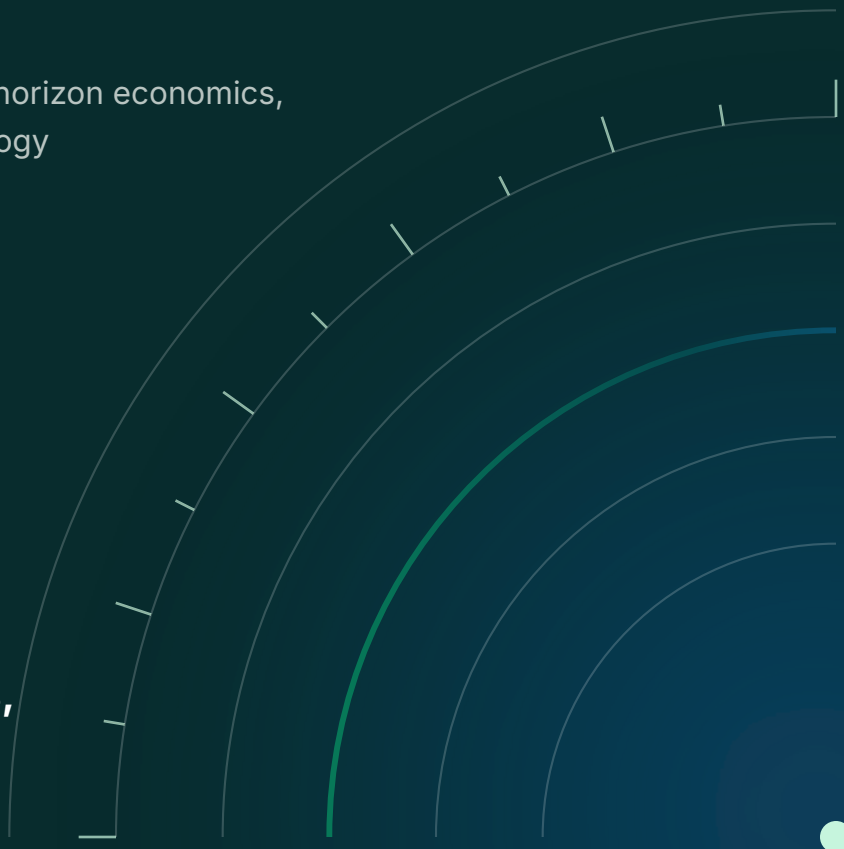
METRIQ

FOUNDATION

LONG-HORIZON SYSTEMS

# Metriq White Paper

Network architecture, long-horizon economics, and public-purpose technology



100+

YEAR HORIZON

**Building for centuries, not cycles.**

VERSION 6.0 / JULY 2026

PUBLICATION REVIEW DRAFT

# Document Control and Publication Notice

This draft replaces the October 2025 public white paper as the working basis for final publication.

| Field | Value |
|---|---|
| Document | Metriq White Paper |
| Version / date | 6.0 / 15 July 2026 |
| Owner | Metriq Foundation, Inc. |
| Status | Publication review draft |
| Scope | Metriq Foundation, Metriq Network, MTRQ, Gravity, OrbitR, Metriq Dynamics, the proposed Centurial Fund, and the operating model that connects them. |
| Supersedes | Metriq Whitepaper version published October 2025. |
| Primary audience | Builders, operators, partners, funders, researchers, prospective users, reviewers, and governance participants. |
| Publication gate | Do not treat this draft as final until board, legal, technical, economic, security, and claims review are complete. |

**IMPORTANT LIMITATION**

This paper is a technical and strategic description, not an investment offering, legal opinion, tax opinion, regulatory certification, audit report, warranty of network performance, or promise that every proposed capability will be delivered. MTRQ is described as the native coin of the Metriq Network; this paper does not represent MTRQ as equity, debt, a claim on Foundation assets, or a right to Foundation profits.

**PUBLICATION DISCIPLINE**

The final public version should preserve explicit evidence states. A roadmap item must remain labeled Proposed until it exists. A benchmark must remain labeled Simulated until its method and environment are published. Production claims require production evidence.

## Evidence-state legend

| State | Meaning | Minimum evidence |
|---|---|---|
| Implemented | Exists in working form. | Inspectable code, service, policy, transaction record, or operating artifact. |
| Simulated | Tested under bounded assumptions. | Configuration, method, dataset or workload, sample window, and results. |
| Proposed | Defined but not delivered. | Design rationale, owner, dependencies, release gate, and known risks. |
| Production validated | Demonstrated under production conditions. | Published method, operating window, exceptions, incidents, and attributable evidence. |

# Contents and Reading Guide

The paper separates current implementation from proposed architecture and separates corporate governance from network consensus.



## How to read this paper

- Organization and governance: Sections 1, 2, 4, 7, 9, 10, and 14.
- Network and software: Sections 5, 6, 11, Appendix A, and the cited repositories.
- Treasury and economics: Sections 6 and 7, Appendix B, and the risk analysis.
- For deployed protocol behavior, reviewed production code and configuration remain authoritative.

# Executive Summary

Metriq is a nonprofit technology builder organized around a direct proposition: build useful systems, deploy them in the real world, and reinvest the value they create into the next generation of technology and mission work.

Metriq Foundation, Inc. is a Florida nonprofit corporation developing infrastructure, software, products, and operating companies. The organization is not designed as a conventional charity whose primary function is fundraising and redistribution. Its intended model is operational: create technical capability, place that capability into real use, generate durable economic and institutional value, and direct that value back into a long-term public-purpose mission. [1][7]

The mission is expressed through three priorities: increase abundance; protect wildlife; and improve health, safety, and access. These priorities are deliberately concrete. They describe outcomes that can be observed, measured, and challenged. They do not require every Metriq project to look philanthropic. A payment system that materially lowers transaction costs, a manufacturing process that increases productive capacity, a traceability system that reduces fraud, or a conservation platform that improves field response can all advance the mission if the results are real and attributable.

The Metriq Network is the decentralized ledger and transaction layer. Gravity is the core and node implementation. OrbitR is the client-facing API and indexing layer. MTRQ is the native coin of the Metriq Network. Metriq Dynamics is a Foundation-owned manufacturing and engineering subsidiary. These names describe different legal, technical, and economic objects; they should not be collapsed into one label.

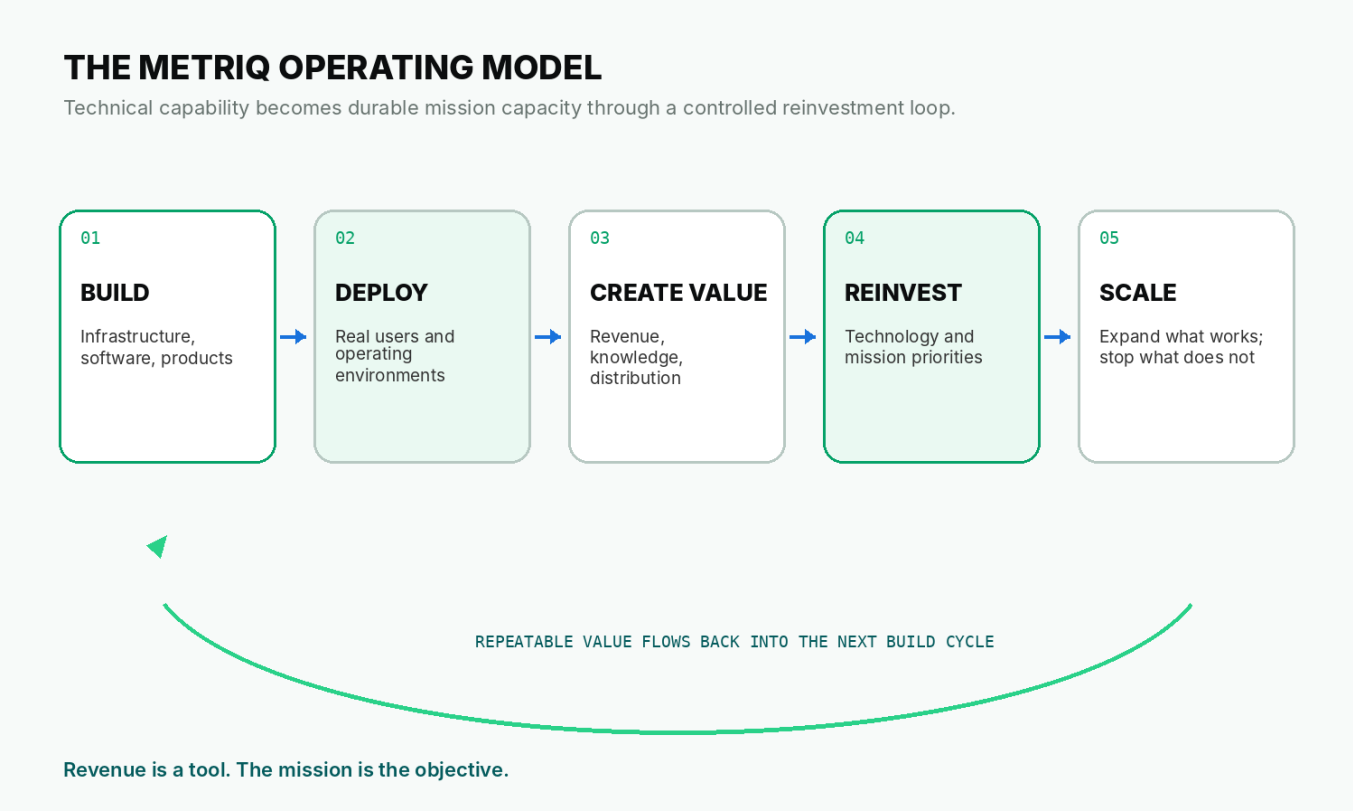



Figure 1. The operating model: build, deploy, create value, reinvest, and scale.

## Current foundation

Public code exists for Gravity and OrbitR. Gravity describes a replicated state machine that maintains a cryptographic ledger and reaches consensus with peers using a modified form of the Stellar Consensus Protocol. OrbitR exposes network functions to applications, including transaction submission, account status, and event streams. Metriq also publishes a network portal identifying a public OrbitR endpoint, four Metriq-operated validators, validator history archives, and a laboratory interface. These are implemented artifacts, but their existence does not by itself establish production scale, independent decentralization, audited security, or a particular throughput or finality level. Those conclusions require separate evidence. [3][4][5]

The documented economic design states a fixed genesis supply of one trillion MTRQ, divided between a 900 billion MTRQ century-scale allocation and a 100 billion MTRQ seed allocation. Equal division of the century-scale amount across one hundred years yields nine billion MTRQ per year. This arithmetic is straightforward; the hard work is institutional. Before the proposed Centurial Fund can be represented as an operating system of long-term funding, Metriq must reconcile the design against authoritative ledger records, establish custody and key controls, adopt an allocation charter, define conflicts and approval thresholds, publish reporting methods, and determine how market, tax, accounting, and regulatory constraints affect each use of funds.

The current public profit commitment is that 100% of profits are pledged to public benefit. The commitment is central to the model but requires precise governing language. Final policy should define which entities are covered; whether the operative term is profit, distributable profit, or another measure; how taxes, reserves, capital expenditure, debt service, working capital, and restricted funds are treated; when transfers occur; who approves them; and how compliance is reported. Precision strengthens the commitment. Ambiguity weakens it.

