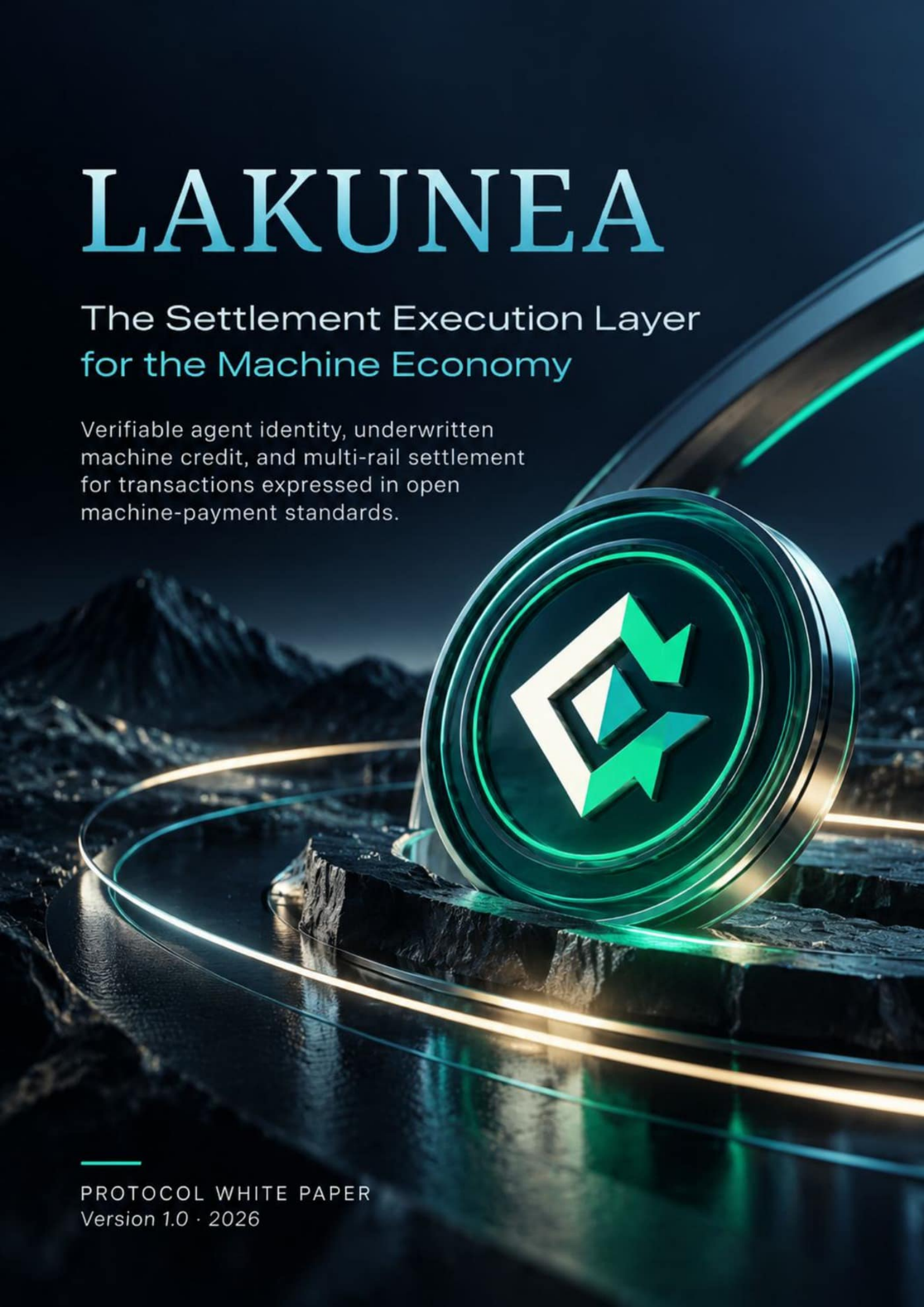
LAKUNEA

The Settlement Execution Layer for the Machine Economy

Verifiable agent identity, underwritten machine credit, and multi-rail settlement for transactions expressed in open machine-payment standards.



PROTOCOL WHITE PAPER

Version 1.0 · 2026

TABLE OF CONTENTS

1.0 Executive Summary

2.0 Market Thesis: The Agentic Settlement Gap

3.0 Protocol Overview and Design Principles

4.0 System Architecture

5.0 The Agent Identity Layer

6.0 The Machine Credit Layer

7.0 The Policy and Authorization Layer

8.0 The Settlement and Interoperability Layer

9.0 The Decentralized Node Alliance and Network Economics

10.0 LKUN Token Economics

11.0 Governance, Treasury, and Progressive Decentralization

12.0 Risk Factors and Compliance Architecture

13.0 Organization, Development Horizons, and Verification

Appendix A — Glossary of Protocol Terms

Appendix B — Parameter Table and Governance-Adjustable Ranges

Abstract

Machine-to-machine payment standards consolidated into neutral, foundation-governed public infrastructure over 2025 and 2026. Those standards specify message formats, authorization semantics, and verification requirements. They do not specify who performs settlement, who vouches for the identity of a transacting agent, who extends credit to software that holds no balance, or how value reaches a service provider whose banking relationships sit outside the dollar-denominated core.

Lakunea operates that layer. The protocol is a permissionless network of settlement nodes that execute payment verification and on-chain clearing for transactions expressed in any of the prevailing open machine-payment standards, together with three functions the standards leave undefined: cryptographically anchored agent identity and behavioral history, an underwritten credit facility that allows reputable agents to transact before funding, and a policy engine that binds every machine expenditure to a revocable delegation from a legally accountable principal.

LKUN is the native settlement and fuel unit of the network. Node admission requires bonded LKUN. Every settled transaction consumes a network fee denominated in LKUN, of which the base component is permanently burned and the priority component accrues to the executing node. Credit underwriting capital is posted in LKUN subject to published haircuts, layered beneath a senior stable-value tranche. Ecosystem emission unlocks against verified, identity-attested commercial settlement volume rather than elapsed time.

1.0 Executive Summary

1.1 The Thesis in One Page: Standards Are Open, Settlement Is Not Solved

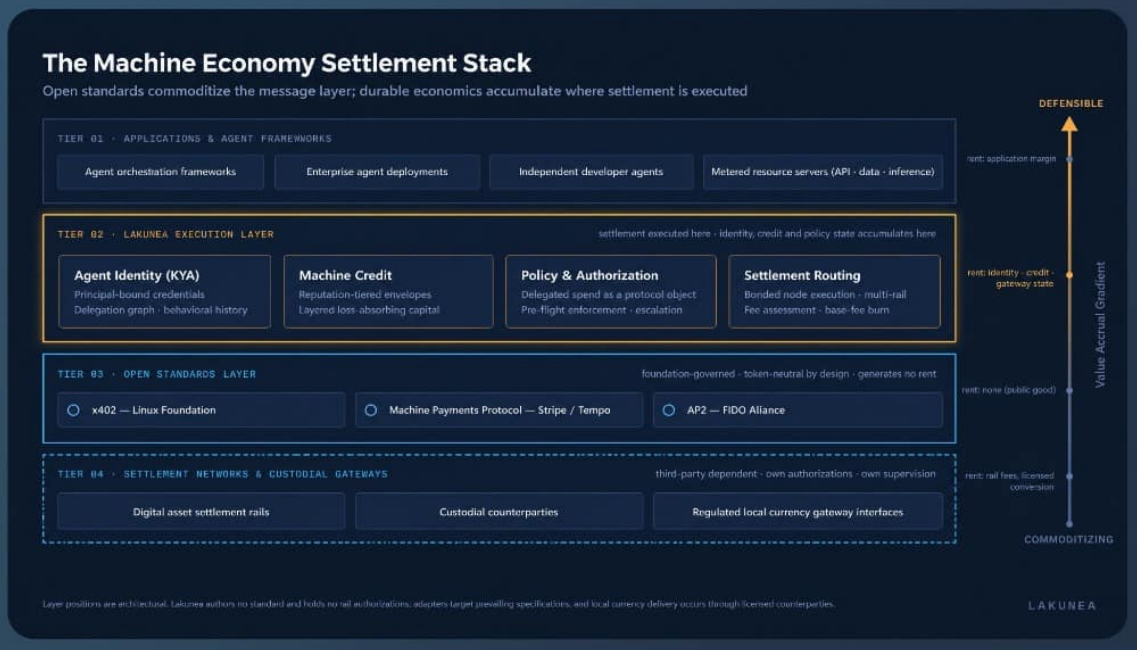
The competition to define how software pays software ended faster than most participants expected, and it ended in the public domain. By April 2026 the x402 specification had been contributed to the Linux Foundation, which stood up a dedicated foundation with Adyen, AWS, American Express, Circle, Fiserv, Google, Mastercard, Microsoft, Shopify, Stripe and Visa among the founding members. Stripe and Tempo had published the Machine Payments Protocol a month earlier. Google's Agent Payments Protocol, released in September 2025 and carried to sixty-plus institutional supporters within two quarters, was donated to the FIDO Alliance in April 2026.

Three standards, three neutral stewards, one shared consequence: the message layer of machine commerce became a public good, and it was designed from the outset to require no proprietary token and no privileged intermediary.

The standards define what a payment request looks like, how a counterparty proves receipt, and what an authorization assertion must contain. They are silent on execution. x402 names the role explicitly and leaves the seat open: a facilitator verifies payment payloads, submits them for on-chain settlement, and returns confirmation, which relieves the resource server of writing any chain-facing logic at all. Coinbase operates a facilitator. The specification permits anyone to.

That seat is where the durable economics of machine commerce accumulate, for a reason familiar to anyone who has studied card networks. Message formats commoditize. Clearing does not. The facilitator holds the position from which identity can be attested, credit can be extended, expenditure can be constrained, and value can be routed into corridors the standards authors never modeled.

Lakunea occupies that position as a network. Settlement nodes post bonded collateral, compete on throughput and reliability, earn fees per transaction cleared, and are subject to slashing for misexecution. Layered over that execution substrate are three functions that no open standard specifies and no single vendor has assembled: verifiable agent identity with persistent behavioral history, an underwritten credit facility for agents that have earned standing but hold no balance, and a policy engine that ties every machine payment to a revocable grant from an accountable principal.



1.2 What Lakunea Is, and the Exclusions That Define It

Lakunea is a settlement execution network. It verifies, clears, and records machine-originated payments across multiple chains and multiple rails, and it maintains the identity, credit, and policy state that makes those payments attributable and constrainable.

The exclusions matter as much as the definition, because each one closes off a failure mode visible elsewhere in the sector:

Lakunea does not author a competing payment standard. Adapters target the prevailing specifications, and broader adoption of any of them increases the volume routable to Lakunea nodes. Forking the message layer would trade a compounding tailwind for a narrow moat.

Lakunea does not require LKUN as a medium of exchange for counterparties who prefer stable-value settlement. Services are denominated in a stable unit of account; LKUN executes the on-chain settlement leg; providers may pre-authorize atomic conversion back to stable assets within the same transaction. Mandating that a service provider hold a volatile balance in order to be paid is the fastest way to ensure the service provider integrates a competitor.

Lakunea does not custody end-user funds, does not operate as a payment institution, and does not represent that its token may be used to discharge obligations denominated in any national currency. Value transfer into local currency corridors occurs through licensed gateway counterparties under their own authorizations.

Lakunea does not underwrite credit exclusively against its own token. Junior underwriting capital is posted in LKUN at a published haircut and sits beneath a senior stable-value tranche, because a credit facility collateralized solely by the asset whose price is correlated with protocol distress is a mechanism for converting a drawdown into an insolvency.

1.3 Four Structural Gaps, Four Protocol Modules

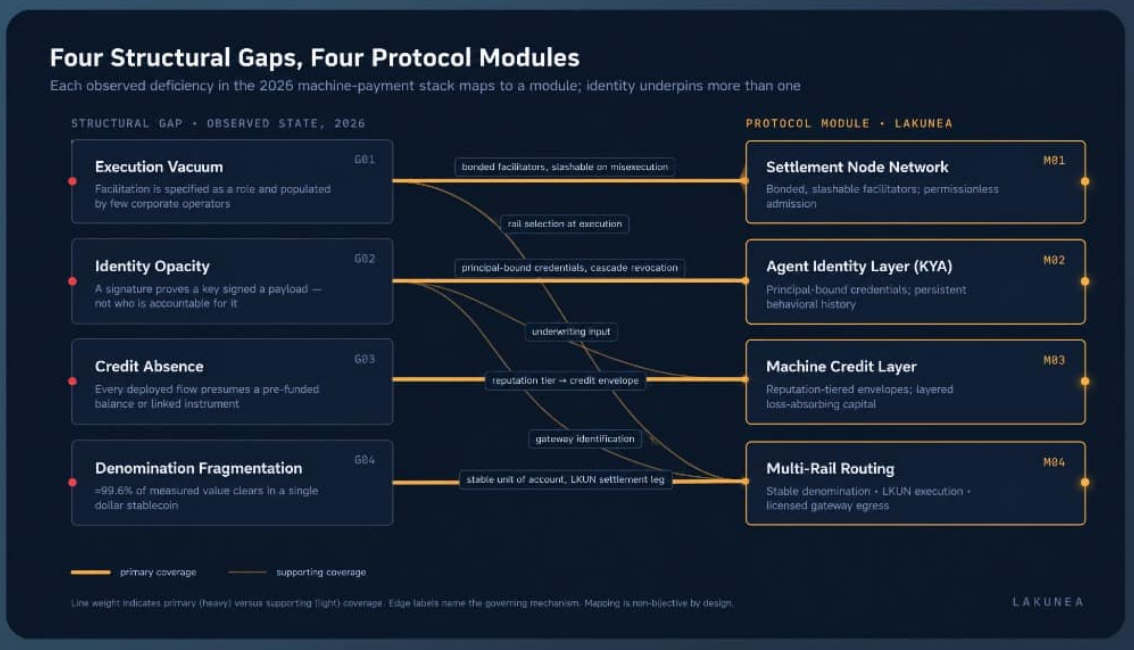
The observed state of machine payments in 2026 exhibits four deficiencies that the standards layer, by construction, does not address.

Execution is unbuilt. Facilitation is specified as a role and populated by a handful of operators, predominantly serving dollar-centric enterprise flow. A specification that anticipates billions of transactions daily cannot depend on a small set of corporate clearing desks without reconstituting the concentration that open standards were written to avoid.

Identity is opaque. A signature demonstrates that a key signed a payload. It does not establish which legal entity stands behind that key, what the key was authorized to do, or whether prior conduct warrants extending it access. NIST's guidance on digital signature verification separates these conditions precisely; the machine payments stack currently collapses them.

Credit is absent. Every deployed agentic payment flow presumes a pre-funded balance or a linked instrument. Human commerce runs on credit, and the counterparty that cannot transact before funding is excluded from the majority of commercial activity. No network currently issues a credit envelope to an agent on the basis of demonstrated behavior.

Denomination is fragmented. Roughly 99.6% of measured agentic settlement value has cleared in a single dollar-denominated stablecoin. That concentration is rational for issuers and processors whose compliance perimeter is the United States. It leaves the API provider, dataset licensor, and inference host operating outside that perimeter with no first-class path from machine revenue to usable local value.



1.4 LKUN at a Glance

Dimension	Design
Function	Native settlement and fuel unit; node and underwriter bonding asset; identity and credit-tier consumption; governance weight
Canonical supply	Fixed at issuance, no mint authority, no perpetual inflation. All incentive distribution draws from pre-allocated tranches
Fee mechanics	Per-transaction network fee split into a burned base component and a priority component paid to the executing node
Issuance architecture	Chain-agnostic canonical supply ledger with attested multi-chain representations; primary issuance chain selected at the distribution window against published criteria
Value accrual	A defined share of protocol revenue is applied to open-market repurchase and burn on a 28-day epochal cadence (at 00:00 UTC), verifiable on-chain

Emission integrity	Ecosystem tranches unlock against verified, identity-attested, non-self-dealing settlement volume. Absent verified volume, no emission occurs
Underwriting discipline	Junior LKUN collateral subject to a 50.0% baseline haircut (governance band: 35.0%–65.0%), subordinated to a senior stable-value tranche, with governance-triggered circuit breakers

The token is load-bearing at four points in the transaction path: a node cannot join without bonding it, a transaction cannot settle without consuming it, an agent cannot receive a credit line without capital posted in it, and an identity cannot be registered or upgraded without expending it. None of these is a discount coupon bolted onto an otherwise token-free system.

1.5 Verification Commitments

Claims in this document are intended to be checkable rather than taken on trust. From the distribution window onward, the protocol publishes:

the treasury address set and every disbursement against it; the repurchase contract address, execution history, and cumulative burn; protocol revenue by source and its allocation across burn, node distribution, and treasury; circulating supply reconciled against the canonical ledger and every mirrored chain representation; the verified-volume counter that gates ecosystem emission, alongside the filtered-out volume and the filter criteria applied; node roster, bonded stake, uptime, and slashing events; and the maturity state of each capability enumerated, revised quarterly.

Market-making arrangements involving token loans, options, or performance-linked compensation are disclosed by quantity and material terms. Liquidity provision positions are lock-verified on-chain.

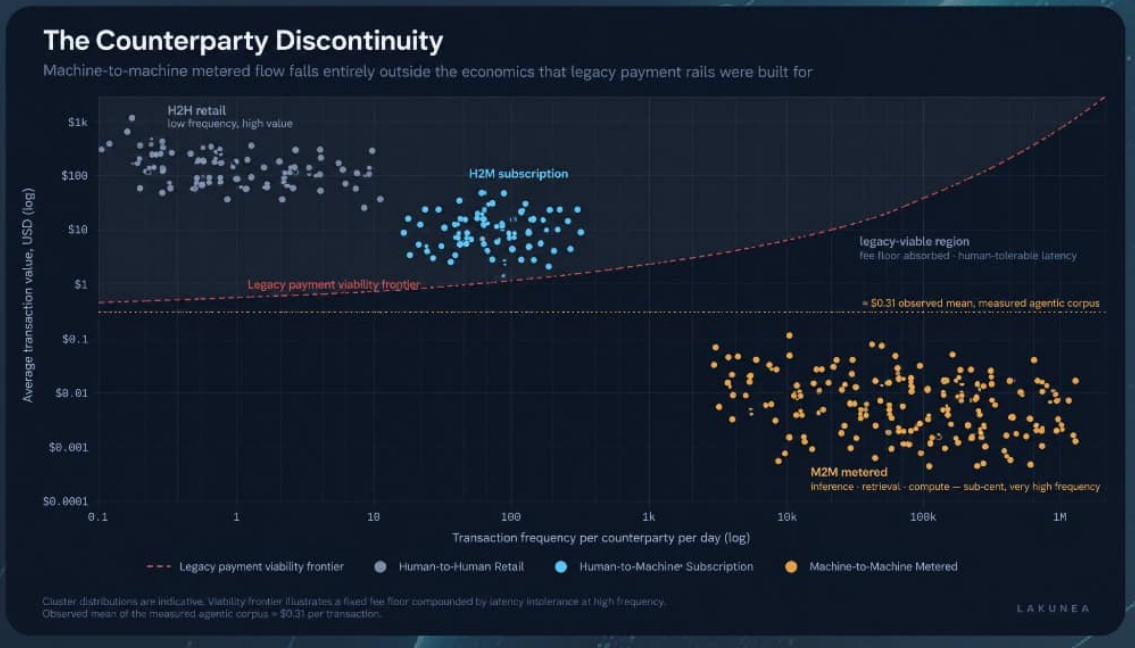
2.0 Market Thesis: The Agentic Settlement Gap

2.1 A Structural Discontinuity, Not an Extension of Existing Payments

Payment infrastructure built for human commerce assumes a transaction value high enough to absorb per-transaction cost, a cadence slow enough for human review, and a counterparty capable of consenting. Machine commerce violates all three assumptions simultaneously, which is why it required new rails rather than new pricing tiers on existing ones.

The measured average across the largest agentic payment corpus to date sits near thirty-one cents. Inference calls, dataset queries, and metered compute frequently clear at sub-cent amounts. At those values, interchange economics invert: the fee exceeds the principal by an order of magnitude or more, and the settlement latency tolerable to a human shopper is fatal to an agent orchestrating a hundred sequential tool calls.

The frequency profile compounds the problem. An agent does not make a purchase decision and then rest. It queries, retries, escalates, cross-checks against a second provider, and pays for the privilege each time. Transaction counts scale with the reasoning depth of the model, not with the population of buyers.



