is structural capability, not cost			
FUNCTION	LRGN protocol-native asset	Fiat escrow bank or custodian held	Loyalty points centralized ledger
Cross-border validator slashing Bond preserved or reduced in the same transaction that verifies the attestation	SUPPORTED Atomic with verification. No custodian in the path; validators in multiple jurisdictions need no common legal entity.	FAILS Requires legal proceeding or a custodian with enforcement rights across every validator jurisdiction.	FAILS Operator discretion. A points balance can be reduced only by the entity that issued it, after the fact.
Atomic Paymaster activation Network fee settled, sponsorship recorded and burn executed in one state transition	SUPPORTED Same settlement layer as the verification contract; executes without latency or counterparty.	FAILS Cannot execute atomically with a smart-contract state change; stablecoin escrow reintroduces custodial risk.	FAILS No on-chain execution surface at all.
Trustless DeSci query settlement Query fee locked, cohort gate checked, burn and contribution split executed without intermediary	SUPPORTED Vault logic prices, locks and settles per query with no party holding funds in between.	FAILS Intermediary required to hold and release; defeats the no-custodian guarantee researchers rely on.	FAILS Not transferable to external research institutions as a settlement instrument.
Governance without legal intermediary Weighted vote executes directly and is censorship-resistant	SUPPORTED Direct execution after timelock; weight granted in proportion to network contribution.	PARTIAL Possible via corporate structure — shareholder-style rights, with legal overhead and jurisdictional dependence.	FAILS Points carry no rights enforceable against the issuer.
Contribution-weighted stake duration Long-held bonds from working participants outweigh transient capital	SUPPORTED Native. Duration and stake size compose on-chain without a registrar.	FAILS Requires bespoke legal instrument per participant class; weaker than what the token does natively.	FAILS Issuer-defined and revocable; cannot anchor a credible commitment.

This analysis makes no claim that LRGN will appreciate in value. It shows that specific protocol functions have no structurally equivalent non-token implementation.



8.0 CANONICAL SUPPLY, ALLOCATION & CAPITAL FORMATION

8.1 Canonical Supply Parameters

Total supply is fixed at 1,000,000,000 LRGN at genesis. There is no minting function after genesis. The supply ceiling is encoded in the base protocol ledger and cannot be altered by governance; governance controls parameters within the system but not the system's capacity to create new tokens.

The fixed cap design follows from the actuarial funding model in Section 3.3. If payer deposits fund rewards, and payer deposits are denominated in a real-world value, and that value flows through the token's utility functions, then the token's function in the system does not require expansion of supply to match growth. Growth in program volume increases the fraction of supply that is locked and burned, which adjusts available supply without new issuance. An inflationary supply would dilute the validators and long-term ecosystem contributors whose bonded positions are meant to reflect enduring economic commitment, not a target for dilution.

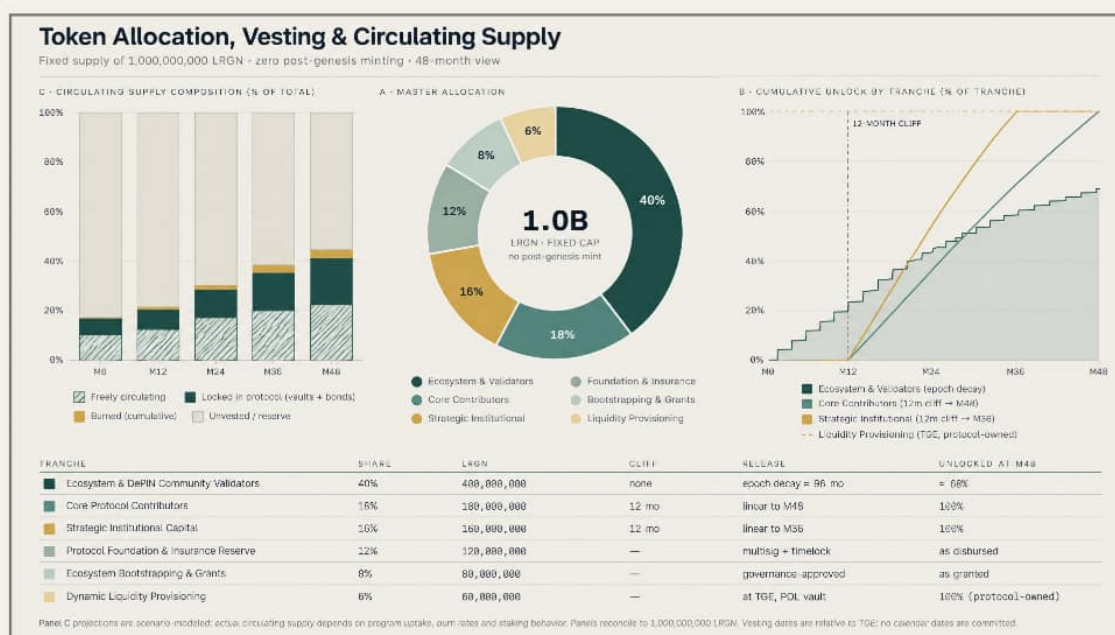
8.2 Structured Allocation Framework

The allocation reflects a network that needs a large organic validator and participant base, a credible technical team with appropriate vesting, strategic institutional relationships to anchor early program demand, and operational reserves that do not depend on secondary market conditions.

Allocation Tranche	Percent age	Primary Purpose
Ecosystem & DePIN Community Validators	40%	Long-term network bootstrapping; epoch-based decay over approximately 96 months
Core Protocol Contributors	18%	Engineering, research, and protocol stewardship
Strategic Institutional Capital	16%	Anchor institutional program partners and early payer relationships
Protocol Foundation & Insurance Reserve	12%	Operational continuity, security reserve, and protocol insurance backstop
Ecosystem Bootstrapping & Grants	8%	Developer grants, research partnerships, clinical advisory
Dynamic Liquidity Provisioning	6%	Protocol-owned liquidity and secondary market depth



The largest single tranche—forty percent—flows to ecosystem and validator functions rather than to team or investors. The logic is that the network's value derives from the physical validator mesh, and the validator mesh will not form if the bootstrapping economics favor other constituencies. A validator who accepts the risk of entering the network during the bootstrap period, before throughput normalizes, should receive a meaningful share of the protocol's total supply in exchange for that risk.