## Strategic thesis

**Technology is the primary instrument.**

Metriq should be judged by the systems it builds, the problems those systems solve, and the operating evidence behind its claims.

**The nonprofit structure changes the destination of value.**

Growth is not rejected. Revenue, product adoption, technical knowledge, data, distribution, and operating capacity can all expand the mission.

**Long horizons can support neglected infrastructure.**

A century-scale allocation can fund work that conventional venture and budget cycles underweight, but only if governance survives leadership, market, and technology changes.

**Evidence must remain ahead of promotion.**

Claims about speed, cost, scale, decentralization, impact, security, and adoption should be tied to published methods and explicit evidence states.

## What this revision changes

- Replaces broad Web3 positioning with a specific operating and institutional thesis.
- Removes unsupported throughput, finality, fee, interoperability, and production-readiness claims.
- Separates implemented software and services from simulated results and proposed programs.
- Standardizes current naming: Metriq Foundation, Metriq Network, MTRQ, Gravity, OrbitR, Metriq Dynamics, and Centurial Fund.
- Replaces a calendar-heavy roadmap with release gates tied to evidence, security, governance, legal review, and production validation.
- Expands the analysis of treasury controls, network concentration, quorum risk, key custody, software supply chain, data governance, market risk, and mission drift.
- Makes impact measurement operational rather than rhetorical.

# Purpose, Mission, and Scope

Metriq exists to build technologies and institutions that produce measurable real-world results over long time horizons.

## 2.1 What Metriq is

Metriq is a technology organization with a nonprofit owner and a long-term public-purpose mandate. It develops open infrastructure, maintains software, forms operating companies, undertakes technical programs, and may allocate capital to projects that advance the mission. The Foundation is the governance and ownership center. It is not synonymous with the Metriq Network, and the network is not synonymous with MTRQ.

This structure is intended to combine two capabilities that are often separated. Technology companies can build, sell, operate, and scale, but their governing objective typically centers on shareholder value. Conventional nonprofit organizations can pursue a public mission, but many lack the product, engineering, commercialization, and capital formation capability needed to build complex infrastructure. Metriq is designed to operate in the gap: use company-building and technical execution as instruments of a nonprofit mission.

**PLAIN-LANGUAGE POSITION**

Metriq builds infrastructure, products, and companies. The value they create is intended to support further technology development and mission-aligned work.

## 2.2 Mission priorities

The mission is not defined by a favored technology. Blockchain, artificial intelligence, manufacturing systems, data infrastructure, cryptography, robotics, communications, and conventional software are means, not ends. A project belongs in the Metriq portfolio only when there is a credible chain from technical work to a mission outcome.

| Priority | Operational meaning | Illustrative questions |
|---|---|---|
| Increase abundance | Lower unit costs, expand productive capacity, increase availability, and widen access to useful goods, services, infrastructure, and knowledge. | Does the system produce more with fewer scarce inputs? Does it lower total cost? Does access expand without creating unacceptable risk? |
| Protect wildlife | Use technology, capital, data, field operations, and partnerships to protect wildlife, habitat, and biodiversity. | Does the system improve detection, prevention, response, enforcement, habitat management, or conservation financing? |
| Improve health, safety, and access | Build or support technologies that improve health, increase safety, remove practical barriers, and extend effective services. | Who gains access? What risk is reduced? What time or cost is saved? What adverse outcomes are avoided? |

## 2.3 Mission tests

A project should not qualify merely because it uses advanced technology or carries positive language. Before resources are committed, the responsible team should state the mission pathway in falsifiable terms: the problem, intended user, mechanism of change, baseline, output, outcome, measurement window, owner, external dependencies, and reasons the project might fail.

- Usefulness: the system solves a material problem for a defined user or operating environment.

- Additionality: Metriq adds capability, capital, coordination, or time horizon that would not otherwise exist on comparable terms.
- Scalability: the result can expand without impact quality collapsing or unit economics becoming irrational.
- Durability: the system can be maintained, governed, funded, and secured after the initial launch.
- Attribution: Metriq can distinguish its contribution from broader market, policy, or partner effects.
- Risk proportionality: technical, financial, legal, safety, and reputational risks are appropriate to the expected outcome.

## 2.4 Scope exclusions

This paper does not provide a protocol specification, source-code audit, offering document, token valuation, tax characterization, charitable-solicitation filing, grant agreement, investment policy, or Foundation bylaws. It also does not disclose patent-sensitive details of Metriq Trade Traceability or proprietary details of Metriq Dynamics systems. Those subjects require separate controlled documents.

The paper describes a target institutional architecture and the presently visible implementation baseline. It does not claim that every policy, committee, fund, product, benchmark, or control described here is already operating. Appendix A records the evidence state assigned to each material capability for this draft.

# Problem Definition and Design Response

Metriq is designed around a set of recurring failures in technology development, infrastructure funding, and mission delivery.

## 3.1 Short-horizon capital

Many infrastructure problems are difficult not because a technical path is unknown, but because the payoff period, coordination burden, or public value does not fit conventional financing. Venture capital optimizes for a finite fund life and high-return exits. Public budgets are exposed to political cycles and procurement friction. Donations are volatile and often restricted. Corporate research budgets can disappear when strategy changes. As a result, foundational work may remain underfunded even when its downstream value is substantial.

A long-horizon treasury can address part of this mismatch, but only if it does more than hold an asset. It must convert time into disciplined allocation. That requires custody, diversification, conflict controls, technical review, staged release, performance monitoring, and the ability to terminate weak programs. A century-long label without these controls is branding, not institutional design.

## 3.2 Misaligned destinations of value

Technology can lower costs and increase productive capacity while concentrating the value it creates in a small ownership group. The Metriq model does not reject profit or scale. It changes their destination. When an operating company, product, or network-linked service succeeds, the resulting value should strengthen the system that created it and support the mission, subject to lawful reserves and operating requirements.

This creates a different optimization problem. Metriq must still compete on product quality, reliability, price, delivery, security, and user experience. Mission status does not excuse weak execution. At the same time, management should not pursue growth that creates material mission conflict, unmanaged legal exposure, unsafe products, extractive user economics, or reputational risk disproportionate to the expected benefit.

## 3.3 Fragmented technical and institutional layers

Decentralized networks are often discussed as if consensus software alone constitutes a usable system. In practice, adoption depends on the full stack: node software, API services, client libraries, documentation, identity and key management, monitoring, incident response, compliance interfaces, business integration, support, and a credible operator ecosystem. Technical components and institutions must be designed together without confusing their roles.

Metriq responds with distinct layers. Gravity maintains and validates ledger state. OrbitR provides application-facing access and indexing. The Metriq Network is the shared transaction layer. The Foundation governs organizational assets and mission resources. Metriq Dynamics provides a commercial manufacturing and engineering path. Future programs can use these capabilities without implying that every program belongs on-chain or that blockchain is the right tool for every problem.

## 3.4 Claim inflation

Emerging-technology organizations routinely convert laboratory targets into public facts. Throughput is quoted without workload or hardware. Finality is stated without percentile distributions or failure conditions. “Decentralized” is inferred from node count without quorum analysis. “Secure” is used without a threat model. “Impact” is measured by money announced rather than outcomes delivered. These practices can accelerate attention, but they also create technical debt in the organization’s credibility.

Metriq’s response is an evidence-state system. Every material claim should identify whether it is implemented, simulated, proposed, or production validated. The underlying evidence should name the owner, date, environment, method, limitations, and source. This is not merely a communications standard. It is a management control that prevents leadership, engineering, legal, and public materials from describing different realities.

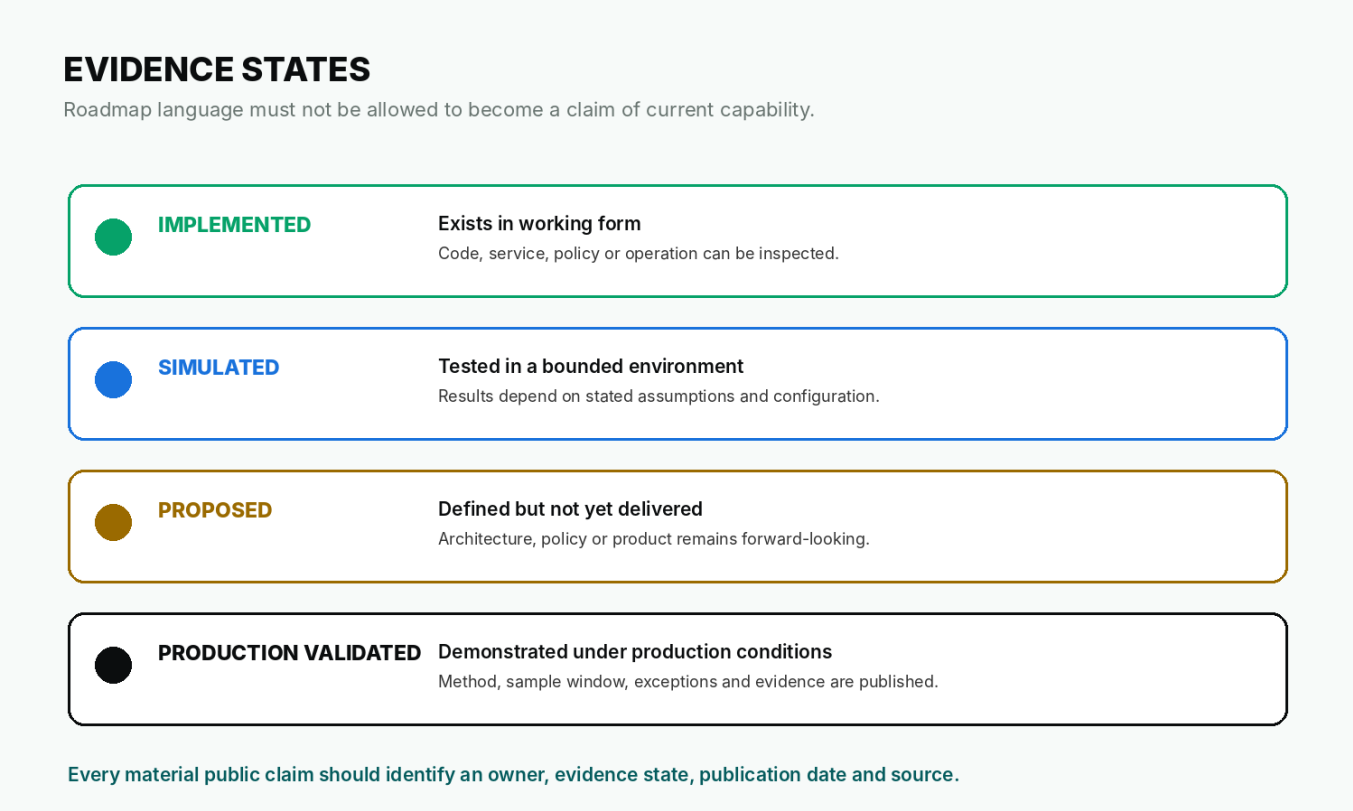



Figure 2. Evidence states used throughout this paper.

