The Light Ecosystem

Master Architecture White Paper

Financial coordination transparency and the Global Digital Commodity Exchange

Version 1.0 | 6 November 2026 | Architecture and institutional discussion draft

Prepared for founders institutional partners governments and implementation teams

The Light ecosystem is a proposed global coordination environment connecting people, organizations, assets, commerce, capital, intelligence, and development. Its purpose is to make opportunities and obligations understandable, help qualified participants work together, and connect resources with accountable delivery.

This paper describes the complete architecture, including the Light Financial System, Gaia Global Treasury and Reserves, the Light Alliance, and a Global Digital Commodity Exchange. It develops the Neo NFT as a digital twin of a physical object or defined lot, linked to evidence, custody, rights, and lifecycle events.

Document status

This is a proposed design and operating model. Features, controls, roles, and service standards describe intended requirements unless expressly identified as source descriptions. The paper does not establish production deployment, an operating exchange license, an adopted token instrument, verified reserves, government authority, or institutional endorsement. Neo NFT is the project concept specified by the founder; no affiliation with another blockchain or product named Neo is implied. Implementation requires the agreements, qualified providers, legal analysis, and tested systems appropriate to each activity.

Contents

Sections 1 to 24 set out the ecosystem architecture and operating model. Appendices specify Neo records transparency access acceptance tests and sources.

1 Executive thesis 3
2 The problem and the proposed global solution 3
3 Ecosystem roles and institutional boundaries 4
4 The architecture of the complete system 5
5 Transparency as an operating capability 6
6 Identity credentials authority and participation 8
7 The Light information model and event record 8
8 Light Treasury reserves and financial records 9
9 Light payments clearing and settlement 10
10 The Global Digital Commodity Exchange 11
11 The Neo NFT physical asset twin 12
12 Neo admission issuance and lifecycle 13
13 Commodity lots transformations and quantity integrity 14
14 Exchange trading escrow and physical delivery 15
15 Light commerce procurement and productive enterprise 17
16 Global project funding and measurable delivery 18
17 Light Intelligence and accountable agents 19
18 Federation interoperability and the technical operating model 19
19 Governance law and institutional participation 20
20 Security resilience and participant protection 21
21 Economics participation and sustainable operation 22
22 Illustrative complete asset transaction 23
23 Illustrative development and impact workflow 24
24 Implementation sequence and acceptance criteria 25
Appendix A Neo twin record specification 25
Appendix B Transparency and access matrix 26
Appendix C Critical acceptance and failure tests 27
Appendix D Definitions and architectural invariants 28
Appendix E Sources evidence and design status 29

1 Executive thesis

We propose the Light ecosystem as shared infrastructure for coordination across financial and productive activity. It brings information about participants, assets, agreements, resources, decisions, and results into a connected environment. Its value lies in helping people understand the relationships that determine whether an opportunity can actually proceed.

The Light Financial System is the financial and information architecture within that environment. It connects treasury records, payment instructions, financial obligations, asset representations, and commerce while preserving the responsibility of each participating provider. It can support conventional money and existing institutions alongside properly defined digital instruments. Participation in a project does not inherently require adoption of a token.

Gaia Global Treasury provides the proposed coordination and stewardship role. Its Reserves arm organizes visibility into resources and obligations, preserving the distinctions between operating liquidity, restricted project resources, administered property, and backing for a defined instrument. The Light Alliance and related participation networks bring the people, organizations, and expertise needed to turn opportunities into work. [F1-F3]

The Global Digital Commodity Exchange is the proposed venue for qualified participants to discover and transact defined rights in physical commodities. The Neo NFT connects an object or lot with its identity, evidence, custody history, and specified rights. It should remain useful throughout the asset's lifecycle, including periods when trading is suspended or the asset has been withdrawn.

Transparency is the discipline connecting these functions. A participant should be able to establish what is being offered, who has authority, what evidence supports it, which obligations exist, and what has happened since the record was created. Access must be appropriate to the audience. Public visibility should reveal useful accountability without exposing identity documents, security-sensitive locations, private commercial terms, or vulnerable beneficiaries.

The architecture is designed as a federation. Organizations and local institutions retain their own mandates while using common identifiers, evidence formats, permissions, and interfaces. The goal is better cooperation across boundaries, with a reliable account of those boundaries. No universal legal jurisdiction, compulsory currency, or unrestricted central control is required for the model to be useful.

The implementation priority is to demonstrate a small number of complete workflows: a verified participant and agreement; a physical asset with a maintained twin; a controlled transaction with reconciled settlement; and a funded project with accepted results. Broader capability should follow evidence of reliable operation and a sustainable service model.

2 The problem and the proposed global solution

Fragmentation across useful systems

An asset may appear in a warehouse system, a supplier catalogue, a financing agreement, a payment record, and a buyer's procurement file. Each record can be individually useful while leaving participants unable to determine whether the descriptions refer to the same object or whether the asset is already pledged, sold, or unavailable.

Development activity has a similar problem. A community need, a technical solution, a qualified operator, and a potential funder may exist without a reliable process for connecting them. Even after an agreement, reporting may fail to connect disbursement, procurement, delivery, and actual service outcomes.

Light addresses these problems by connecting records and responsibilities around real activities. It should reduce repeated information entry, make unresolved conditions visible, and help participants discover relevant capabilities. It should not claim that every existing institution is opaque or that a new ledger automatically makes information true.

A global network with bounded commitments

The proposed global solution is a network of interoperable services and accountable operators. A participant can publish an opportunity, verify a role, exchange evidence, enter an agreement, transact through an appropriate provider, and retain a record of the result. The network supplies a consistent way to connect those steps.

Global scope requires local competence. Assets remain subject to the law and physical conditions relevant to them. Public projects follow the authority and processes of their institutions. Data access follows applicable rights and agreements. Common technology improves coordination; it does not eliminate those responsibilities.

The unit of progress

Progress should be measured through completed, reviewable activities: an accepted inspection, a valid transfer, a reconciled payment, a commissioned facility, or a resolved complaint. Membership growth and transaction counts can indicate use, but should not substitute for evidence of quality, resilience, or public benefit.

3 Ecosystem roles and institutional boundaries

The Light ecosystem comprises connected functions rather than one undifferentiated financial entity. The following roles are proposed architectural responsibilities. Their legal operators, appointments, and service agreements must be identified before implementation.

Component	Intended role	Boundary that remains explicit
Light ecosystem	Shared environment for participation and coordinated activity	Affiliation does not itself create a legal or financial mandate
Light Financial System	Information financial and integration architecture	Actual regulated services require appropriately authorized operators
Gaia Global Treasury	Coordination resource administration and stewardship	Each resource retains its owner restrictions and governing agreement
GGT Reserves	Umbrella reserve policy liquidity and obligation visibility	Reserve backing is defined for each specific instrument
Light Alliance and SaintAgent	Relationships capabilities participation and collaboration	Identity reputation and membership are separate from transaction authority

Component	Intended role	Boundary that remains explicit
Global Digital Commodity Exchange	Defined market workflows for admitted commodity interests	Product eligibility and venue activity require separate approval
Neo NFT and asset registry	Physical asset twins evidence and rights linkage	Token control does not automatically establish physical title
Projects and productive enterprises	Implementation services procurement and development	Delivery remains the responsibility of identified sponsors and operators

The public GGT About page describes collaboration, registry, intelligence, funding, and stewardship tools and sets out a technology-platform notice. This is a source description of the platform's positioning, not an independent audit of its listed features. The present paper extends the proposed architecture and should not be read as a statement that every component is already available. [P1]

The founder's prior planning materials describe Light Banking, Light Treasury, Light Assets, Light Commerce, Light Intelligence, and Light Settlement. We preserve those workstreams and connect them through a shared information and authority model. Light Banking refers here to provider integrations and account-related services under the appropriate operator, not a claim that the ecosystem itself is a licensed bank. [F1]

4 The architecture of the complete system

Shared foundations and distinct applications

The proposed architecture has common foundations for identity, authority, evidence, policy, and events. Applications use those foundations for treasury, commerce, projects, asset twins, intelligence, and institutional reporting. External services perform the activities assigned to them, including banking, custody, inspection, logistics, and legally effective transfers.