8.3 Vesting Schedule & Physics

Core protocol contributors vest over four years with a twelve-month cliff. No tokens reach contributors before the twelve-month mark; at month twelve, the cliff tranche releases; monthly linear thereafter through month forty-eight. The standard schedule for a technical team with a multi-year product roadmap: long enough to signal commitment, structured to align incentives with protocol milestones rather than TGE date.

Strategic institutional partners vest over three years with a twelve-month cliff, then monthly linear through month thirty-six. The shorter duration relative to contributors reflects that institutional payer relationships may turn over on a different timeline than protocol development cycles, and locking partners longer than necessary to demonstrate commitment creates unnecessary friction for renewal.



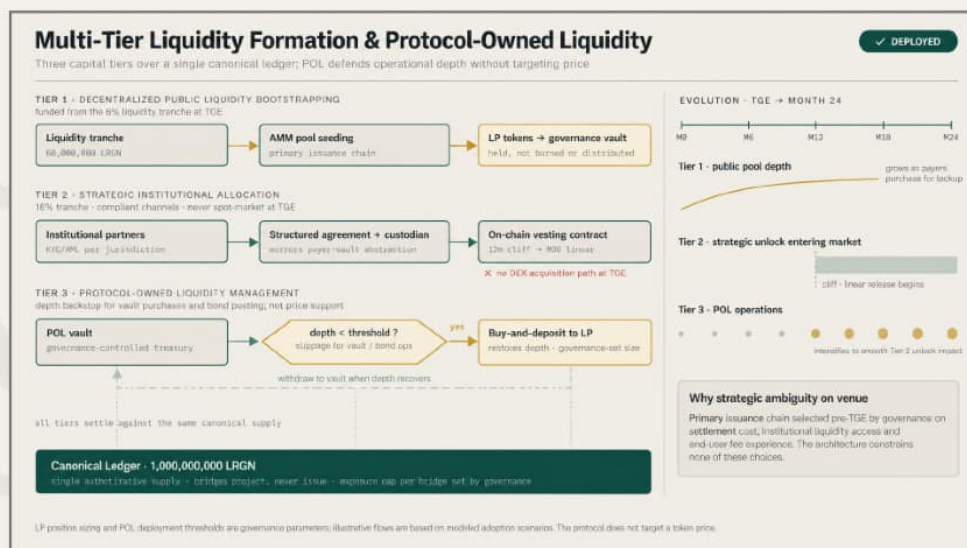
Ecosystem and validator incentives use an epoch-based decay rather than a linear cliff-and-unlock. Each epoch—roughly a calendar quarter—releases a tranche calculated to decline gradually over approximately eight years. Early epochs are larger, compensating bootstrap-period risk; later epochs are smaller but still meaningful, sustaining the validator economic model after the network has reached steady-state throughput. The decay function is public and governance-adjustable within a bounded range.

Foundation reserves are subject to multi-signature controls with a time-lock on any disbursement above a threshold, both for operational expenditures and for the insurance reserve. The insurance reserve can only be deployed to cover smart contract losses from audited exploits; it cannot be redirected to team compensation, marketing, or secondary market purchases.

8.4 Chain-Agnostic Canonical Supply Model

The canonical supply lives on a single authoritative ledger. Every LRGN token in existence is accounted for there. Representation on other execution chains—for liquidity tiers access, user-facing transaction costs, or ecosystem compatibility—is a bridge projection of canonical tokens rather than independent issuance.

Bridges are certified by governance. A new execution chain is added by a governance proposal that specifies the bridge module's security model, the custodian arrangement for canonical tokens locked in the bridge, the maximum bridge exposure limit (capped as a percentage of total supply to bound systemic risk), and the audit requirements for the bridge contract. Governance can revoke a bridge if security conditions change. The canonical ledger records all bridge issuances, so at any point total outstanding supply across all chains equals the canonical maximum minus burned tokens minus any bridge exposure not yet settled.





8.5 Dynamic Multi-Tier Liquidity Formation

The capital formation framework avoids a single mechanism precisely because different participant classes have different requirements and different legal constraints.

Decentralized public liquidity bootstrapping operates through standard AMM pool seeding, funded from the liquidity provisioning tranche, with the LP position held in a governance-controlled treasury rather than burned or distributed. This gives governance the ability to manage market depth over time rather than irrevocably surrendering the initial liquidity position.

Strategic institutional allocation moves through compliant channels. Institutional partners do not acquire tokens through public DEX trades; they operate through structured agreements with the Foundation that involve KYC/AML requirements appropriate to their jurisdiction, vesting contracts enforced on-chain, and in some cases local custodian arrangements that parallel the gateway structure in Section 6.1. The compliance posture here mirrors the payer vault framework: the crypto mechanics happen behind an abstraction layer that presents participating institutions with a relationship that fits their existing compliance frameworks.

Protocol-owned liquidity serves as a market depth backstop. When secondary market liquidity falls below a threshold that would produce excessive slippage for payer vault purchases or validator bond operations, the POL vault can deploy capital to restore depth. This is not price support in the conventional sense—the protocol does not target a token price—but it does ensure that the protocol's operational functions (vault lockup, bond posting) are not disrupted by temporary liquidity events in secondary markets.

9.0 DECENTRALIZED PROTOCOL GOVERNANCE

9.1 Bicameral Governance Topology

Decisions in a health protocol split into two categories that cannot be governed by the same process. Capital allocation, fee schedules, chain selection, liquidity parameters, and treasury management are economic questions where a weighted vote is a reasonable aggregation of preference. Which clinical milestone counts as evidence of adequate adherence, whether a proposed intervention falls inside the protocol's non-diagnostic boundary, and what audit standard applies to a maternal care program are clinical and ethical questions where weighted voting produces the wrong answer. A token holder with no medical training voting on whether a blood pressure threshold is clinically meaningful is not decentralized governance; it is a liability.