## 3.5 The resulting design requirements

| Problem | Design response | Failure if absent |
|---|---|---|
| Short capital horizons | Century-scale release design with staged controls and periodic reauthorization. | Capital is exhausted, stranded, or deployed on projects that cannot survive market cycles. |
| Value concentration | Foundation ownership and a defined profit commitment. | Commercial success separates from the mission or becomes dependent on voluntary leadership choices. |
| Technology without adoption | Operating companies, product pathways, integration support, and user-focused deployment. | The network remains an engineering artifact without durable users. |
| Institutional opacity | Entity boundaries, public reporting, evidence states, conflict controls, and auditability. | Users cannot determine who controls what, which claims are current, or how resources are allocated. |
| Network concentration | Independent operators, quorum analysis, geographic and infrastructure diversity, and transparent validator information. | A nominally decentralized network depends on a small group, hosting provider, or key set. |
| Mission rhetoric without measurement | Outcome definitions, baselines, attribution, cost-effectiveness, and termination criteria. | Programs optimize for announcements, activity, or branding rather than results. |

## 3.6 Cross-layer implications

The design responses are mutually dependent. A long-horizon treasury cannot compensate for weak products, a nonprofit owner cannot make an unreliable network useful, and open source code cannot establish decentralization when operations remain concentrated. Each layer must satisfy its own operating standard while exposing enough evidence for the other layers to rely on it.

The architecture should therefore be managed as a set of controlled interfaces rather than a single brand narrative. Treasury releases depend on reconciled balances and approved purposes. Product launches depend on user, technical, economic, security, and legal evidence. Network claims depend on observable software, service, operator, and quorum data. Mission claims depend on baselines, outcomes, attribution, and full cost.

This approach favors staged commitments, explicit owners, reversible decisions, and termination authority. It also makes failure more informative. A failed pilot with preserved evidence can improve the next decision; an unbounded program without a stopping rule only consumes capacity and obscures responsibility.

# Entity Boundaries and Operating Model

A coherent ecosystem requires explicit ownership, authority, and responsibility at every layer.

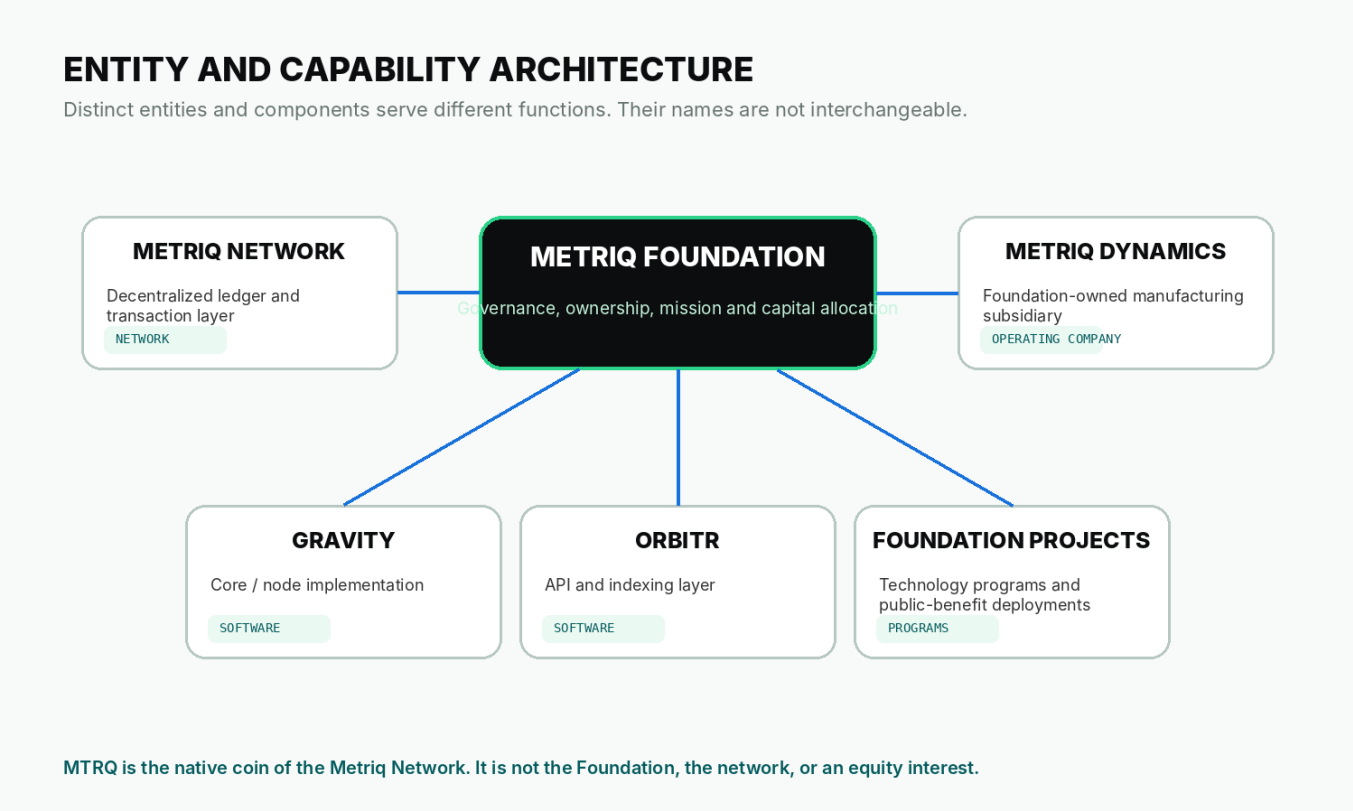



Figure 3. Metriq entity and capability architecture.

## 4.1 Metriq Foundation

Metriq Foundation, Inc. is the organizational and governance center. It holds the nonprofit mission, appoints or oversees organizational leadership under its governing documents, owns or controls designated intellectual property and subsidiaries, adopts treasury and grant policies, and is responsible for accurate public claims about Foundation activities. The Foundation may operate technical services, but its authority over organizational assets should not be confused with unilateral authority over a decentralized network.

## 4.2 Metriq Network

The Metriq Network is the shared ledger and transaction environment created by nodes running compatible software and selecting trust relationships sufficient to reach consensus. The network's decentralization is a property of actual operator independence, quorum structure, software diversity, infrastructure diversity, and control distribution. It is not established merely by calling the network decentralized.

## 4.3 MTRQ

MTRQ is the native coin of the Metriq Network. It is used by the protocol for network-native operations, including payment of configured transaction fees and other functions supported by the ledger. MTRQ should not be described as ownership in Metriq Foundation or Metriq Dynamics, a contractual claim on profits, or an entitlement to Centurial Fund allocations unless a separate, legally valid instrument expressly creates such a right.

## 4.4 Gravity

Gravity is the Metriq core and node implementation derived from the Stellar Core codebase. It maintains a local ledger copy, validates and applies transactions, participates in consensus, and exposes administrative and peer functions needed to operate a node. Public source code is an important transparency mechanism, but code availability is not a substitute for reviewed release processes, secure configuration, dependency management, reproducible builds, vulnerability handling, or operator competence. [4]

## 4.5 OrbitR

OrbitR is the application-facing API and indexing layer derived from Horizon. It sits between client applications and Gravity, enabling applications to submit transactions, query accounts and ledger state, and subscribe to event streams. OrbitR is not the consensus layer and should not be treated as the authoritative source of ledger truth when a direct ledger or node-level verification is required. [3][5]

## 4.6 Metriq Dynamics

Metriq Dynamics, Inc. is a Foundation-owned manufacturing and engineering subsidiary. Its role is to turn product intent into physical output and repeatable production capability through machining, additive processes, engineered products, advanced surfaces, assembly, testing, process planning, and automation. It creates a commercial path that can generate revenue, production knowledge, supplier relationships, equipment capability, and operating data. Those capabilities can support the Foundation mission, but the subsidiary remains subject to customer, safety, quality, export-control, employment, tax, and corporate obligations distinct from network governance. [7]

## 4.7 Foundation projects and future operating entities

The Foundation may undertake projects directly or form additional entities when a distinct liability, regulatory, capital, staffing, or market structure is justified. New entities should not be created merely to brand a program. Each entity should have a written purpose, ownership map, reserved powers, board or manager authority, financial reporting path, intellectual-property rules, conflict policy, dissolution treatment, and relationship to the profit commitment.

## 4.8 Build, deploy, create value, reinvest, scale

The operating loop begins with a defined problem and a build decision. Metriq then develops the minimum credible capability needed to test the thesis, deploys it with real users or operating partners, measures the technical and economic result, and determines whether the capability should be expanded, revised, licensed, transferred, maintained as infrastructure, or terminated. Value can take multiple forms: revenue, margin, code, patents, datasets, operational knowledge, distribution, supplier access, trained personnel, credibility, or reduced cost.

Reinvestment is not automatic spending. It is a capital-allocation decision. Resources should be directed to the next highest-value mission opportunity after considering liquidity, reserves, operating obligations, risk concentration, technical dependencies, and the expected marginal result. Projects that fail should be closed or redesigned. The discipline to stop weak work is part of the mission.

**OPERATING RULE**

No entity should rely on mission language to avoid ordinary standards of product quality, financial control, legal compliance, security, or customer service.

## 4.9 Responsibility matrix

| Domain | Primary responsibility | Required boundary |
|---|---|---|
| Foundation governance | Board and authorized Foundation officers | Corporate decisions must follow governing documents and conflict controls. |
| Network consensus | Independent validator operators through configured quorum relationships | The Foundation cannot claim decentralized consensus where operators or quorum sets remain materially controlled. |
| Protocol releases | Maintainers and approved release process | Release authority, signing keys, build provenance, testing, and emergency procedures must be documented. |
| MTRQ treasury | Authorized custodians and treasury governance | No single individual should have unilateral transfer authority over material balances. |
| Commercial operations | Management of each operating company | Subsidiary obligations and customer funds must remain separately accounted for. |
| Mission allocation | Foundation under board-approved policy | Programs require documented purpose, diligence, milestones, evidence, conflicts, and closeout. |
| Public claims | Named claim owner with legal/technical review | Every material claim must have an evidence state, source, date, and approval path. |

# Metriq Network Architecture

The network is a layered system: consensus and ledger state in Gravity, application access and indexing in OrbitR, and governance distributed among actual operators and users.

## 5.1 Architectural baseline

Gravity publicly describes itself as a replicated state machine that maintains a local copy of a cryptographic ledger and processes transactions in consensus with peers. The implementation uses a modified form of the Stellar Consensus Protocol, a construction of Federated Byzantine Agreement. OrbitR provides the client-facing API between applications and Gravity. Metriq's public portal identifies four Metriq-operated validator endpoints, a public OrbitR endpoint, validator history archives, and a laboratory interface. [3][4]

For this paper, these artifacts are classified as Implemented because code and public services can be inspected. The classification is deliberately narrow. It does not state that the network has achieved a particular user count, value secured, independent validator set, geographic distribution, throughput, latency, uptime, adversarial resilience, or external audit result.

| Layer | Function | Current evidence state | Primary verification source |
|---|---|---|---|
| Gravity | Ledger validation, transaction application, peer communication, consensus participation, history and node operations. | Implemented | Public source repository, build/test artifacts, node configuration, and live operator evidence. |
| OrbitR | Transaction submission, account and ledger queries, event streams, indexing, and application-facing API services. | Implemented | Public source repository, API endpoint, service monitoring, and integration tests. |
| Metriq Network | Shared state produced by compatible nodes and overlapping quorum relationships. | Implemented, with decentralization unvalidated | Node observations, quorum configuration, history archives, network telemetry, and independent operator evidence. |
| Smart-contract capability | Programmable contract execution beyond native ledger operations. | Proposed unless a reviewed production release is demonstrated | Protocol release, execution environment, security review, documentation, and production transactions. |
| Cross-network bridges | Movement or representation of assets and data across networks. | Proposed | Bridge design, custody model, verification mechanism, audit, monitoring, and incident controls. |
| Performance profile | Throughput, finality, fees, capacity, uptime, and resource requirements. | Unvalidated for public production claims | Published benchmark method and production operating evidence. |

## 5.2 Consensus model

Federated Byzantine Agreement differs from proof-of-work and proof-of-stake systems because consensus authority is not allocated by computational work or protocol-defined stake weight. Each validator configures a quorum set: the nodes or organizations it is prepared to rely on. The validator also sets a threshold. Combinations of trusted nodes sufficient to meet that threshold form quorum slices. A quorum is a set of nodes sufficient to reach agreement in which every participating node contains a quorum slice within the set. [6]

The flexibility is operationally valuable because membership can remain open and each validator can make its own trust decisions. The same flexibility creates configuration risk. Safety depends on sufficient quorum intersection. Liveness depends on avoiding blocking sets and unavailable dependencies. A network can contain many nodes and still be operationally centralized if their quorum sets depend on the same small group, if keys are controlled by one party, or if the nodes share the same hosting, software release, geography, or administrative path.