2.2 The Standards Layer Consolidated and Was Deliberately Left Token-Neutral

Four developments over an eighteen-month window settled the message layer.

x402 was released by Coinbase, adopted by API providers seeking metered access control, and contributed to the Linux Foundation in April 2026, where a dedicated foundation now governs it with the payment industry's incumbents as founding members. The specification's settlement modes — immediate exact-amount, variable upto pricing for consumption-based services, and batch settlement against escrowed funds with off-chain vouchers redeemed in a single on-chain transaction — cover most metered commercial patterns.

The Machine Payments Protocol from Stripe and Tempo, published in March 2026, addresses the same problem from the processor side, with emphasis on programmatic coordination between machine counterparties and on reconciliation into existing merchant ledgers.

AP2 approached the question from authorization rather than settlement, specifying how an agent proves it was mandated to transact and how liability attaches when it exceeds that mandate. Its transfer to the FIDO Alliance placed it alongside the authentication standards it structurally resembles.

Each of these is governed by a neutral body, and each was written to function without a specification-native token. That design choice was correct for a public standard. It also means the standards layer generates no economic rent and cannot capture the value of the traffic it enables.



2.3 The Execution Vacuum

The facilitator role exists because resource servers do not want chain-facing code. A provider charging for an API endpoint wants to return a payment-required response, receive a verified confirmation, and serve the request. The facilitator absorbs payload verification, signature checking, nonce management, chain submission, finality tracking, and failure handling.

That workload is real infrastructure, and the entities currently performing it are few. Coinbase operates the reference facilitator. Fireblocks joined the x402 Foundation in May 2026 with security extensions covering request integrity and spend governance, serving institutional counterparties with existing custody relationships. The servicing bias is toward enterprises that already hold dollar balances and already clear compliance review.

An open standard cleared by a small number of corporate operators has reconstituted, at the execution tier, exactly the dependency that open standardization was meant to dissolve. The gap is structural rather than a matter of insufficient competitors: facilitation at scale requires bonded accountability, geographic distribution for latency, and an economic model that rewards reliability. A company can supply the first and the third for its own book. Neither a company nor a consortium of companies supplies permissionless entry for a node operator in a market its compliance team has not prioritized.

2.4 The Integrity Problem

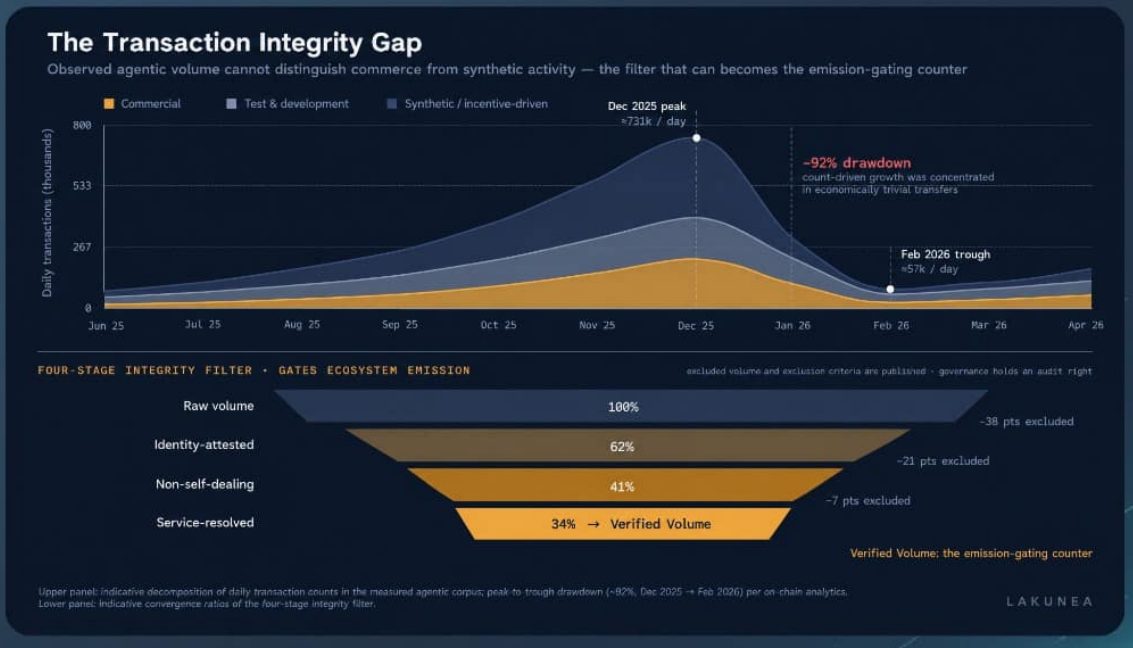
The most widely cited adoption figures for agentic payments do not measure what they appear to measure, and any protocol building on those flows should say so before an investor discovers it independently.

The headline corpus: approximately 165 million transactions by roughly 69,000 active agents, cumulative value near $50 million, as of late April 2026. Those numbers describe genuine infrastructure in use. They also describe something considerably more ambiguous on inspection.

Independent analysis attributes a substantial share of transaction growth to meme-token activity rather than commercial service consumption. Sector commentary through 2026 has estimated that roughly half of measured volume reflects testing and development rather than arm's-length commerce. Daily transaction counts fell approximately 92% from a December 2025 peak to a February 2026 trough. The composition of value transferred shifted materially over the same period, with transactions above one dollar rising from under half of total transferred value to the large majority, which indicates that the earlier count-based growth was concentrated in economically trivial transfers.

Three readings of this data are available. The dismissive reading treats the sector as narrative-driven and premature. The credulous reading cites the cumulative totals and moves on. The third reading, which this protocol adopts, is that a payment network whose volume statistics cannot distinguish commercial settlement from self-dealing has a measurement problem, and that measurement problems in payment systems are solved by identity.

This reframing has a direct consequence for protocol design rather than merely for tone. If commercial volume cannot be distinguished from synthetic volume, then any incentive program keyed to volume is an invitation to manufacture the latter. Lakunea therefore gates ecosystem emission on a filtered counter: transactions must carry an attested identity credential, must not be self-dealing between related identities, and must resolve to a delivered service. Volume that fails these tests is recorded and excluded. The filter is published, the exclusions are published, and governance holds an audit right over the counter.



2.5 The Denomination Problem

Concentration in agentic settlement is extreme. Measured flows have cleared overwhelmingly in a single dollar-denominated stablecoin, on the order of 99.6% of value in sampled datasets. Processors and merchants selected that instrument for defensible reasons: transparent reserve attestation, established banking relationships, and a compliance posture that survives institutional review.

The consequence falls on the supply side of machine commerce outside the dollar core. Consider the economically identical positions of two providers of the same inference endpoint. The first holds a US banking relationship and receives dollar-denominated stable value that is functionally cash. The second operates in a high-growth digital economy whose central bank prohibits virtual assets as payment instruments, whose tax treatment of digital asset receipts differs from ordinary revenue, and whose banking channel for converting stable value to local currency runs through a small number of licensed intermediaries. The second provider's machine revenue is nominally identical and practically encumbered.

That asymmetry is not a minor operational friction. It determines which developers can build a business on machine-metered revenue and which cannot, and it therefore determines where the supply side of the agentic economy is permitted to form. The settlement corridors where the constraint binds most tightly are also, in several cases, the corridors with the largest developer populations and the lowest cost of software production.

Addressing this requires an abstraction the standards do not provide: a routing layer that accepts a transaction expressed in any standard, denominates it in a stable unit of account, executes settlement on the most cost-efficient available rail, and delivers value to the provider through whichever licensed gateway is authorized in that provider's jurisdiction. The protocol does not itself hold local payment authorizations and does not represent that it does. It holds the routing logic, the reconciliation record, and the integration surface that licensed gateway operators connect to.

2.6 The Credit Problem

Every agentic payment flow in production requires funds in place before the transaction. The agent holds a balance, or draws on a linked instrument belonging to its principal, or the transaction fails.

Human commerce does not operate this way, and has not for centuries. Trade credit, settlement netting, and revolving facilities exist because requiring pre-funding for every transaction strands working capital and excludes counterparties whose creditworthiness exceeds their current liquidity. A software agent with eighteen months of clean settlement history, a verified principal, and a zero dispute rate is, by any reasonable underwriting standard, a better credit than an unknown agent holding a funded balance. No network currently prices that distinction.

The spend-governance tooling that has appeared addresses the inverse problem. It constrains agents that already control funds, which is the concern of an institution worried about an agent overspending. The unaddressed case is the agent with standing and no balance: an independent developer's agent that could serve paying customers if it could draw on model and compute capacity before collecting revenue.

Underwriting that case requires persistent identity, behavioral history, loss-absorbing capital, and a default resolution path. The first two are prerequisites for the second two, which is why the credit layer sits above the identity layer in this architecture and cannot be built without it.

3.0 Protocol Overview and Design Principles

3.1 Positioning: Protocol-Agnostic by Architecture

Adapter-based compatibility is easy to claim and difficult to sustain. Most protocols that describe themselves as standard-neutral maintain a privileged path for their own message format and treat external standards as second-class integrations that degrade over time.

Lakunea has no native message format. The protocol's internal representation of a payment obligation is a normalized settlement instruction: a tuple of payer identity reference, payee address, denominated amount, asset and rail selection, validity window, nonce, policy grant reference, and a hash commitment to the originating request. Every supported standard is translated into that representation by an adapter, and the settlement engine operates only on the normalized form.

This has a testable consequence. Adding support for a new standard requires writing an adapter and a conformance test suite; it requires no change to the settlement engine, the credit ledger, the identity registry, or the fee mechanism. A standard that gains adoption becomes routable within a development cycle. A standard that loses adoption is deprecated by removing an adapter, with no residual coupling.

The engine sees no difference between an exact-amount immediate settlement, a variable-price consumption charge resolved after delivery, and a voucher redeemed against escrowed funds. Those are settlement modes, selected per transaction by cost and latency constraints, and the normalization layer flattens them into a common lifecycle.

3.2 Design Principles

Execution accountability must be collateralized. A node that verifies a payment and authorizes service delivery before on-chain finality is extending a short-duration guarantee. That guarantee is worth what the node has at risk. Bonded stake sized against throughput, with slashing for misexecution, is what distinguishes a settlement network from a set of API endpoints that happen to speak the same protocol.

Identity precedes credit, and credit precedes scale. The sequencing is not a product roadmap preference. An unidentified counterparty cannot be underwritten, and an agent economy in which every participant must pre-fund every transaction will remain a fraction of the size of one in which standing substitutes for balance. Each layer is a prerequisite for the layer above, which constrains the order in which the protocol can usefully be built.

The unit of account and the unit of settlement are separable. Providers price in stable value because their costs are denominated in stable value. The protocol settles in LKUN because the fee mechanism, the bonding requirement, and the burn are denominated in LKUN. Collapsing these two functions into one asset forces a choice between an economically inert token and a service provider carrying unwanted price exposure. Keeping them separate, with atomic conversion at the settlement boundary, avoids the choice.

Measured volume is worthless unless it is filtered. Any metric that gates emission, sets fee tiers, or determines reputation must be resistant to manufacture by the party it rewards. The integrity filter described in 2.4 is therefore not a reporting convention layered on top of the protocol; it is the input to the emission contract, and its exclusion criteria are governance-auditable.

Assurance claims must be labeled by modality. Some properties are cryptographically proven. Others are attested by a credential issuer, sampled by monitoring, or enforceable only through contract. A protocol that presents all four as equivalent has misrepresented its own guarantees, and the misrepresentation will be discovered at the worst possible moment by a counterparty relying on the wrong one.

Design Principles and Rejected Anti-Patterns

Each principle is stated with the mechanism that implements it and the sector pattern it explicitly forecloses

PRINCIPLE	IMPLEMENTED MECHANISM	ANTI-PATTERN EXPLICITLY REJECTED
01 **Execution accountability must be collateralized** — A guarantee before finality is worth what the guarantor can lose	**Throughput-scaled bonding** — Node bond sized to trailing peak exposure × coverage ratio; slashing on demonstrable misexecution; residual burned, not redistributed	**Unbonded facilitation** — Verification endpoints with nothing at risk — settlement guarantees worth nothing
02 **Identity precedes credit; credit precedes scale** — An unidentified counterparty cannot be underwritten	**Layered dependency** — Credit envelopes computed at principal level from KYA history; facility activation gated on identity operation and assurance review	**Credit on unverified identity** — Pre-funded-only flows, or lending against a key with no accountable principal
03 **Unit of account and unit of settlement are separable** — Providers price in stable value; the protocol settles in LKUN	**Denomination · execution · atomic egress** — Stable quote → LKUN settlement leg with fee burn → optional conversion back to stable within the same transaction	**Token mandated as medium of exchange** — Forcing providers to hold a volatile balance — the fastest route to integration refusal
04 **Measured volume is worthless unless filtered** — Any metric that rewards a party must resist manufacture by that party	**Four-stage integrity filter as emission input** — Identity-attested → non-self-dealing → service-resolved; exclusions published; governance audit right	**Emission keyed to gross volume** — Incentives that convert synthetic traffic into token distribution
05 **Assurance claims must be labeled by modality** — Proven, attested, monitored, and contractual are not equivalent	**Four-modality labeling** — Every property carries its assurance class; signature validity is never presented as assertion truth	**Undifferentiated "trustless" claims** — Presenting attested or contractual properties as cryptographically guarantted

Mechanism references: bonding §9.2 · credit gating §8.7 · unit-of-account abstraction §8.4 · integrity filter §2.4 and §10.6 · assurance modalities §4.3.

LAKUNEA

4.0 System Architecture

4.1 Layered Architecture

Six layers, with two cross-cutting concerns that intersect all of them.

The **Client and Agent SDK** layer exposes the protocol to agent frameworks and resource servers. For an agent, it wraps delegation retrieval, policy pre-flight checks, payload construction, and credential presentation. For a resource server, it wraps the payment-required response, the verification call, and receipt handling. The SDK is deliberately thin: it constructs and signs, and holds no discretionary logic that a caller cannot reproduce independently.

Standard Adapters translate between external message formats and the normalized settlement instruction. Each adapter is responsible for format parsing, scheme-specific semantics such as variable-price resolution, and conformance assertions against the source specification. Adapter output is validated against a schema before it reaches the engine, and an adapter cannot inject fields the engine does not recognize.

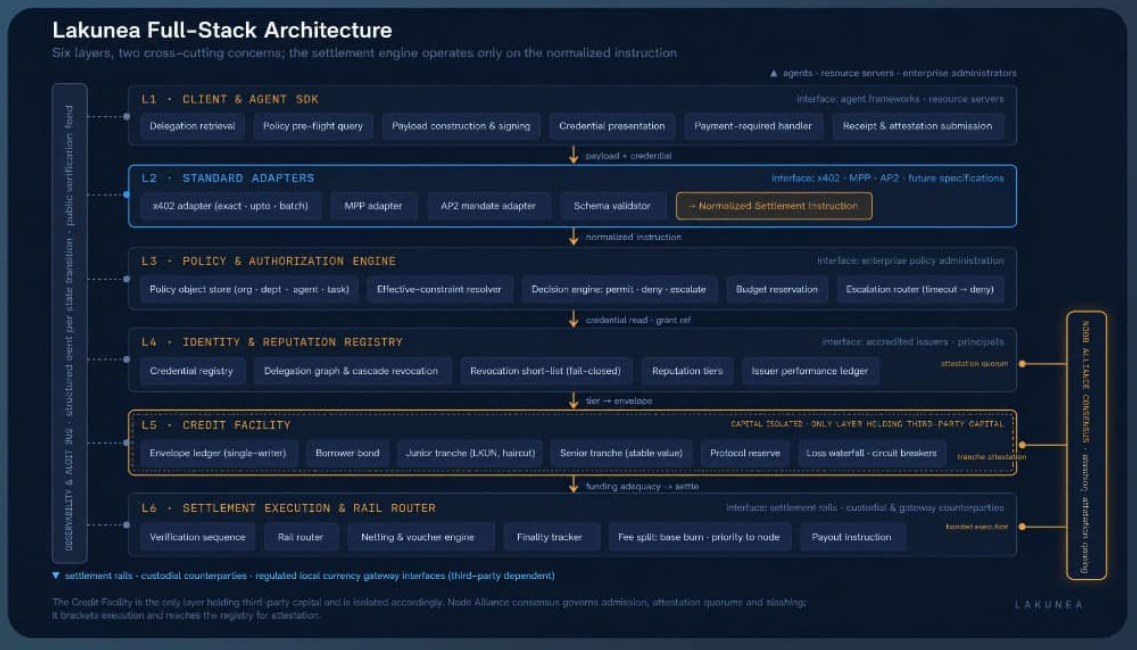
The **Policy and Authorization Engine** holds delegation state and evaluates every instruction against the grant chain that purports to authorize it. Its output is a signed authorization decision — permit, deny, or escalate — carrying a grant reference that becomes part of the settlement record. The engine is queryable before a transaction is attempted, which allows an agent to avoid constructing payloads that will be rejected.

The **Identity and Reputation Registry** maintains credential issuance, delegation graphs, revocation status, and the behavioral history from which reputation tiers are derived. Registry reads are on the critical path of every verification; registry writes occur at credential lifecycle events and at settlement outcome resolution.

The **Credit Facility** holds underwriting capital, computes and enforces credit envelopes, records drawdowns and repayments, and executes the loss waterfall on default. It is the only layer that holds third-party capital, and it is isolated accordingly.

The **Settlement Execution and Rail Router** performs payload verification, selects the settlement mode and rail, submits or batches on-chain operations, tracks finality, applies the fee split, and issues payout instructions. Node operators run this layer.

Cutting across all six: an **Observability and Audit Bus** that emits a structured event for every state transition, forming the reconciliation record and the public verification feed; and the **Node Alliance consensus mechanism** described in 9.0, which governs node admission, attestation quorums, and slashing adjudication.



4.2 The Settlement Execution Path

The lifecycle below describes the immediate-settlement case with a credit-funded payer. Variations for escrow-voucher and netted batch modes are noted where they diverge.

An agent requests a resource. The server responds with payment requirements: scheme identifier, amount or pricing function, accepted assets and rails, recipient address, a nonce, a validity window, and optional facilitator hints.

Before constructing a payload, the agent's client queries the policy engine with the proposed transaction. The engine walks the delegation chain from the agent's credential to the accountable principal, checks the counterparty against scope restrictions, tests the amount against the remaining budget in the applicable envelope, and returns a decision. A deny terminates the attempt locally, without a failed on-chain operation. An escalate suspends the transaction and notifies the human approver bound to that envelope.

On a permit, the client constructs the payment payload: a typed-data structure signed by the agent's key, containing the settlement parameters, the nonce, the expiry, and the grant reference. The KYA credential is presented alongside it, either as a full credential or as a selective disclosure proof exposing only the attributes the verification requires.

The payload travels with the retried request. The resource server forwards it to a settlement node's verification endpoint.

Verification is where the node takes on risk, and it comprises a fixed sequence: signature recovery against the credential's declared key; credential status check against the registry, including revocation and expiry; nonce uniqueness check against the replay registry for that payer; amount and recipient match against the server's stated requirements; policy grant validity and non-exhaustion; and funding adequacy, which for a credit-funded payer means available envelope rather than available balance.

The node returns a verification result. On success, the resource server delivers the service immediately.

Service delivery precedes on-chain finality by design. An agent orchestrating a chain of tool calls cannot wait for block confirmation between steps, and a protocol that forces it to will be routed around. The node therefore guarantees the payment to the resource server at verification time and carries the exposure until settlement confirms. That exposure is why nodes are bonded, and why bond sizing is a function of throughput rather than a flat entry fee. The resource server's claim in a failure case runs against the node's bond, which is the substantive difference between a bonded settlement network and a verification API.