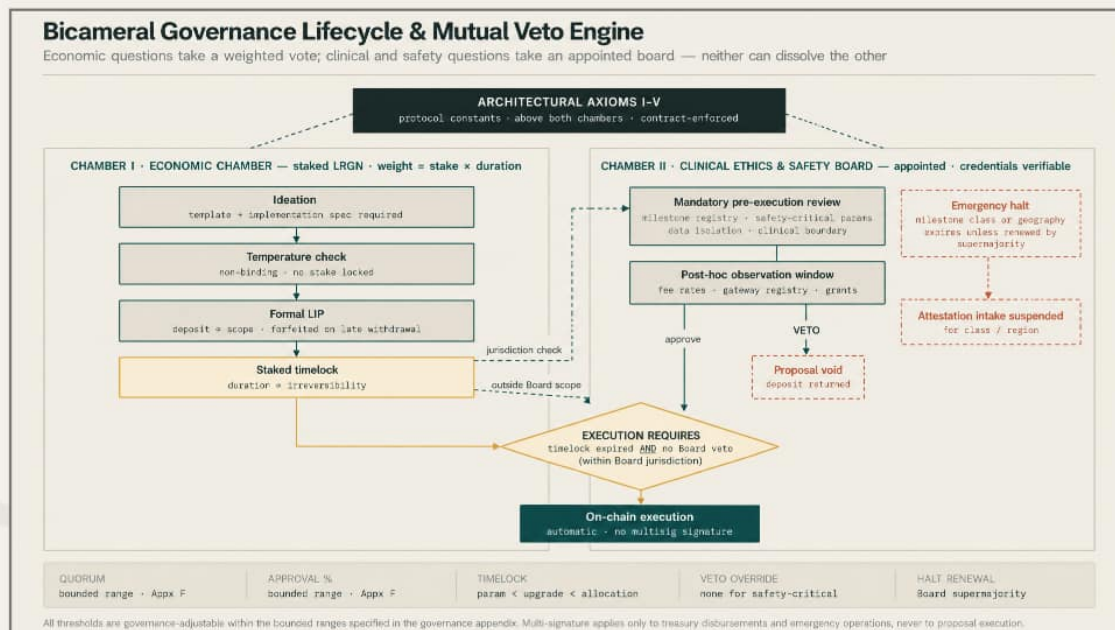


The protocol therefore separates authority into two chambers with distinct memberships and distinct powers.

The **Economic Chamber** consists of staked LRGN holders and governs the parameter space: protocol fee rates, validator tier bond ranges, burn allocations across the three channels in Section 7.1-7.2, gateway registry modifications, bridge certification, and treasury disbursements from the ecosystem grant tranche. Voting weight combines stake magnitude with stake duration, so a bond held through a full program cycle carries more influence than a position opened for a single vote.

The **Clinical Ethics & Safety Board** is appointed rather than elected, staffed by licensed practitioners, health informatics specialists, and independent bioethicists whose credentials are verifiable against jurisdictional professional registries. The Board holds three powers. It must approve any change to the milestone registry before the change becomes executable. It holds a unilateral veto over any Economic Chamber proposal that affects participant safety, data isolation, or the protocol's clinical boundary. And it can halt attestation intake for a specific milestone class or geography when evidence suggests a safety problem, with the halt expiring unless renewed under a supermajority threshold.

Neither chamber can dissolve the other, and neither can amend the architectural axioms in Section 1.3. The axioms sit above both as protocol constants enforced at the contract layer.





9.2 Deterministic Proposal Lifecycle

Every proposal follows the same five stages, and the contract enforces the sequence. There is no discretionary fast path for proposals from the Foundation or from large holders.

Ideation. A proposal begins as a forum discussion with a standard template: the change proposed, the parameter affected, the rationale, the expected effect on protocol metrics, and the implementation specification if the change touches contract code. Proposals without an implementation specification are rejected at intake rather than queued.

Temperature Check. A non-binding signal vote establishes whether the proposal has sufficient support to justify the cost of a formal review period. Signal votes do not commit capital and do not lock any stake; they exist to filter proposals that would waste validator and Board attention.

Formal LIP Submission. A Larasguna Improvement Proposal requires a minimum stake deposit proportional to the scope of the change. The deposit is returned on execution or on a clean rejection; it is forfeited if the proposal is withdrawn without a vote after reaching the review stage, which prices spam submissions.

Staked Timelock. Passing proposals enter a timelock before execution. The duration scales with the change's reversibility: parameter adjustments have short timelocks, contract upgrades and bridge certifications have longer ones, and changes to token allocation mechanics have the longest. During the timelock, holders can exit positions they no longer wish to maintain under the new parameters, and the Board can exercise its veto if the change falls within its jurisdiction.

On-Chain Execution. Execution is automatic if the timelock expires without a veto or a challenge. There is no signature required from a multi-signature committee for proposal execution; the multi-signature applies only to treasury disbursements and to emergency operations specified in Section 9.3.

9.3 Progressive Decentralization Framework

The protocol launches under a transitional stewardship arrangement and transitions to full decentralized operation against measurable maturity thresholds rather than a fixed schedule. Three thresholds govern the transition.

The **validator decentralization threshold** is met when bonded validator capacity and attestation throughput are distributed such that no single operator, accreditation partner, or geographic cluster accounts for more than a specified share of network attestations. The threshold exists because a network dominated by one operator's validators is a centralized service with a decentralized interface.



The **payer diversification threshold** is met when funded program volume is spread across a minimum number of independent payer classes (employer, insurer, statutory fund, research consortium) with no single payer exceeding a cap on total protocol activity. A protocol dependent on one large payer is exposed to a single counterparty's policy change.

The **governance participation threshold** addresses the risk that decentralization produces low-turnout apathy rather than distributed authority. It requires sustained participation rates above a floor across a defined number of consecutive proposal cycles before the stewardship function is dissolved.

Until all three are met, the Foundation retains two reserved powers: the ability to pause specific protocol functions in response to a security incident through a multi-signature emergency path with a bounded maximum duration, and the ability to slow or halt token unlocks if a governance attack on the vesting contracts is detected. Both powers expire permanently when the thresholds are satisfied, and both are constrained by on-chain time limits that prevent indefinite activation.