The identity layer identifies a participant or organization. The authority layer establishes what that participant may do and for whom. The evidence layer preserves records and their verification scope. The policy layer determines whether a requested action is permitted. Business services then carry out approved workflows and record their results.

The ledger layer records financial and asset movements under the relevant rules. The integration layer exchanges instructions and confirmations with external systems. The intelligence layer reads permitted information to explain context, surface exceptions, and suggest useful next steps. Governance and security apply across every layer.

Sources of authority for records

Each important fact needs a defined authoritative source. A warehouse may be authoritative for its custody acknowledgements. A legal registry may determine a registered interest. A bank confirms the status of its account. A project committee records its own approval. The Light platform can connect these sources without claiming to replace all of them.

Where records disagree, the system should expose the conflict and route it to the responsible parties. It should not silently select the most recent favorable value. A correction should identify the prior record, reason, authority, and effect on dependent transactions.

Deployment model

A practical first deployment can use a conventional application database, a financial subledger, protected document storage, an append-only audit log, and adapters to qualified external services. Distributed ledgers can be added where several independent parties need shared control or verification. A new blockchain is not a prerequisite for the initial coordination and project workflows.

Institutional or regional nodes can operate within agreed scopes while sharing approved records. Shared identifiers and interfaces should allow a participant to cooperate across nodes without placing every confidential record in a central repository. The federation needs contracts and operational coordination as well as common software.

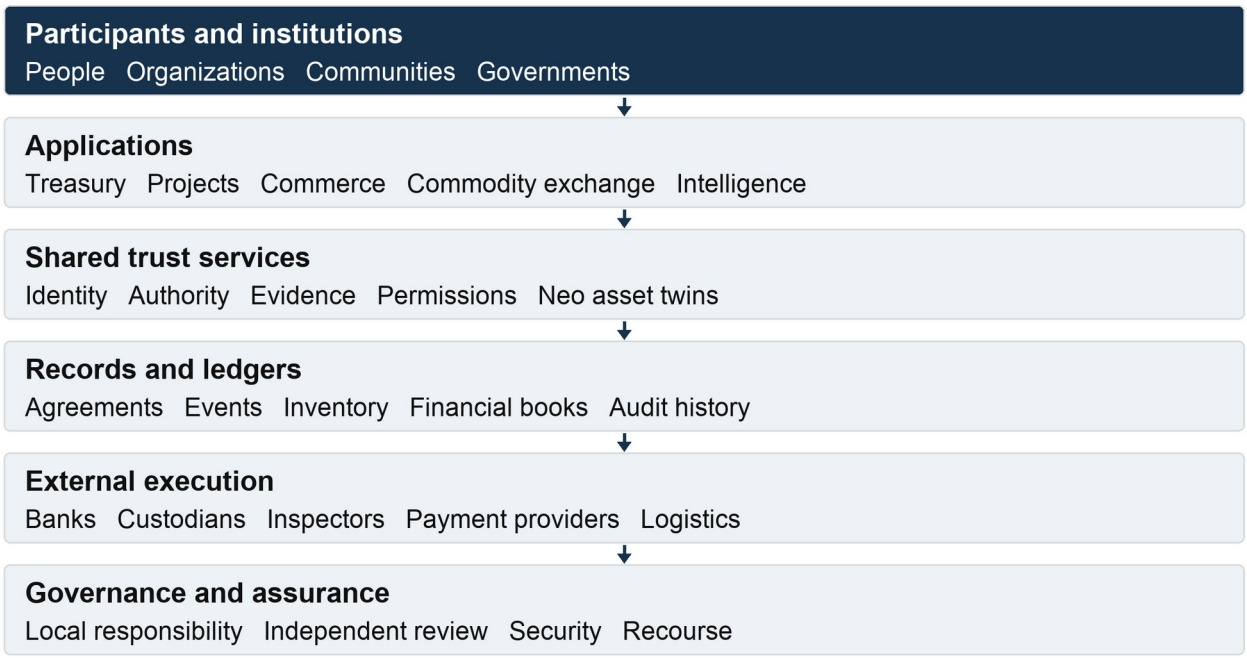


Figure 1 shows the proposed architecture. The layers describe responsibilities and interfaces, not a requirement that one operator control every system.

5 Transparency as an operating capability

What a participant should be able to establish

Transparency begins with answerable questions. What is the claim? Who made it? What evidence supports it? What did the reviewer actually check? When was it checked? What remains conditional? What changed? Who approved the action? Who can dispute the record? These questions should be reflected in the underlying records and user experience.

A dashboard should distinguish a reported asset from a verified one, a funding interest from cleared money, and an approved project from delivered services. It should identify the date and scope of each measure. Totals should explain exclusions and avoid combining unavailable resources with spendable liquidity.

Evidence with scope and time

Verification should attach to a claim and its evidence, not become a permanent general badge. A review of a person's identity does not validate their investment offer. A past assay does not establish that the inspected material remains in custody today. An account statement does not necessarily establish that its balance is unrestricted.

The proposed evidence record includes the claim, subject, issuer, reviewer, method, source, relevant jurisdiction, date, expiry or review trigger, limitations, and current status. Revocation or supersession should update the records that rely on it. Critical transactions should check validity at the time of action rather than depend on a screenshot.

Privacy and selective disclosure

Public information can include program criteria, fee schedules, capability status, aggregate outcomes, and assurance summaries. Counterparties may need detailed evidence about a specific transaction. Auditors may need broader records under confidentiality. Regulators and competent authorities receive the access required by the applicable process.

The design should therefore provide audience-specific access. A buyer can verify that an approved custodian holds an eligible lot without obtaining public access to the exact secure location of every asset. A donor can see that a project milestone was accepted without receiving protected information about a child beneficiary.

The limits of cryptographic proof

A digital signature can identify the signing key and detect alteration under the relevant scheme. A document digest can help establish that two copies match. Neither proves that the original statement was accurate, the signer was properly authorized, or the asset exists. The platform needs institutional accountability and physical verification in addition to cryptography.

Selective disclosure and zero-knowledge techniques may support narrowly defined proofs, such as an attribute check without disclosing a full identity record. Their use requires tested protocols and a clear description of what the proof establishes. They should not be invoked as a general claim that every confidential financial fact is verifiable without evidence access.

Corrections and public accountability

Transparency includes the ability to discover errors. The system should preserve the history of a material statement, show its corrected status, and notify dependent users when appropriate. Sensitive data may require deletion or restricted retention under applicable rules; the audit design should preserve only the information necessary to establish the correction and its authority.

6 Identity credentials authority and participation

People organizations and representation

The identity model should distinguish natural persons, legal organizations, public bodies, projects, and software agents. An individual can hold several roles without those roles being merged. A person acting for an organization needs a record of representation, scope, limits, duration, and revocation.

Membership and identity checks serve different purposes. Membership establishes access to a service under its terms. Identity evidence supports an attribute. Transaction eligibility may require additional review. Reputation concerns observed performance. None should automatically confer the others.

Verifiable credentials

Credentials can express assertions such as an approved organizational role, inspection qualification, or completion of training. W3C Verifiable Credentials Data Model 2.0 offers a reference for expressing credentials and presentations. Credential verification still requires a trust policy for the issuer, appropriate status checks, and consideration of the claim's relevance. Cryptographic validity alone should not determine business acceptance. [R1]

The platform should avoid forcing a single identity technology on every jurisdiction or community. Conventional verified accounts and interoperable credentials can coexist. Participants should be able to understand which information is required and why, and obtain help when documents or connectivity are limited.

Permission and delegation

Permissions should be checked at the service and data layers. Hiding a button is not access control. A coordinator may be allowed to prepare a proposal without signing it. An inspector may add a report without approving issuance. A treasury officer may review a payment without being allowed to alter its recipient.

Delegated authority should expire, be revocable, and remain visible in decision records. Organization departure, compromised credentials, or loss of a mandate should trigger access changes. Automated agents require a named accountable owner and a narrowly bounded scope.

Participation without forced financial exposure

Researchers, volunteers, community representatives, and project participants should be able to contribute without being required to buy a financial product. Where a service has a fee, it should be clear what that fee purchases. A paid account should not imply priority for grants or endorsement of a business proposal.

7 The Light information model and event record

Connected records

The proposed shared model includes participants, roles, authority, organizations, relationships, assets, rights, evidence, agreements, projects, contributions, obligations, transactions, decisions, and outcomes. Stable identifiers allow records in different applications to refer to the same underlying subject.