SCP prioritizes safety and fault tolerance over uninterrupted liveness. Under adverse quorum conditions, the correct behavior may be to stop externalizing new ledger values rather than finalize conflicting state. Public descriptions should therefore avoid presenting consensus latency as an unconditional constant. Timing depends on workload, network conditions, configuration, implementation, failure mode, and the measurement definition.

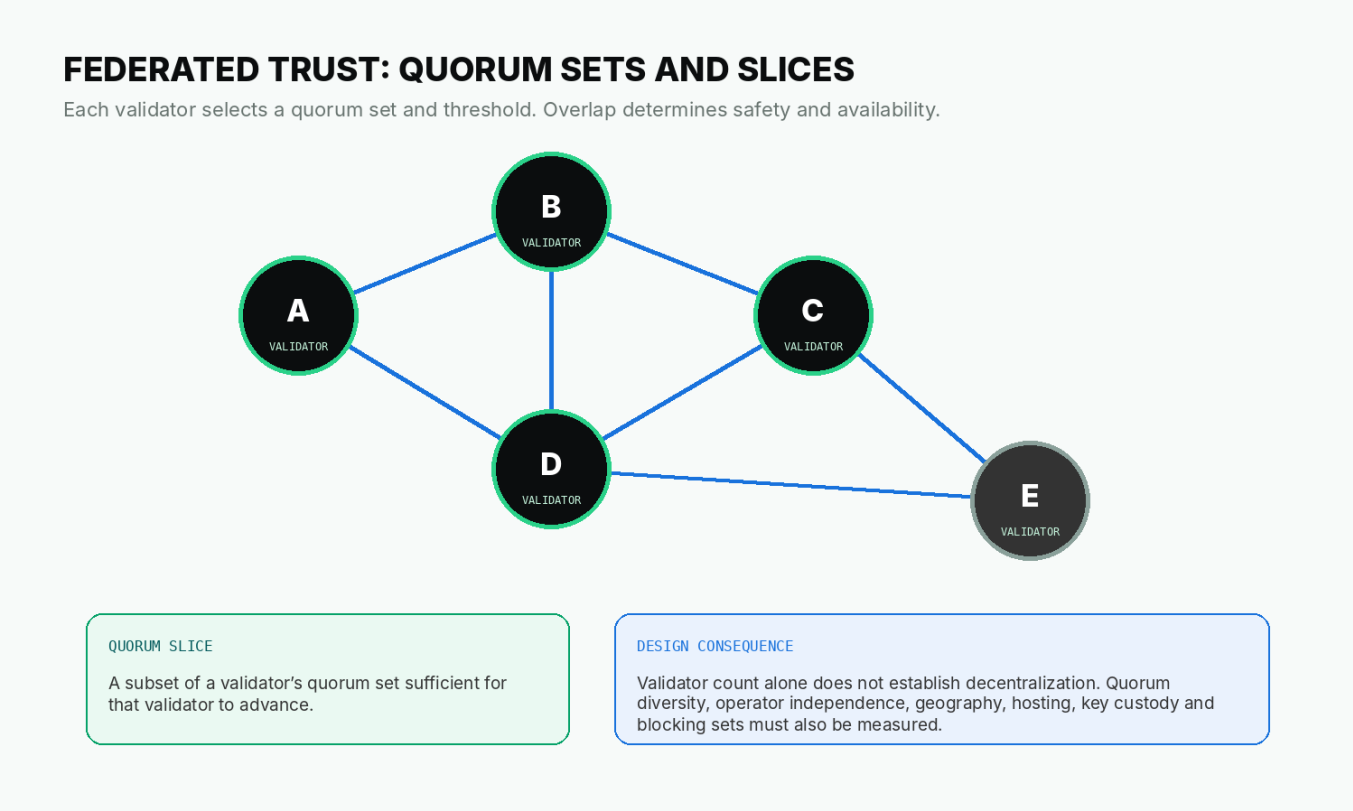



Figure 4. Federated trust relationships and the distinction between validator count and actual decentralization.

## 5.3 Transaction lifecycle

An application constructs an operation or transaction, identifies the source account, sets sequence and fee parameters, and produces the required signatures. The application may submit the serialized transaction through OrbitR or another compatible interface. A receiving Gravity node performs protocol validation, including format, signature, sequence, balance, authorization, reserve, and operation-specific checks. Valid candidate transactions are considered during the nomination and ballot phases of consensus. Once a transaction set is externalized, each compliant node applies the operations deterministically and advances ledger state. OrbitR indexes the resulting ledger and makes relevant resources available to applications.

This lifecycle creates several different assurance points. A transaction accepted by an API is not necessarily included in a ledger. A transaction included in one node's pending queue is not final. A successful ledger application does not prove that the underlying business transaction was lawful, authorized off-chain, free of fraud, or supported by accurate external data. Applications must distinguish network validity from business validity.

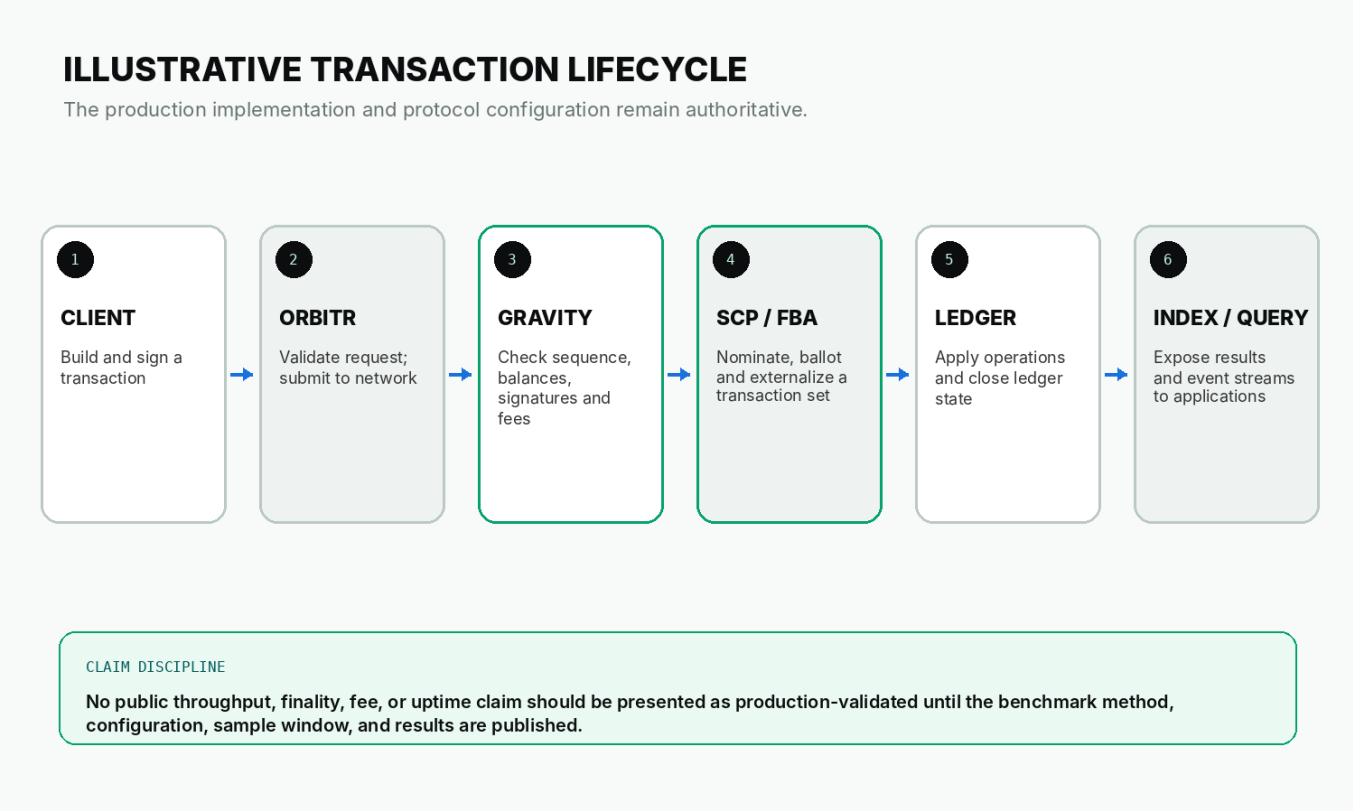



Figure 5. Illustrative transaction lifecycle from client construction through ledger indexing.

## 5.4 Validator and operator architecture

Metriq's portal lists four validators operated by Metriq. This provides a visible operational baseline but also creates a clear concentration question: how many validating organizations are independent of the Foundation, how are their quorum sets configured, and what failures can block or split the network? A credible decentralization program should be based on measurable operator diversity rather than a target node count. [3]

- Operator independence: distinct legal ownership, staffing, administrative access, financing, and incident authority.
- Key independence: separate validator and release keys, protected by documented hardware or threshold controls.
- Infrastructure diversity: different hosting providers, autonomous systems, regions, operating environments, and failure domains.
- Quorum diversity: published quorum sets, thresholds, blocking-set analysis, and change history.
- Software diversity: controlled release adoption, staged rollout, rollback procedures, and avoidance of simultaneous unsafe upgrades.
- Observability: public or reviewable uptime, peer, ledger, archive, version, and incident information.
- Exit and continuity: procedures for replacing unavailable or compromised operators without ad hoc central intervention.

## 5.5 Performance and fee claims

The prior white paper and legacy website materials included numeric claims about transactions per second, settlement time, payment-channel capacity, and fees. This revision does not repeat those figures as validated facts. Performance claims are highly sensitive to transaction type, signature count, database state, ledger-close configuration, validator hardware, network topology, history settings, API load, test duration, percentile, failure injection, and whether the result is measured at submission, validation, externalization, indexing, or application confirmation.

A publishable benchmark should define the software commit and build, network size and quorum configuration, hardware, storage, operating system, database, geographic topology, transaction mix, account distribution, duration, warm-up period, success criteria, error rate, ledger-close distribution, CPU and memory use, bandwidth, API lag, and raw output. Production validation should add real operating windows, maintenance periods, incidents, exceptions, and independent review. Until that evidence exists, Metriq should describe performance as a target or measured test result tied to its method, not as a universal property of the network.