10.0 GO-TO-MARKET & NETWORK EXPANSION

10.1 Phase I: High-Density Archipelagic Launch Corridors

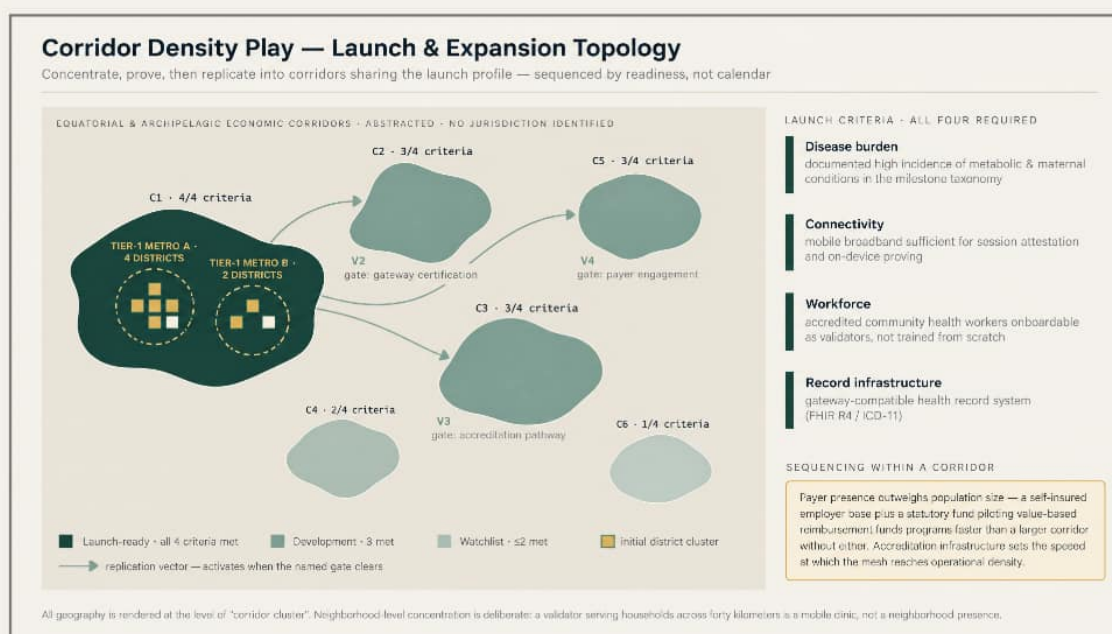
Network deployment concentrates rather than disperses. A validator mesh is only useful where validator density is sufficient for audit redundancy and participant coverage, and validator density requires enough participant volume to fund validator income. Spreading the initial cohort thin across a wide geography produces neither.

The corridor selection criteria are specific. Candidate regions must have documented high incidence of the metabolic and maternal health conditions the protocol's milestone taxonomy addresses, sufficient mobile broadband penetration to sustain the session attestation and proof generation the stack requires, an existing accredited community health workforce whose members can be onboarded as validators rather than trained from scratch, and a record infrastructure compatible with the gateway specification in Section 4.4. A region meeting three of four criteria is a future-phase target; a region meeting all four is a launch candidate.



Two secondary criteria shape sequencing within a qualifying corridor. Payer presence matters more than population size: a corridor with a self-insured employer base and a statutory fund already piloting value-based reimbursement will fund programs faster than a larger corridor without either. And validator accreditation infrastructure—the existence of professional bodies that can certify practitioners, and of health informatics programs that can supply the terminal operators—determines how quickly the mesh reaches operational density.

The initial launch concentrates in tier-1 archipelagic metropolises and their surrounding dense districts, with a deliberate choice to concentrate further into a small number of contiguous districts rather than spreading across the whole of a metropolis. Neighborhood-level concentration is what makes the community health validator relationship meaningful; a validator serving participants scattered across forty kilometers is functioning as a mobile clinic, not as a neighborhood presence.



10.2 Phase II: Sovereign Network Replication Vector

Replication targets corridors that share the launch region's structural profile rather than corridors that share its language or legal system. The profiles that matter for replication are the ones the protocol's mechanics depend on: near-universal mobile broadband, an accredited community health workforce existing outside hospital employment, a payer landscape with at least one entity already experimenting with outcome-based reimbursement, and a health record infrastructure capable of gateway integration.



Each replication target requires a full readiness assessment before a validator cohort is recruited. The assessment covers gateway compatibility testing, accreditation pathway verification with local professional bodies, gateway partner certification for local-currency disbursement, and a payer engagement phase that precedes program activation. Replication does not follow a calendar; it follows assessment completion, which means the second and third corridors may activate in either order depending on which one clears the prerequisites first.

The expansion economics are favorable relative to initial launch because the protocol's core infrastructure—contracts, proof circuits, milestone registry, account abstraction—is reused unchanged. What each new corridor requires is local: validator onboarding, gateway certification, payer relationship development, and any corridor-specific milestone registry additions to reflect the local disease burden. The milestone registry is designed for additive variation, and adding a corridor-specific milestone does not require redeploying the contracts.

10.3 Phase III: Global Preventive Infrastructure Layer

The final phase position treats the protocol as neutral infrastructure that any payer class in any jurisdiction can connect to through a certified gateway and a certified validator cohort. Multinational insurers running wellness programs across multiple countries use the protocol as a single verification and settlement layer rather than integrating country-by-country. Research consortia access federated cohort data across corridor boundaries with the privacy guarantees intact. Employers with globally distributed workforces fund care programs that use the same milestone taxonomy and the same audit standards regardless of where employees live.

The chain-agnostic architecture in Section 8.4 supports this position because jurisdiction-specific execution chains and settlement paths can be added without fragmenting supply or requiring the milestone registry to know which chain a given attestation will settle on. A corridor running on a low-cost settlement layer optimized for its fee environment and a corridor running on a layer chosen for institutional integration compatibility carry the same canonical token and participate in the same governance process.

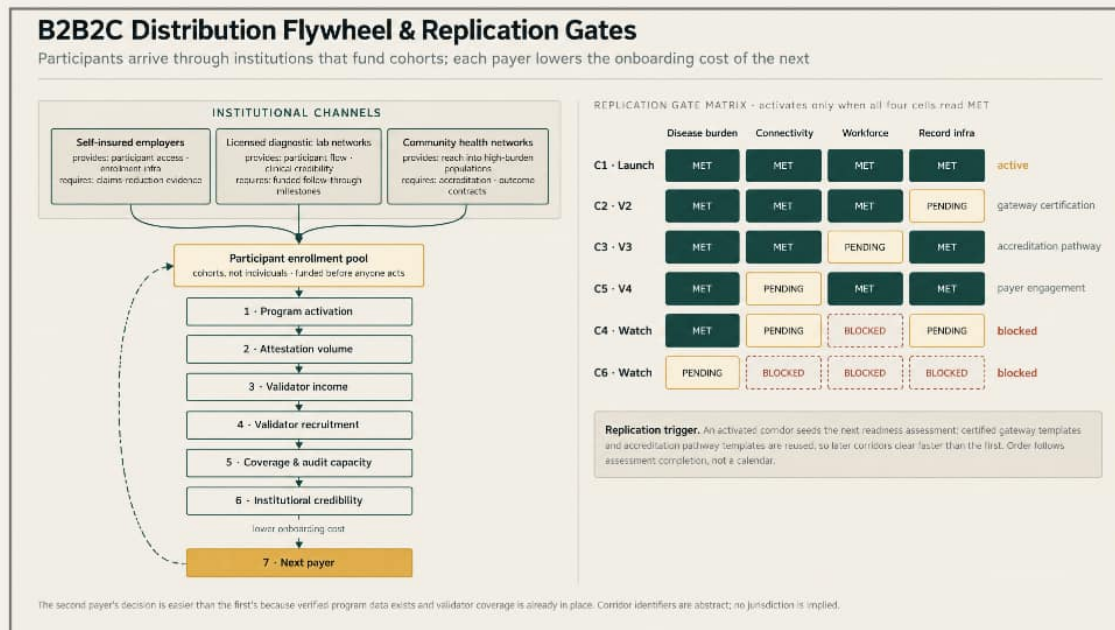
10.4 Institutional B2B2C Acquisition Flywheel