Relationships should state their type and status. A potential supplier, an approved supplier, and a contracted supplier are different relationships. A proposed partnership should not appear as a confirmed institutional affiliation. Every material relationship should identify the source and the party entitled to change it.

Events and current views

An event records an action or observation: an inspection was signed, a lot entered custody, a payment instruction was approved, or a milestone was accepted. The current view is derived from the relevant events and rules. Historical events should not be overwritten to make the current screen look consistent.

Each event should identify its subject, event type, actor, role, occurrence time, recording time, source, prior version, and supporting evidence. The distinction between occurrence and recording time matters when a warehouse reports a movement after a connectivity outage. Sequence checks should identify missing or conflicting updates.

GS1 EPCIS provides a useful reference for supply-chain event information and physical observations. The Light implementation should map relevant concepts into its own documented schemas rather than claim conformance without testing. [R2]

Evidence and content storage

Sensitive documents should reside in protected storage with access logs, retention rules, versioning, and appropriate backups. Shared ledgers can hold minimal references or digests where justified. References need durable retrieval arrangements; a token pointing to an unavailable web page is not an adequate evidence strategy.

Data quality controls should check required fields, units, identity references, signatures, dates, and inconsistent quantities. Human reviewers should resolve substantive conflicts. A system can validate the format of an assay report without being competent to establish that the assay was properly performed.

8 Light Treasury reserves and financial records

Separate resources and obligations

Light Treasury should organize financial information across the ecosystem without implying common ownership of all assets. GGT Reserves supplies the proposed umbrella view of reserve policy, resource categories, liquidity, and obligations. Each entity, program, and instrument must retain its governing terms. [F2, F3]

The minimum categories are operating resources, restricted project resources, assets administered for others, strategic holdings, and reserves supporting defined instrument obligations. Asset admission should record ownership, control, custody, valuation, restrictions, encumbrances, and verification status. A mandate to administer an asset should remain distinct from ownership.

Financial accounting and participant balances

A financial subledger should use entries that balance under the chosen accounting model and reconcile with the organization's books and external accounts. Participant balances need a defined legal meaning: a record

of held funds, a payable, service credit, asset quantity, or another specified entitlement. The interface should not make every balance resemble an insured bank deposit.

Cash in an omnibus account, where such an arrangement is appropriate, needs reconciliation to participant liabilities and the applicable safeguarding structure. An internal transfer between participants changes the subledger but does not itself create new external assets. On-chain wallet balances should likewise reconcile to obligations, fees, and restrictions.

Instruments within the ecosystem

GGT utility, GGG, and a possible Reserves instrument should have separate names, rights, issuance conditions, and reporting. The Neo NFT is an asset-specific twin, not automatically a currency or treasury reserve token. A platform can connect these instruments while preventing the same asset from being presented as independently available backing for incompatible promises.

The reserve information service should identify which assets are eligible for which obligation. When an asset is pledged, traded, withdrawn, impaired, or disputed, affected reserve calculations should change. Unverified values should remain outside certified or independently reviewed totals.

Liquidity and reporting

Funding capacity should follow cleared eligible resources after restrictions, commitments, near-term obligations, and approved buffers. An asset valuation is not immediate liquidity. Reports should show as-of dates, valuation methods, significant liabilities, concentration, and exceptions. The broader knowledge and capability reserve remains strategically useful without being counted as cash or collateral.

9 Light payments clearing and settlement

Provider responsibilities

Light should connect to appropriate banking, payment, custody, and settlement providers through explicit agreements. Each integration should identify the service, jurisdiction, eligible users, asset types, account ownership, instructions, fees, and exception handling. The platform must distinguish preparing an instruction from executing a regulated service.

Payment status should be precise. Created, authorized, submitted, accepted, rejected, pending, confirmed, reconciled, and legally final describe different conditions. A successful application response should not be used as the sole evidence that funds are irrevocably available.

Clearing and reconciliation

Clearing establishes the obligations generated by agreed transactions under the applicable rules. Netting, credit extension, central-counterparty functions, and settlement guarantees should not be implied by the word clearing. Each requires a separate legal and operating design if introduced.

Reconciliation compares instructions, external confirmations, subledger entries, and fees. Differences need an owner, age, and resolution record. Unique instruction identifiers and controlled retries should prevent duplicate execution when a network response is delayed.

Finality and linked exchanges

The contract and provider rules must define when each obligation becomes final. For asset purchases, the goal is to reduce the risk that one party gives value without receiving the agreed performance. Suitable mechanisms may include controlled escrow, pre-funded settlement, or a delivery-versus-payment arrangement supported by the actual systems.

The CPMI-IOSCO Principles for Financial Market Infrastructures offer reference principles for legal basis, settlement finality, linked obligations, and operational risk. They are used here as design references, not as evidence that Light is an FMI or satisfies the standards. [R3]

Cross-system transfers should not be called atomic unless the design actually guarantees the relevant all-or-nothing outcome. Physical delivery is normally a separate event from payment or transfer of a digital record. The transaction terms should state where risk, title, custody, and delivery obligations change.

10 The Global Digital Commodity Exchange

Purpose and initial scope

The Global Digital Commodity Exchange is the proposed arm for discovery, qualification, trading, and settlement of defined commodity interests associated with physical goods. It should connect market participants with current evidence and an enforceable transaction structure. The market product is the specified right or delivery obligation; the digital interface makes it understandable and manageable.

The recommended initial scope is a limited spot workflow for clearly identified, physically verified, custodied goods, using request-for-quotation or negotiated offers. Additional auctions, order books, financing, derivatives, or pooled products require their own product rules, permissions, controls, and validation. They should not be assumed to exist because a marketplace interface is available.

Participants and independent functions

Participants may include qualified sellers, buyers, custodians, inspectors, logistics providers, settlement providers, and authorized intermediaries. Each role needs eligibility criteria and an agreement. An intermediary's representation must be verified before it can offer goods for a principal.

Inspection, custody, market operation, and financial execution should have distinguishable responsibilities. If related organizations provide several services, conflicts and dependencies should be disclosed and managed. Paying a listing or verification fee should not determine the outcome of asset admission.

Product admission

A commodity product specification should identify asset type, grade, quantity unit, acceptable inspection, custody requirements, location category, permitted title or claim structure, transfer restrictions, settlement terms, delivery options, fees, and dispute process. A generic NFT listing is not a sufficient product specification.

Different commodities require different rules. Gold bars have serial, weight, and fineness records. Agricultural lots may require moisture, contamination, origin, storage, and shelf-life data. Industrial metals may require grade and testing standards. Equipment involves serial identity, condition, maintenance, and possible liens. A single verification badge cannot adequately describe all of these.

Market conduct and information

Listings should show the offer, relevant evidence scope, latest eligible state, restrictions, costs, and expiry. Rules should address who can revise a quote, how offers are accepted, order priority where applicable, cancellation, erroneous trades, conflicts, and suspension. Market data should distinguish an indicative quotation from an executed transaction.

The exchange should monitor self-dealing, wash activity, misleading supply, duplicate listings, and price manipulation appropriate to its model. It should publish applicable fees and ensure that execution statistics do not count cancelled or failed transfers as completed trade. This is proposed market design, not a claim of established venue operation.

11 The Neo NFT physical asset twin

Definition and purpose

The founder defines the Neo NFT as the digital twin of a physical object. In this architecture, it is a durable digital identity for an object or a precisely defined lot, connected to evidence, rights, custody, events, and current eligibility. Its usefulness comes from maintaining those connections throughout the physical lifecycle. [F4]

The twin should represent one recognized asset identity within the relevant registry domain. That domain may involve a serialized object, a sealed lot, or another asset-specific definition. The relationship must remain clear when the asset changes location, owner, condition, quantity, or legal status.

The identity and the rights are distinct

A Neo NFT identifies the asset and links to a defined rights record. That record should state whether the instrument represents ownership, a contractual delivery claim, a warehouse-receipt interest, a custody reference, or an informational record. The interface should use the appropriate language for that instrument.