**BENCHMARK RULE**

Do not publish a single throughput or finality number without the workload, environment, percentile distribution, failure conditions, and source data needed to reproduce it.

## 5.6 Protocol evolution

Gravity and OrbitR are derived from mature upstream systems, which reduces the cost of starting from first principles but creates an ongoing fork-management burden. Metriq must decide which upstream changes to merge, which protocol features to activate, how to review incompatible changes, and how to prevent a naming migration from obscuring inherited technical behavior. Legacy references remaining in source, documentation, domains, package paths, and tests should be tracked as migration debt rather than ignored.

Protocol evolution should proceed through written proposals, compatibility analysis, security review, test-network evidence, operator notification, activation thresholds, rollback planning, and post-activation monitoring. Emergency release authority should be narrow, time-limited, logged, and reviewed after use. If the network becomes meaningfully independent, protocol governance should include operators and users who are not controlled by the Foundation.

## 5.7 Developer and operator experience

A technically credible network must be operable by parties that did not write it. The minimum developer surface includes accurate build instructions, supported platforms, version compatibility, APIs, SDK examples, test assets, error semantics, security guidance, and a clear distinction between test and production environments. The minimum operator surface includes capacity planning, key management, peer configuration, quorum design, monitoring, alerting, backup, history publication, upgrade, rollback, incident response, and end-of-life guidance.

Documentation should be treated as a release artifact with owners, review gates, and version matching. A feature that exists only in source or in an internal operator's knowledge is not a usable public capability. Conversely, documentation must not describe a future feature as available simply because upstream code contains related functionality.

# MTRQ and Network Economics

MTRQ is the native coin of the Metriq Network. Its technical functions, supply design, treasury treatment, and market risks must be described separately.

## 6.1 Native-coin functions

A native coin can support protocol functions that are difficult to express through an external asset. It can denominate base transaction fees, satisfy minimum-balance or reserve rules where configured, provide a network-native transfer asset, and act as an intermediary within ledger-native exchange functions. Requiring a nonzero fee also creates a marginal cost for spam and resource consumption. The effectiveness of these functions depends on actual protocol configuration and market conditions.

MTRQ should be described in technical terms first. Promotional statements about scarcity, future value, returns, or guaranteed utility are inappropriate for this paper. The existence of a fixed nominal supply does not establish value. Value depends on demand, liquidity, distribution, user activity, legal access, custody, market integrity, technical reliability, and confidence in governance.

## 6.2 Documented supply design

| Component | Amount | Share of stated genesis supply | Evidence position |
|---|---|---|---|
| Stated genesis supply | 1,000,000,000,000 MTRQ | 100% | Documented design; reconcile against authoritative genesis configuration and ledger records before final publication. |
| Centurial allocation | 900,000,000,000 MTRQ | 90% | Documented long-horizon allocation; operating custody and release controls require verification. |
| Seed allocation | 100,000,000,000 MTRQ | 10% | Documented initial allocation; historical use and remaining balances require reconciled reporting. |
| Equal annual century tranche | 9,000,000,000 MTRQ | 0.9% of genesis supply per year | Arithmetic result of dividing 900 billion by 100; actual release mechanics and authority require policy and technical verification. |

The table records the economic design stated in prior Metriq materials. It is not an independent attestation that all amounts remain in the stated accounts, that custody arrangements are complete, or that releases have occurred exactly as designed. The final paper should link to an auditable supply and custody report that identifies genesis accounts, current balances, historical transfers, locks or constraints, signers, and reconciliation date.

## 6.3 Fee design and spam resistance

A fee that is too high impairs useful activity; a fee that is too low may fail to price congestion or deter abuse. The economically relevant measure is not a marketing comparison to card fees or a fraction of a cent at one exchange rate. It is the relationship among resource use, fee-bidding behavior, network capacity, asset volatility, user value, and adversarial cost.

Metriq should publish the base-fee configuration, surge or bidding behavior where applicable, transaction resource limits, minimum balances, and examples of expected costs for common operations. Fee changes should follow a controlled governance process. Applications offering "zero-fee" user experiences should disclose who pays the network costs, how abuse is controlled, whether pricing can change, and what happens if subsidies end.

## 6.4 Treasury economics

A treasury dominated by the network's native coin faces correlated risk. The asset's price, liquidity, and reputation may decline precisely when the network requires more funding. Selling to finance operations can affect the market, and expectations of future releases can affect demand. A responsible treasury policy should therefore separate nominal token allocations from operating budgets, establish liquidity horizons, limit concentration where legally and operationally feasible, define sale and hedging authority, and prohibit undisclosed market support or preferential dealing.

- Liquidity planning: maintain forecasted operating obligations in forms appropriate to their timing and risk.
- Market-impact controls: use preapproved execution methods, counterparties, limits, and reporting for material sales or transfers.
- Custody controls: threshold authorization, hardware-backed keys, separation of duties, recovery, rotation, and incident procedures.
- Counterparty controls: diligence, legal terms, sanctions screening where applicable, concentration limits, and reconciliation.
- Accounting controls: consistent valuation, realized and unrealized treatment, restrictions, related-party disclosure, and audit trail.
- Information controls: prevent insiders from trading or transacting on material nonpublic treasury, product, listing, or partnership information.

## 6.5 Distribution and concentration

Supply distribution affects network economics and public confidence even when consensus is not stake-weighted. Concentrated balances can increase market volatility, create governance perceptions, expose custody single points, and make ecosystem participation dependent on discretionary grants. Metriq should publish a distribution methodology that distinguishes Foundation-controlled balances, subsidiaries, vendors, employees, grants, ecosystem recipients, exchanges, operational accounts, and circulating supply. Labels should be based on documented control, not assumptions from addresses alone.

Any grant, vendor payment, incentive, investment, or sale involving MTRQ should define vesting or use restrictions where appropriate, disclosure requirements, conflicts, return or clawback rights, tax responsibility, sanctions and jurisdictional limits, and reporting. Programs should be designed to produce durable network participation, not temporary wallet counts or transaction volume that disappears when incentives stop.

## 6.6 Market and legal boundaries

The legal characterization of a digital asset can depend on the transaction, purchaser expectations, marketing, governance, jurisdiction, and ongoing conduct. Calling MTRQ a utility coin does not resolve those questions. Metriq should avoid statements that purchasers will profit from Foundation efforts, that the Foundation will maintain a price, or that MTRQ provides rights not established in enforceable documents. Exchange access, custody, payment use, grants, compensation, and cross-border transfers each require separate review.

**NO OWNERSHIP CLAIM**

MTRQ is not described in this paper as equity in Metriq Foundation or Metriq Dynamics, a donation receipt, a debt instrument, or a contractual right to Foundation profits or assets.

## 6.7 Economic measurement

| Metric | Why it matters | Required context |
|---|---|---|
| Active funded accounts | Indicates whether users can transact. | Definition of active, observation window, bots, internal accounts, and subsidy dependence. |
| Successful operations | Shows actual ledger use. | Operation mix, failures, internal traffic, batching, and economic purpose. |
| Fee burden | Measures user cost. | Asset price, operation type, sponsorship, congestion, and comparison basis. |
| Liquidity and depth | Affects practical convertibility and treasury execution. | Venue quality, jurisdiction, spread, depth at size, counterparty risk, and wash-trading controls. |
| Treasury runway | Tests institutional durability. | Asset mix, restricted balances, obligations, burn rate, price assumptions, and stress scenarios. |
| Distribution concentration | Identifies market and governance exposure. | Control-based address labeling, custodial aggregation, vesting, and related parties. |

## 6.8 Economic decision discipline

Economic management should separate ledger supply, treasury holdings, accounting value, realizable liquidity, operating runway, and mission allocation authority. These are different quantities. A large nominal balance can coexist with limited cash capacity, restricted use, weak market depth, or unacceptable concentration risk. Budgets should therefore be denominated in the currency of the underlying obligation and stress-tested against price, liquidity, counterparty, and operating-cost scenarios.

No release, grant, sale, investment, or subsidy should be justified by token availability alone. The decision record should state the objective, beneficiary, amount, valuation method, restrictions, alternatives considered, expected evidence, concentration effect, liquidity effect, tax and legal treatment, conflicts, and the event that would pause or terminate the commitment. Treasury performance should be evaluated by mission and operating capacity preserved—not by price appreciation or volume in isolation.

# The Proposed Centurial Fund

The Centurial Fund is intended to convert a century-scale MTRQ allocation into durable support for infrastructure, ecosystem growth, operating capability, and mission work.

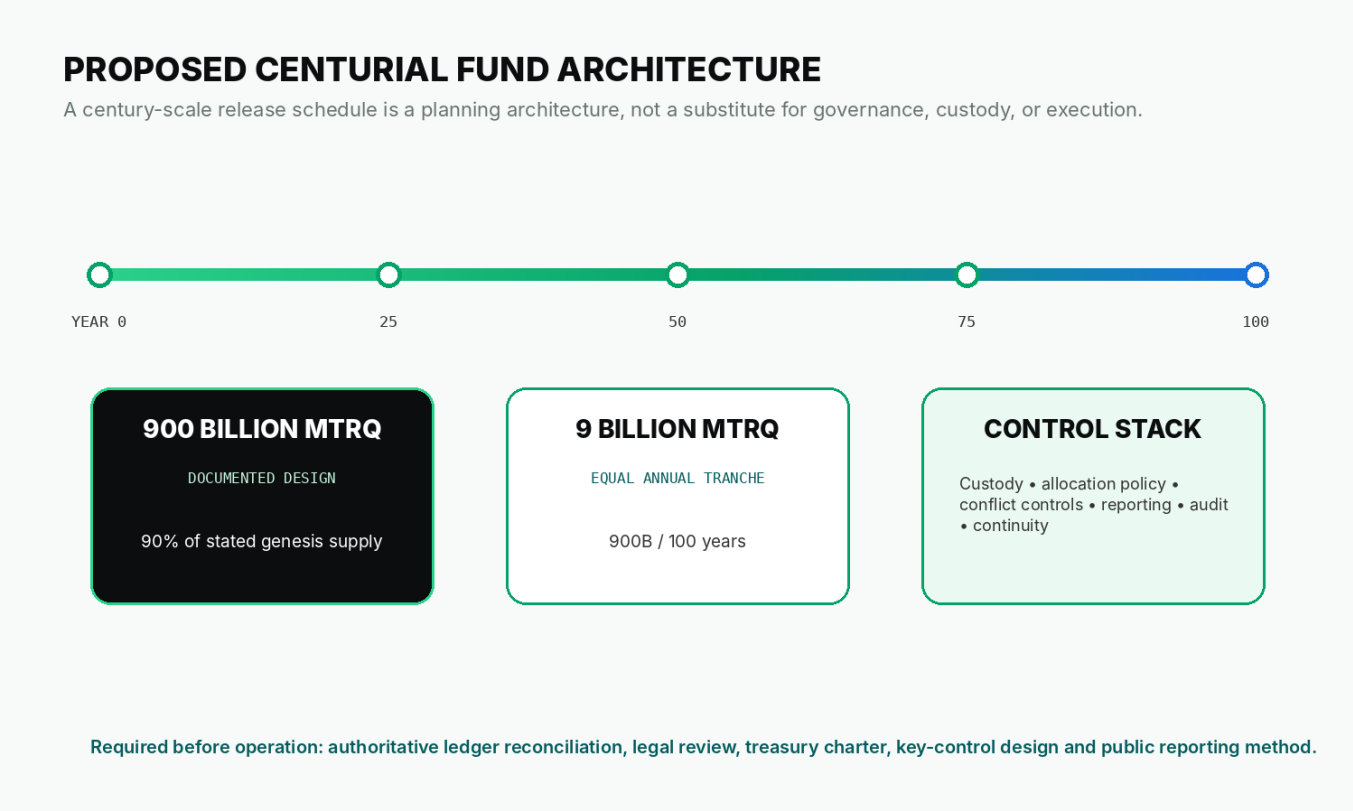



Figure 6. Proposed Centurial Fund release architecture and required control stack.