Participant acquisition runs through institutions rather than through direct consumer marketing. The economics of the protocol make this the only viable channel: the reward budget comes from payers, and payers fund cohorts, not individuals.



Three institution classes generate the initial volume. Self-insured employers with large workforces and documented metabolic disease burden have both the financial motivation (claims reduction) and the administrative capability (benefits enrollment infrastructure) to launch quickly. Licensed diagnostic lab chains that already conduct screening campaigns have the participant flow and the clinical credibility, and they convert screening from a one-time event into a program with funded follow-through. Municipal and regional community health networks have the deepest reach into the populations where preventable acute admissions concentrate, and they are the most likely to be experimenting with outcome-based contracts under their own budget pressure.

The flywheel turns as follows. An institution funds a cohort program, which recruits participants and generates attestation volume, which funds validator income, which draws additional validators into the corridor, which improves coverage and audit capacity, which makes the protocol a more credible counterparty for the next institutional payer. The second payer's decision is easier than the first payer's because verified program data exists and because validator coverage is already in place. Each successive payer reduces onboarding cost and increases the protocol's ability to negotiate favorable program terms.



10.5 Cultural Localization Framework

Care-journey design varies by household structure and daily rhythm; protocol mechanics do not. Localization adjusts scheduling, notification timing, dietary guidance content, and caregiver participation defaults, while leaving the attestation standard, milestone taxonomy, proof circuits, and slashing rules identical across corridors. A milestone that meets the registry standard in one corridor meets it in every corridor, which is what makes cross-corridor aggregate data scientifically usable.



Four localization dimensions recur across target corridors. Scheduling adapts to working-hour patterns and commuting time, since a screening appointment offered at a fixed weekday time will be missed by participants whose employment does not permit it. Dietary guidance is written against locally available and affordable foods rather than imported reference diets, and it is reviewed by local nutrition professionals rather than adapted from another corridor's materials. Periodic observance calendars that involve fasting or altered eating patterns require specific care-plan variations produced by clinical review, including explicit guidance on when a participant should suspend a fasting-related milestone and consult a practitioner; the protocol never structures a milestone in a way that rewards continuing a fasting practice against clinical advice. And multi-generational household structures determine the default configuration of family care accounts, with the sponsor role assigned to whichever household member typically controls health spending decisions absent a participant override.

The localization layer is deliberately thin. It sits in the care-orchestration tier, which is jurisdictional by design, and it never modifies the layers below. A corridor can choose its scheduling defaults; it cannot choose whether a proof requires a bonded validator.

10.6 Phase-Gate Progression Framework

Execution is organized into four gates, each with entry requirements, mandatory deliverables, and pause criteria that halt progression rather than allowing an incomplete stage to be treated as complete.

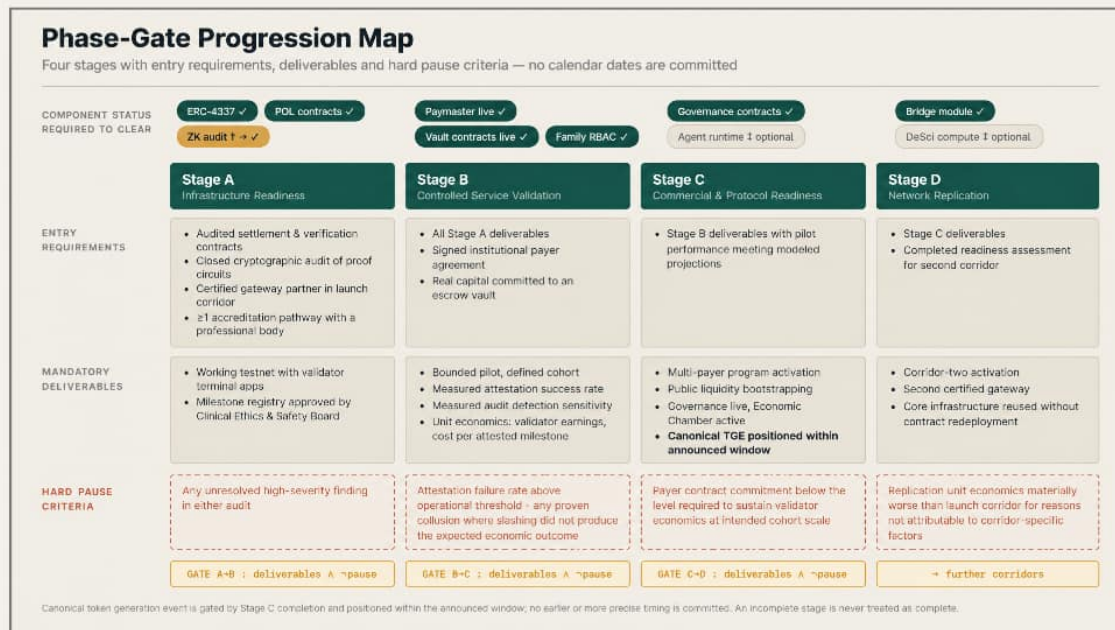
Stage A — Infrastructure Readiness. Entry requires audited contracts for the settlement and verification layers, a completed cryptographic audit of the proof circuits, a certified gateway partner in the launch corridor, and at least one accreditation pathway established with a professional body. Deliverables are a working testnet with validator terminal applications and a milestone registry reviewed and approved by the Clinical Ethics & Safety Board. Pause criterion: any unresolved high-severity finding in either audit.