ERC-721 is a possible technical interface for identifying and transferring non-fungible tokens. Its standard functionality does not determine the legal effect of transferring rights in a physical asset. The implementation may use another technology if it better fits the requirement. No chain is selected by this paper. [R4]

UNIDROIT's principles treat the legal effect of a link between a digital asset and another asset as a matter for applicable other law. The Neo structure therefore requires jurisdiction-specific terms and institutional acknowledgements, not merely an assertion that token ownership equals physical ownership. [R5]

Physical binding

The physical identity should use appropriate combinations of serials, measurements, photographs, assay or inspection data, packaging, tamper-evident seals, and custody records. Tags, QR codes, RFID, sensors, or physical fingerprints can assist identification. Each method has failure modes, including copying, substitution, tampering, calibration error, and loss.

The admission process should state how the asset is matched to the record and how identity is re-established after a material change. A token cannot independently prevent a dishonest person from presenting false physical evidence. Qualified checks, accountable custody, and periodic reconciliation remain necessary.

The maintained twin

The Neo record should show current custody, rights status, condition, quantity, encumbrances, verification dates, restrictions, and relevant lifecycle events. Documents remain versioned, and new evidence supersedes prior claims without erasing their history. A photograph or inspection should never be presented as continuously current unless an appropriate monitoring process supports that statement.

The NFT is one representation of that twin. The underlying asset record should remain accessible to authorized participants even if a token is frozen, a blockchain is unavailable, or the asset is no longer eligible for exchange trading. Historical provenance has value after the tradable claim has ended.

12 Neo admission issuance and lifecycle

Admission before issuance

A proposed admission sequence establishes the applicant and its authority, defines the asset, checks rights and restrictions, performs the required inspection, obtains custody acknowledgement, and resolves duplicate or conflicting claims. Issuance follows only after the responsible admission authority accepts the evidence for a defined purpose.

The evidence should identify who may rely on each report and when further inspection is required. A verifier's qualification should match the asset and method. Insurance should identify the insured interest, limits, exclusions, duration, and party responsible for claims; the word insured alone is not sufficient.

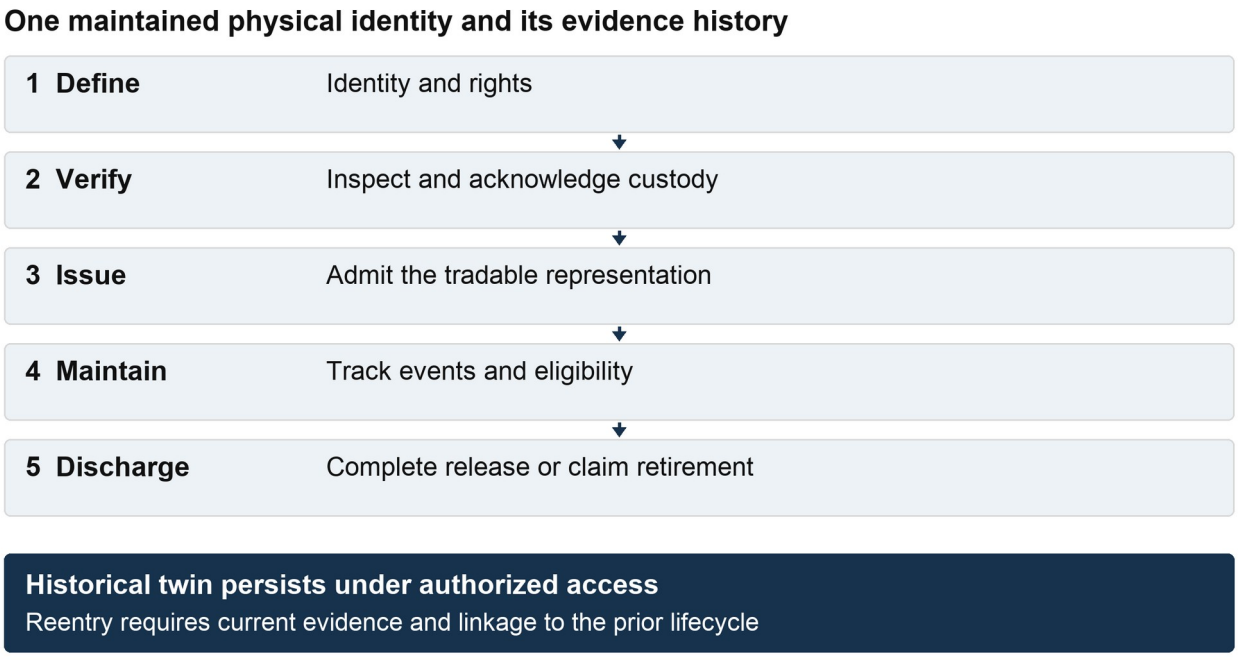


Figure 2 separates the physical lifecycle from trading eligibility. A maintained asset record can continue after a tradable instrument is retired.

Independent status dimensions

A single status such as verified is insufficient. The proposed model tracks identity, custody, rights, condition, encumbrance, evidence freshness, trading availability, and delivery state separately. The policy engine derives eligibility from those dimensions and the proposed action.

An inspected lot may remain in custody while its evidence is expired. An owned asset may be pledged and therefore unavailable for sale. A listed lot may become quarantined after a discrepancy. Each case needs an accurate representation without losing the other valid facts.

Issuance controls

The registry should maintain the canonical asset identifier, authorized issuer, contract or ledger namespace, token identifier if used, and controlling rights record. Issuance must be unique under the relevant product rules. The event should record the accepted evidence version and applicable terms.

Attempts to register a known identifier, overlapping lot, or inconsistent quantity should be blocked for review. Cross-platform duplication cannot be eliminated by a local database alone. The control model also needs contractual representations, custodian coordination, registry checks where available, and consequences for false declarations.

Sale pledge and release

The system should distinguish tradable, reserved for a transaction, pledged, suspended, and retired states. A pledge should identify the secured party, permitted actions, and release conditions. A sale lock should prevent another incompatible transaction while a settlement is pending.

Token transfer rules must enforce the product's eligibility policy. A standard transfer function that bypasses restrictions would undermine the model. If transfers occur outside the approved workflow, the governing terms and system must specify the effect and process for resolving conflicting control or rights records.

Withdrawal retirement and reentry

When goods leave the custody or rights structure supporting a tradable claim, that claim must be discharged or otherwise updated under the product rules. The tradable representation may be burned, locked, or marked retired. Burning alone is not proof that delivery occurred, and physical delivery alone should not leave an unfulfilled digital claim circulating.

The asset's identity and history can persist as a non-tradable record. Reentry requires a new admission check, current custody and condition evidence, and explicit linkage to the prior lifecycle. Replacement of a lost token or compromised key must invalidate or immobilize the conflicting representation so recovery does not create a duplicate claim.

13 Commodity lots transformations and quantity integrity

Objects lots and units

The twin model must distinguish unique objects from measured lots. A serialized bar can be individually identified. A bulk commodity may be defined by quantity, grade, location, storage compartment, and

allowable tolerance. The registry should record both measured quantity and the basis on which an eligible claim is expressed.

Units must be explicit and compatible. Gross weight, net weight, dry weight, fine-metal content, and packaging quantity are different measures. The system should retain the original measurement and any approved conversion method. A display conversion should not silently change the entitlement.

Splits and combinations

Splitting a lot should retire or constrain the parent claim and create authorized child records whose total eligible quantity reconciles to the parent, adjusted for documented losses, sampling, or other permitted changes. Combining lots should identify all inputs, relevant grades, new measurements, and the resulting product specification.

These are physical and legal events as well as data operations. A competent party must attest to the actual transformation. An automated calculation cannot establish that the warehouse performed the split correctly or that a mixed lot satisfies its stated quality.

Processing and depletion

Processing may change quality, form, or quantity and can create several outputs from several inputs. The records should preserve lineage, method, yield, waste, and responsibility. Parent instruments should no longer represent physical goods that have been consumed or transformed beyond their original specification.

Perishable or consumable goods need expiry, deterioration, recall, and disposal procedures. Eligibility can end before physical destruction. The market must know whether a claim is suspended for inspection, withdrawn, replaced, or extinguished. Unresolved quantity differences should block new incompatible commitments.

Fractional interests

Fractional financial interests are a separate product decision. Dividing economic claims does not physically divide an indivisible object. Any fractional instrument needs defined rights, governance, custody, fees, exit treatment, and legal analysis. The first commodity pilot should avoid adding this complexity unless its purpose requires it.