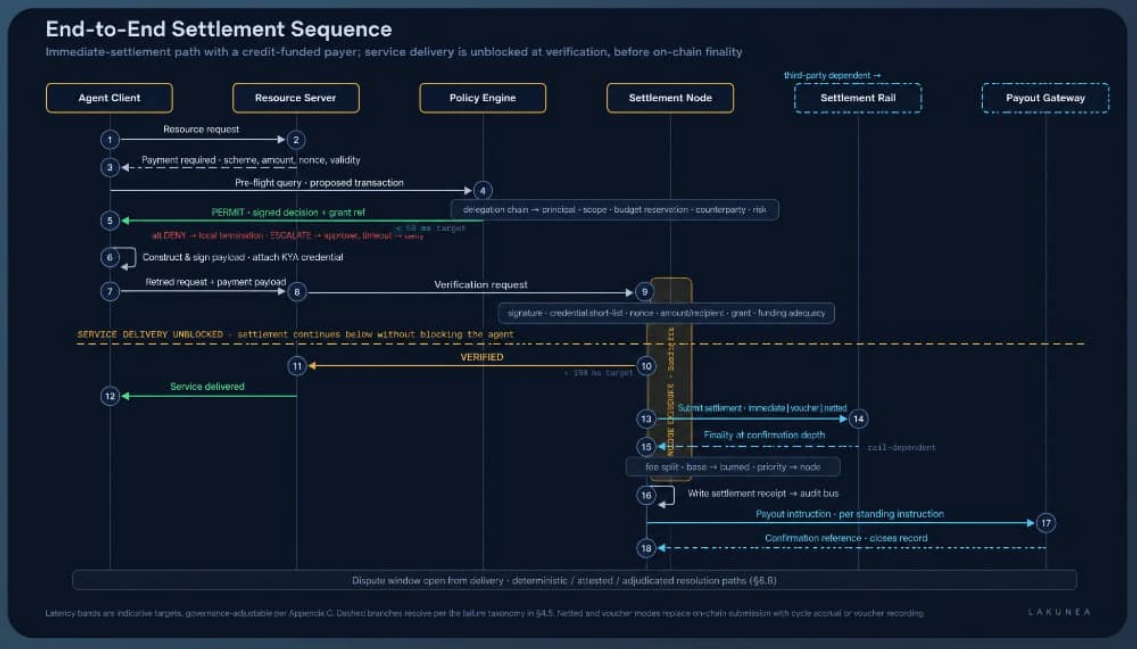
Settlement then executes according to mode. Immediate settlement submits the transaction to the selected rail. Voucher mode records the signed voucher against the payer's escrow position for later batch redemption. Netted mode accrues the obligation to an open netting cycle for that payer-payee pair, with periodic net settlement on-chain — the economically necessary mode for sub-cent transactions, where per-transaction on-chain cost would exceed the principal by orders of magnitude.

The network fee is assessed on settlement. Its base component is burned; its priority component accrues to the executing node.

A settlement receipt is written to the audit bus, linking the request hash, grant reference, credential identifier, verification result, service delivery attestation, fee components, and chain transaction hash. This record is the reconciliation primitive: it allows a principal to answer, for any expenditure, which agent incurred it, under which delegation, for which delivered service, at what cost, cleared by which node.

Payout to the provider resolves through one of three paths, per the provider's standing instruction: atomic conversion to a stable asset within the settlement transaction; credit to a multi-gateway custodial position; or an instruction to a regulated local currency gateway interface, which executes under its own authorizations and returns a confirmation reference that closes the record.

A dispute window opens at delivery and closes after 72 hours (259,200 seconds post-delivery). Within it, either party may raise a claim, which suspends the affected obligation and routes to the resolution process.



4.3 Trust Boundaries and Assurance Modalities

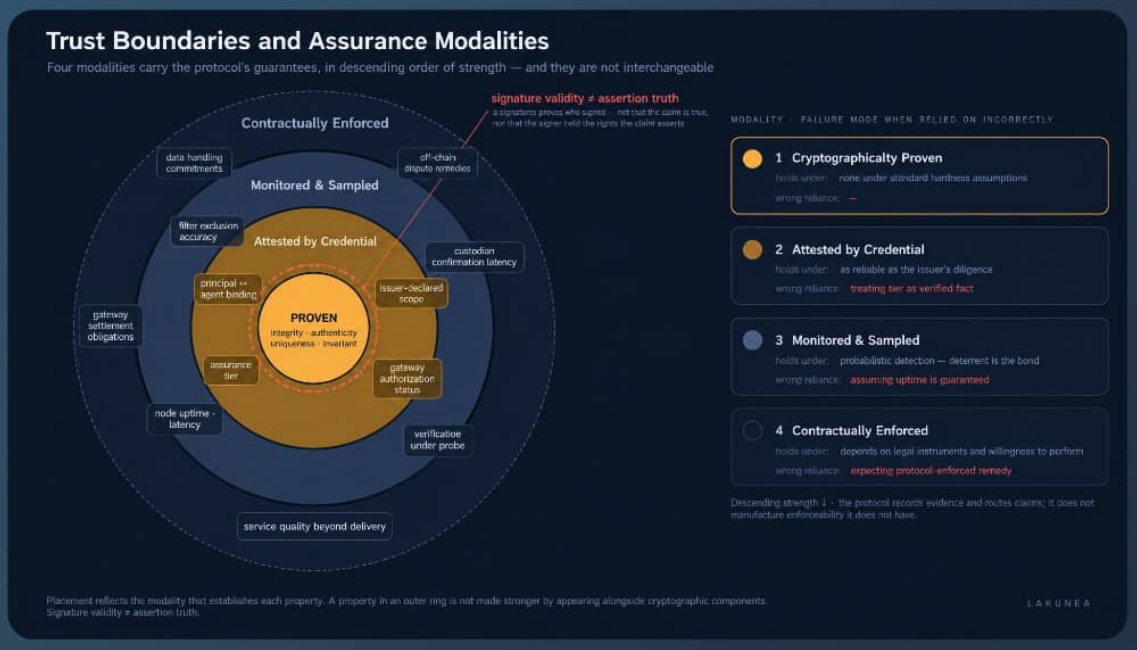
Four modalities carry the protocol's guarantees, in descending order of strength.

Cryptographically proven properties hold under standard hardness assumptions without reference to any party's behavior. Payment payload integrity, signature authenticity, nonce uniqueness within a registry, and the supply invariant across canonical and mirrored representations fall here. So does the non-forgeability of a credential presentation, though not the truth of what the credential asserts.

Attested by credential properties are as reliable as their issuer. That an agent belongs to a particular legal entity, that the entity passed an onboarding check at a given tier, that a gateway operator holds a specified authorization — these are assertions by an identifiable issuer, verifiable as to origin and integrity, and no stronger than the issuer's diligence. A signature establishes that a subject signed a statement. It does not establish that the statement is true, and it does not establish that the signer held the rights the statement claims.

Monitored and sampled properties are established statistically. Node uptime, latency distribution, correct verification behavior under audit probes, and the integrity filter's exclusion accuracy are measured continuously and sampled adversarially. Detection is probabilistic; the deterrent is the bond.

Contractually enforced properties depend on legal instruments and the parties' willingness to perform. Service quality beyond delivery confirmation, gateway settlement obligations, data handling commitments, and dispute outcomes requiring off-chain remedy sit here. The protocol records evidence and routes claims; it does not manufacture enforceability it does not have.



4.4 State, Finality, and Reorganization Handling

Protocol state divides into four classes with distinct consistency requirements.

The canonical supply ledger is authoritative for total and circulating LKUN. Mirrored representations on other chains are subordinate, and the aggregate invariant across all representations is verified continuously by attestation nodes. Bridge attestation state is treated as third-party dependent and disclosed as such.

Registry state — credentials, delegations, revocations, reputation tiers — requires strong consistency on reads that gate verification. Revocation propagation latency is the critical parameter: a credential revoked but not yet reflected in the registry read path is an exploitable window. The registry therefore maintains a revocation short-list with aggressive propagation and treats a stale read as a verification failure rather than a pass.

Credit ledger state — envelopes, drawdowns, repayments, collateral positions, haircut-adjusted capacity — is strongly consistent and single-writer per envelope. Concurrent drawdown attempts against one envelope serialize rather than resolving optimistically.

Settlement state is eventually consistent by construction, because it is ultimately anchored to chains with differing finality characteristics.

Finality handling distinguishes two rail classes. Deterministic-finality rails provide a block height beyond which reversion requires a protocol failure, and settlement is treated as final at that height plus a margin. Probabilistic-finality rails require a confirmation depth policy calibrated per rail to the cost of reversion at the transaction's value, with higher-value settlements held longer.

Reorganization within the confirmation window invalidates a submitted settlement without invalidating the service that was already delivered. The node resubmits, absorbing the additional cost. If resubmission fails because the payer's funding position changed during the reorg, the obligation converts to a claim against the node's bond, and the node's recovery against the payer proceeds through the credit ledger or the dispute process. Losses from reorganization sit with the node, which is the correct placement: the node chose the rail and the confirmation depth.

Voucher double-redemption is prevented by a redemption registry keyed on voucher hash, checked atomically at redemption. Netting cycles are closed by a committed cycle boundary; obligations arriving after the boundary accrue to the next cycle rather than reopening a closed one.

5.0 The Agent Identity Layer

5.1 What a Signature Establishes, and What It Does Not

A verified signature supports one conclusion: the holder of a particular private key signed a particular message, and the message was not altered afterward. NIST's guidance on signature verification separates this from the conditions required to draw any inference about a real-world actor, which include assurance that the public key is validly bound to an identified subject and that the binding remains current.

The machine payments stack routinely elides the distinction. An agent presents a signature, a resource server verifies it, and service is delivered — without establishing which entity is accountable for the agent, what that entity authorized it to do, or whether prior conduct warrants extending access.

Consider a payment payload signed by key 0x7a3f.... Verification tells the resource server that the payload is authentic and unmodified. It does not tell the server whether the key belongs to an agent operated by a well-capitalized enterprise or to one spun up eleven minutes earlier; whether the operator authorized the purchase of this category of service; whether the key was compromised yesterday; or whether the same operator has forty other agents with a combined dispute rate above forty percent. Each of these is material to the delivery decision, and none is answerable from the signature.

The gap is not a defect in the standards. AP2 addresses authorization semantics specifically, and its move to the FIDO Alliance placed it among the authentication specifications it structurally resembles. What the standards leave undefined is the registry: who issues the credential, what diligence backed its issuance, where revocation state lives, and how behavioral history accumulates across counterparties rather than remaining siloed in each resource server's private logs.

5.2 The Principal–Agent Delegation Model

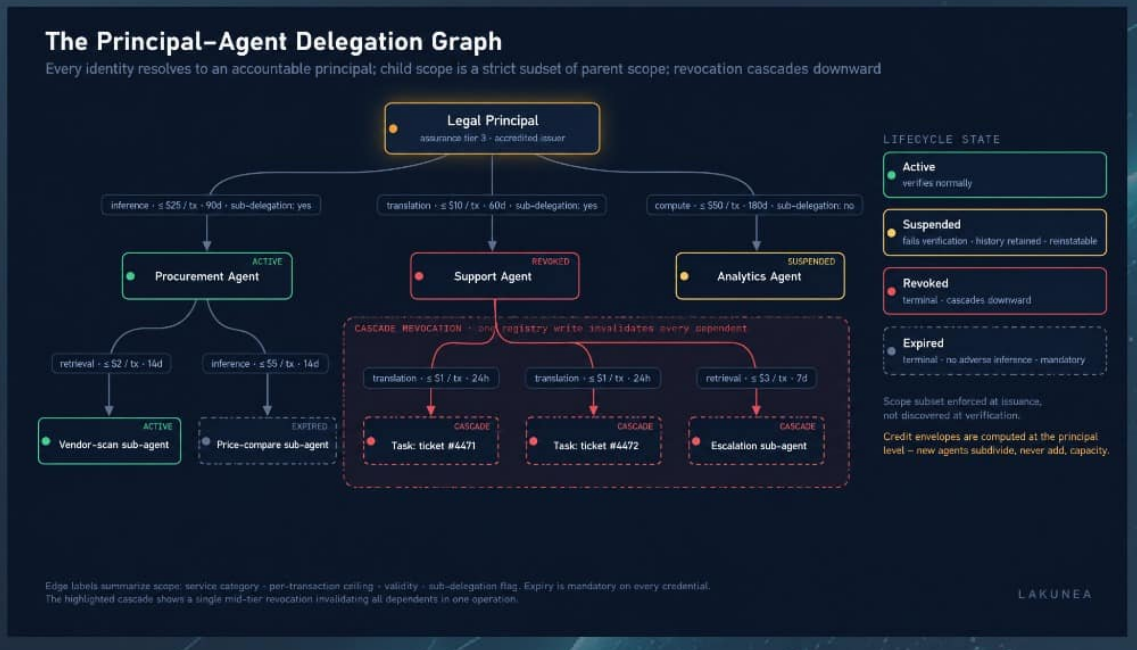
Every identity in the registry resolves to an accountable legal principal. This is the load-bearing constraint of the layer, and the credit facility in 6.0 cannot be built without it.

A principal is an entity capable of bearing obligation: a company, a partnership, a registered sole proprietor, an institution. Principals are onboarded at one of several assurance tiers, differentiated by the diligence performed and the attestations obtained, and the tier bounds everything downstream — the credential types the principal may issue, the credit envelope its agents can reach, and the settlement corridors available to it.

Below the principal sits a delegation graph. The principal issues agent credentials, each carrying a scope: permitted service categories, counterparty constraints, amount ceilings, temporal validity, and whether the agent may itself delegate further. An agent authorized to sub-delegate issues task-scoped credentials to sub-agents, and the scope of a child credential is constrained to a subset of its parent's. A parent cannot grant what it does not hold, and the registry enforces this at issuance rather than discovering the violation at verification.

Revocation propagates downward. Revoking an agent credential invalidates every credential beneath it in the same operation, because the alternative — orphaned sub-agents transacting under a scope whose source has been withdrawn — is the failure mode that makes delegation chains unusable in practice.

Four states govern the lifecycle. Active credentials verify normally. Suspended credentials fail verification but retain history and may be reinstated, which is the state applied during an investigation. Revoked is terminal and cascades. Expired is terminal without adverse inference, and expiry is mandatory: every credential carries a maximum validity (365 days for principal credentials, 90 days for agent credentials, and 7 days for task-scoped allocations), so that an abandoned agent ceases to be a live attack surface through inaction rather than requiring an affirmative revocation that no one remembers to perform.



5.3 Credential Schema, Issuance, and Revocation

Credentials follow the verifiable credential data model, with the protocol's own semantics carried in a claim set rather than in a bespoke format. The choice is deliberate: an existing standard carries existing tooling, and the alternative is maintaining a parser that nobody else has tested.

A credential binds a subject identifier to a public key, names its issuer, declares the assurance tier under which it was issued, enumerates its scope, sets its validity window, and references the parent credential in the delegation chain. It carries no behavioral history — history lives in the registry and is queried separately, so that a credential presentation does not go stale the moment a settlement outcome is recorded.

Issuance follows two paths. Principal onboarding is performed by an accredited issuer against tier-specific diligence requirements, producing a principal credential whose tier is itself an attestation by that issuer. Agent credential issuance is performed by the principal, is permissionless within the principal's tier limits, and is recorded in the registry at issuance so that the delegation graph is complete rather than discoverable only through presentation.

Revocation is where the engineering difficulty concentrates. The registry maintains two structures: a full status record, authoritative but not latency-optimized, and a revocation short-list carrying recent revocations with aggressive propagation to every verification endpoint. Verification reads the short-list on the critical path and the full record asynchronously. A verification endpoint whose short-list is stale beyond a bounded threshold fails closed, refusing to verify rather than verifying against data it cannot vouch for. The tradeoff is explicit: availability is sacrificed to prevent the window between revocation and propagation from becoming an exploitable interval.

Distinguishing an issuer's diligence from the protocol's guarantee matters here. That a principal credential asserts a given assurance tier is an attestation by the issuing party, verifiable as to origin and integrity, and no stronger than that party's underwriting. The protocol publishes issuer performance — credentials issued, subsequent default rates, revocations for cause — so that counterparties can price an issuer's attestation rather than treating all tiers as equivalent regardless of who granted them.

5.4 Behavioral History and Reputation

Reputation is computed from settlement outcomes and expressed as a tier. Tiers, not continuous scores, because a tier is legible to an underwriting rule and a two-decimal score invites false precision about data that does not support it.

Five inputs, weighted:

Settlement history depth — count and aggregate value of verified settlements that resolved without dispute. Value is weighted logarithmically; an agent that settles a million sub-cent transactions cleanly has demonstrated something different from one that settles a hundred at higher value, and the model should not treat volume alone as the dominant signal.

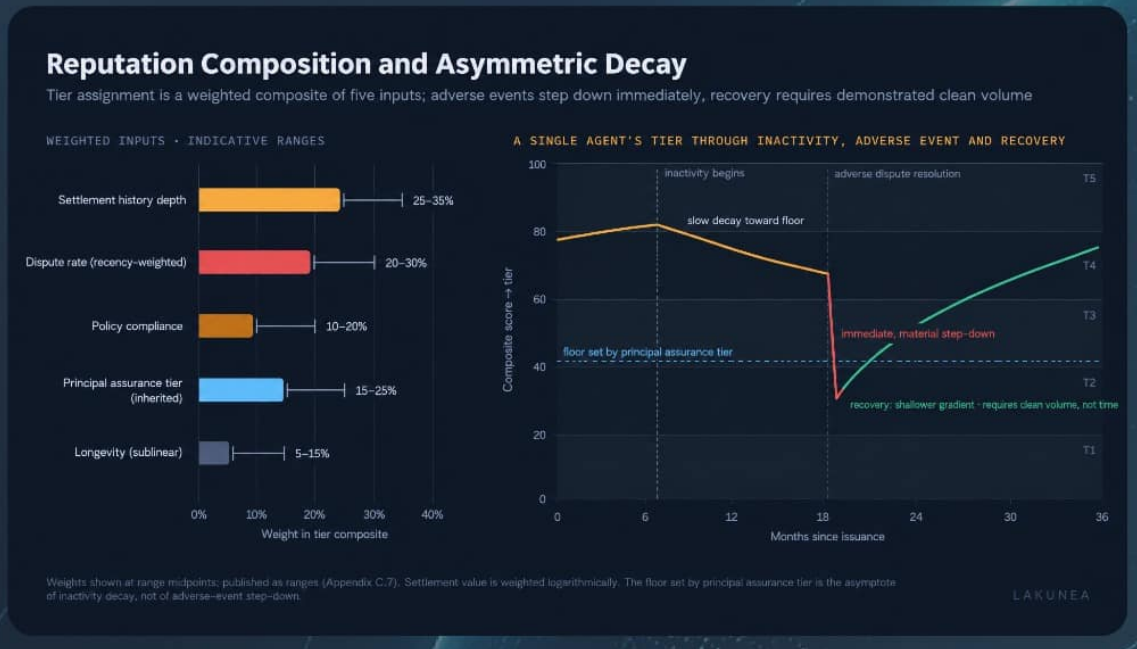
Dispute rate — disputes raised against the agent as a proportion of settlements, net of disputes resolved in the agent's favor. Weighted by recency, since a dispute pattern from fourteen months ago carries less information about present behavior than one from last week.

Policy compliance — the ratio of authorization requests permitted to requests denied or escalated for scope violation. A high denial rate indicates an agent repeatedly attempting transactions outside its mandate, which is a control-quality signal about the principal as much as a behavioral signal about the agent.

Principal assurance tier — inherited, and the reason a newly issued credential from a high-tier principal does not start at zero. An agent's initial standing is a function of who vouches for it; subsequent standing is a function of what it does.

Longevity — time since issuance with continuous activity. Weighted modestly, and specifically not linearly, since age without volume establishes little.

Decay and recovery are asymmetric. Inactivity decays reputation slowly toward the floor set by the principal's tier. A default or an adverse dispute resolution drops the tier immediately and materially, and recovery requires demonstrated clean volume over a trailing 90-day window (minimum 50,000 verified settlements) rather than the passage of time. This asymmetry is priced deliberately: the credit facility's loss exposure is a function of how quickly a deteriorating credit can re-enter a high tier, and a symmetric recovery curve would make the tier meaningless as an underwriting input.



6.0 The Machine Credit Layer

6.1 Credit as the Missing Primitive

Pre-funding every transaction is a constraint that human commerce abandoned centuries ago, for a reason that applies with equal force to software counterparties: requiring capital in place before each purchase strands working capital and excludes buyers whose creditworthiness exceeds their liquidity.

The agentic economy has reproduced the constraint by default rather than by design. Every deployed flow assumes either a funded balance or a linked instrument belonging to the principal. An agent with two years of clean settlement history, a high-tier principal, and no disputes cannot transact if its balance is empty, while an unknown agent with a funded wallet transacts freely. No network currently prices that difference, which means the information encoded in behavioral history is discarded at precisely the moment it would be most useful.