Stage B — Controlled Service Validation. Entry requires Stage A deliverables plus a signed institutional payer agreement with real capital committed to an escrow vault. Deliverables are a bounded pilot with a defined cohort, measured attestation success rates, measured audit detection sensitivity, and a unit-economics dataset covering validator earnings and protocol cost per attested milestone. Pause criteria: attestation failure rate above the operational threshold, or any proven collusion incident in which the slashing mechanism did not produce the expected economic outcome.



Stage C — Commercial & Protocol Readiness. Entry requires Stage B deliverables with pilot performance meeting the modeled projections. Deliverables are multi-payer program activation, decentralized public liquidity bootstrapping per Section 8.5, governance contracts live with the Economic Chamber active, and the canonical token generation event positioned within its announced window. Pause criterion: payer contract commitment below the level required to sustain validator economics at the intended cohort scale.

Stage D — Network Replication. Entry requires Stage C deliverables plus a completed readiness assessment for the second corridor. Deliverables are corridor-two activation, a second certified gateway, and demonstrated reuse of the core infrastructure without contract redeployment. Pause criterion: replication unit economics materially worse than launch-corridor economics for reasons not attributable to corridor-specific factors.





11.0 PROTOCOL STEWARDSHIP, CONTRIBUTOR GUILDS & GOVERNANCE ARCHITECTURE

11.1 The Larasguna Foundation Fiduciary Mandate

The Foundation is chartered as an independent, non-profit stewardship entity. Its mandate is narrow by construction: it holds the canonical repository, administers ecosystem grants, maintains the accreditation registry partnerships, and executes treasury operations under multi-signature control. It does not hold clinical authority, does not adjudicate attestations, and holds no power over the milestone registry beyond submitting proposals that the Clinical Ethics & Safety Board reviews like any other submission. Protocol code is published open-source under a permissive license from the first release; the Foundation's repository role is custodianship of a public artifact rather than ownership of it, and any contributor guild can fork the canonical codebase if the Foundation's stewardship is judged inadequate.

Treasury operations run through a multi-signature vault with time-locked disbursement paths above a defined threshold. Foundation personnel do not hold unilateral spending authority, and no single signer can activate an emergency function. Statutory registrations are established across qualifying digital asset supervisory jurisdictions before canonical network genesis, with the specific selection governed by where the protocol's operational functions require a legal presence rather than by tax optimization.

11.2 Specialized Engineering & Research Working Groups

Protocol development is distributed across four standing contributor guilds, each holding a defined technical mandate and each operating under merit appointment from the Foundation with input from the Economic Chamber.

The **Distributed Systems & Consensus Guild** owns the settlement layer, bridge modules, and validator mesh contracts. The **Cryptographic Privacy & Zero-Knowledge Working Group** owns the circuit registry, proving key lifecycle, and the federated compute specification. The **Health Informatics & Interoperability Consortium** owns the gateway interface, the HL7 FHIR R4 mapping layer, and the milestone registry's technical schema. The **Mechanism Design & Tokenomics Desk** owns vault logic, fee schedules, slashing parameters, and the burn channel allocations.



Guild membership is disclosed at the credential level: members' professional certifications, institutional affiliations of record, and technical contribution history are published, subject to the operational security constraints in Section 11.4. What the protocol publishes is which guild holds which mandate and what qualifications that guild requires; individual personnel records remain in the Foundation's compliance system rather than in protocol documentation.

11.3 Independent Clinical & Cryptographic Ethics Council

The Clinical Ethics & Safety Board described in Section 9.1 operates alongside an independent council with an overlapping but distinct mandate. Where the Board reviews milestone changes and exercises veto authority over safety-critical proposals, the Council holds standing responsibility for the protocol's boundary conditions: maintaining the definition of what falls inside and outside the protocol's non-diagnostic scope, reviewing adverse event reports from deployed programs, and commissioning external review of the federation's privacy guarantees as the research query mechanism matures.

Council membership includes licensed practitioners, a health data protection specialist, and at least one member from a jurisdiction outside the protocol's initial operational regions, so that the protocol's ethics review is not self-referential to a single legal tradition. Council findings are published with program-level detail and without participant-identifying information.

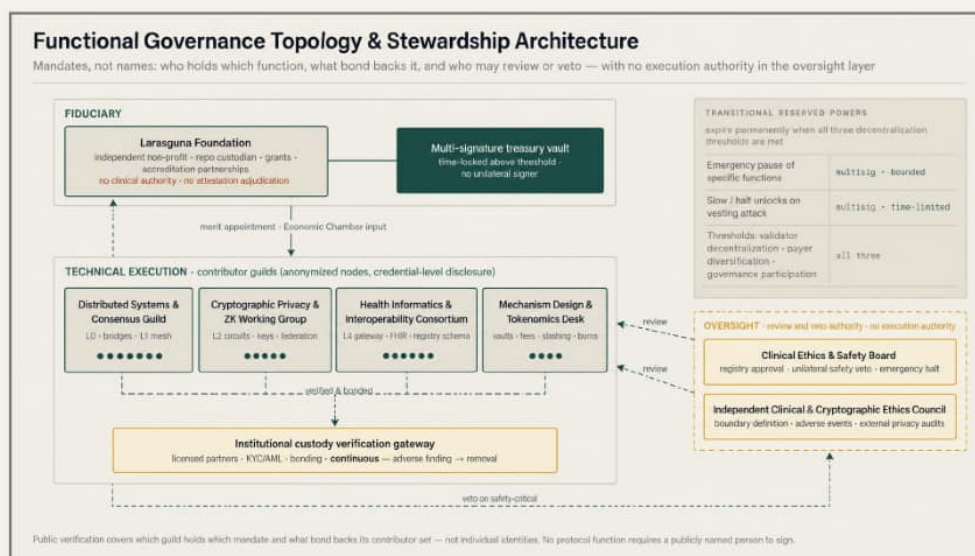
11.4 Contributor Privacy & Institutional Custody Verification

Critical healthcare infrastructure attracts adversaries, and the people who maintain it are targets for social engineering and coercion. Publishing a roster of the individuals who control the protocol's settlement contracts, hold proof system key material, or oversee clinical data isolation would convert the protocol's most sensitive functions into a public list of pressure points.