14 Exchange trading escrow and physical delivery

Qualification and order formation

Before a firm transaction, the exchange should establish the parties' identity, authority, eligibility, and accepted product terms. The seller's right to offer the asset and the asset's current eligibility must be checked again at the relevant decision point. Evidence that was valid at listing may have expired or changed before acceptance.

A quotation should identify the specific asset or lot, quantity, price basis, settlement asset, fees, delivery option, offer expiry, and conditions. Acceptance should create a versioned trade record. A late response to an expired quote should not become a trade without renewed agreement.

Reservation and controlled execution

The accepted trade should reserve the relevant inventory or instrument and prevent another incompatible sale or pledge. The buyer's funding process then follows the agreed provider rules. A screenshot, pending bank transfer, or unconfirmed transaction should not be treated as final money merely because the user interface reports submission.

The seller's asset control and the buyer's payment capacity should be checked before release. The product agreement should identify the escrow operator or other settlement mechanism, release conditions, timeouts, permitted cancellation, and treatment of a failed leg. Light should not imply that it holds escrow funds unless an identified entity actually performs that role under appropriate arrangements.

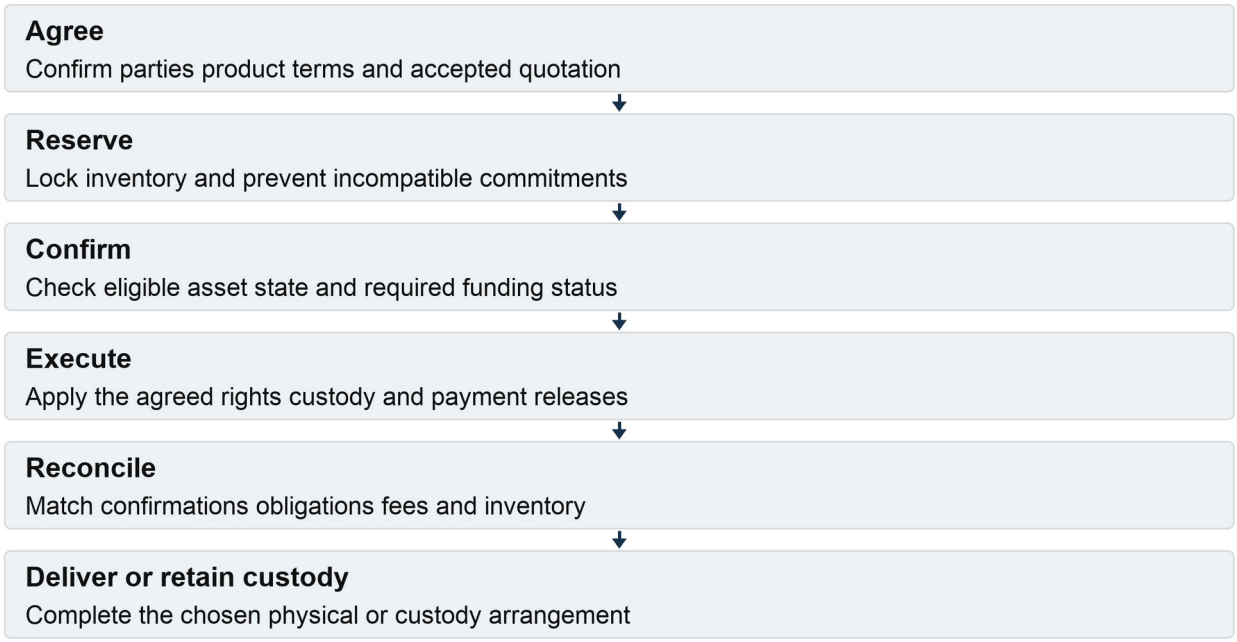


Figure 3 shows the proposed controlled transaction sequence. Technical coordination reduces execution risk but does not remove the need for enforceable agreements or reliable external providers.

Financial rights and physical movement

Where goods remain in an approved warehouse after sale, completion may involve a change in the person entitled under the custody arrangement without physical movement. The custodian should acknowledge the change through the agreed mechanism. A token movement alone should not be assumed to update the custodian's obligations.

Where the buyer requests delivery, the transaction must also define logistics, collection authorization, inspections, transport insurance, export or import requirements, and the point at which risk and title change. These may occur at different moments. The buyer should see a precise account of each obligation.

Warehouse release should require a valid request from the entitled party, settlement of relevant obligations, absence of incompatible restrictions, and controlled discharge of the claim. Logistics records should confirm handover and acceptance. The final reconciliation should connect the financial settlement, updated rights, inventory change, and instrument status.

Exceptions and disputes

If payment fails before a binding release, reserved inventory can be unlocked under the agreed rules. If one leg has become irreversible, the system needs an exception procedure rather than pretending to reverse history. Resolution may involve the relevant provider, a contractual remedy, insurance where applicable, or a competent dispute forum.

Material disputes should suspend the affected activity, preserve evidence, identify who can authorize resumption, and inform parties whose rights may be affected. A dispute about one lot should not automatically expose unrelated confidential records. The decision record should state the issue, authority, evidence considered, remedy, and remaining obligations.

15 Light commerce procurement and productive enterprise

Commerce linked to evidence

Light Commerce should connect buyers, suppliers, goods, services, projects, and fulfillment. Listings should distinguish availability claims, indicative offers, firm quotations, signed orders, and accepted delivery. The marketplace should make responsibilities and fees visible before commitment.

The same record model can support a machine sale, an engineering service, or project procurement without pretending that each is a commodity token. Product- and service-specific terms should establish delivery, acceptance, warranty, intellectual-property permissions, and payment conditions. A Neo twin can support equipment provenance while the service agreement governs installation and maintenance.

Procurement and conflicts

Funded projects should connect procurement to approved scope and budgets. Review should address supplier competence, price comparison, related parties, and delivery capacity. A marketplace recommendation should not become an undisclosed paid endorsement. Material departures from program procurement rules require recorded approval.

The system should connect a purchase order to invoices, receipt evidence, acceptance, and the corresponding payment. Quantity, currency, and tax treatment should remain explicit. If an invoice changes after approval, the change should trigger the applicable review rather than inherit the prior authorization automatically.

Knowledge services and contribution

Participants can contribute knowledge, facilities, equipment, and time. The platform should identify whether the arrangement is paid work, volunteering, a license, a donation, or an exchange of services. Each form has different rights and obligations. Recognition units should not be presented as wages or redeemable money unless the applicable arrangement actually provides those rights.

The commercial objective is to improve useful connections and reduce avoidable coordination costs. Revenue, growth, and network activity should be assessed alongside delivery quality, unresolved disputes, affordability, and the operating burden on participants.

16 Global project funding and measurable delivery

Needs become implementable projects

GGT's coordination role begins with evidence of need and a responsible sponsor. Project development should establish the local context, technical scope, approvals, budget, delivery organization, operating plan, and intended outcomes. The Light Alliance can help assemble complementary capabilities while the platform records who has committed to what. [F2]

Resource matching should respect instrument differences. A grant, loan, investment, supplier credit, and procurement contract are not interchangeable funding categories. The recipient should understand the obligations before accepting support. Paying a membership or application fee should not imply funding approval.

Funding and treasury controls

A project allocation should be supported by eligible resources and an authorized decision. A pledge remains separate from receipt; receipt remains separate from allocation; disbursement remains separate from accepted work. Treasury forecasts should account for restrictions, prior commitments, fees, and operating buffers.

Where resources come from a reserve structure, the responsible parties must establish that the intended use is permitted. A project should not consume assets required to meet an incompatible holder obligation. Any financing secured by an asset should identify the lender, pledge, conditions, costs, and effects on asset availability.

Milestones and evidence

Agreements should define what evidence establishes completion and who can accept it. Payment can be staged against preparation, procurement, installation, and commissioning as appropriate. Some commercial arrangements require advance payment; those exposures should be protected and disclosed rather than hidden behind a claim that every payment follows completion.

The platform should connect milestone evidence to the relevant budget, supplier records, inspection, payment, and decision. A change in scope should preserve the original baseline and the reason for amendment. Delays should prompt reforecasting and corrective action before the next material commitment.

Outcomes and ongoing operation

Outputs describe what was delivered. Outcomes describe changes experienced by users or communities. A water installation may be complete while service reliability remains poor. A training program may record attendance without demonstrating new capability. Evaluation should therefore specify baseline, method, time period, limitations, and ongoing operator responsibility.