The spend-governance tooling that entered the sector in 2026 addresses the inverse concern. Fireblocks joined the x402 Foundation in May 2026 with extensions covering request integrity and spend governance — capabilities built for institutions worried that an agent with access to funds might overspend. The unmet case runs the other way: an agent with standing and no balance.

The economic consequence is concentrated on the supply side of independent development. A developer whose agent could serve paying customers profitably, but who must fund model and compute consumption before collecting revenue, faces a working capital requirement that scales with usage growth. Growth becomes self-limiting. Credit converts that constraint into a financing cost, which is what credit has always done.

6.2 Underwriting: From Tier to Envelope

An envelope is a revolving limit attached to a principal, drawable by its agents within their individual scope ceilings, repayable from settlement proceeds or funded directly.

Envelope size is a function of four inputs, applied in sequence rather than as a weighted sum.

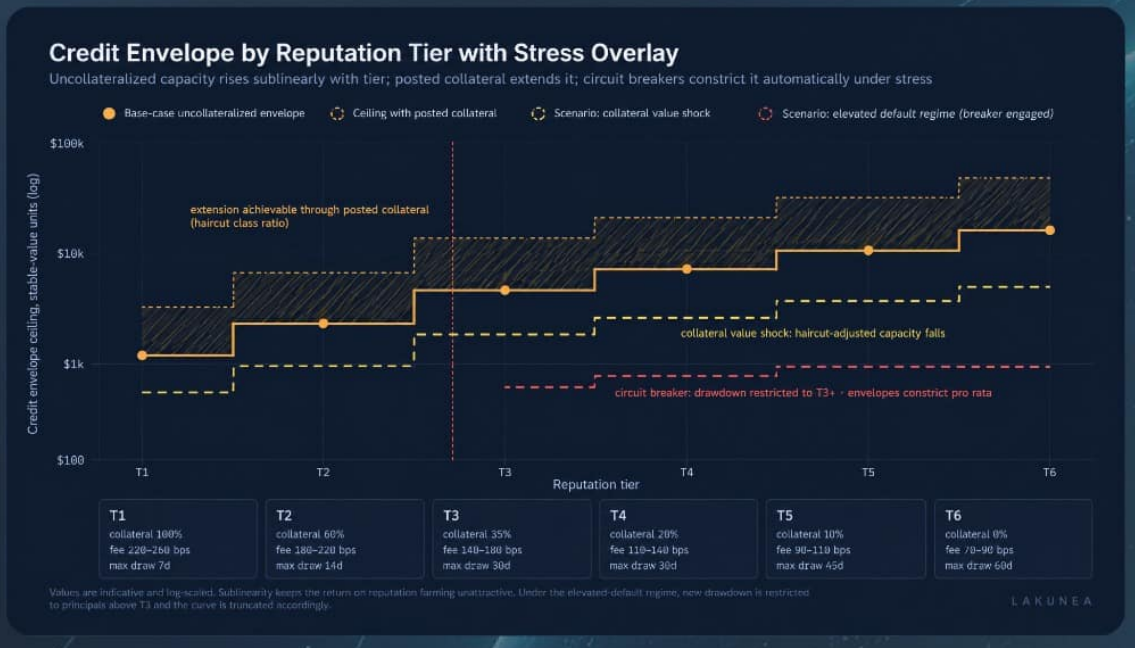
The principal's assurance tier sets an outer bound. No amount of accumulated agent reputation lifts a principal above the ceiling attached to the diligence performed at onboarding, because the diligence is what establishes recourse in a default.

Within that bound, aggregate reputation across the principal's agents determines position on a sublinear curve. The sublinearity is deliberate, as set out: a principal at a high tier receives a larger envelope than one at a low tier, but not proportionally larger, which keeps the return on reputation-farming unattractive.

Realized settlement velocity adjusts the envelope toward observed need. A principal settling consistently against an envelope receives capacity commensurate with that pattern; one holding an unused envelope sees it trimmed, since unused capacity is underwriting capital held against no fee income.

Collateral posted by the principal, if any, extends the envelope beyond the uncollateralized limit at a ratio set by the collateral's haircut class. This is the path by which a new principal with no history obtains meaningful capacity immediately, and the path by which an established principal exceeds what its reputation alone supports.

Utilization is priced. Drawn balances accrue a guarantee fee, denominated in stable value and assessed per period of outstanding exposure, with the rate set by tier. The fee compensates the capital providers who bear loss and the protocol reserve that sits beneath them. It is structured as a fee for a guarantee rather than as interest on a loan, a characterization chosen for its consistency with the underlying economics — the capital providers are bearing the risk of the agent's non-performance, which is a guarantee function — and one that carries a secondary benefit in jurisdictions where interest-bearing structures face additional constraints.



6.3 Capital Structure of the Facility

Capital sits in four positions with strictly ordered loss absorption.

Borrower bond. A principal drawing against an uncollateralized envelope posts a bond sized as a fraction of the envelope. It absorbs first loss on that principal's default, which aligns the drawer with the facility before any third-party capital is touched.

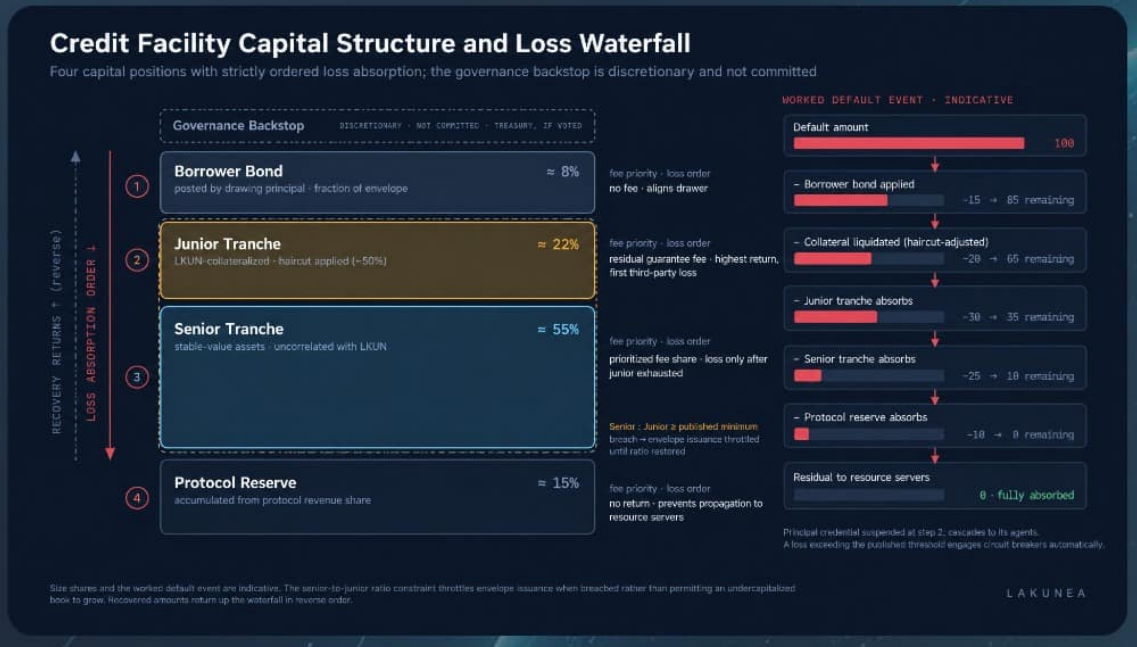
Junior tranche. Underwriting capital posted in LKUN, subject to a published haircut. Junior capital earns the residual guarantee fee after senior claims, and absorbs loss second. Haircut discipline is treated in 6.4.

Senior tranche. Underwriting capital posted in stable-value assets. Senior capital earns a lower, prioritized share of guarantee fees and absorbs loss only after junior capital is exhausted.

Protocol reserve. Capital accumulated from a share of protocol revenue, absorbing loss after both tranches. Its function is to prevent a loss event that exhausts underwriting capital from propagating to resource servers who delivered service in good faith.

Beyond the reserve, governance may authorize a backstop from treasury. This is discretionary, is not a commitment, and is disclosed as such — a facility that represents an unlimited backstop has misrepresented its capital structure.

Tranche sizing is governed by a required ratio of senior to junior capital, which the facility maintains by throttling envelope issuance when the ratio deteriorates rather than by permitting an undercapitalized book to continue growing.



6.4 Collateral Composition, Haircuts, and Correlation

A credit facility collateralized solely by the token of the protocol it serves converts a drawdown into an insolvency. The correlation is the problem: conditions that stress the facility — falling settlement volume, rising defaults, deteriorating sentiment — are precisely the conditions under which the collateral asset declines, so collateral value falls at the moment claims against it rise.

Three mechanisms address this.

Haircuts on LKUN collateral are set with reference to observed volatility and market depth, and are revised on a published schedule rather than at the discretion of whoever is inconvenienced by the revision. An indicative haircut in the range of fifty percent means a unit of LKUN collateral supports half its spot value in envelope capacity. Governance may adjust within a published band; adjustment outside the band requires the higher threshold described in 11.1.

Senior tranche depth maintains a mandatory 3:1 ratio (minimum 75.0% senior stable assets to maximum 25.0% junior LKUN)

Concentration limits cap exposure to any single principal at 5.0% of active facility capacity, and cap aggregate exposure to correlated principals at 15.0% — for instance, multiple principals whose agents consume from the same small set of resource providers. Correlated exposure is the channel through which a shock to one segment of the agentic economy becomes a facility-wide loss event.

6.5 Loss Absorption and Default Resolution

Default is defined as failure to repay a drawn balance by its deadline, following a 48-hour grace period with automated on-chain notice. It is not defined by reputation deterioration, which triggers envelope constriction rather than a default event.

Resolution proceeds in order. The borrower bond is applied. The principal's credential is suspended, halting further drawdown and cascading to its agents. Posted collateral, if any, is liquidated at the haircut-adjusted value, with any recovery above the haircut returned to the principal. The junior tranche absorbs residual loss pro rata. If junior capital is exhausted, the senior tranche absorbs the remainder; the protocol reserve absorbs anything beyond that.

Reputation consequences are recorded against the principal permanently and against its agents with the asymmetric recovery described in 5.4. Recovery of the defaulted amount, where the principal's identity supports legal recourse, proceeds off-chain, and recovered amounts are returned up the waterfall in reverse order.

A rolling 30-day default rate exceeding 3.0% triggers Tier 1 circuit breakers (issuance pause), 5.0% triggers Tier 2 (20% pro-rata envelope constriction), and composite losses exceeding 8.0% trigger Tier 3 full facility shutdown automatically, without requiring a governance vote — the interval a vote would consume is the interval during which a correlated loss event propagates.

7.0 The Policy and Authorization Layer

7.1 Delegated Spending as a Protocol Object

An enterprise deploying forty agents across a dozen teams has a control problem before it has a payments problem. Which agent may purchase which category of service, up to what amount, from which providers, within what period, and who answers for it when the monthly reconciliation shows eleven thousand dollars of inference spend against a project nobody authorized.

Existing answers live outside the settlement path. Spend limits are configured in a vendor dashboard, budget approval happens in a procurement system, and reconciliation occurs after the fact when someone exports a CSV. The settlement layer executes whatever arrives and learns nothing about whether it should have.

Lakunea treats the authorization grant as a protocol object that travels with the transaction. Every settlement instruction carries a reference to the grant that authorized it, the grant is evaluated before the payload is constructed, and the grant reference is written into the settlement receipt. The reconciliation question becomes a lookup rather than a reconstruction.

The practical consequence for an enterprise is that budget enforcement moves from detection to prevention. An agent attempting a transaction outside its envelope receives a denial at pre-flight, and no payload is signed, no verification is attempted, and no on-chain operation occurs. The control is not a report generated after the money moved.

7.2 The Policy Object Model

Four object types, nested, with inheritance flowing downward and constraints intersecting rather than overriding.

An **organization envelope** is the outermost bound, attached to a principal. It sets aggregate ceilings across all periods, permitted service categories, prohibited counterparties, and the settlement corridors available to the organization. Nothing beneath it can exceed it.

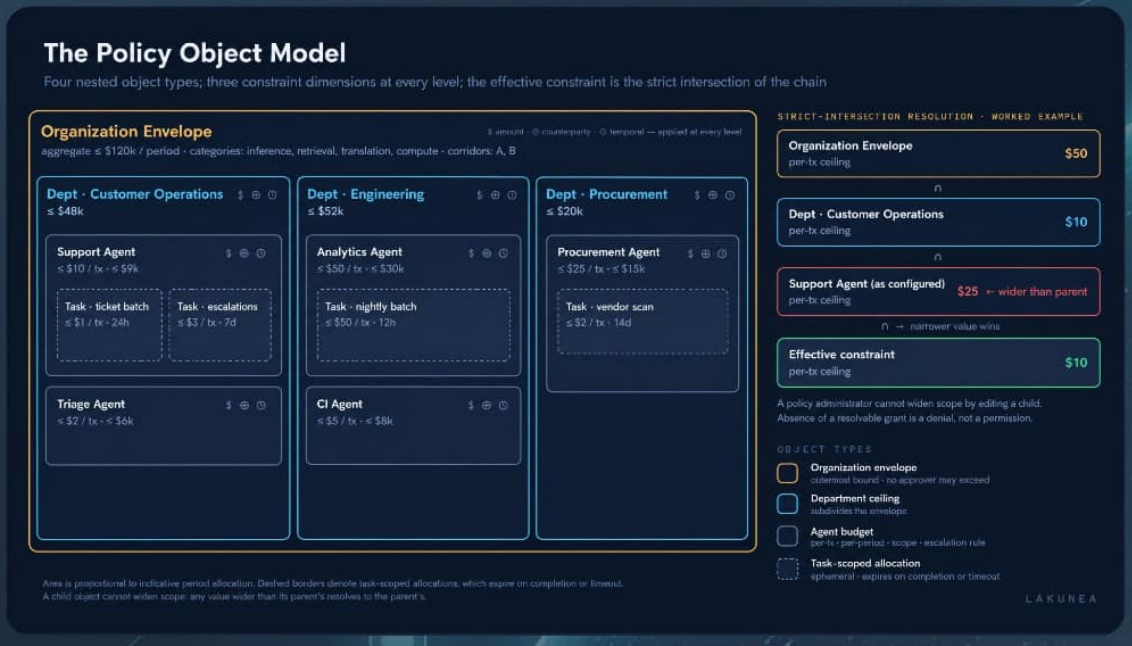
Department ceilings subdivide the organization envelope. They exist because the reporting structure that owns a budget is rarely the structure that owns an agent, and forcing a one-to-one mapping between agents and budget lines produces either sprawling envelope counts or meaningless aggregation.

Agent budgets attach to a specific agent credential. They carry per-transaction ceilings, period ceilings, counterparty scope, and the escalation rule that applies when a request exceeds them.

Task-scoped allocations are ephemeral, issued for a defined workload and expiring on completion or timeout. An agent orchestrating a research task receives an allocation sized to the task, and the allocation vanishes afterward rather than remaining as standing capacity.

Three constraint dimensions apply at every level: amount, expressed as per-transaction and per-period ceilings; counterparty, expressed as allow-lists, deny-lists, or category permissions; and temporal, expressed as validity windows and rate limits.

Inheritance is strict intersection. A department ceiling permitting a category the organization envelope prohibits grants nothing. An agent budget with a per-transaction ceiling above its department's ceiling is bounded by the department's. The engine computes the effective constraint as the intersection of every level in the chain, which means a policy administrator cannot accidentally widen scope by editing a child object — a property that matters more in practice than it sounds, since most policy misconfigurations in conventional systems arise from an override at a lower level that nobody audits.



7.3 The Authorization Decision Engine

Evaluation is a fixed sequence of predicates, ordered so that the cheapest and most decisive checks execute first.

Identity validation resolves the presented credential, confirms active status against the revocation short-list, and walks the delegation chain to the accountable principal. A failure here terminates immediately; every subsequent check presumes a valid, unrevoked credential.

Policy resolution locates the applicable objects in the nesting chain and computes the effective constraint set. A transaction with no resolvable grant is denied, which makes the absence of a policy a denial rather than a permission.

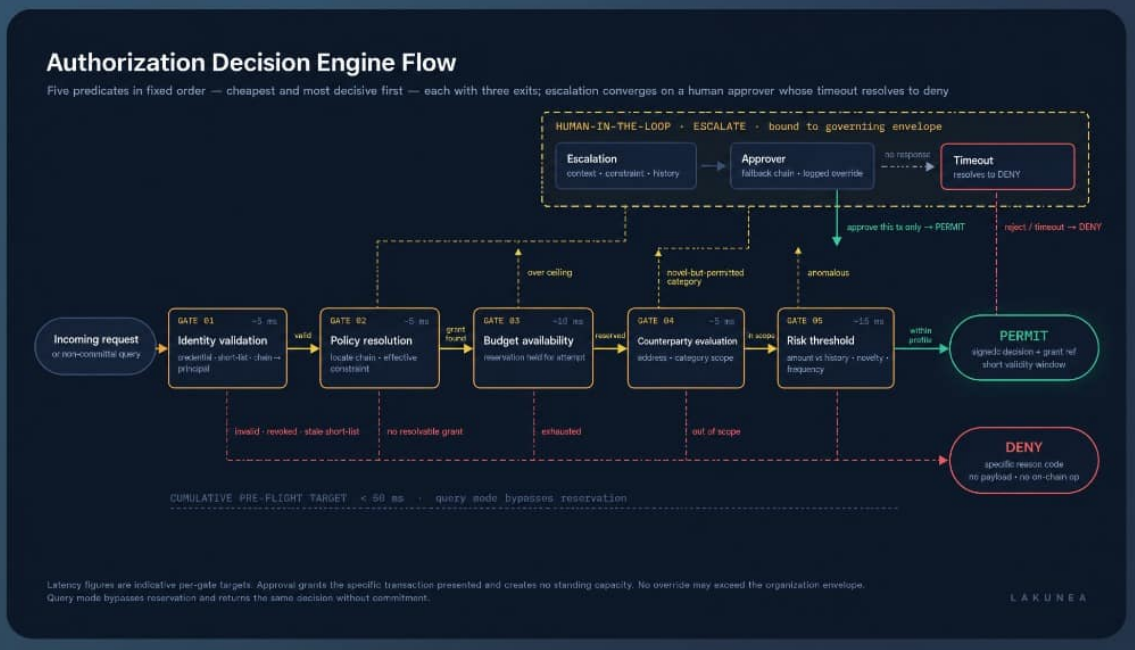
Budget availability tests the requested amount against remaining capacity in every applicable ceiling, and does so with a reservation rather than a read. The requested amount is held against the budget for the duration of the transaction attempt and released on failure. Without reservation, an agent issuing concurrent requests could overdraw a budget by racing the interval between the availability read and the settlement write.

Counterparty evaluation tests the payee against scope, at both the specific-address and category level.

Risk threshold evaluation compares the transaction's profile against the agent's tier: an unusual amount relative to history, an unfamiliar counterparty, an anomalous frequency pattern. This check produces escalation more often than denial, since a novel-but-legitimate transaction should route to a human rather than fail.

Three outcomes. Permit returns a signed authorization decision carrying the grant reference, valid for a 120-second (or 10-block) window to prevent an authorization from being banked and used later. Deny returns a reason code specific enough for the calling agent to adapt, which is a deliberate choice — an opaque denial produces retry loops that consume capacity and teach the agent nothing. Escalate suspends the transaction and notifies the approver bound to the governing envelope.

The engine is queryable without commitment, so an agent planning a multi-step workload can determine in advance which steps are authorized and adjust its plan rather than discovering the constraint mid-execution.



7.4 Reconciliation, Attribution, and the Audit Trail

The settlement receipt described in 4.2 is the reconciliation primitive, and the policy layer contributes the attribution chain that makes it useful.

For any expenditure, the record answers: which agent transacted, under which credential, within which delegation chain from which principal, against which policy object, for which service delivered by which counterparty, at what fee, cleared by which node, settled on which rail, at which finality, with which payout resolution. Where escalation occurred, it names the approver and the justification.

This is what an enterprise finance function requires to treat machine expenditure as a cost category rather than an anomaly. It is also what an auditor requires, and the two requirements have converged as agentic spend has grown from rounding error to line item.

Attribution is queryable along three axes: by agent, producing that agent's complete expenditure history; by policy object, producing consumption against a specific budget; and by counterparty, producing total spend with a given provider across all agents and departments — the view that supports vendor negotiation and that is essentially unobtainable when each agent holds its own credentials and its own payment relationship.