The protocol therefore operates its core engineering and clinical research functions through decentralized working-group mandates rather than named individuals. Contributors' identities, professional credentials, and beneficial ownership positions are verified and bonded through licensed institutional custody partners operating under anti-money-laundering and know-your-customer frameworks applicable to their jurisdictions. Verification is continuous rather than one-time: a contributor who loses professional standing or acquiring an adverse compliance finding is removed from guild standing through the custody partner's reporting relationship.



Governance actions execute through multi-signature vaults, timelocks, and the Care Council framework. No protocol function requires a publicly named individual to sign. This arrangement trades some of the transparency that open-source projects conventionally provide—the public can verify which guild holds which mandate and what the bond backing each guild's contributor set is, but not who the individuals are—for reducing the attack surface that targeted coercion of known persons would create against health infrastructure handling millions of participants.



12.0 SYSTEMIC RISK TAXONOMY & DISCLOSURES

12.1 Regulatory & Cross-Jurisdictional Classification Risks

Token classification varies across jurisdictions, and no single characterization is stable. A regulatory authority may determine that LRGN constitutes a security, a financial instrument, a commodity, or a digital asset subject to a bespoke framework, and that determination can change as the protocol's utility profile evolves. Health data regulation adds a second layer of jurisdictional variation: frameworks governing protected health information, cross-border transfer, and local processing requirements differ materially across the corridors referenced in Chapter 10, and a compliance posture that satisfies one authority may fail another. Requirements applicable to digital asset intermediaries—licensing, custody standards, anti-money-laundering obligations, marketing restrictions—apply to counterparties the protocol depends on, and a counterparty's loss of standing can suspend a settlement path without protocol-level fault. Any of these developments may require contract changes, restrict participant eligibility in a jurisdiction, delay program activation, or interrupt disbursement channels.



12.2 Smart-Contract, ZK-Circuit & Physical Oracle Attack Surfaces

Smart contracts may contain vulnerabilities despite audit. Zero-knowledge circuits depend on soundness assumptions that a future cryptanalytic advance could weaken, and trusted setup ceremonies carry contamination risks even where multi-party protocols make them improbable. Bridge modules that project canonical supply onto execution chains introduce custodial and messaging risks bounded by governance-set exposure limits, which limit but do not eliminate systemic loss. Physical oracle manipulation remains the most likely attack path: a colluding validator and participant can produce a false attestation that randomized audit may fail to detect, and the slashing schedule prices this attack rather than preventing it outright. Edge runtime compromise, including device-level malware targeting the secure enclave or the terminal application, is a live threat against a participant population using consumer devices with varying security postures.

12.3 Token Liquidity, Market Dynamics & Volatility

Payer willingness to fund outcome-based programs at the modeled levels is unproven at scale; if avoidance estimates prove optimistic, program funding falls below the level required to sustain validator economics. Validator recruitment and retention may underperform projections, particularly where accreditation pathways are slow or where local alternatives offer steadier income. Incumbent healthcare platforms, insurers, and sovereign digital health programs may build competing verification infrastructure or impose requirements that favor domestic providers. Token liquidity may be insufficient to support vault purchases and bond operations without price impact, and secondary market conditions can diverge from protocol fundamentals for extended periods.

12.4 Health Delivery Boundaries & Forward-Looking Disclosures

The protocol provides coordination, attestation, and settlement infrastructure. It does not practice medicine, does not diagnose or treat any condition, and does not replace licensed healthcare professionals. Clinical protocols are authored and reviewed by licensed practitioners operating under their own professional obligations and jurisdictional regulations.

This document contains forward-looking statements regarding protocol development, program adoption, cost-avoidance modeling, and network expansion. These statements rest on assumptions that may prove incorrect, and actual results may differ materially. Modeled figures are identified as such in the accompanying figures and are not observed outcomes. Nothing in this document constitutes investment advice, a financial promotion, an offer to sell, or a solicitation to buy any token or security in any jurisdiction. Prospective participants and counterparties should obtain independent legal, financial, and medical advice applicable to their circumstances.



BACK MATTER

References & Source Dates

The citations below anchor each empirical claim in the main text to a verifiable public source. Where a figure is derived from a composite of multiple published sources, the citation identifies each contributing source individually. All source dates fall on or before September 2026.

[1] Global health expenditure allocation and curative vs. preventive spending ratios.

- World Health Organization. *Global Health Expenditure Database*. Geneva: WHO; updated annually. Available at: <https://apps.who.int/nha/database>
- Xu, K., Soucat, A., Kutzin, J. et al. *Public Spending on Health: A Closer Look at Global Trends*. WHO/HIS/HGF/HF Working Paper No. 18.3. Geneva: World Health Organization; 2018. Available at: <https://apps.who.int/iris/handle/10665/276728>
- Institute for Health Metrics and Evaluation (IHME). *Global Burden of Disease Study 2019: Health Spending by Source, 1995–2019*. The Lancet. 2023; 401(10383): 1183–1197. DOI: 10.1016/S0140-6736(23)00198-8

The 82%–88% curative share cited in Section 2.1 represents the range across the composite population of reporting systems in the WHO database, cross-referenced against the IHME disaggregation of spending by function. The ratio has been directionally stable across reporting cycles from 2015 to the most recent available edition.

[2] Post-screening adherence decay in asymptomatic chronic conditions.

- Chowdhury, R., Khan, H., Heydon, E. et al. *Adherence to cardiovascular therapy: a meta-analysis of prevalence and clinical consequences*. European Heart Journal. 2013; 34(38): 2940–2948. DOI: 10.1093/eurheartj/eh295
- Kruk, M.E., Gage, A.D., Arsenault, C. et al. *High-quality health systems in the Sustainable Development Goals era: time for a revolution*. The Lancet Global Health. 2018; 6(11): e1196–e1252. DOI: 10.1016/S2214-109X(18)30386-3
- Osterberg, L. & Blaschke, T. *Adherence to Medication*. New England Journal of Medicine. 2005; 353(5): 487–497. DOI: 10.1056/NEJMra050100



The 6%–10% adherence band at day 180 in Section 2.3 is modeled from the Chowdhury et al. meta-analytic finding that approximately 50% of chronic disease patients in high-income settings are non-adherent within 12 months, adjusted downward for emerging-market settings using the Kruk et al. quality-of-care framework, which documents steeper adherence decay where follow-up infrastructure is weaker. The figure is a scenario input for protocol design, not a single-study observed outcome.

[3] Metabolic and nutritional prevalence in equatorial and archipelagic corridors.