The impact record can support learning and replication. It should also record failure, harm, and unresolved issues. Participation in a humanitarian program should not require public exposure of sensitive personal information or agreement with a financial or spiritual product.

17 Light Intelligence and accountable agents

Intelligence connected to context

Light Intelligence should help participants understand their permitted records, discover relevant relationships, identify missing evidence, and act on well-defined opportunities. Its outputs should explain the sources, dates, assumptions, and uncertainty relevant to the recommendation. The purpose is usable decision support.

The proposed knowledge model connects a person to an authorized role, an asset to evidence, a commitment to an agreement, and an outcome to accepted records. Founder discussions describe purpose-aware value and semantic relationships. Here those ideas become an implementable model of linked records and permissions; no new physical theory is assumed. [F1, F2]

Agent roles

A treasury agent can monitor liquidity forecasts and unresolved reconciliations. An asset agent can track expiring inspections or custody changes. An opportunity agent can identify relevant programs and participants. A project agent can prepare status reports. A risk agent can identify anomalies. Each should have a defined owner, data scope, tool permissions, and escalation route.

An agent preparing a payment should not acquire the authority to approve it. An agent reading an uploaded document should not follow embedded instructions to disclose private data. Human approval should remain necessary for the material actions defined by policy, including financial releases, rights changes, disputed decisions, and significant public claims.

Evaluation and oversight

Testing should cover factual accuracy, missing sources, misleading confidence, unequal outcomes, privacy leakage, malicious inputs, and unauthorized tool use. Monitoring should identify failures in actual use, not only performance on prepared examples. The NIST AI Risk Management Framework provides a voluntary reference for organizing this work, not a certification of Light. [R6]

Research and matching systems should make paid visibility and conflicts understandable. Users should be able to dispute material errors and obtain a human response. A generated trust score should not become an unexplained barrier to funding, participation, or another consequential opportunity.

18 Federation interoperability and the technical operating model

Shared interfaces and local responsibility

Light should provide documented interfaces for identity references, permissions, assets, evidence, events, treasury records, transactions, and outcomes. Integrations need clear ownership, authentication, authorization, versioning, and error handling. A useful network requires compatible meanings as well as compatible file formats.

Institutional nodes should define what data they retain locally and what they share. Agreements should identify controllers, processors, permitted purposes, retention, correction, cross-border transfers, and exit arrangements. A shared participant identifier should not become an unrestricted global dossier.

Reliable transaction processing

State changes within one service should be committed consistently. External instructions should be published only from confirmed internal records and carry unique identifiers. Retries should be safe against duplicate execution. Confirmations should be matched to the original instruction and should not be accepted solely because their format looks valid.

The design should specify how services detect out-of-order messages, missing events, stale evidence, and conflicting updates. Material asset and financial actions require stronger consistency than ordinary search results. A recently updated public dashboard should not be the authority for releasing an asset if the authoritative custody service is unavailable.

Ledgers and public networks

A shared or public ledger may support transaction references, token control, or independently verifiable commitments. Private financial and case records generally require protected storage. The selected architecture should document consensus assumptions, governance, fees, capacity, custody, finality, upgrades, and recovery.

Cross-chain representations should not create duplicate rights. If a bridge is introduced, it must define the canonical asset, locking or retirement of representations, message verification, failure handling, and legal continuity. Blockchain bridges are not part of the recommended first pilot.

Availability and offline conditions

Users with intermittent connectivity may prepare records offline, but actions requiring current control, eligibility, or funds should not finalize without the necessary checks. The interface should distinguish saved drafts from committed transactions. Deferred reporting from a custodian should carry its actual occurrence and submission times.

The network should define degraded modes. Research and read-only records may remain available when financial execution is paused. Resilience is improved by a deliberate restriction on unsafe activity rather than by presenting every service as continuously executable.

19 Governance law and institutional participation

Governance across the ecosystem

The proposed governance model separates ecosystem standards, entity management, treasury decisions, asset admission, exchange operations, and independent assurance. Shared standards should explain interoperability and minimum controls. They should not create authority over resources owned by a participant without its valid agreement.

Governing bodies should approve their mandates, delegation, budgets, risk limits, and material service changes. Conflicts should be disclosed, related-party decisions reviewed, and complaints protected from retaliation. The organization deciding a dispute should not be assumed independent merely because it operates within the same brand.

Rights and applicable law

Each material service requires analysis of the actual activity, jurisdiction, participant, instrument, and contractual structure. Tokenization does not eliminate requirements concerning property, custody, securities, commodities, payments, money transmission, data, tax, consumer protection, or sanctions where applicable. Public and member-facing statements should use the scope supported by that analysis.

UNCITRAL's Model Law on Electronic Transferable Records offers a reference for functional equivalence, control, and integrity of relevant electronic records. It is a model for enactment, not a universal law automatically governing every Neo NFT. The instrument and relevant jurisdictions must establish whether and how those concepts apply. [R7]

Governments and national programs

Institutional engagement should begin with a defined problem, responsible public counterpart, proposed service, funding structure, and evidence requirements. A government or central bank contact should not be presented as approval of the ecosystem. A memorandum supporting discussions should remain distinct from authority to handle funds or execute a project.

Country programs should preserve public procurement, budget, approval, and oversight responsibilities. Local data and sovereign considerations should be addressed through the relevant institutions. Light's global ambition is compatible with cooperation among jurisdictions; it does not require claiming a mandate to replace them.

Indigenous rights and sensitive knowledge

Communities should control representation and use of cultural knowledge, heritage, and sensitive location data. Registry participation should not transfer ownership or consent. Proposed commercial use requires the appropriate permissions and benefit arrangements. Some valuable information should remain undisclosed or uncommercialized.

20 Security resilience and participant protection

Threat model

The design should assume forged asset documents, impersonated principals, compromised keys, malicious insiders, colluding inspectors, duplicate inventory, manipulated sensors, cyberattacks, and vendor failure. It should also account for ordinary mistakes, including wrong addresses, unit conversion errors, stale account details, and inaccurate project reports.

Controls should follow the consequence of failure. A search recommendation can tolerate a different review process from an asset release. Financial and rights-changing actions require explicit authority, current evidence, independent approval where appropriate, and a complete record.

Technical controls

The proposed baseline includes strong authentication, least-privilege access, separation of duties, encryption, secure secret storage, controlled administrative access, software review, tested backups, and monitored

interfaces. Custody keys require an appropriate institutional design, recovery procedure, and protection against a single compromised device or person.

Third-party integrations should be assessed for data access, subcontractors, service continuity, incident notification, and exit. Smart contracts, if used, require independent review proportionate to their role, controlled deployment, upgrade rules, and emergency procedures. A completed code audit does not prove physical inventory or legal rights.

Recovery and incident response

The operating plan should define service priorities, recovery-time and recovery-point objectives, detection, containment, investigation, evidence preservation, notification, and restoration. Targets should be set against the actual service and tested before publication. No availability or recovery performance is asserted by this paper.

The NIST Cybersecurity Framework is a reference for organizing risk management and operational accountability. Adoption of selected practices is not the same as certification or demonstrated resilience. [R8]

Participant recourse and continuity

Participants need channels to report compromise, incorrect records, unsafe activity, and disputed transactions. Recovery of a key or account should include identity and rights checks while protecting against fraudulent replacement requests. Records should remain exportable under the governing terms if a service closes or a participant leaves.

Child protection and other sensitive programs require qualified personnel, restricted case handling, referral routes, and applicable safeguarding procedures. A community reputation mechanism should not be used as the sole basis for deciding a safeguarding case.

21 Economics participation and sustainable operation

Revenue tied to defined services

Potential operating revenue includes subscriptions, research or workflow services, project administration fees, asset admission and inspection charges, and appropriately authorized transaction services. The responsible entity should publish what each fee purchases and distinguish its charges from those of external custodians, banks, inspectors, and logistics providers.

Verification costs should not influence the substance of a review. If the platform earns transaction revenue, governance should address the incentive to admit unsuitable assets or encourage unnecessary trading. Staff compensation and referral arrangements should be visible to the relevant approving body.