Export interfaces target accounting system formats rather than proposing a new one. An organization's machine expenditure should land in the general ledger through the same path as its other payables.

8.0 The Settlement and Interoperability Layer

8.1 Multi-Rail Settlement Topology

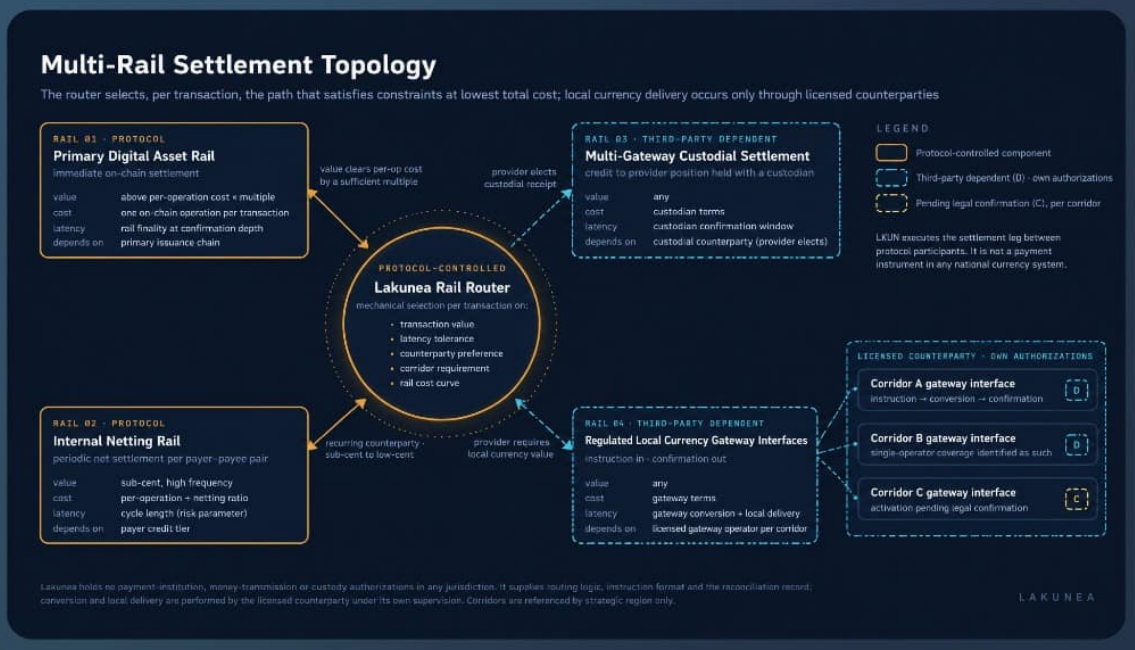
The rail router selects, per transaction, the path that satisfies the transaction's constraints at the lowest total cost. Four rail classes are addressable, and the selection among them is mechanical rather than discretionary.

The **primary digital asset rail** carries immediate on-chain settlement where the transaction's value justifies the per-operation cost and where the counterparties accept on-chain receipt as final.

The **netting rail** accrues obligations between a recurring payer-payee pair and settles the net position periodically on-chain. Its economics are examined; it is the only viable path for sub-cent settlement.

Multi-gateway custodial settlement credits value to a provider's position held with a custodial counterparty, from which the provider draws on its own schedule. This suits providers who prefer a custodial relationship to direct on-chain receipt, and providers whose own compliance posture requires a regulated intermediary in the path.

Regulated local currency gateway interfaces deliver value into a local currency corridor through a licensed gateway operator. The protocol holds the routing logic, the instruction format, the reconciliation record, and the integration surface. The gateway operator holds the authorizations, performs the conversion, and bears the regulatory obligations attaching to it. Lakunea does not hold payment institution authorizations in any jurisdiction, does not custody end-user funds, and does not represent that its token discharges obligations denominated in any national currency. Availability of any specific corridor depends on a licensed counterparty being authorized and operationally integrated, which is disclosed as Third-Party Dependent.



8.2 Chain-Agnostic Canonical Supply Model

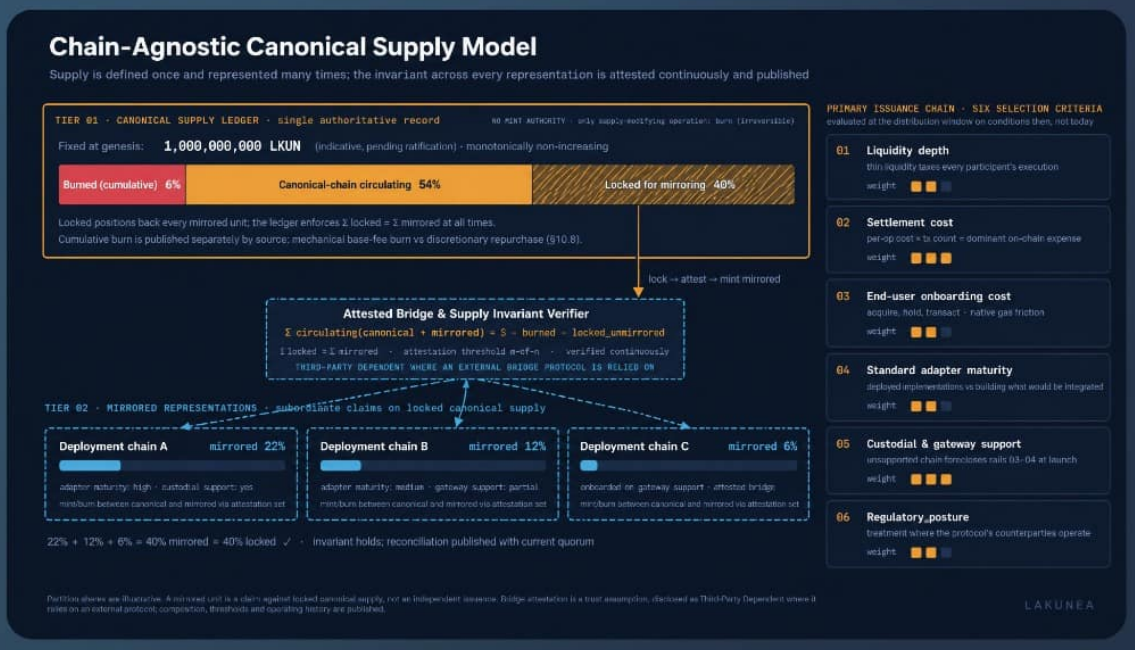
LKUN supply is defined once and represented many times.

A **canonical supply ledger** is the single authoritative record of total supply, burned supply, and the allocation of unburned supply across chain representations. It is deployed as a contract on a chain selected for finality characteristics and operational cost, and it holds no mint authority — total supply is fixed at genesis, and the ledger's only supply-reducing operation is burn.

Mirrored representations exist on additional chains, each backed by a locked position on the canonical ledger. A mirrored unit is not an independent issuance; it is a claim against canonical supply, and the ledger enforces that the sum of locked positions equals the sum of mirrored representations at all times.

The **supply invariant** is the property that aggregate circulating supply across the canonical ledger and every mirrored representation equals canonical supply minus burned supply minus locked-but-unmirrored positions. Attestation nodes verify this continuously and publish the reconciliation, because a supply invariant that is true but unverifiable is indistinguishable from one that is false.

Bridge attestation is the model's principal dependency and is labeled accordingly. The attestation set that authorizes mint-and-burn operations between the canonical ledger and mirrored representations is a trust assumption, disclosed as Third-Party Dependent where it relies on an external bridge protocol, and its composition, thresholds, and operational history are published. The protocol does not claim that cross-chain representation carries the same assurance as canonical-chain holdings.



8.3 Primary Issuance Chain Selection

The chain on which LKUN first issues is selected at the distribution window against six published criteria, evaluated on conditions at that time rather than on conditions today.

Liquidity depth — the depth of venues and pools available on that chain for the asset pairs LKUN will trade against, since a token issued into thin liquidity imposes execution cost on every participant regardless of protocol quality.

Settlement cost — the per-operation cost of the settlement, fee-assessment, and burn operations that occur on every transaction. This criterion weighs heavily, because settlement cost multiplied by transaction count is the protocol's dominant on-chain expense.

End-user onboarding cost — the friction and cost for a node operator, underwriter, or agent principal to acquire, hold, and transact the asset, including the cost of acquiring the chain's native gas asset.

Standard adapter maturity — the availability and operational maturity of the prevailing machine payment standards on that chain, since a chain with no deployed standard implementations requires the protocol to build what it would otherwise integrate.

Custodial and gateway support — whether the custodial counterparties and gateway operators the protocol needs already support that chain, since an unsupported chain forecloses the multi-gateway and local corridor rails at launch.

Regulatory posture — the treatment of the chain and its ecosystem in jurisdictions where the protocol's counterparties operate.

The criteria are published in advance and the selection is disclosed with the reasoning applied. Flexibility is retained deliberately: conditions across these six dimensions have shifted materially within single quarters through 2025 and 2026, and committing to a chain before the distribution window would substitute a stale judgment for a current one. Mirrored representations follow on additional chains as gateway support and adapter maturity develop.

8.4 Unit-of-Account Abstraction

Three stages separate what a service costs from what moves on-chain.

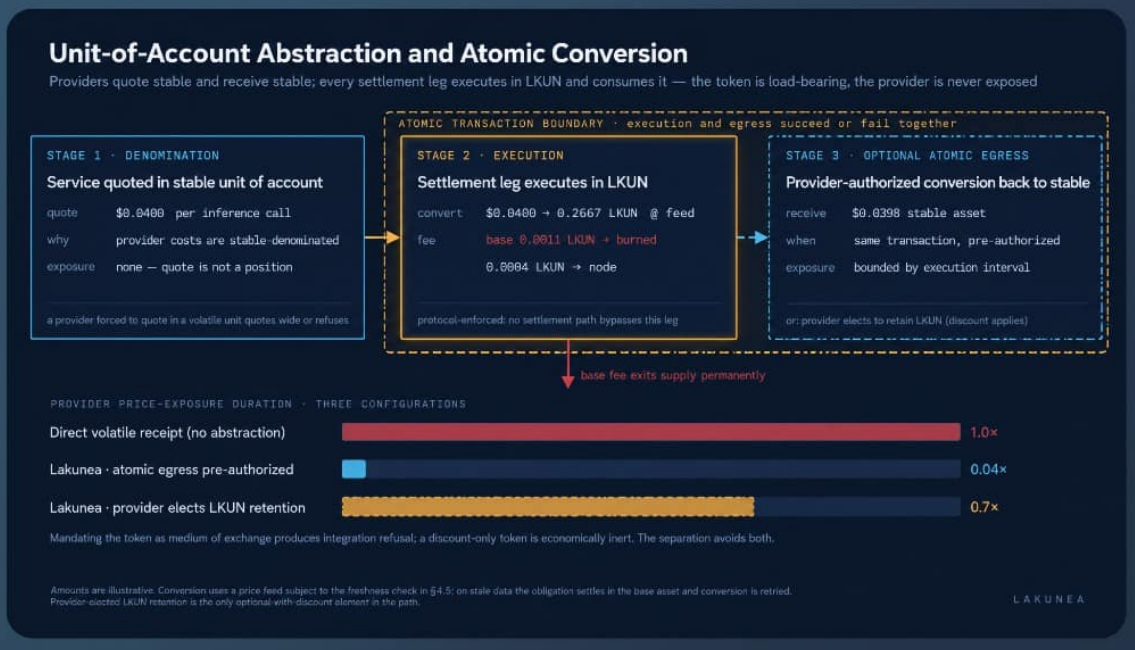
Denomination. Services are priced in a stable unit of account. A provider charging for inference sets a price in stable terms because its costs are in stable terms, and a provider forced to quote in a volatile unit will either quote wide or refuse to quote.

Execution. The settlement leg executes in LKUN. The obligation is converted at the prevailing rate from a price feed subject to the freshness check described, the network fee is assessed in LKUN, its base component burns, and its priority component accrues to the executing node. Every settled transaction therefore consumes LKUN irrespective of what the counterparties denominate in, which is the mechanism by which the token is load-bearing rather than optional.

Optional atomic egress. A provider may pre-authorize conversion back to a stable asset within the same atomic transaction. Where authorized, the provider's exposure to LKUN price movement is bounded by the execution interval rather than by its holding period.

The result is that a provider quotes stable, receives stable, and never holds a volatile balance, while the protocol's fee mechanism, burn, and bonding all denominate in LKUN. A design that mandated providers hold the token would produce integration refusal; a design in which the token merely offered a discount would produce an economically inert asset. The separation avoids both outcomes without requiring either party to accept a position it does not want.

Where a provider declines atomic egress and elects to hold LKUN, the discount structure in 10.2 applies, and the election is the provider's.



8.5 Regulated Local Currency Gateway Interfaces

A provider whose operating currency is not the unit in which machine revenue clears faces the conversion problem described in 2.5. The protocol's response is an interface specification and a routing capability, not a payment service.

The interface defines what the protocol supplies to a gateway operator — a settlement instruction with payee reference, amount, source asset, target currency, and the reconciliation identifier — and what the gateway returns: acceptance or rejection, a conversion reference, and a settlement confirmation. Everything between those two boundaries is the gateway operator's function, performed under its own authorizations, subject to its own compliance obligations, and priced on its own terms.

The division of responsibility is stated precisely because the distinction is where the protocol's regulatory position rests. Lakunea routes and records. It does not convert, does not hold local currency, does not custody provider funds, and does not intermediate a payment into any national currency system. Where a jurisdiction restricts the use of digital assets as payment instruments, the protocol's position is that its token is not used as one: the token executes a settlement leg between protocol participants, and delivery of local currency value to a provider occurs through a licensed entity performing a conversion it is authorized to perform.

Corridor availability is a function of licensed counterparties existing, being willing, and completing integration. The protocol does not assert that any specific corridor will be available, and corridor status is published individually with its maturity state. Corridors are referenced throughout this document at the level of strategic region rather than by jurisdiction, and the protocol makes no representation about regulatory treatment in any specific market, which remains a question for local counsel and for the licensed counterparty operating in it.

9.0 The Decentralized Node Alliance and Network Economics

9.1 Structure and Mandate

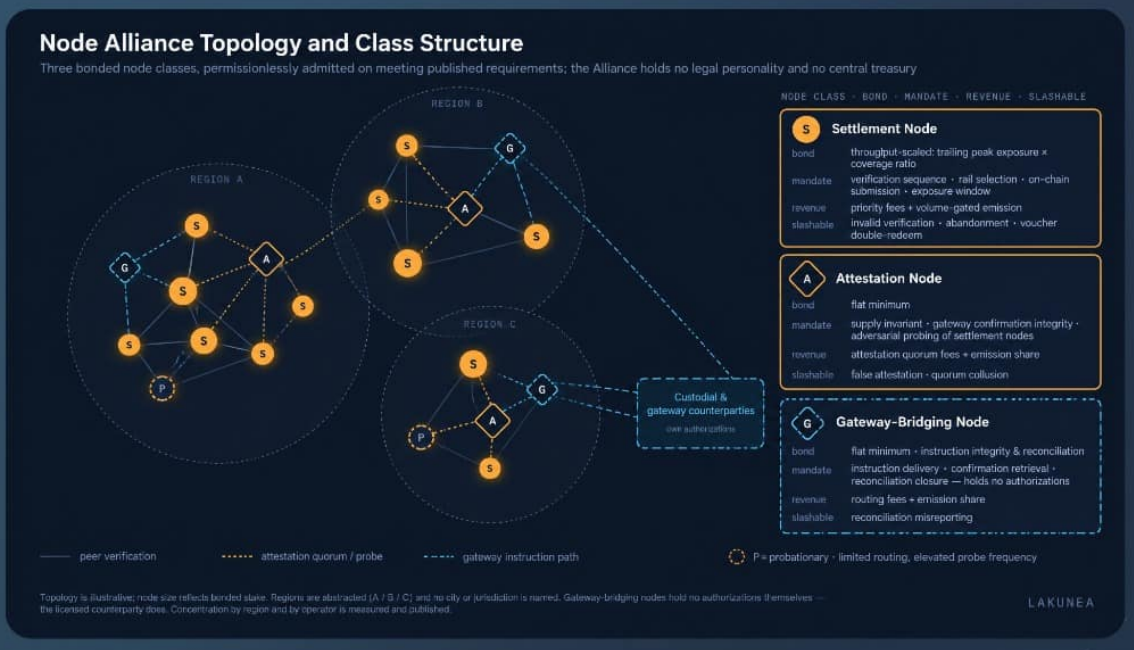
The Decentralized Node Alliance is the set of bonded operators that perform settlement execution, attestation, and gateway bridging for the protocol. It holds no legal personality, no central treasury, and no admission authority vested in any single party. Membership is a state in the protocol's registry, entered by meeting published requirements and exited by withdrawal or by slashing.

The Alliance's mandate is narrow and mechanical: execute verification and settlement correctly, attest to state the protocol cannot prove cryptographically, and adjudicate disputes that reach the panel path. It does not set fees, allocate treasury, or amend protocol parameters — those are governance functions under 11.0, and separating them from execution prevents the operators who earn fees from setting them.

Two properties make the Alliance structurally different from a set of service providers running compatible software.

Operators carry priced exposure. The verification-before-finality design in 4.2 means a node guarantees payment to a resource server before on-chain settlement confirms, and the resource server's claim in a failure case runs against the node's bond. Bond sizing scales with throughput because exposure scales with throughput, which makes bonding a reserve against settlement risk rather than an entry fee.

Correct execution is adversarially verified. Attestation nodes probe settlement nodes with transactions whose correct handling is known in advance, and misbehavior detected through probing is slashable on the same terms as misbehavior detected through a counterparty claim. Detection is probabilistic; the deterrent is the bond.



9.2 Node Classes, Admission, and Bonding

Settlement nodes perform the verification sequence in 4.2, select rails, submit or batch on-chain operations, and bear the exposure window. Their bond is sized against a rolling measure of exposure: peak concurrent unsettled obligations over a trailing window, multiplied by a coverage ratio set by governance. A node approaching its bond-implied capacity ceiling either bonds more or is routed less traffic, and the router enforces the ceiling rather than relying on the operator to observe it.

Attestation nodes verify properties the protocol cannot prove from chain state alone: the supply invariant across canonical and mirrored representations, gateway confirmation integrity, and settlement node behavior under probe. They participate in quorums with a threshold set per attestation type. Their bond is flat rather than throughput-scaled, since their exposure arises from attesting falsely rather than from carrying obligations.

Gateway-bridging nodes operate the technical interface to custodial counterparties and corridor gateways. They hold no authorizations themselves — the licensed counterparty holds those — and their function is instruction delivery, confirmation retrieval, and reconciliation closure. Their bond covers instruction integrity and reconciliation accuracy. This class carries the protocol's highest third-party dependency and is disclosed accordingly.

Admission requires bonded stake at or above the class minimum (250,000 LKUN for settlement nodes, 100,000 LKUN for attestation nodes, and 500,000 LKUN for gateway-bridging nodes), a registered operator identity at a specified assurance tier, technical conformance against a published test suite, and a 14-day probationary period (requiring 50,000 probe transactions with 100% zero-fault verification) during which the node receives limited routing and is probed at elevated frequency. Probation exists because a node's reliability is unobservable before it has executed, and routing full traffic to an unproven operator transfers that uncertainty to counterparties.

Admission is permissionless in the sense that meeting the requirements is sufficient and no party may refuse a conforming operator. It is not costless, and the distinction is deliberate: an unbonded permissionless network of settlement guarantors would be a network of guarantees worth nothing.

9.3 Node Lifecycle

Six states. Probationary — admitted, bonded, receiving limited routing at elevated probe frequency. Active — full routing eligibility, weighted by performance. Constrained — bond insufficient for current throughput or performance below threshold, routing reduced pending remedy. Suspended — excluded from routing pending investigation of a claim or probe failure, bond locked, existing obligations transferred to standby capacity. Withdrawing — voluntary exit, no new routing, bond locked until all outstanding obligations settle and the dispute window on the last of them closes. Slashed — terminal for the bonded position, with the operator identity permitted to re-enter only at probationary status and an elevated bond requirement.

The withdrawal lock is the parameter operators care about most. Bond cannot be released while obligations remain unsettled or disputable, which means exit takes exactly 21 days (504 hours) to clear trailing dispute and settlement windows. An exit path that released bond immediately would let an operator abandon exposure it had already taken on, and the resource servers holding that exposure would have no recourse.