## 7.1 Design rationale

The central idea is to avoid exhausting the network's principal allocation during early market cycles. Equal annual tranches create a simple reference schedule and force a long planning horizon. The design can support infrastructure that requires continuous maintenance, ecosystem programs that compound over time, and mission work whose benefits do not fit short investment horizons.

Simplicity at the supply level does not eliminate complexity at the institutional level. An annual tranche can be too large in a weak market, too small during rapid expansion, or economically inappropriate if released without regard to liquidity, legal constraints, prior-year reserves, program capacity, or risk. The schedule should therefore define a maximum available amount, not an obligation to distribute or sell the full amount each year. Unused authority should remain controlled under a stated carryforward or re-locking rule.

## 7.2 Proposed allocation purposes

Legacy Metriq materials describe five broad uses: development, network growth, network support, enterprise investment, and direct public benefit. The categories remain useful if they are converted into governed programs with distinct objectives, decision rights, conflicts, and measurement.

| Program | Purpose | Example eligible uses | Principal control question |
|---|---|---|---|
| Development | Build and maintain Foundation and network capability. | Engineering, security, operations, documentation, infrastructure, legal work, research, staff, and necessary overhead. | Is the cost necessary, competitively sourced, budgeted, and tied to a deliverable or operating obligation? |
| Network growth | Increase useful independent participation. | Developer grants, integrations, tooling, operator support, standards work, and ecosystem infrastructure. | Does the recipient create durable capability rather than subsidized activity? |
| Network support | Remove adoption friction and strengthen distribution. | User onboarding, education, communications, market infrastructure, liquidity support subject to legal review, and partner enablement. | Are incentives transparent, time-limited, measurable, and free from misleading market activity? |
| Enterprise | Build or invest in operating capability aligned with the ecosystem or mission. | Subsidiaries, joint ventures, equipment, product companies, strategic investments, and commercial pilots. | Are economics, governance rights, related-party terms, downside exposure, and exit or reinvestment paths documented? |
| Mission programs | Fund measurable outcomes beyond network development. | Abundance, wildlife conservation, health, safety, and access projects. | Is the causal pathway credible, outcome measurable, partner capable, and cost proportionate to the result? |

## 7.3 Treasury charter

Before material operation, the board should adopt a treasury charter defining the fund's purpose, protected principal or release logic, authorized accounts, signers, approval thresholds, custody providers, permitted assets and transactions, liquidity requirements, diversification authority, prohibited transactions, conflict rules, valuation, reporting, audit, emergency powers, succession, and policy-review cycle.

The charter should distinguish allocation approval from transaction execution. A board or committee may approve a program, but treasury personnel or custodians should execute transfers under separate controls and reconcile them to the approval. Material transfers should require threshold authorization and independent confirmation. No single founder, officer, director, employee, contractor, or custodian should be able to authorize and execute a material transfer alone.

## 7.4 Annual allocation process

1. Reconcile beginning balances, prior releases, restrictions, signer status, and authoritative ledger records.
2. Approve a rolling multi-year operating forecast and minimum liquidity reserve.
3. Determine the annual amount available under the century schedule and any carryforward rules.
4. Allocate by program only after technical, financial, legal, security, conflict, and mission review appropriate to the decision.
5. Stage commitments through milestones rather than transferring full amounts when performance uncertainty is material.
6. Record decisions, dissent, conflicts, valuation assumptions, recipient identity, conditions, and evidence requirements.
7. Publish a report separating authorizations, commitments, transfers, expenditures, returned funds, unrealized balances, and measured outcomes.
8. Conduct an annual control review and periodic independent audit or agreed-upon procedures appropriate to the fund's maturity and risk.

## 7.5 Enterprise investments and subsidiaries

Enterprise activity can create durable revenue and technical capacity, but it also creates conflicts and loss exposure. The Foundation should establish an investment policy covering mandate, concentration, valuation, diligence, approval, board seats, related parties, information rights, follow-on funding, impairment, exit, and reinvestment of proceeds. Investments should not be justified solely by a claim that the company may use the network. The commercial thesis and mission thesis should each stand on their own.

Transactions with Foundation directors, officers, employees, major donors, vendors, recipients, or their affiliates require heightened disclosure and independent approval. Terms should be at least as favorable to the Foundation as reasonably available alternatives, supported by contemporaneous evidence, and reviewed without participation by the conflicted person.

## 7.6 Grant and program controls

Open applications can broaden participation but do not replace portfolio strategy. The Foundation should publish eligibility, review criteria, decision authority, conflicts, restricted uses, payment schedule, reporting, intellectual-property treatment, publicity rights, data protection, sanctions and jurisdictional restrictions, monitoring, termination, and clawback provisions. Selection should be documented against a consistent rubric.

Program evaluation should consider the counterfactual: what would happen without Metriq? Funding activity that would occur on the same terms without Metriq may still be worthwhile, but it should not be credited as fully additional. Outcome reporting should separate direct outputs from downstream effects and should disclose uncertainty rather than converting estimates into facts.

## 7.7 Stress scenarios

| Scenario | Potential consequence | Required response |
|---|---|---|
| MTRQ price declines materially | Nominal allocation supports less operating activity; pressure to sell may deepen market impact. | Reduce discretionary commitments, protect critical operations, update valuation and liquidity assumptions, and avoid price-support representations. |
| Liquidity is insufficient at required size | Transfers or sales produce excessive slippage or cannot be executed lawfully. | Stage execution, diversify funding sources where authorized, defer noncritical uses, and disclose constraints. |
| Key compromise or custodian failure | Loss, freeze, unauthorized transfer, or inability to access funds. | Threshold custody, offline recovery, incident plan, transaction limits, monitoring, insurance evaluation, and tested continuity. |
| Leadership transition | Authority becomes unclear or mission priorities shift without process. | Documented succession, reserved powers, board independence, signer rotation, policy continuity, and record preservation. |
| Regulatory restriction | Exchange, custody, grant, sale, or cross-border activity becomes limited. | Jurisdictional review, compliant alternatives, transaction suspension, reserve planning, and updated program design. |
| Program capacity is lower than available tranche | Pressure to spend weakens diligence and outcome quality. | Carry forward or retain authority; do not allocate merely to exhaust an annual amount. |

**EVIDENCE POSITION**

The Centurial Fund is treated in this paper as a Proposed architecture unless and until Metriq publishes reconciled accounts, governing policy, custody and signer controls, release history, and operating reports sufficient to establish implementation.

# Deployment and Commercialization Strategy

Metriq's thesis depends on converting technical capability into systems that users adopt, pay for, maintain, and improve.

## 8.1 From infrastructure to use

A network does not create public value merely by existing. It creates value when an application, product, institution, or operating process uses it to accomplish something better than available alternatives. Metriq should therefore start with the operating problem and choose the minimum architecture that solves it. Some problems need a shared ledger; others need conventional databases, manufacturing, machine learning, identity, payments, sensors, or human coordination. "Built by Metriq" should not automatically mean "placed on the Metriq Network."

Deployment decisions should compare the network against centralized and hybrid alternatives across cost, latency, reliability, privacy, auditability, interoperability, governance, reversibility, and user burden. A decentralized component is justified when multiple parties need shared state or verifiable coordination without granting one party exclusive control, and when the resulting governance and key-management burden is acceptable.

## 8.2 Product and company pathways

| Pathway | Use when | Advantages | Controls |
|---|---|---|---|
| Foundation infrastructure | The capability is a common layer whose broad availability advances the mission and ecosystem. | Open access, standardization, shared learning, and reduced duplication. | Maintenance funding, governance, security ownership, service levels, and deprecation policy. |
| Foundation program | The work directly delivers a mission outcome and does not require a separate commercial entity. | Direct mission control and integration with partners or grants. | Program charter, budget, outcome metrics, data policy, safety review, and closeout criteria. |
| Operating subsidiary | Commercial execution, liability separation, customer contracts, regulated activity, equipment, or specialized staffing justify a distinct entity. | Market discipline, focused management, customer revenue, and reusable operating capability. | Board oversight, related-party rules, capitalization, profit treatment, reporting, and dissolution path. |
| Joint venture or partner deployment | Another party has essential distribution, regulatory standing, field capability, or domain expertise. | Faster adoption and reduced duplication. | Authority, IP, data, economics, branding, compliance, incident, and exit terms. |
| Open-source project | Broad participation and inspectability are strategically important. | Community review, portability, and reduced lock-in. | License clarity, maintainer governance, security policy, contributor rules, release provenance, and sustainability. |

## 8.3 Metriq Dynamics as an operating capability

Metriq Dynamics gives the ecosystem a physical-production path. It can manufacture repeat parts, build engineered products, develop advanced surfaces, assemble and test systems, and convert repeatable work into documented production routes. Strategically, this matters because many technology organizations stop at software, research, or prototypes. A manufacturing subsidiary can carry ideas through design review, process planning, tooling, quality control, supplier coordination, production, and feedback.

The subsidiary should be evaluated as a real operating company. Relevant measures include quote conversion, backlog quality, gross margin, on-time delivery, first-pass yield, nonconformance, rework, customer concentration, equipment utilization, cash conversion, safety, training, supplier performance, and repeat revenue. Claims about autonomous manufacturing should identify the level of human review, machine authority, validation, and production evidence. A demo that drafts a route is not the same as an autonomous system authorized to execute it.

## 8.4 Metriq Trade Traceability

Metriq Trade Traceability is a Foundation technical program focused on physical identity and evidence-conditioned traceability. The commercial objective is to make verification deployable within ordinary manufacturing and supply-chain workflows rather than require a custom capture process for every downstream customer. Because the program includes patent-sensitive architecture and remains subject to engineering, security, privacy, standards, legal, and freedom-to-operate work, this paper describes only the strategic role.

A traceability system must distinguish identity, authentication, custody, status, and compliance evidence. A ledger record can preserve an issued statement; it cannot guarantee that the physical item was correctly identified, that a sensor was accurate, that an operator followed procedure, or that an external certification was valid. The system therefore depends on controlled enrollment, signed credentials, exception handling, authorized lifecycle events, privacy-aware resolution, and clear evidence classes. Detailed architecture belongs in the separate controlled MTT white paper and patent materials.

## 8.5 Payments and low-cost services

Lower-cost payment and transaction services remain a plausible mission-aligned pathway because merchant fees, settlement friction, reconciliation, chargebacks, access restrictions, and cross-border complexity can impose meaningful costs. Any zero-fee or near-zero-fee product, however, must explain its full economics. Network fees may be subsidized, but fraud, support, compliance, conversion, liquidity, refunds, hardware, software, disputes, and customer acquisition still have costs.

A production payment service would require a legal entity and jurisdictional plan; banking, custody, money-transmission, consumer, sanctions, data, and tax analysis; transaction monitoring proportionate to the model; security and fraud controls; reserve and settlement design; customer support; loss allocation; transparent pricing; and a path to sustainable unit economics. Until those elements exist, payment processing should remain Proposed rather than presented as an available Foundation service.