Resource protection

Restricted project money and dedicated instrument reserves should not subsidize general operating deficits unless the relevant agreement lawfully permits it. Issuing internal units does not generate external cash by itself. Treasury runway should follow eligible unrestricted liquidity and forecast expenditure.

The service model must account for the cost of human verification, reconciliation, support, disputes, assurance, and local participation. Those activities do not disappear through automation. Pricing should be

tested against actual demand and affordability, with clear provision for sponsored or limited access where appropriate.

Adoption and useful network effects

Initial adoption should focus on a few communities with a real coordination problem, qualified participants, and measurable value from the workflow. A network grows in usefulness when participants contribute accurate information, complete work, and retain trust. Raw profile counts and nominal token supply do not establish that usefulness.

Organizations should be able to participate through conventional agreements and familiar payment methods. Digital instruments should be introduced where their rights and operational advantages are clear. This reduces unnecessary barriers and gives the ecosystem a practical path to adoption.

22 Illustrative complete asset transaction

Scenario and scope

The following is a hypothetical workflow, not an actual transaction, market quotation, or statement of GGT assets. Assume an eligible seller offers a lot of ten individually identified gold bars, each recorded as one kilogram gross weight with its own accepted assay and fineness information. The contract defines the relevant commercial quantity and settlement price; no current market price is assumed here.

The seller's authority, rights, encumbrances, custodian, and inspection reports are reviewed. Each bar receives a canonical asset identity. A lot record groups the ten bars without creating a second independent claim over the same quantity. The Neo representation links to the approved lot rights and current evidence.

Quote acceptance and reservation

A qualified buyer requests a quotation. The seller provides a firm offer identifying the ten bars, quantity basis, settlement asset, fees, delivery choice, and expiry. Acceptance creates a trade record and locks the lot against incompatible trading or pledging. The buyer sees the latest eligible evidence and the exact obligation it is acquiring.

The buyer funds the agreed settlement mechanism. The provider confirms the required payment state through a verified channel. The system checks that the custodian's acknowledgement and rights conditions remain valid. A stale inspection, new lien, or quantity discrepancy would suspend execution for review.

Rights transfer in custody

Assume the buyer elects to leave the bars in approved custody. The transaction terms define the legally effective transfer and the custodian's recognition of the buyer's entitlement. The Neo control record is updated through the permitted workflow, the custodian acknowledges the change, and the settlement provider releases payment when the agreed conditions are met.

The final record connects the contract, asset lock, evidence versions, payment confirmation, rights change, custody acknowledgement, and fees. Reconciliation confirms that each bar appears once in inventory and that no conflicting active claim remains. A public market summary can show an eligible completed transaction without disclosing private commercial documents.

Later delivery or pledge

If the buyer later requests physical delivery, the withdrawal workflow verifies its authority, resolves fees and restrictions, arranges logistics, and discharges the tradable custody claim. The historical twin remains. If the buyer instead pledges the lot under a valid financing agreement, the encumbrance record changes and incompatible sale is blocked until release.

This example demonstrates the purpose of the full architecture. Identity establishes the actors. Evidence supports admission. Policy governs actions. The exchange organizes agreement. Settlement providers move value. Custody maintains the physical relationship. The Neo twin preserves continuity across those events.

23 Illustrative development and impact workflow

A defined need and delivery team

This example is hypothetical and is not a funded GGT program. Assume a regional cooperative needs a cold-storage facility to reduce crop losses. A researcher documents the need and baseline. A local operator, technical partner, and supplier develop a proposal covering site authority, energy, capacity, user access, operating costs, maintenance, and approvals.

The Light platform connects those participants and records their responsibilities. A funder reviews the proposal under its program criteria. The resulting agreement identifies the instrument, recipient, eligible budget, conditions, procurement rules, milestone evidence, and reporting. GGT's treasury records the commitment separately from cleared receipts.

Procurement linked to physical assets

The equipment supplier provides serial identities, specifications, warranties, and required test evidence. Where useful, Neo twins support records for major equipment. Their role is maintenance and provenance unless a separately defined tradable right is established. Installing a twin does not turn every project item into an investment instrument.

Payments follow the agreed procurement and milestone structure. Delivery records connect to invoices and accepted equipment. Installation and commissioning require the designated technical acceptance. The project workspace preserves changes, delays, and corrective decisions alongside successful milestones.

Service and learning

After handover, the operator records utilization, service reliability, maintenance, user charges, and crop-loss observations under the agreed method. The outcome report explains baseline, period, seasonal effects, and limitations. Private user or business data remains protected.

The treasury closes the project accounts and handles unused resources under the agreement. The platform compares the outcome with the original objective. A future replication decision uses the operating evidence, cost, and local conditions. Successful delivery contributes knowledge to the wider network without implying a financial return to unrelated token holders.

24 Implementation sequence and acceptance criteria

Foundation and common records

The first phase should establish entity responsibilities, service boundaries, the authority model, common identifiers, evidence classifications, participant terms, and the claim register. Acceptance requires coherent records and a demonstrated ability to correct, revoke, and export them. The initial platform should avoid financial commitments beyond its actual capacity.

Asset twin pilot

The second phase should admit a limited asset class with an identified owner, qualified verifier, contracted custodian, defined rights, and a single registry domain. Acceptance requires an end-to-end trace from physical inspection to current twin state, including duplicate detection, evidence expiry, a discrepancy, and controlled withdrawal.

Exchange and settlement pilot

The third phase should test a bounded spot transaction through an appropriate settlement provider. Acceptance requires a consistent trade record, effective inventory lock, verified funding status, rights and custody updates, fee reconciliation, and resolution of a failed or disputed transaction. No derivatives, fractional products, or bridges are assumed in this first market pilot.

Treasury and project pilot

A parallel or subsequent pilot should demonstrate cleared funding, restricted-resource treatment, approved release, supplier delivery, milestone acceptance, and outcome reporting. It should show that physical records and financial books reconcile, and that evidence supports the claimed result.

Federation and expansion

Expansion should follow independent review of legal scope, security, reliability, costs, participant recourse, and delivery outcomes. New jurisdictions, asset classes, instruments, and providers each require assessment. A successful interface demonstration should not be generalized into evidence of global production capacity.

No completed phase, launch date, throughput, asset balance, or financial return is asserted here. The roadmap is sequenced by demonstrable prerequisites. Leadership should attach schedules and budgets after personnel, agreements, dependencies, and acceptance methods are established.

Appendix A Neo twin record specification

The following is a proposed minimum data specification. Product-specific fields and access rules should supplement it. A field records a fact or assertion with provenance; its presence alone does not prove the assertion.

Record group	Minimum content	Required distinction
Canonical identity	Asset identifier registry domain issuer and lifecycle links	One physical identity can have several records but not unexplained competing claims

Record group	Minimum content	Required distinction
Physical description	Object or lot type serials quantity units grade and condition	Measurement identity and commercial entitlement may use different bases
Rights and parties	Owner claimant controller representative and governing terms	Key control custody and ownership remain distinct
Physical binding	Identification method seals images inspection and relevant fingerprints	Tags and images support checks but can be copied or become stale
Custody	Custodian agreement location access scope and acknowledgement	Secure location details need restricted visibility
Evidence	Issuer reviewer method date version expiry and limitations	Verification belongs to a defined claim and time
Encumbrances	Pledges liens holds competing claims and release terms	An existing right may limit availability for another action
Market state	Eligibility quote trade lock suspension and current policy version	Listing is different from trade completion
Quantity lineage	Parents children transformation inputs outputs losses and units	Eligible claims must reconcile after physical changes
Settlement	Agreement instructions confirmations fees and finality status	Submission confirmation reconciliation and legal finality differ
Delivery	Release authority logistics handover acceptance and claim discharge	Physical movement and financial settlement are separate events
Continuity	Recovery replacement retirement and authorized historical access	Retiring a tradable claim need not erase the asset history

Appendix B Transparency and access matrix

This matrix describes a proposed access model. Specific access follows law, consent, legitimate purpose, contracts, and service responsibilities. Publication should also consider inference risk from combining apparently harmless fields.