9.4 Node Unit Economics

A settlement node's revenue has two components and its costs have three, and the economics must clear without reference to token appreciation.

Revenue: **priority fees** from settled transactions, accruing per transaction cleared; and **milestone-gated emission** from the ecosystem tranche, allocated across nodes in proportion to verified settlement volume executed.

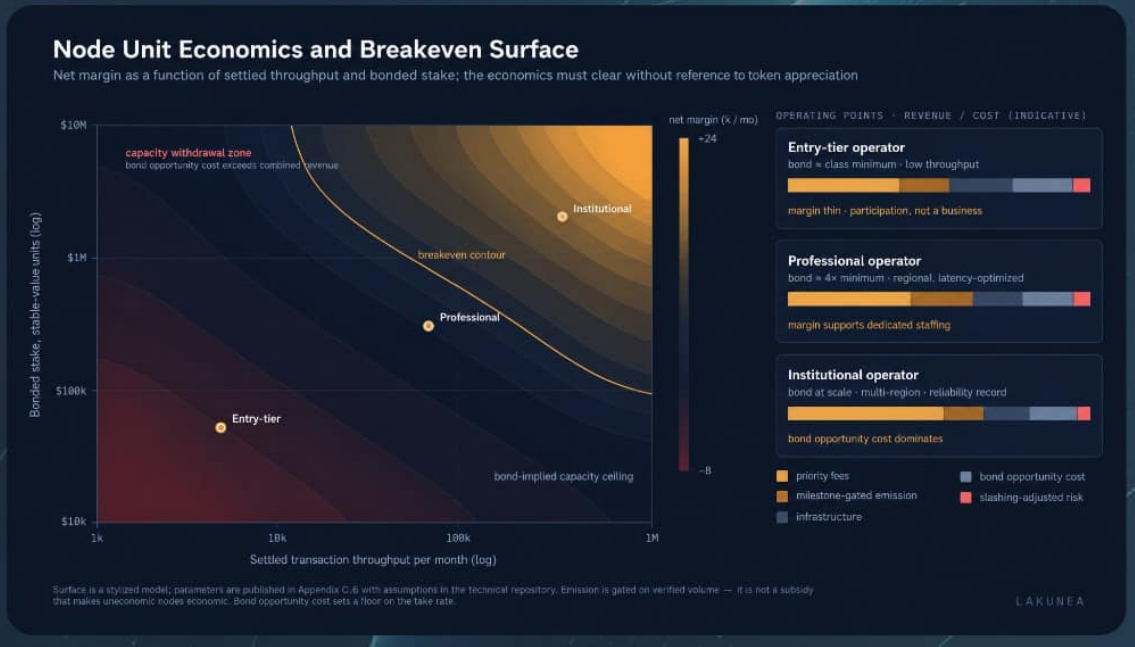
Costs: **infrastructure** — compute, bandwidth, registry read capacity, monitoring, and the operational staffing a production settlement service requires; **bond opportunity cost** — the return foregone on capital locked as bond, which is the dominant cost for a well-run node at moderate throughput; and **slashing-adjusted risk** — expected loss from execution failure, reorganization exposure absorbed, and probe failure, priced as a running charge rather than as a tail event.

Three operator profiles illustrate the curve. An entry-tier operator bonds near the class minimum, clears low volume, and covers infrastructure and bond cost with thin margin — viable as a participation position, not as a standalone business. A professional operator bonds a multiple of the minimum, invests in regional placement and latency optimization to capture routing preference, and operates at a margin sufficient to justify dedicated staffing. An institutional operator bonds at scale, runs multiple regional nodes, and competes primarily on reliability record, which is the input the router weights most heavily.

Two properties of the model are worth stating plainly because they constrain the protocol's growth path.

Emission is not a subsidy that makes uneconomic nodes economic. It is gated on verified volume under 10.6, which means an operator cannot earn emission without clearing real transactions for real counterparties. A node that cannot cover its costs from priority fees plus volume-proportional emission is a node the network does not need at current throughput.

Bond opportunity cost sets a floor on the take rate. Priority fees must, in aggregate, compensate locked capital at a rate competitive with its alternatives, or bonded capacity withdraws and the network's settlement capacity contracts. This places a hard lower bound on how far fee competition can compress the network's pricing, and it is the reason the protocol does not present a race to zero fees as an achievable outcome.



9.5 Slashing

Slashing applies to demonstrable execution failure, not to performance shortfalls. Poor latency, low uptime, or declining reliability produce reduced routing through the constrained state; they do not confiscate bond.

Condition	Detection	Penalty basis
Verification of an invalid payload	Counterparty claim or probe	120% of the obligation verified (100% counterparty restitution, 20% burned)
Settlement abandonment mid-execution	Attestation quorum timeout	5,000 LKUN flat fee plus 15% of abandoned obligation value
False attestation	Quorum disagreement with subsequent proof	25% of bonded stake (25,000 LKUN), escalating to 100% on repetition
Double-redemption of a voucher	Redemption registry conflict	Full obligation value plus penalty
Reconciliation misreporting	Audit against gateway confirmation	Proportional to misreported value
Collusion between settlement and attestation nodes	Cross-correlation analysis and probe	Full bond of all colluding parties

Adjudication follows the dispute process, with the panel drawn from nodes excluded from the transaction at issue. Slashed amounts are applied first to making the harmed counterparty whole, with the remainder burned. Burning the residual rather than distributing it to other nodes removes the incentive for operators to manufacture claims against competitors.

Appeal lies to governance at the elevated threshold in 11.1. The appeal is on the record and does not suspend the penalty, since a suspended penalty pending appeal is an invitation to appeal reflexively.

9.6 Geographic Distribution and Resilience

Verification latency is dominated by the registry read path, and registry read latency is dominated by distance. Regional node placement is therefore a competitive variable rather than a resilience nicety: a node positioned near a concentration of agent activity captures routing preference on latency-sensitive traffic that a distant node cannot serve within the target band.

The protocol's resilience requirement is that no single region's failure removes settlement capacity for transactions originating elsewhere, which requires both distributed node placement and distributed registry read replication. Concentration is measured and published — share of settled volume by region, share of bonded stake by region, and the largest single-operator share of each. Where concentration exceeds a published threshold, governance may adjust routing weights to favor under-represented capacity, at a cost in latency that is disclosed rather than hidden.

Corridor coverage introduces a second distribution problem. A gateway-bridging node serving a corridor is the protocol's only path into that corridor, and a single operator per corridor is a single point of failure for every provider routing through it. The target is redundant gateway-bridging capacity per active corridor; current coverage by corridor is published with its maturity state, and corridors operating with single-operator coverage are identified as such.

9.7 Cold Start

A settlement network has the standard two-sided bootstrapping problem with an additional constraint: node capacity must exist before the first transaction, since a transaction arriving at a network with no bonded nodes simply fails.

Sequencing addresses this in four stages, each gated on the previous rather than on elapsed time.

Capacity precedes demand. A minimum viable node set is bonded and conformance-tested before the network accepts external traffic, with initial capacity contributed by operators whose participation is secured through the network bootstrap allocation in 10.5 rather than through fee expectations that cannot yet be met.

Demand is seeded on the supply side of machine commerce, not the demand side. Resource providers — API operators, dataset licensors, inference hosts — integrate first, because a provider with payment-required endpoints and no paying agents loses nothing, while an agent with no accepting providers gains nothing. Provider integration is the cheaper side to subsidize and the side that creates the reason for agents to arrive.

Corridor capability is activated per corridor as licensed counterparties integrate, and each activation makes provider integration attractive to a population of providers for whom settlement was previously encumbered. This is the protocol's primary provider-acquisition channel: providers whose machine revenue was difficult to realize in usable form have a reason to integrate that providers in the dollar core do not.

Credit activates last. It requires the identity layer operating with accumulated history, a capitalized senior tranche, and completion of the assurance review, and extending credit before those conditions hold would underwrite counterparties whose behavior has not been observed using capital that has not been stress-tested.

Emission across all four stages is gated on verified volume, which means the bootstrap does not distribute tokens against projected activity. An operator, provider, or integrator earns from the tranche by clearing or generating settlement that survives the integrity filter.

10.0 LKUN Token Economics

10.1 The Token Necessity Test

A network that could function without a token and issues one anyway has created an unnecessary risk for its participants and an unnecessary question for its regulators. The test applied here is whether removing LKUN would break a mechanism the protocol requires.

Three mechanisms break.

Settlement guarantees require slashable collateral. A node guarantees payment to a resource server before finality, and that guarantee is worth what the node can lose. Bonding in an external asset is conceivable but places the network's security budget outside its own control and outside governance's ability to adjust coverage ratios as exposure patterns change. The bond must be an asset the protocol can slash, price, and require in proportion to throughput.

Fee-to-burn coupling requires a protocol-native fee unit. A fee assessed in an external asset can be distributed but cannot be burned in a way that accrues to network participants, and the mechanism connecting settlement volume to supply reduction disappears.

Credit underwriting requires a junior capital instrument whose holders are aligned with network performance. Junior capital exists to be wiped out before senior capital, and the parties willing to take that position are those with exposure to the network's success. An external asset in the junior position attracts capital indifferent to protocol outcomes.

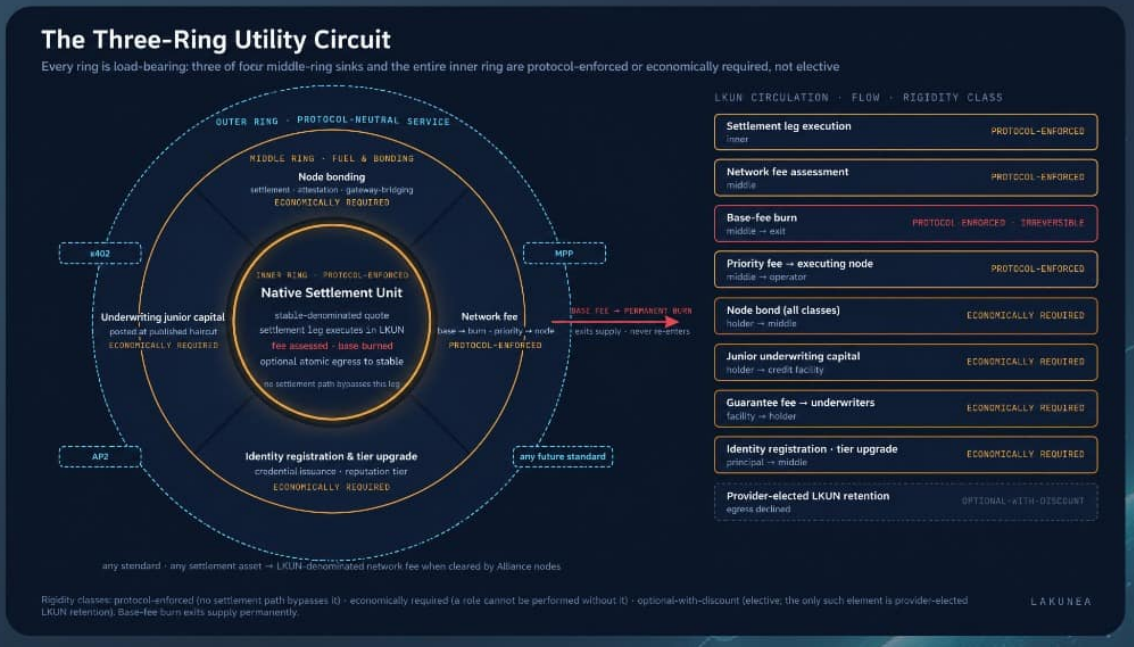
What LKUN is not required for: paying for services, which is denominated in stable value; discharging obligations in any national currency, which occurs through licensed counterparties; or accessing the network, which is permissionless for agents and providers alike. The token is load-bearing in the protocol's security and incentive mechanisms and deliberately absent from the payment experience.

10.2 Utility Architecture: The Three-Ring Model

Inner ring — native settlement unit. Every settled transaction executes its on-chain leg in LKUN. Services denominate in stable value, conversion occurs at the settlement boundary, and providers may elect atomic egress. The consumption is protocol-enforced: there is no settlement path that bypasses it.

Middle ring — fuel and bonding. Network fees are assessed in LKUN on every settlement. Settlement, attestation, and gateway-bridging nodes bond in LKUN. Junior underwriting capital is posted in LKUN at published haircuts. Credential registration and reputation-tier upgrades consume LKUN. Each of these is economically required rather than optional: a node cannot operate unbonded, an underwriter cannot hold a junior position in another asset, and a settlement cannot occur without a fee.

Outer ring — protocol-neutral service. Transactions expressed in any supported standard, settling in any supported asset, generate LKUN-denominated network fees when cleared by Alliance nodes. Adoption of any machine payment standard increases the volume routable to the network, and the fee accrues irrespective of what the counterparties transact in.



The rigidity classification matters for assessing the model. Discount-driven utility is elective and collapses when the discount is outweighed by holding cost. Protocol-enforced and economically-required utility persists as long as the network processes transactions. Three of the four middle-ring sinks and the entire inner ring fall in the latter categories.

10.3 Supply Policy

Canonical supply is fixed at genesis at 1,000,000,000 LKUN. The canonical ledger holds no mint authority. Its only supply-modifying operation is burn, which is irreversible.

All distribution — ecosystem incentives, node emission, bootstrap allocation — draws from tranches carved out of genesis supply. No allocation is funded by issuance, which means total supply is monotonically non-increasing from genesis and the only direction supply can move is down.

The design choice forecloses a common failure pattern. A protocol with mint authority faces recurring governance pressure to fund initiatives through issuance, and the pressure intensifies precisely when treasury is depleted and the token price is weak. Removing the authority removes the option.

10.4 Fee Mechanics

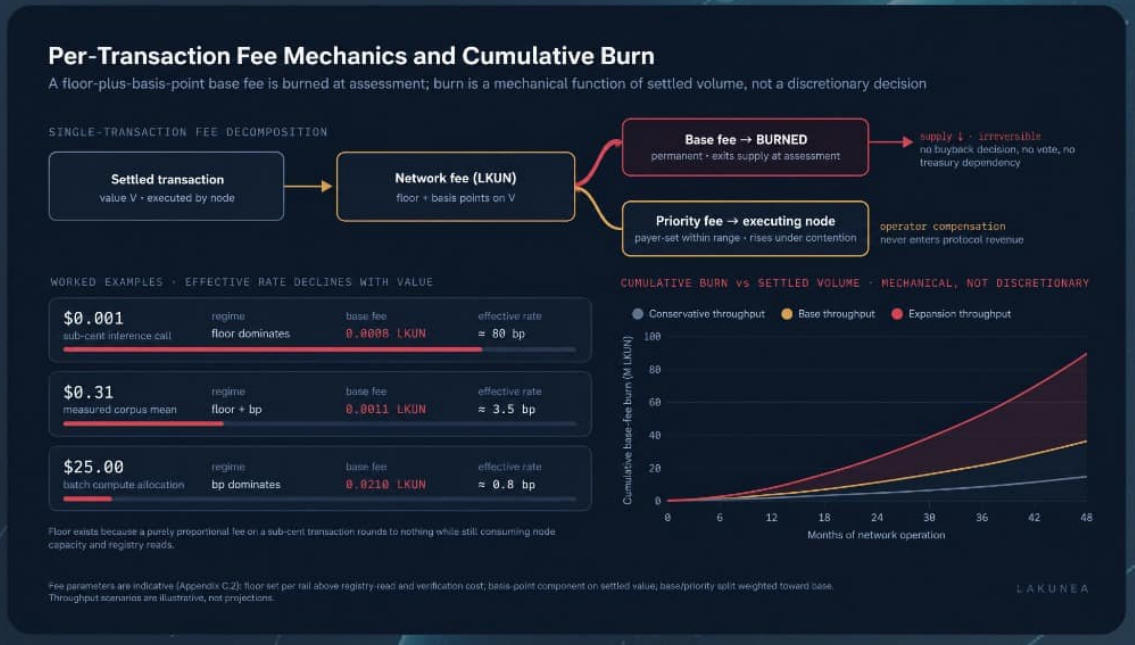
Each settled transaction carries a network fee with two components.

The base fee is burned permanently. It is calculated as a base floor of 0.0005 LKUN plus a 2.5 basis-point (0.025%) charge on settled value, with the floor dominating for sub-cent transactions and the basis-point component dominating above a threshold. The floor exists because a purely proportional fee on a sub-cent transaction rounds to nothing while still consuming node capacity and registry reads.

The priority fee accrues to the executing node. It is set by the payer within a published range, and higher priority fees receive preferential routing during capacity contention. Under normal conditions the priority fee sits near the range floor; it rises when capacity is constrained, which is the mechanism by which the network prices scarcity to operators rather than rationing it arbitrarily.

The split between base and priority is governance-adjustable within a published band.

Burn is therefore a direct function of settled transaction count and value, verifiable per transaction and cumulatively. It does not depend on a discretionary buyback decision, on treasury sufficiency, or on a governance vote. A network processing transactions burns supply; a network processing none burns none, and the accounting is transparent in both cases.



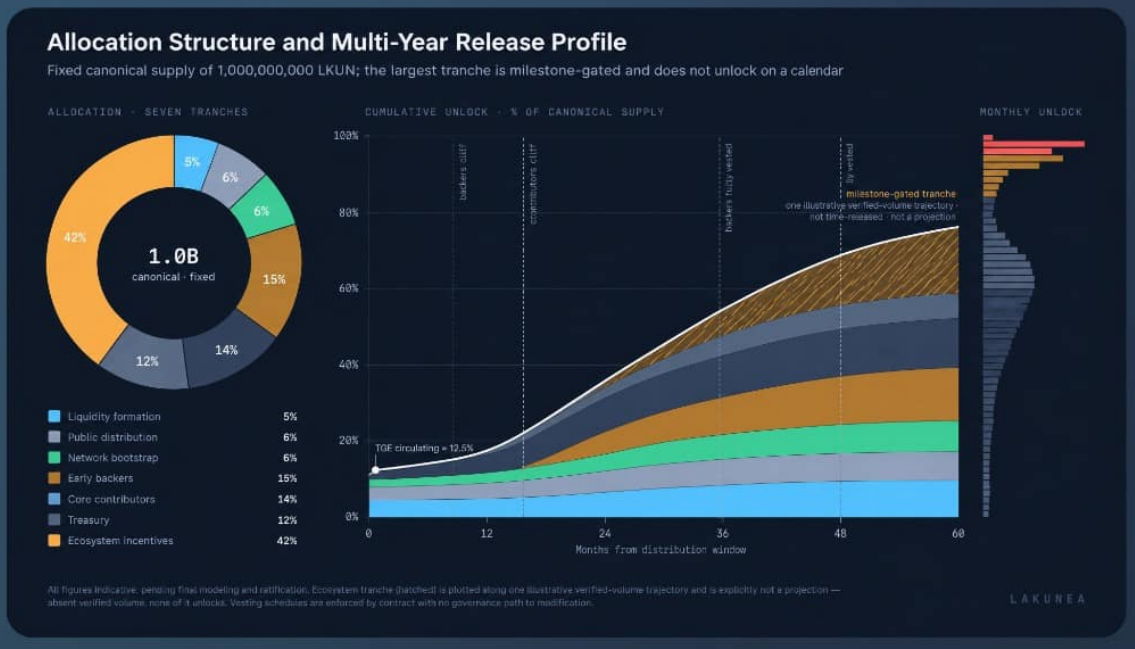
10.5 Allocation Structure

Tranche	Share	Purpose	Release basis
Ecosystem incentives	42%	Node emission, provider integration, developer incentives	Milestone-gated on verified volume
Early backers	15%	Capital formation	Cliff then linear
Core contributors	14%	Contributor compensation	Extended cliff then linear
Treasury	12%	Governance-directed ecosystem funding, reserve accumulation	Governance proposal, annual cap
Network bootstrap	6%	Initial node capacity, corridor activation, founding provider integration	Participation-earned
Public distribution	6%	Multi-tier capital formation	Partial at distribution, remainder linear
Liquidity formation	5%	Venue and pool liquidity	Available at distribution, positions lock-verified

Two features distinguish this structure from the sector norm.

The ecosystem tranche is the largest and is entirely milestone-gated. It does not vest on a schedule, and unverified volume produces no emission from it regardless of how much time passes. A protocol whose largest tranche unlocks on a calendar has committed to sell pressure independent of whether the network works.

The network bootstrap tranche is earned through participation rather than allocated to identified recipients in advance. Operators who bond initial capacity, providers who integrate before the network has paying volume, and gateway counterparties who complete corridor integration draw from it against defined contributions. Allocating it to named parties before the contributions exist would convert a bootstrap incentive into a pre-distribution.