## 8.6 Partner selection

Partnerships should be chosen for capability, not logo value. A partner is strategically useful when it contributes distribution, users, data, regulatory authorization, infrastructure, field access, scientific expertise, manufacturing capacity, capital, or independent validation that Metriq cannot efficiently reproduce. Each partnership should begin with a written problem definition and measurable contribution.

- Mission fit and clear benefit to users or the ecosystem.
- Technical compatibility and realistic integration burden.
- Financial capacity, lawful source of funds, and sustainable economics.
- Security, privacy, data-rights, export-control, sanctions, and regulatory posture appropriate to the activity.
- Reputation and conduct consistent with Metriq's obligations.
- Defined intellectual property, publicity, support, incident, termination, and post-termination treatment.
- No dependency so concentrated that the partner can unilaterally disable a critical Metriq capability without a continuity plan.

## 8.7 Commercial discipline

Mission-aligned pricing does not require pricing every product below cost. Sustainable pricing should cover the resources needed to deliver quality, maintain security, support customers, invest in capacity, and withstand failures. Subsidies should be explicit, budgeted, time-bounded, and evaluated against measurable additionality. Cross-subsidies should not obscure whether a product has viable demand or create obligations the Foundation cannot sustain.

Product decisions should be based on a staged evidence funnel: problem evidence, user evidence, technical feasibility, unit economics, controlled pilot, security and legal readiness, production release, and scale. A project should not advance simply because it is technologically interesting or because sunk cost makes termination uncomfortable.

> **DEPLOYMENT STANDARD**
>
> A credible Metriq project must answer three questions: who uses it, what becomes materially better, and what evidence would cause Metriq to stop or change course?

## 8.8 Pilot selection

A pilot should be selected because it resolves a specific uncertainty at acceptable cost. Priority should go to problems with an identifiable user or buyer, a credible path to deployment, an evidence window short enough to inform the next decision, and downside that can be contained. A technically impressive demonstration is not a useful pilot when there is no decision it can change.

- State the user, problem, existing alternative, and reason the alternative is insufficient.
- Identify the single highest-value uncertainty the pilot is designed to reduce.
- Define success, failure, safety, legal, economic, and mission thresholds before execution.
- Cap financial exposure, data exposure, user exposure, and operational dependency.
- Assign an owner with authority to pause, redesign, transfer, or close the work.

## 8.9 Closure, transfer, and learning

Projects should have an orderly end state. Closure requires protection of users and counterparties, disposition of funds and assets, preservation or deletion of data as required, intellectual-property and license treatment, security shutdown, contract termination, staff and vendor transition, and a final evidence record. A capability may also be transferred to a subsidiary, partner, open-source community, or independent operator when that structure is more durable and the responsibilities are explicit.

The Foundation should publish an appropriate post-project record for material programs: what was attempted, what evidence was produced, what changed, what failed, what remains uncertain, and why the next decision was made. The objective is institutional learning, not retrospective promotion.

# Mission Priorities and Measurement

Metriq's mission becomes operational only when each program identifies a causal pathway, baseline, measurable result, and accountable owner.

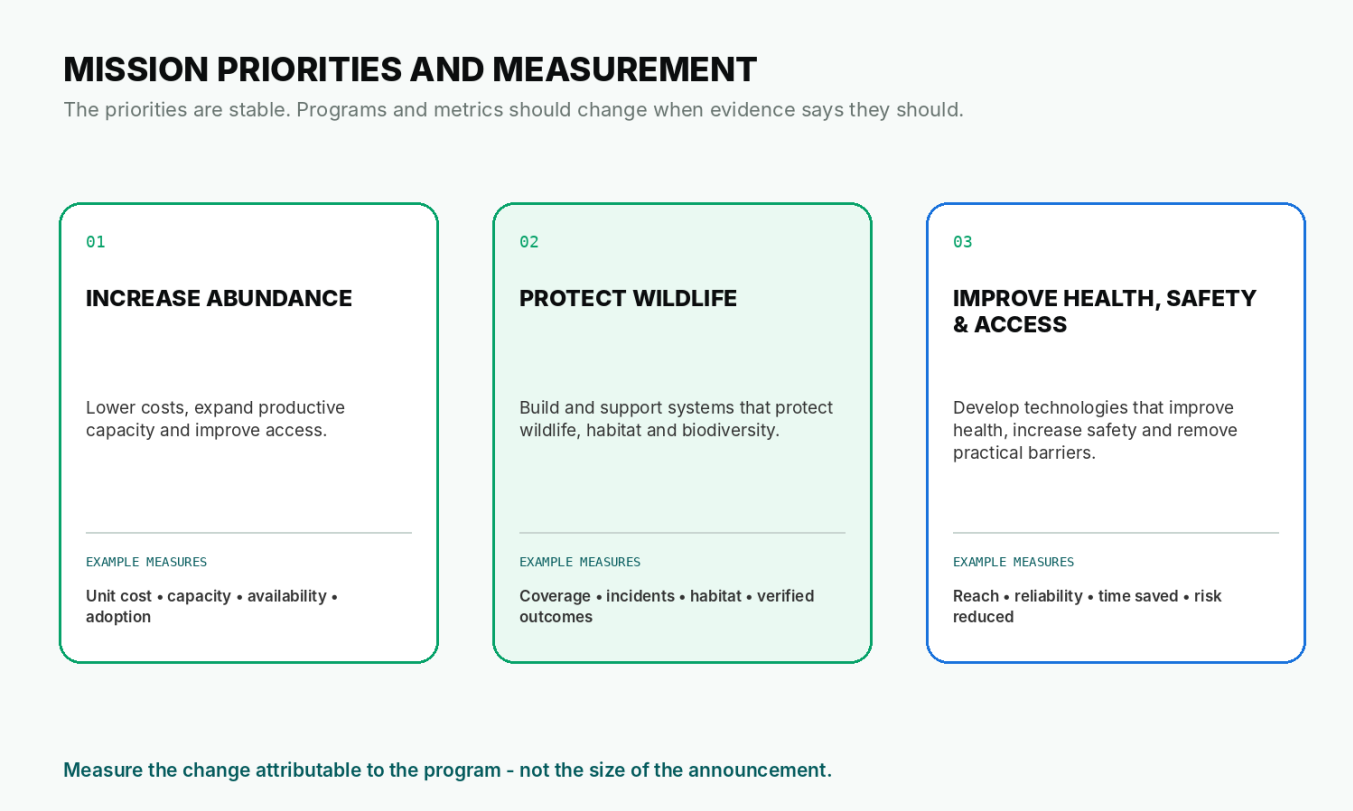



Figure 7. Mission priorities and example measurement categories.

## 9.1 Theory of change

Metriq's general theory of change is that technical and operating capability can create compounding public value. The Foundation builds or controls useful infrastructure and companies. Those systems reduce costs, create revenue, increase knowledge, and expand distribution. The resulting resources are reinvested into additional capability and selected mission programs. Successful deployments generate evidence and institutional learning that improve the next allocation decision.

This theory can fail at several points. The technology may not solve the problem. Users may not adopt it. Revenue may not cover the cost of delivery. Leadership may allocate resources poorly. A commercial success may drift from the mission. A mission program may produce activity without outcomes. Measurement is therefore not an after-action communications exercise; it is how the Foundation tests the operating model.

## 9.2 Increase abundance

Abundance refers to practical availability: more useful capability at lower total cost, with fewer avoidable barriers. It does not mean that every resource becomes unlimited or free. The relevant objective is to increase productive capacity, efficiency, access, and resilience in areas where constraints materially affect human opportunity or institutional capability.

| Measurement level | Examples | Analytical caution |
|---|---|---|
| Inputs | Capital, engineering hours, equipment, compute, partner resources. | Inputs show effort, not benefit. |
| Outputs | Units produced, transactions processed, integrations completed, tools released, people trained. | Outputs can increase while user value remains unchanged. |
| Outcomes | Lower unit cost, shorter cycle time, higher availability, increased adoption, reduced downtime, expanded geographic or demographic access. | Use a baseline and control for subsidies, market changes, and selection effects. |
| Long-term effect | Sustained productivity, lower structural cost, stronger infrastructure, or new capability that persists after Metriq support. | Attribution becomes harder over time; avoid claiming the entire downstream effect. |

## 9.3 Protect wildlife

Wildlife conservation is a technical and operational field, not a communications category. Useful interventions may include sensors, remote imaging, acoustic monitoring, satellite and aerial analysis, identity and traceability, field communications, ranger tools, habitat mapping, biodiversity data, enforcement support, rehabilitation systems, conservation finance, and supply-chain controls. Selection should be driven by the conservation mechanism and local operating context, not by whether the technology is fashionable.

Metrics should match the intervention. Examples include coverage area, detection probability, response time, false-positive rate, verified incidents, patrol efficiency, habitat condition, population indicators, bycatch, mortality, release outcome, enforcement action, or avoided land conversion. Sensitive location data, species data, and enforcement information may require access control. Publishing everything on a public ledger can create risk rather than transparency.

## 9.4 Improve health, safety, and access

This priority covers systems that improve health, reduce operational risk, increase safety, remove practical barriers, and extend access to effective services or tools. It is intentionally broader than healthcare and more concrete than an abstract social-benefit label. Relevant projects might address diagnostics, assistive technology, safety systems, verified supply chains, disaster response, workplace risk, access to essential infrastructure, or tools that allow people to act with greater independence.

Health and safety claims require heightened discipline. Pilot evidence should not be described as clinical effectiveness or safety certification. Regulated products must follow applicable design controls, validation, quality systems, reporting, and professional oversight. Personal and health information should be minimized, segregated, and protected. A public blockchain should not be the default repository for identifiable sensitive data.

## 9.5 Measurement framework

9. Define the decision: what question will the metric change?
10. Establish the baseline before intervention where feasible.
11. Distinguish reach, output, outcome, and long-term effect.
12. State the unit of analysis and observation window.
13. Track quality, failure, and adverse effects alongside success.
14. Identify what would have happened without the program and how that estimate was formed.

15. Record the full cost, including staff, infrastructure, partner, compliance, and opportunity cost.
16. Separate results attributable to Metriq from results attributable to partners or external conditions.
17. Publish uncertainty, limitations, missing data, and material methodology changes.
18. Use predeclared continuation, expansion, redesign, and termination thresholds for major programs.

## 9.6 Portfolio allocation

A balanced mission portfolio can combine infrastructure, commercial capability, direct programs, and high-risk research. Allocation should consider expected outcome, probability of success, time to evidence, reversibility, capital intensity, operational burden, correlation with other projects, and strategic learning. High-uncertainty projects may be justified when the potential value is large and the experiment is bounded. They should not be funded as if their outcome were certain.

The Foundation should report both successes and closed projects. A terminated program can be a positive governance outcome when the decision is timely, evidence-based, and documented. Hiding failed work creates incentives to continue it and prevents other organizations from learning from the result.