- NCD Risk Factor Collaboration (NCD-RisC). *Worldwide trends in diabetes since 1980: a pooled analysis of 751 population-based studies with 4.4 million participants*. The Lancet. 2016; 387(10027): 1513–1530. DOI: 10.1016/S0140-6736(16)00618-8
- UNICEF / WHO / World Bank Group. *Levels and Trends in Child Malnutrition: UNICEF–WHO–World Bank Joint Child Malnutrition Estimates – Key Findings of the 2023 Edition*. Available at: <https://data.unicef.org/resources/jme-report-2023/>
- International Diabetes Federation. *IDF Diabetes Atlas, 10th Edition*. Brussels: IDF; 2021. Available at: <https://diabetesatlas.org/>

Diabetes prevalence progression cited in Section 2.2 is anchored to the NCD-RisC pooled analysis and calibrated against the IDF Atlas regional estimates for Southeast Asian and Western Pacific regions. Childhood stunting figures reflect the UNICEF–WHO–World Bank Joint Child Malnutrition Estimates. Point estimates are corridor-representative composites; they are not attributed to a single jurisdiction.

[4] Mass screening campaign outcomes and post-detection follow-through.

- Gakidou, E., Mallinger, L., Abbott-Klafter, J. et al. *Management of diabetes and associated cardiovascular risk factors in seven countries: a comparison of data from national health examination surveys*. Bulletin of the World Health Organization. 2011; 89(3): 172–183. DOI: 10.2471/BLT.10.080820
- World Health Organization. *HEARTS Technical Package for Cardiovascular Disease Management in Primary Health Care*. Geneva: WHO; 2016. Available at: <https://www.who.int/publications/i/item/hearts-technical-package>

The sub-4% controlled-status rate among newly identified cases in Section 2.3 is consistent with the Gakidou et al. cross-country analysis of management gaps between detection and control, particularly in middle-income settings where the gap is largest. The HEARTS technical package provides the clinical framework against which "controlled status" is defined for the protocol's milestone taxonomy.



[5] Account abstraction and ERC-4337 specification.

- Ethereum Foundation. *ERC-4337: Account Abstraction Using Alt Mempool*. Ethereum Improvement Proposals. 2021. Available at: <https://eips.ethereum.org/EIPS/eip-4337>

The account abstraction implementation referenced in Section 4.5 conforms to this standard.

[6] Zero-knowledge proof systems and Circom framework.

- iden3. *Circom: A Robust and Scalable Language for Building Complex Zero-Knowledge Circuits*. Documentation and source repository. Available at: <https://iden3.io/>

The circuit development framework referenced in Section 4.3.

[7] HL7 FHIR R4 interoperability standard.

- Health Level Seven International. *HL7 FHIR Release 4*. Available at: <https://hl7.org/fhir/R4/>

The health record interoperability standard referenced in Section 4.4.

Note on sourcing convention. Empirical claims in this document are anchored to identified, publicly accessible sources with verifiable DOIs or institutional URLs. Where a figure is a range assembled across multiple studies or reporting systems, the contributing sources are listed individually. Where a figure is a modeled scenario input rather than an observed outcome, the main text and figure captions state so at the point of use.



Glossary of Protocol Terms

Attestation — A complete Proof of Care object: a bonded validator's session signature paired with a client-side zero-knowledge proof, admissible to the verification contract only when both parts reference the same commitment.

Bond tier — The tiered stake classification governing a validator's milestone eligibility, fee rate, and slashing exposure. Three tiers operate in the initial network.

Canonical supply — The single authoritative ledger on which all LRGN supply is accounted for. Representation on other execution chains projects from it and does not create parallel issuance.

CHV (Community Health Validator) — A certified practitioner holding an accreditation-bound signing key and posted LRGN bond, authorized to attest physical preventive care sessions within a defined milestone scope.

Clawback — The contract-enforced return of unspent payer capital at program conclusion, along one of three paths defined at vault activation.

Commitment — A cryptographic hash binding a clinical value or action record to a session without disclosing the value. The artifact that crosses from the participant's device into protocol state.

DCVM (Decentralized Care Validator Mesh) — The physical validator network taken as infrastructure: terminals, accredited practitioners, bonded collateral, and the geographic distribution that supplies audit redundancy.

Epoch — The release interval for ecosystem and validator incentive tranches, roughly one calendar quarter, with a declining allocation across approximately ninety-six months.

ERC-4337 — The account abstraction standard under which protocol accounts are created as smart contracts rather than externally owned key pairs, enabling biometric authentication, social recovery, and sponsored transaction settlement.

k-anonymity threshold — The minimum contributing-cohort size, set at $k \geq 50$, below which an aggregated research query output is withheld.

LIP (Larasguna Improvement Proposal) — The formal governance submission format requiring an implementation specification and a stake deposit proportional to change scope.

Milestone registry — The versioned catalogue of verifiable preventive milestones, each entry specifying the clinical rule, evidence standard, validator accreditation class, and funding weight. Changes require Clinical Ethics & Safety Board approval.



Payer vault — The on-chain escrow contract holding institutional program capital, with locked funding schedules, release conditions, and clawback rules.

Paymaster — The ERC-4337 component that settles network transaction costs on a participant's behalf from a pre-funded LRGN pool, removing gas acquisition from the user experience and burning LRGN per sponsored interaction.

PoC (Proof of Care) — The protocol's attestation primitive, defined in Section 3.1.

POL (Protocol-Owned Liquidity) — Liquidity positions funded and held by the protocol treasury to maintain secondary market depth for operational functions, not as a mechanism targeting token price.

Proof-of-care vs. proof-of-wellness — A distinction the protocol enforces. Attestation concerns whether an agreed action occurred under qualified observation. It does not concern a participant's clinical condition, and no reward is indexed to a health outcome produced by the participant.

SHGI (Sovereign Health Gateway Interface) — The read-only, consent-gated integration layer mapping external health record systems to protocol-legible commitments, enforcing one-way data flow at the network layer.

Slashing — Bond forfeiture following a proven violation, bifurcated into partial slash for negligence and full slash for proven collusion.

TEE (Trusted Execution Environment) — The device-level secure enclave in which raw clinical values are processed during proof construction and where proposed client-side agent runtimes execute.

zk-SNARK — The succinct non-interactive proof system used by the attestation engine, constructed in Circom with circuit hashes pinned in verification contracts.