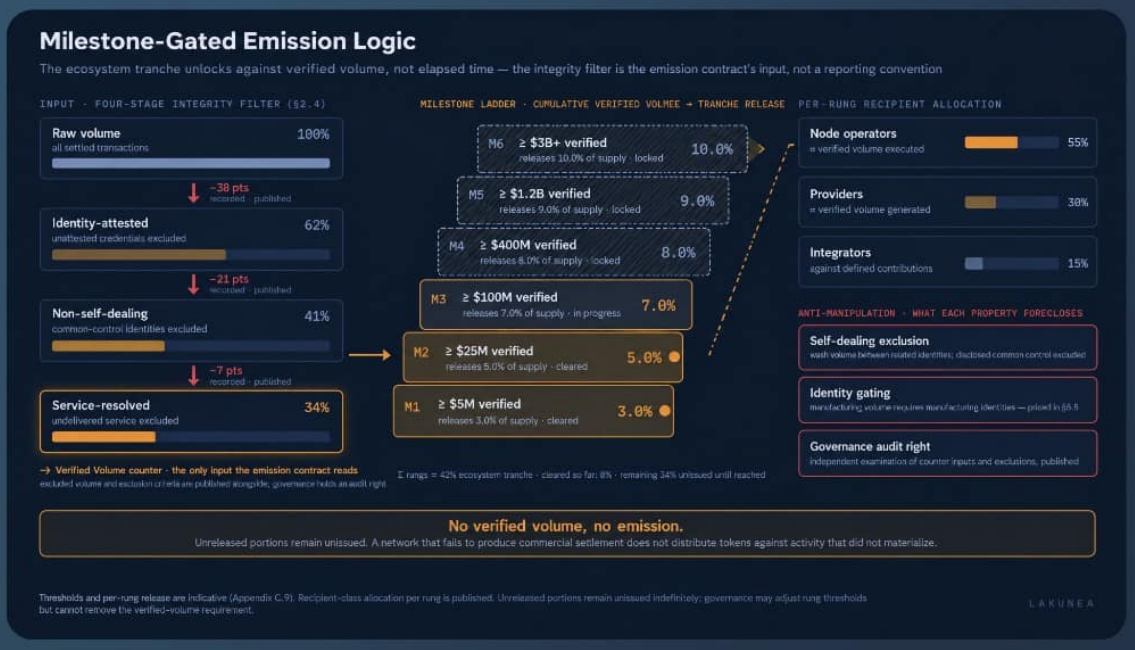
10.6 Release Schedule and Milestone-Gated Emission

Scheduled tranches follow published cliffs and linear vesting: core contributors carry the longest cliff, with no release in the initial period following distribution; early backers carry a shorter cliff with linear release thereafter; public distribution releases partially at the distribution window with the remainder linear; liquidity is available immediately with positions lock-verified on-chain; treasury releases only against governance proposals subject to an annual cap expressed as a proportion of remaining treasury balance.

The ecosystem tranche follows a different rule entirely. Its unlock is a function of the verified volume counter defined in 2.4 — transactions carrying an attested identity credential, not self-dealing between related identities, resolving to a delivered service. Volume failing any of these tests is recorded, excluded, and published alongside the exclusion criteria applied.

Ecosystem emission unlocks across four cumulative verified volume rungs: Milestone 1 ($50M unlocks 10% / 42M LKUN); Milestone 2 ($250M unlocks 20% / 84M LKUN); Milestone 3 ($1B unlocks 30% / 126M LKUN); Milestone 4 ($5B unlocks remaining 40% / 168M LKUN). Release is allocated across recipient classes in published proportions: node operators in proportion to verified volume executed, providers in proportion to verified volume generated, and integrators against defined contributions. Absent verified volume, no portion of the tranche unlocks, and the tokens remain unissued indefinitely.

Three anti-manipulation properties are built into the counter. Self-dealing exclusion removes transactions between identities resolving to the same principal or to principals with disclosed common control. Identity gating means volume from unattested credentials does not count, which makes manufacturing volume require manufacturing identities. Governance audit right permits independent examination of the counter's inputs and exclusions, with the examination published.



10.7 Protocol Revenue and Allocation

Protocol revenue is defined narrowly: the base fee component of network fees, plus the protocol's share of guarantee fees from the credit facility, plus corridor routing fees where applicable. It excludes priority fees, which are node compensation and never enter protocol control. It excludes gross settled value, which belongs to the transacting parties. A protocol reporting settled value as revenue has reported a number that is not its own.

Allocation follows a strictly enforced three-way split: **35% Burn / 35% Node and Underwriter Distribution / 30% Treasury and Reserve**:

Burn — the base fee component is burned at assessment, as described in 10.4. This portion is mechanical and requires no allocation decision.

Node and underwriter distribution — guarantee fee shares to senior and junior tranche providers, and supplemental node distribution from corridor routing fees.

Treasury and reserve — accumulation to the protocol reserve that sits beneath the credit facility's capital structure, and to treasury for governance-directed use.

The split is governance-adjustable within published bands. Adjustment beyond those bands requires the elevated threshold in 11.1.

10.8 Capital Formation Architecture

Distribution follows a dynamic multi-tier structure, retaining strategic flexibility across channel composition rather than committing to a single venue or method in advance.

Available components include public liquidity bootstrapping mechanisms, ecosystem contribution rounds through which participants who have generated verified activity access allocation on defined terms, and compliant institutional channels for qualified participants under applicable exemptions. The composition, sequencing, and relative weight of these components is determined at the distribution window against market conditions, venue availability, and the jurisdictional analysis current at that time.

Two constraints hold regardless of composition. Distribution to participants in any jurisdiction occurs only through channels that satisfy that jurisdiction's requirements as advised by local counsel, and retail access in jurisdictions with a licensing regime for digital asset trading occurs through licensed intermediaries under that regime rather than through direct protocol sale. The protocol's issuing entity does not offer or sell to persons in jurisdictions where doing so would require authorizations it does not hold.

Participant verification applies across all channels, with scope and depth calibrated to channel and jurisdiction.

11.0 Governance, Treasury, and Progressive Decentralization

11.1 Governance Scope

Two categories of protocol property exist, and the boundary between them is fixed at deployment rather than determined by vote.

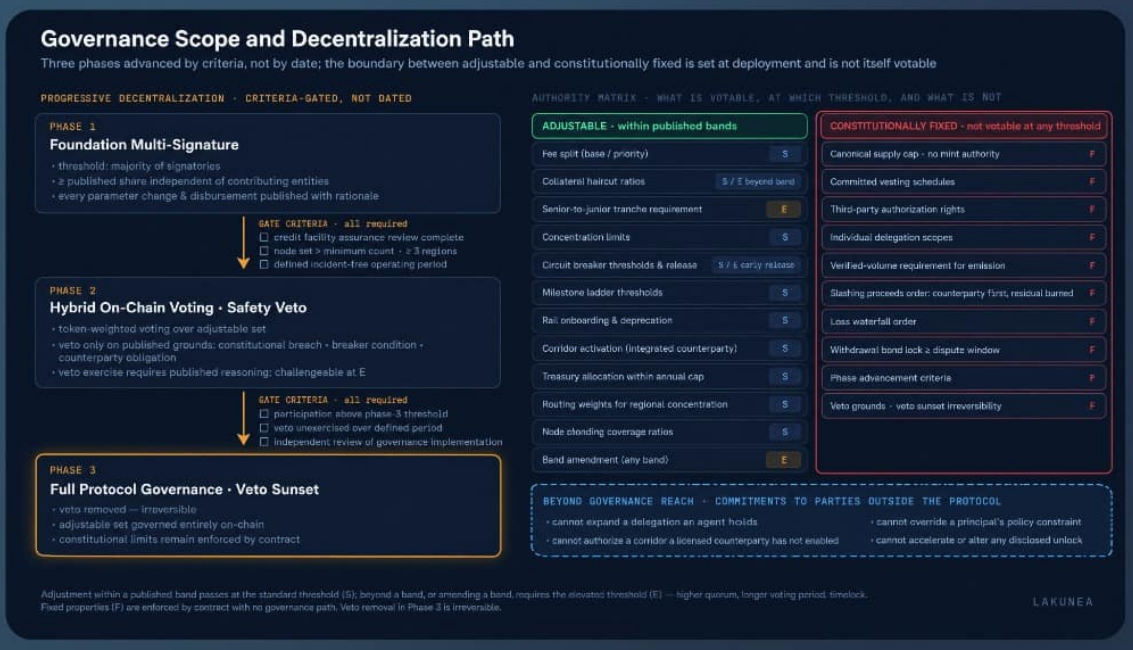
Adjustable parameters are subject to governance within published bands. Fee split allocation between base and priority components. Collateral haircut ratios and the senior-to-junior tranche requirement. Concentration limits in the credit facility. Circuit breaker thresholds and release conditions. Milestone ladder thresholds for ecosystem emission. Rail onboarding and deprecation. Corridor activation where a licensed counterparty has completed integration. Treasury allocation subject to the annual cap. Routing weight adjustments for regional concentration. Node bonding coverage ratios.

Adjustment within a band passes at the standard threshold. Adjustment beyond a published band, or amendment of a band itself, requires the elevated threshold — a higher quorum, a longer voting period, and a timelock before execution. The escalation exists because the bands encode risk limits, and a governance process that can widen its own risk limits at the standard threshold has no risk limits.

Constitutionally fixed properties are not votable at any threshold. Canonical supply cap and the absence of mint authority. Committed vesting schedules for allocated tranches. Third-party authorization rights, including the delegation grants held by policy principals and the scope constraints attached to credentials. The verified-volume requirement for ecosystem emission, as distinct from the thresholds on the ladder, which are adjustable. Slashing proceeds application order — counterparty made whole first, residual burned.

The vesting entry deserves emphasis. A governance process capable of accelerating its own unlock has converted every disclosed schedule into an expression of intent. The schedules are enforced by contract without a governance path to modification, which means an investor reading the release curve is reading a constraint rather than a plan.

The third-party rights entry is the one most often absent from governance frameworks that otherwise look rigorous. A vote cannot expand a delegation an agent holds, cannot override a policy constraint set by a principal, and cannot authorize access to a corridor a licensed counterparty has not enabled. Governance holds authority over the protocol's own parameters and none over commitments made to parties outside it.



11.2 Progressive Decentralization

Three phases, advanced by criteria rather than by date.

Phase one operates under foundation multi-signature control, with a threshold requiring a majority of signatories including a minimum proportion who are independent of the protocol's contributing entities. Every parameter change and treasury disbursement is published with its rationale. This phase exists because a protocol whose credit facility has not been stress-tested against live data and whose node set has not demonstrated reliability requires a response time that a governance vote cannot deliver.

Phase two introduces on-chain voting over the adjustable parameter set, with the foundation retaining a safety veto exercisable only on a defined and published set of grounds: a proposal that would breach a constitutional limit, one that would engage a circuit breaker condition, or one whose execution would violate an obligation to a licensed counterparty. Veto exercise requires published reasoning and is itself subject to challenge at the elevated threshold. Advancement to this phase is gated on the credit facility completing its assurance review, the node set exceeding a minimum operator count and geographic distribution, and a defined period of incident-free operation.

Phase three removes the veto. Advancement is gated on demonstrated governance participation above a threshold, on the veto having gone unexercised for a defined period, and on completion of an independent review of the governance implementation. The veto's removal is irreversible.

The phases are described without dates because a decentralization schedule expressed in quarters is a commitment to advance whether or not the conditions warrant it, and the failure mode — handing control to an unprepared governance process because a calendar said so — is worse than a delay.

11.3 Treasury Architecture and Spend Controls

Treasury holds the allocated tranche, accumulated protocol revenue directed to it under 10.7, and any recovered amounts returned through the credit waterfall.

Four controls apply.

The annual cap limits disbursement to a maximum of 8.0% of remaining treasury balance per 365-day rolling period rather than to an absolute amount, which means the constraint tightens as the balance depletes rather than permitting a fixed drawdown that accelerates in relative terms. The cap is constitutionally fixed as a mechanism; its level is adjustable at the elevated threshold.

Disbursement above a defined size requires a proposal with a stated objective, a defined recipient, and a reporting obligation on outcomes. Below that size, delegated operational spending proceeds under a published budget with retrospective disclosure.

Reserve accumulation to the credit facility's protocol reserve is prioritized ahead of discretionary spending until the reserve reaches its target proportion of facility capacity. A treasury funding ecosystem initiatives while the reserve beneath a live credit facility is underfunded has mispriced its own obligations.

Treasury holdings composition is published, including the proportion held in LKUN versus stable assets. A treasury denominated entirely in its own token cannot fund operations through a drawdown, which is precisely when funding is required.

Addresses, balances, and every disbursement are published on the cadence.

11.4 Proposal Lifecycle

A proposal passes through five stages: publication for comment, during which the proposal is public and unvotable; sponsorship, requiring support from holders above a minimum threshold to reach the ballot, which filters proposals with no constituency; voting (5-day window for Standard proposals with 4% quorum and >50% threshold; 14-day window for Elevated proposals with 10% quorum and >66.7% supermajority); timelock (48 hours for Standard, 7 days for Elevated) but not yet executed; and execution.

The timelock is the stage that matters for participants who do not vote. It provides an interval in which a passed proposal that a participant considers adverse can be responded to — by exiting a position, withdrawing bond, reducing a credit drawdown, or raising a challenge — before the change takes effect. Timelock duration scales with the proposal's threshold class, and constitutional challenge proposals carry the longest.

Voting weight is token-based with a delegation mechanism. The protocol does not implement quadratic or reputation-weighted voting, on the assessment that both introduce identity requirements at the governance layer that can be circumvented at a cost lower than the influence they confer, and the resulting complexity obscures rather than improves accountability.

12.0 Risk Factors and Compliance Architecture

12.1 Compliance-by-Architecture: Functional Separation

The protocol's regulatory position rests on a separation of three functions across three distinct categories of actor. The separation is architectural — it determines what each actor is technically capable of doing, not merely what it undertakes contractually — and each boundary is designed to prevent a specific regulatory characterization from propagating across it.

The issuing and protocol entity publishes the protocol's reference implementation, holds and governs the canonical supply ledger under the constraints in 11.0, and maintains the registries. It does not execute settlement, does not hold participant funds, does not take custody of any asset belonging to a transacting party, and holds no payment, money transmission, or custody authorizations in any jurisdiction. Its economic relationship to the network runs through protocol revenue allocation and treasury, both of which are transparent and constrained. It cannot execute a settlement, because settlement execution requires a bonded node position and the entity holds none.

The settlement execution network — the bonded node set described in 9.0 — performs verification, clearing, and on-chain submission. Nodes are independent operators, permissionlessly admitted on meeting published requirements, and economically compensated through priority fees and volume-gated emission. A node holds settlement positions transiently in the course of executing a transaction and bears exposure during the confirmation window under 4.2. It does not hold participant balances, does not convert between digital assets and national currencies, and does not deliver value into any national currency system. A node's technical capability ends at on-chain settlement and instruction issuance.

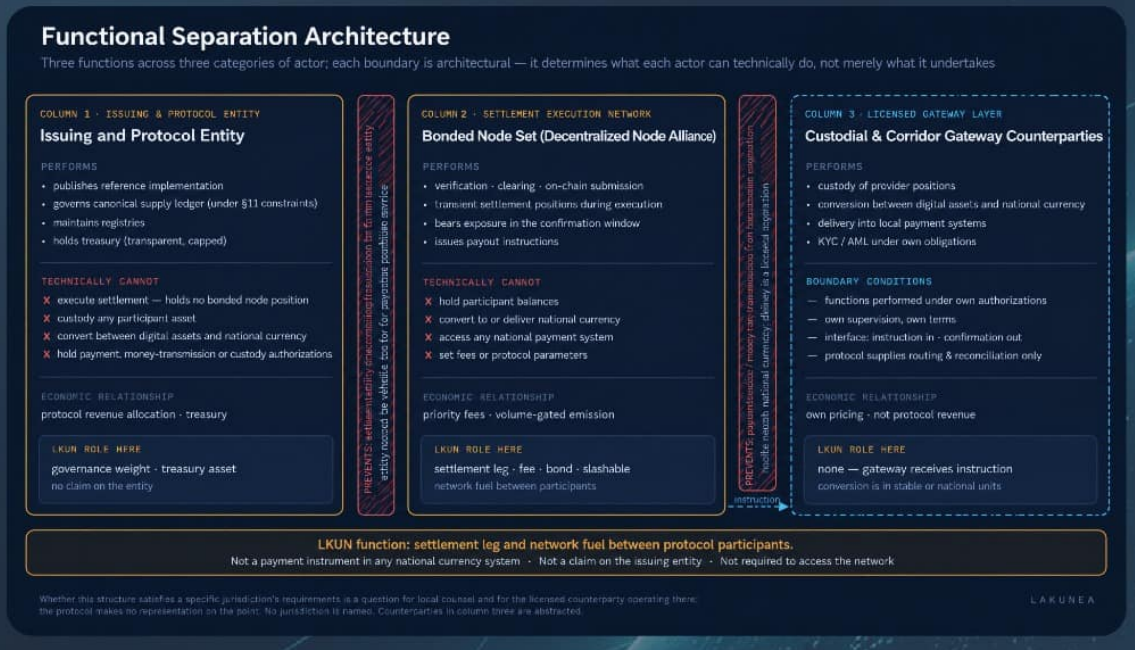
The licensed gateway layer comprises custodial counterparties and corridor gateway operators, each holding its own authorizations in the jurisdictions where it operates. These entities perform custody, conversion between digital assets and national currencies, and delivery of value into local payment systems. They are counterparties to the protocol through a defined interface — instruction in, confirmation out — and they perform their functions under their own regulatory obligations, on their own terms, subject to their own supervision. The protocol supplies routing logic and reconciliation records. It does not supply the authorization under which conversion occurs, and it cannot perform conversion itself.

Three consequences follow from the separation, and each is the reason a particular boundary exists.

The protocol entity's inability to execute settlement means that a characterization of settlement activity attaching to node operators does not attach to the entity, and that the entity cannot be the party through which an unauthorized payment service is provided.

The node network's inability to convert or deliver national currency means that node operation does not constitute payment services or money transmission in the jurisdictions where operators are located, notwithstanding that transactions they clear may ultimately result in local currency delivery through a gateway.

The gateway layer's independent authorization means that where a jurisdiction restricts the use of digital assets as payment instruments, the protocol's participants are not using them as such. The token executes a settlement leg between protocol participants; delivery of local currency value to a provider is performed by a licensed entity carrying out a conversion it is authorized to perform. Whether that structure satisfies a specific jurisdiction's requirements is a question for local counsel and for the licensed counterparty operating there, and the protocol makes no representation on the point.



12.2 Token Characterization

LKUN is designed as a protocol-native settlement and collateral asset. Its functions — settlement leg execution, fee payment, node and underwriter bonding, credential and tier consumption, governance weight — are consumptive and participatory within the network.

LKUN does not represent equity in any entity, a debt claim against any entity, a right to profits or distributions from any entity, or a claim on assets held by any entity. Protocol revenue allocation to burn reduces supply through a mechanical process; it is not a distribution to holders and confers no entitlement. Junior tranche participation in guarantee fee income arises from posting capital into a loss-bearing position and is compensation for risk borne, available to any participant who posts capital and not an attribute of holding.

Characterization is jurisdiction-specific and is not determined by design intent. The protocol's position is that its analysis has been conducted with counsel in the jurisdictions relevant to its distribution and operations, that distribution occurs only through channels appropriate to each jurisdiction under that analysis, and that the analysis may be wrong or may be superseded. A regulator reaching a different conclusion could require changes to distribution, to secondary trading access, to specific functions, or to the protocol's operation in a market. This risk is not mitigable by drafting and is disclosed as material.

Where a jurisdiction operates a licensing regime for digital asset trading, access for participants in that jurisdiction occurs through licensed intermediaries under that regime. Listing on any venue is subject to that venue's own admission process, which the protocol does not control and does not represent as secured.

13.0 Organization, Development Horizons, and Verification

13.1 Contributor Structure and Functional Mandates

Protocol development is carried out by a core contributor group engaged through the issuing entity. Node operation, custodial relationships, and gateway integration sit with independent parties under 9.0 and 12.1, which means the contributing structure described here holds no operational position in settlement execution and no authorization in any payment corridor.