Information	Intended audience	Design requirement
Product rules fees and service status	Public and prospective participants	Clear version dates and material limitations
Aggregate resources and outcomes	Public where approved	Definitions as-of dates exclusions and assurance scope
Asset eligibility and relevant proof	Qualified transaction counterparties	Current scoped evidence with protected security details

Information	Intended audience	Design requirement
Identity and representation evidence	Authorized reviewers and relevant providers	Minimum necessary disclosure with access records
Detailed contracts and instructions	Parties responsible providers and authorized reviewers	Confidential versioned records and documented reliance
Full financial and inventory reconciliations	Responsible management assurance and competent authorities	Traceable books supporting evidence and exception access
Child protection or sensitive community records	Qualified authorized personnel only	Separate restricted workflow and safeguarding procedures
Audit history and corrections	Access appropriate to the issue and role	Preserve material accountability while respecting data rights

Appendix C Critical acceptance and failure tests

The proposed tests establish what a pilot should demonstrate. They are not claims that a deployed Light system has passed. Test records should identify the configuration, expected result, actual evidence, reviewer, and unresolved exceptions.

1. An unauthorized user cannot view protected evidence or execute a rights-changing action through either the interface or direct service requests.

2. Revoking a representative's authority prevents new commitments while preserving the lawful history of actions taken during a valid mandate.

3. An expired or withdrawn inspection blocks a transaction requiring that evidence and informs affected authorized participants.

4. A duplicate asset identity or overlapping lot cannot create a second eligible claim without review and reconciliation.

5. Concurrent purchase attempts cannot sell the same eligible inventory twice. A pending pledge blocks an incompatible sale under the product rules.

6. A split or processing event preserves quantity and lineage according to the approved measurement and loss rules. Consumed parent claims cannot remain independently tradable.

7. Delayed messages retries and repeated confirmations do not duplicate payments issuance or asset releases. Conflicting confirmations create an exception.

8. Failure of a settlement leg follows the agreed unwind or exception process. The system never reports an irreversible external action as reversed merely because its internal status changed.

9. Physical withdrawal discharges or updates the relevant tradable claim and custody record. Reentry requires current evidence and linkage to the prior lifecycle.

10. Lost credentials or compromised keys can be addressed through the approved recovery process without creating two simultaneously exercisable representations of the same claim.

11. A malicious uploaded document cannot instruct an AI agent to expose private data grant itself permissions or initiate an unauthorized transaction.

12. A project release cannot exceed its eligible resources or bypass required acceptance. Final reporting reconciles funding spending unused resources and the evidence supporting the outcome.

13. Service interruption triggers the approved degraded mode and a tested recovery. Records restored from backups remain consistent with external confirmations.

14. A material public claim can be traced to current supporting evidence. Revocation or correction updates affected disclosures and reporting.

Appendix D Definitions and architectural invariants

Light ecosystem means the proposed network of participants, services, agreements, and productive activity described in this paper. Light Financial System means its financial information and integration architecture. A component name does not establish legal status or deployment.

Neo NFT means the founder's proposed digital twin representation for a physical object or defined lot. The twin contains identity and lifecycle context; the separate rights record specifies any legally effective entitlement. The term does not select a blockchain or assert affiliation with an unrelated Neo product.

Global Digital Commodity Exchange means the proposed arm organizing admitted commodity transactions and related workflows. GDTX in earlier Global.1 materials is a related exchange concept; naming, legal operator, product scope, and any final acronym should be reconciled before publication or launch.

Canonical identity means the recognized identity for an asset within a specified registry domain. A canonical record is not a guarantee that no false or competing representation exists outside that domain.

Custody means holding or controlling an asset under an applicable arrangement. Ownership, beneficial interest, a delivery claim, a security interest, and administrative authority describe different rights. Possession of a digital key does not resolve all of them.

Attestation means a statement by an identified issuer concerning a defined fact or condition. Verification establishes only the scope actually reviewed. An oracle supplies external information to a system; it cannot remove the risk of inaccurate external information.

Settlement finality means the legally relevant completion of an obligation under applicable rules. Technical confirmation and financial reconciliation contribute evidence but need not establish the same fact.

Reserve backing means eligible resources supporting a defined obligation. The wider reserve of knowledge, relationships, and capability should not be counted indiscriminately as financial backing.

The proposed invariants are practical requirements. One physical interest should not support incompatible exercisable claims. Material asset changes require maintained records. Every financial release requires authority and eligible capacity. Evidence must remain scoped and current for its use. Participant rights must remain understandable through failure, correction, and closure. The model should preserve these requirements across every application and integration.

Appendix E Sources evidence and design status

The research cutoff is 6 November 2026. Founder materials establish intended scope and vision. Public descriptions establish what a source states. Official standards and principles inform design considerations without endorsing Light. All extended architecture, workflows, controls, and examples in this paper are proposals unless explicitly identified otherwise. No independent production audit was performed.

[F1] Light Financial System architecture specification supplied in Pasted text(2).txt and discussed in Refine Financial Core. Planning source for banking, treasury, assets, commerce, intelligence, settlement, identity, governance, and interface workstreams. A build specification is not evidence of completed implementation.

[F2] Founder mission manuscript and planning discussions in Designing A Light Financial System. Source for coordinated impact, purpose-aware value, research, human capability, the Light Alliance, and measurable outcomes. Earlier narrative drafts were treated as planning material rather than independent factual evidence.

[F3] Gaia Global Treasury Institutional White Paper and Gaia Global Treasury Reserves The Umbrella Treasury Arm. Companion discussion papers prepared in this conversation. Used for consistency of the proposed resource categories, reserve concepts, and institutional distinctions; not independent evidence of assets, authority, or deployment.

[F4] Current founder instruction. Extends the Light ecosystem to include a Global Digital Commodity Exchange and identifies the Neo NFT as the digital twin of a physical object. The detailed lifecycle and operating design in this paper develop that instruction as proposed architecture.

[P1] Gaia Global Treasury About. Public description of collaboration and stewardship tools and the technology-platform notice, reviewed during the related papers. https://gaiaglobaltreasury.org/About

[P2] Global.1 homepage and existing white paper. Reviewed in the browser during the related papers. Context for GGT, GGG, member participation, and the GDTX exchange concept. No asset backing or legal effect is independently established by those descriptions. https://gaiaglobal.one/ and https://gaiaglobal.one/whitepaper

[R1] W3C. Verifiable Credentials Data Model v2.0, Recommendation dated 15 May 2025. Reference for credential representation and presentations; issuer trust and business acceptance remain implementation responsibilities. https://www.w3.org/TR/vc-data-model-2.0/

[R2] GS1. EPCIS Standard and official explanatory material on Electronic Product Code Information Services. Reference for interoperable supply-chain events and physical observations. No conformance is asserted. The commercial overview page could not be fetched directly; the standards reference and official explanation were retrieved. https://ref.gs1.org/standards/epcis and https://support.gs1.org/support/solutions/articles/43000755325-what-is-electronic-product-code-information-services-epcis-

[R3] CPMI and IOSCO. Principles for Financial Market Infrastructures. Reference for legal basis, finality, linked exchanges, governance, and operational risk; not a determination that Light is an FMI or complies with the principles. https://www.bis.org/committees/cpmi/pfmi/overview

[R4] Ethereum Improvement Proposals. ERC-721 Non-Fungible Token Standard. Reference for one possible NFT interface. The standard does not itself determine a physical-asset rights structure. https://eips.ethereum.org/EIPS/eip-721

[R5] UNIDROIT. Principles on Digital Assets and Private Law, adopted in 2023. Principle 4 and related commentary concern linked assets and the role of applicable other law in establishing the link and its effects. https://www.unidroit.org/instruments/digital-assets-and-private-law/overview/ and https://www.unidroit.org/wp-content/uploads/2024/01/Principles-on-Digital-Assets-and-Private-Law-linked-1.pdf

[R6] NIST. AI Risk Management Framework. Voluntary reference for AI governance, evaluation, and monitoring. No certification is implied; revisions and relevant current guidance should be assessed during implementation. https://www.nist.gov/itl/ai-risk-management-framework

[R7] UNCITRAL. Model Law on Electronic Transferable Records, adopted 13 July 2017. Reference for functional equivalence, control, and integrity of relevant electronic records. The official page's indexed text was retrieved after direct access was blocked. Local enactment and applicable substantive law require separate assessment. https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_transferable_records

[R8] NIST. Cybersecurity Framework and CSF 2.0 resources. Reference for organizing cybersecurity risk management. No implementation, performance, or certification claim is made. https://www.nist.gov/cyberframework