Four mandates own the technical and economic subsystems at this stage. Each carries a defined scope, published in outline so that a counterparty can identify the accountable party for a given subsystem rather than addressing questions to the project generally, and each is compensated from the core contributor tranche under the vesting terms in 10.5.



Lukas A. Zimmermann

Core Protocol and Distributed Systems Lead

Zimmermann holds a B.Sc. in Computer Science from ETH Zürich and an M.Sc. in Distributed Systems from EPFL. He spent nine years in low-level systems engineering within high-concurrency transaction environments, most recently as Principal Systems Architect at SIX Digital Exchange (SDX) in Zurich, where his work covered transactional message bus partitioning, high-availability ledger replication, and sub-second settlement pipelines running across distributed financial gateways.

His mandate covers the node alliance consensus engine, mempool behavior under contention, and deterministic finality execution paths. The verification-before-finality design described in 4.2 and the reorganization handling in 4.4 fall within this scope, as does the conformance behavior a node must demonstrate before admission under 9.2. Throughput characteristics under verification load — the constraint examined — are a direct consequence of the design decisions this mandate controls.



Bastiaan van Lynden-Cappelle

Settlement Rails and Gateway Architecture Lead

Van Lynden-Cappelle holds an M.Sc. in Systems and Control Engineering from Delft University of Technology and has worked on cross-border payment rails and automated liquidity rebalancing for more than a decade. At Adyen in Amsterdam he served as Senior Gateway Architect, with responsibility centered on ISO 20022 message translation layers, multi-currency clearing pipelines, and liquidity orchestration across European and Southeast Asian banking interfaces.

He is responsible for the rail router topology in 8.1, the multi-gateway custodial interface specification in 8.5, and the technical specification for regulated local currency gateway interfaces. The interface discipline that section describes — instruction in, confirmation out, with the licensed counterparty performing conversion under its own authorizations — is a specification problem before it is a legal one, and the message-translation experience behind this mandate is where the adapter layer in 4.1 and the gateway specification share their engineering approach.



Dr. Seiichiro Kashiwabara

Identity and Cryptographic Assurance Lead

Kashiwabara holds a Ph.D. in Mathematical Sciences and Information Security from Tokyo Institute of Technology and previously held a research fellowship at the Cyber Security Research Centre at Nanyang Technological University. His published work covers zero-knowledge verifiable credentials, cryptographic accumulator trees, and Sybil-resistant identity graphs, and he has contributed over a sustained period to open decentralized identity frameworks in the Asia-Pacific region.

The principal–agent–delegation graph, the credential verification lifecycle, and the behavioral scoring model in 5.4 sit under this mandate. The design constraint operating throughout is the one stated in 5.1: a signature establishes that a key signed a payload and nothing further, and every mechanism in the identity layer has to add assurance without contradicting that limit. Accumulator-based revocation propagation addresses the short-list latency problem in 5.3; the Sybil cost analysis rests on the same body of work.



Devavrat Seshadri-Narayanan

Mechanism Design and Financial Risk Architect

Seshadri-Narayanan holds a B.Tech in Computer Science from the Indian Institute of Technology Madras and an M.Sc. in Quantitative Finance from the National University of Singapore. He worked as a quantitative risk modeler with institutional liquidity desks and fintech credit infrastructure in Singapore, specializing in dynamic collateral haircut modeling, multi-tranche default waterfalls, and algorithmic circuit-breaker design for automated debt facilities.

His mandate covers the formalization of the machine credit layer, collateral haircut calibration, loss absorption mechanics, and the stress testing framework. The haircut discipline in 6.4 and the automatic breaker behavior in 6.5 originate here, as does the conservative baseline adopted for net supply planning — a modeling stance rather than a communications choice, and one that sets treasury and reserve policy accordingly.

Functional titles in this section describe scope within the protocol. Prior institutional affiliations denote employment history; they do not indicate current affiliation with, endorsement by, or representation of those institutions. Open mandates are published as they are defined, and a mandate whose scope is unassigned is disclosed as such.

13.2 Research and Advisory Council

The council advises. It holds no executive authority, votes on no protocol parameter, and controls no treasury. Where an advisory position materially shapes a disclosed design decision, the relevant section of this document says so. Where the council's view differs from the protocol's position, the protocol's position governs and the difference is not presented as a consensus that does not exist.



Jonathan K. L. Cheng, LL.M.

Senior Regulatory and Gateway Policy Advisor

Cheng holds an LL.M. in International Financial Law from King's College London and an LL.B. from the National University of Singapore (NUS), and has practiced for more than eighteen years in Southeast Asian cross-border payment infrastructure, digital asset sandbox governance, and central banking regulatory interfaces. He has advised regional payment gateway consortia on non-custodial intermediary compliance and on cross-border currency regulation across ASEAN corridors.

He advises on the compliance-by-architecture separation framework in 12.1, on liability allocation for non-custodial node operators, and on regulatory interoperability models for emerging market payment corridors. His role is advisory in the strict sense: counsel of record in each jurisdiction relevant to distribution and operation is separately engaged, and no view expressed by the council constitutes a legal opinion on which a participant, counterparty, or gateway operator may rely. The protocol's statements about regulatory treatment carry the qualification given in 12.1 and 12.2 for that reason.

Additional council seats are constituted as the corresponding workstreams are defined. Council mandates are published, and appointments are disclosed along with the scope each member advises on, so that a counterparty can distinguish advice on corridor regulation from advice on contract security or on identity architecture. Where a council member holds a position elsewhere that bears on a protocol design decision, that interest is disclosed in the relevant section.

13.3 Development Horizons

Progression is gated on verifiable criteria. No horizon carries a date, and advancement occurs when the gate criteria are met rather than when a period elapses.

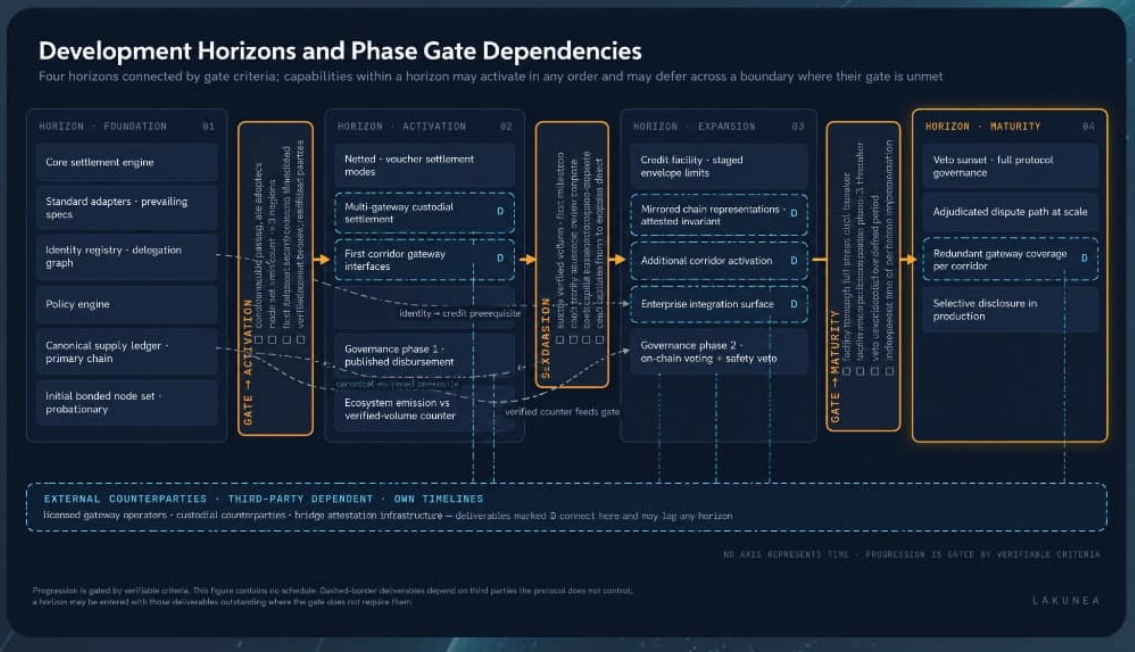
Foundation. Core settlement engine, standard adapters for the prevailing specifications, identity registry with delegation graph, policy engine, canonical supply ledger on the primary issuance chain, initial bonded node set under probationary routing. Gate to Activation: conformance suite passing across all adapters, node set exceeding minimum operator count with distribution across at least three regions, completion of the first independent security review with findings remediated, verified settlement occurring between unaffiliated counterparties.

Activation. Netted and voucher settlement modes, multi-gateway custodial settlement, first corridor gateway interfaces where licensed counterparties have integrated, governance phase one operating with published disbursement, ecosystem emission beginning against the verified volume counter. Gate to Expansion: sustained verified settlement volume above the first milestone threshold, credit facility assurance review complete, senior tranche capitalized to its required ratio, node set operating without a slashing event attributable to a systemic defect.

Expansion. Credit facility live under staged envelope limits, mirrored chain representations with attested supply invariant, additional corridor activation, enterprise integration surface, governance phase two with on-chain voting and the safety veto. Gate to Maturity: credit facility operating through a full stress cycle including at least one circuit breaker engagement and release, governance participation above the phase three threshold, veto unexercised over the defined period, independent review of the governance implementation complete.

Maturity. Veto sunset and full protocol governance, adjudicated dispute path operating at scale, redundant gateway coverage across active corridors, selective disclosure in production.

Capabilities within a horizon may activate in any order, and a capability may be deferred across a horizon boundary where its gate criteria are unmet. The horizons describe dependency, not sequence in time.



Appendix A — Glossary of Protocol Terms

Terms are defined as used in this document. Where a term also carries an industry meaning that differs, the protocol's usage governs within this document and the divergence is noted.

Agent. A software process transacting under a credential issued by a principal. An agent holds a key, presents a credential, and transacts within a scope it cannot exceed. It is not a legal person and bears no obligation; obligation attaches to its principal.

Agent budget. A policy object attached to a specific agent credential, carrying per-transaction and per-period ceilings, counterparty scope, and an escalation rule.

Assurance tier. A classification attached to a principal credential, reflecting the diligence performed at onboarding by the issuing party. The tier bounds credential issuance rights, credit envelope ceiling, and corridor availability. A tier is an attestation by its issuer and carries that issuer's reliability, not the protocol's.

Attestation node. A node class verifying properties the protocol cannot establish from chain state alone: the supply invariant, gateway confirmation integrity, and settlement node behavior under adversarial probe. Bonded at a flat requirement.

Base fee. The burned component of the network fee. calculated as a base floor of 0.0005 LKUN plus a 2.5 basis-point (0.025%) charge on settled value. Burn occurs at assessment and is irreversible.

Bond. Slashable collateral posted in LKUN as a condition of node admission. For settlement nodes, sized against a trailing measure of exposure multiplied by a governance-set coverage ratio.

Canonical supply ledger. The authoritative record of total supply, cumulative burn, and the allocation of unburned supply across chain representations. Holds no mint authority.

Circuit breaker. An automatic constraint on credit facility operation, engaged on threshold breach without governance action. Effects escalate from issuance suspension through pro-rata envelope constriction to facility closure for new drawdown.

Constrained. A node lifecycle state entered when bonded stake is insufficient for current throughput or performance falls below threshold. Routing is reduced pending remedy. Distinct from suspension, which follows a claim or probe failure.

Corridor. A path by which settled value reaches a provider in a national currency, operated by a licensed gateway counterparty under its own authorizations. Corridors are referenced in this document at the level of strategic region.

Credit envelope. A revolving limit attached to a principal, drawable by its agents within their individual scope ceilings. Sized from assurance tier, aggregate agent reputation on a sublinear curve, realized settlement velocity, and posted collateral.

Decentralized Node Alliance (DNA). The set of bonded operators performing settlement execution, attestation, and gateway bridging. Holds no legal personality, no central treasury, and no admission authority vested in any party. Membership is a registry state.

Delegation graph. The directed structure linking a principal to its agents and their sub-agents, with scope constrained to a subset at each level. Revocation propagates downward.

Effective constraint. The intersection of every policy constraint in a nesting chain. A child object specifying wider scope than its parent yields the parent's narrower value.

Escalation. Suspension of a transaction pending approval by a human approver bound to the governing envelope. Timeout resolves to denial.

Gateway-bridging node. A node class operating the technical interface to custodial counterparties and corridor gateways. Performs instruction delivery, confirmation retrieval, and reconciliation closure. Holds no authorizations itself.

Guarantee fee. The charge assessed on drawn credit balances per period of outstanding exposure, denominated in stable value, rate set by tier. Compensates capital providers bearing loss and the protocol reserve. Structured as a fee for a guarantee.

Haircut. The discount applied to collateral value in computing envelope capacity. An indicative fifty percent haircut means a unit of LKUN collateral supports half its spot value in capacity.

Immediate settlement. A settlement mode incurring one on-chain operation per transaction. Viable where transaction value exceeds per-operation cost by a sufficient multiple.

Integrity filter. The four-stage pipeline converting gross observed volume into verified volume: identity attestation, self-dealing exclusion, service resolution. Exclusions and criteria are published; governance holds an audit right.

Junior tranche. Underwriting capital posted in LKUN at a published haircut, absorbing loss after the borrower bond and before the senior tranche. Earns residual guarantee fee after senior claims. May be wiped out entirely.

KYA (Know Your Agent). The identity layer comprising credential issuance, the delegation graph, revocation state, and behavioral history from which reputation tiers derive.

Mirrored representation. LKUN on a chain other than the canonical ledger's, backed by a locked position on the canonical ledger. Not an independent issuance.

Netting rail. A settlement mode accruing obligations between a recurring payer-payee pair and settling the net position periodically on-chain. Obligations remain individually recorded, attributable, and disputable; only value transfer aggregates.

Network fee. The per-transaction charge assessed in LKUN at settlement, split into a burned base component and a priority component accruing to the executing node.

Normalized settlement instruction. The protocol's internal representation of a payment obligation, produced by a standard adapter and the only form the settlement engine operates on.

Organization envelope. The outermost policy object, attached to a principal. Sets aggregate ceilings, permitted service categories, prohibited counterparties, and available corridors. No individual approver may authorize a transaction outside it.

Primary issuance chain. The chain on which LKUN first issues, selected at the distribution window against six published criteria evaluated on conditions at that time.

Principal. An entity capable of bearing obligation, onboarded at an assurance tier, issuing agent credentials within tier limits. The accountable party for every transaction beneath it in the delegation graph.

Priority fee. The component of the network fee accruing to the executing node. Set by the payer within a published range; higher values receive preferential routing under capacity contention.

Probationary. The initial node lifecycle state. Bonded and admitted, receiving limited routing at elevated probe frequency, pending demonstrated reliability.

Protocol reserve. Loss-absorbing capital accumulated from a share of protocol revenue, positioned beneath both credit tranches. Prevents a loss event exhausting underwriting capital from propagating to resource servers that delivered service in good faith.

Protocol revenue. The base fee component of network fees, the protocol's share of guarantee fees, and corridor routing fees. Excludes priority fees, which are node compensation, and excludes gross settled value, which belongs to the transacting parties.

Reputation tier. A discrete classification derived from settlement history depth, dispute rate, policy compliance, inherited principal tier, and longevity. Decays slowly on inactivity; drops immediately and materially on default or adverse dispute resolution, with recovery requiring demonstrated clean volume.

Resource server. A provider of a metered digital service — API, dataset, model inference, compute, tool endpoint — that responds to unpaid requests with payment requirements and delivers on verification.

Selective disclosure. A proof exposing only the credential attributes a verification predicate requires. A resource server checking tier eligibility receives a proof of threshold satisfaction rather than the tier value.

Senior tranche. Underwriting capital posted in stable-value assets, earning a prioritized share of guarantee fees and absorbing loss only after junior capital is exhausted. Its depth is the facility's primary capital adequacy decision.

Settlement node. A node class performing the verification sequence, rail selection, on-chain submission, and bearing exposure during the confirmation window. Bonded against throughput.

Slashing. Confiscation of bond for demonstrable execution failure. Proceeds are applied first to making the harmed counterparty whole; the residual is burned rather than distributed to other nodes.

Task-scoped allocation. An ephemeral policy object issued for a defined workload, expiring on completion or timeout.

Verified volume. Gross settled volume surviving the integrity filter. Gates ecosystem tranche emission. Absent verified volume, no emission occurs regardless of elapsed time.

Voucher mode. A settlement mode in which the payer escrows funds on-chain, receives signed vouchers for individual consumption, and the provider redeems in batch against the escrow. Payer accepts capital lockup; provider accepts no exposure beyond escrow adequacy.

Appendix B — Parameter Table and Governance-Adjustable Ranges

Threshold class indicates the governance process required for adjustment: S standard threshold, E elevated threshold with higher quorum, extended voting period, and timelock, F constitutionally fixed and not votable.

B.1 Supply and Distribution

Parameter	value	Class
Canonical total supply	1,000,000,000 LKUN	F
Mint authority	None	F
Ecosystem incentives tranche	42%	F
Early backers tranche	15%	F
Core contributors tranche	14%	F
Treasury tranche	12%	F
Network bootstrap tranche	6%	F
Public distribution tranche	6%	F
Liquidity formation tranche	5%	F
Initial circulating share at distribution	10–15%	F
Committed vesting schedules	As published	F
Liquidity position lock term	≥ 24 months	E

Tranche shares and vesting schedules are enforced by contract without a governance path to modification. A governance process able to accelerate its own unlock would convert every published schedule into a statement of intent.

B.2 Fee Mechanics

Parameter	value or range	Class
Base fee floor	0.002 EVM-equiv in LKUN + 10 bps. Priority range: $0.0002-equiv to 200% of Base.	S
Base fee proportional component	Basis points on settled value	S
Base/priority allocation	Weighted toward base; band published	S
Base/priority band amendment	—	E
Priority fee range	Payer-set within published range	S
Base fee destination	Permanent burn	F
Priority fee destination	Executing node	F

B.3 Protocol Revenue Allocation

Parameter	value	Class
Burn share	35%	S within band
Node and underwriter distribution	35%	S within band
Treasury and reserve	30%	S within band
Band amendment	—	E
Reserve accumulation priority over discretionary spend	Until target ratio reached	E

B.4 Credit Facility

Parameter	value or range	Class
LKUN collateral haircut	50.0% (Permitted Governance Band: 35.0% – 65.0%)	S within band
Haircut band amendment	—	E
Senior-to-junior ratio requirement	3 : 1 (Min. 75.0% Senior Stable Asset)	E
Single-principal concentration limit	Proportion of facility capacity	S
Correlated-exposure aggregate limit	Proportion of facility capacity	S
Borrower bond as share of envelope	Tier-dependent	S
Guarantee fee rate by tier	Band per tier	S
Envelope sublinearity curve	Published function	E
Reserve target as share of facility capacity	Published	E
Loss waterfall order	Bond → junior → senior → reserve	F
Recovery return order	Reverse of waterfall	F

B.5 Circuit Breakers

Trigger	Effect	Release
Default rate threshold 1	New envelope issuance suspends	Metric recovery held over defined period
Default rate threshold 2	Existing envelopes constrict pro rata with notice	As above

Collateral value decline threshold	Drawdown restricted to principals above specified tier	As above
Senior-junior ratio breach	Envelope issuance throttled until ratio restored	Ratio restoration
Severe composite condition	Facility closed to new drawdown; repayment continues	E-threshold governance action plus metric recovery

Breakers engage automatically. Early release requires the elevated threshold, placing the burden on the party asserting that conditions have improved.

B.6 Node Parameters

Parameter	value or range	Class
Settlement node bond coverage ratio	Multiple of trailing peak exposure	S
Attestation node bond	Flat minimum	S
Gateway-bridging node bond	Flat minimum	S
Probationary routing share	Fraction of eligible routing	S
Probationary probe frequency	Elevated multiple of standard	S
Withdrawal bond lock	≥ longest applicable dispute window	F
Attestation quorum threshold	Per attestation type	E
Routing weight: reliability component	Published weighting	S
Regional concentration threshold	Share of settled volume or bonded stake	S
Slashing proceeds application	Counterparty made whole, residual burned	F

B.7 Identity and Reputation

Parameter	value or range	Class
Credential maximum validity	Mandatory expiry, duration by type	S
Revocation short-list staleness threshold	Bounded; exceeded fails closed	E
Reputation input weights	Published ranges, five inputs	S
Inactivity decay rate	Published	S
Adverse event step-down	Immediate, magnitude published	E
Recovery volume requirement	Clean volume over defined window	E
Reputation floor by principal tier	Published per tier	S