## 9.7 Public reporting

| Report element | Minimum content |
|---|---|
| Program identity | Owner, partners, jurisdiction, evidence state, start date, and status. |
| Problem and baseline | Defined problem, affected users or environment, baseline method, and limitations. |
| Resource commitment | Cash, MTRQ, staff, equipment, in-kind support, restrictions, and valuation method. |
| Outputs and outcomes | Results against predeclared measures, including failures and adverse effects. |
| Attribution | Metriq contribution, partner contribution, external factors, and counterfactual assumptions. |
| Decision | Continue, scale, redesign, pause, close, or transfer, with the reason and next gate. |

## 9.8 Cost-effectiveness and additionality

Outcome reporting is incomplete without cost and an alternative. Metriq should estimate the full resources consumed, identify what comparable result could have been achieved through a grant, purchase, partnership, policy change, or existing provider, and explain why Metriq participation added something material. Additionality may come from lower cost, faster execution, technical capability, risk tolerance, coordination, distribution, or a longer time horizon; it should not be presumed from organizational involvement alone.

Cost-effectiveness comparisons will often be uncertain, especially in research and conservation. The response should be sensitivity analysis rather than false precision. Report the assumptions that drive the conclusion, show a reasonable range, identify nonfinancial constraints, and revise the estimate when operating evidence changes. A program with a strong mission narrative but weak marginal value should not displace a more effective use of the same resources.

# Governance, Accountability, and Claims

The Foundation's credibility will depend less on stated intentions than on the quality of its decision rights, records, controls, and corrections.

## 10.1 Governance principles

| | |
|---|---|
| **Authority must be explicit.**<br>Every material decision should identify the legal entity, governing body, delegated role, threshold, and record that authorizes it. | **Oversight must be independent enough to matter.**<br>A board cannot provide effective oversight if operational leadership controls all information, all votes, and all material approvals without counterbalance. |
| **Conflicts must be managed before the decision.**<br>Disclosure after a related-party transaction is not equivalent to independent review and approval before commitment. | **Records must support reconstruction.**<br>A reviewer should be able to determine what was decided, by whom, with what evidence, under which policy, and how the result was monitored. |
| **Claims must be owned.**<br>Every material public statement should have a named owner and a source capable of supporting it. | **Correction is part of governance.**<br>Metriq should correct inaccurate, outdated, or overstated claims promptly and preserve the reason for the change. |

## 10.2 Board and management

The board sets mission, strategy boundaries, reserved powers, executive accountability, major capital policy, conflicts, and organizational risk tolerance. Management operates within those boundaries. Combining founder, executive, and board roles can be practical during early development, but it increases key-person and oversight risk. As the Foundation controls larger assets, operating companies, grants, and public claims, the board should increase independent competence in finance, technology, security, nonprofit governance, law, treasury, risk, and mission domains.

Board materials should include operating performance, treasury position, risk register, related-party activity, security incidents, regulatory developments, subsidiary reporting, major claims, and mission outcomes. Minutes should document decisions and conflicts without exposing sensitive security or personal information. Executive compensation and related-party arrangements should follow documented, independent processes appropriate to nonprofit status.

## 10.3 Committees and delegated authority

Committees can improve focus but should not become informal centers of unrecorded authority. A committee charter should define scope, membership, independence, expertise, quorum, voting, recusal, information rights, delegated limits, escalation, records, and sunset or review. Potential committees include audit and finance, treasury, grants and mission allocation, technology and security, compensation and governance, and enterprise investment.

Delegations should use financial and risk thresholds. Routine operating decisions can be delegated to management. Material treasury transfers, related-party transactions, formation or disposal of subsidiaries, major protocol commitments, significant public claims, and changes to the profit commitment or century architecture should remain reserved to the board or a properly authorized committee.

## 10.4 The profit commitment

Metriq's public position is that 100% of profits are pledged to public benefit. The final policy should be stated in language that can be administered and audited. "Profit" can mean accounting net income, taxable income, free cash flow, distributable surplus, or another measure. Each produces different outcomes. The policy must also address subsidiaries, joint ventures, minority investments, retained earnings, reserves, working capital, capital expenditure, debt, taxes, restricted funds, losses, intercompany charges, and timing.

A practical formulation may apply to distributable profits of covered Foundation-owned operating companies after lawful obligations, board-approved reserves, and documented reinvestment requirements. The policy should state whether reinvestment in mission-aligned technology counts as public-benefit deployment, whether transfers are mandatory or subject to solvency tests, how exceptions are approved, and what is reported publicly. Final language requires legal, tax, accounting, and board review.

**DRAFTING ISSUE FOR FINAL RELEASE**

The website's concise phrase can remain. The white paper and governing policy must define the covered entities and financial measure behind it.

## 10.5 Conflicts of interest

- Annual and transaction-specific disclosure by directors, officers, committee members, employees with authority, and material advisers.
- Recusal from discussion, information, recommendation, approval, execution, and monitoring where the conflict is material.
- Independent evidence that terms are fair and in the Foundation's interest.
- Heightened review for compensation, loans, asset transfers, investments, grants, employment, vendor contracts, and intellectual-property arrangements involving insiders or affiliates.
- Public disclosure where required or necessary to explain a material decision, balanced against legitimate privacy and security needs.
- Central conflict register with periodic review and enforcement consequences.

## 10.6 Claims governance

Claims governance applies to websites, white papers, social media, grant materials, investor or partner discussions, exchange materials, product pages, repositories, interviews, presentations, and generated content. The same claim should not be "Proposed" in an engineering document and "Live" in marketing. Metriq should maintain a controlled claim register containing the exact claim, scope, evidence state, owner, source, review date, expiration or refresh date, permitted contexts, and required qualification.

| Claim category | Required evidence before unqualified publication |
|---|---|
| Network throughput or finality | Published benchmark or production method, configuration, percentiles, failure conditions, window, and raw evidence. |
| Fees or user cost | Current protocol configuration, operation type, sponsorship, asset-price basis, and full product costs where relevant. |
| Decentralization | Operator and key independence, quorum and blocking-set analysis, hosting and geographic diversity, and change history. |
| Security | Defined threat model, controls, review scope, unresolved findings, incident history, and date; avoid absolute language. |

| Claim category | Required evidence before unqualified publication |
|---|---|
| Adoption | Defined active-user or customer metric, period, exclusions, internal activity, and subsidy dependence. |
| Financial commitment | Approved policy, covered entities, financial definition, exceptions, transfers, and reconciliation. |
| Impact | Baseline, method, attribution, cost, outcome window, uncertainty, and partner contribution. |
| Regulatory or compliance status | Jurisdiction, scope, date, responsible professional or authority, conditions, and limitations. |

## 10.7 Transparency without security theater

Transparency does not require publishing every key, contract, vulnerability, personal record, trade secret, or conservation location. It requires publishing enough information for stakeholders to understand authority, evidence, material risk, financial flows, and outcomes while protecting legitimate confidential interests. Redactions and aggregation should be explained. Security-sensitive details can be made available to qualified reviewers under controlled access.

Public dashboards should expose source and freshness. A number without its definition, timestamp, and data path can create false confidence. Where data is generated by Metriq-controlled systems, the report should identify the control and any independent verification. Where an external partner supplies data, attribution and validation responsibilities should be stated.

## 10.8 Document and policy hierarchy

| Level | Examples | Authority |
|---|---|---|
| Governing documents | Articles, bylaws, board resolutions, subsidiary documents, reserved powers. | Controlling legal authority subject to law. |
| Board policies | Treasury, conflicts, grants, investment, security oversight, records, claims, whistleblower, privacy. | Board-approved operating constraints. |
| Technical standards | Protocol specifications, release policy, key management, benchmark method, incident playbooks. | Approved technical control baseline. |
| Program charters | Defined project purpose, owner, budget, metrics, risks, data, partners, and release gates. | Authorizes a bounded program. |
| Public documents | White papers, website, reports, dashboards, repository documentation. | Communication; cannot expand authority beyond controlling documents. |

# Security, Resilience, and Privacy

Security is a system property spanning code, operators, keys, infrastructure, vendors, users, governance, and incident response.

## 11.1 Security objectives

The security objective is not to eliminate all failure. It is to prevent unacceptable failure where practical, detect it quickly, limit the blast radius, preserve trustworthy evidence, recover safely, and learn from the event. Different layers have different objectives. Consensus requires ledger safety and availability. APIs require authentication, rate control, integrity, and resilience. Treasuries require authorization and custody. Operating companies require customer-data, production, safety, and intellectual-property controls. Mission programs may require protection of personal, health, location, or species data.

| Asset or function | Primary threats | Required control themes |
|---|---|---|
| Consensus and ledger state | Malicious or misconfigured validators, quorum failure, protocol defect, unsafe upgrade, denial of service, history corruption. | Quorum analysis, staged releases, peer policy, monitoring, archive verification, rollback and incident coordination. |
| Release pipeline | Compromised maintainer, dependency attack, malicious build, signing-key loss, unreviewed code, secret leakage. | Protected branches, review, CI isolation, provenance, SBOM, dependency scanning, reproducible or verified builds, signed releases, rotation. |
| OrbitR and public services | API abuse, injection, denial of service, data inconsistency, credential compromise, privacy leakage. | Input validation, least privilege, rate limiting, segmentation, caching controls, monitoring, patching, service isolation, privacy review. |
| Treasury and privileged keys | Theft, coercion, loss, insider abuse, unauthorized transfer, signer unavailability. | Threshold authorization, hardware-backed keys, geographic separation, transaction policy, independent confirmation, recovery and tested continuity. |
| Customer and program data | Unauthorized access, overcollection, secondary use, breach, reidentification, unlawful transfer. | Data minimization, classification, access control, encryption, retention, vendor controls, consent or lawful basis, deletion, incident response. |
| Physical operations | Unsafe automation, defective product, export-control breach, counterfeit input, equipment compromise, process drift. | Human release gates, quality system, calibration, traceability, safety interlocks, supplier control, export screening, CAPA and change control. |

## 11.2 Threat modeling

Each system should maintain a threat model proportionate to its risk and update it when architecture, users, data, dependencies, or deployment changes. The model should identify assets, trust boundaries, actors, entry points, assumptions, abuse cases, controls, residual risk, and evidence. It should include accidental failure and insider risk, not only external attackers.

For the network, the threat model should cover validator compromise, quorum misconfiguration, eclipse and peer attacks, denial of service, malformed transactions, protocol and database defects, history archive tampering, unsafe configuration, version skew, dependency vulnerabilities, operator error, and coordinated legal or infrastructure disruption. For treasury systems, it should include signer coercion, device compromise, social engineering, malicious proposals, address substitution, approval fatigue, lost keys, and custodian insolvency or freeze.

## 11.3 Secure development and release

- Defined supported branches and release channels; no production release from an uncontrolled personal branch.
- Mandatory review for security-sensitive and consensus-critical changes, with specialist review where appropriate.
- Automated tests, static analysis, dependency and secret scanning, and documented handling of false positives.
- Software bill of materials and dependency inventory for production releases.
- Build provenance and signed release artifacts; verify that the deployed binary corresponds to reviewed source.
- Separation of development, test, staging, and production credentials and data.
- Versioned configuration, change approval, rollback procedure, and emergency release policy.
- Security contact, vulnerability intake, severity method, remediation targets, coordinated disclosure, and public advisories when needed.
- Post-release monitoring and a defined support and end-of-life policy.

Inherited code should not be assumed secure because the upstream project is mature. Fork-specific changes, delayed merges, custom dependencies, renamed packages, configuration differences, and unsupported versions create their own attack surface. Metriq should maintain a documented delta from upstream and a process for evaluating upstream security advisories and protocol changes.

## 11.4 Validator operations

Validator operators should use hardened systems, least privilege, protected keys, restricted administrative access, authenticated configuration changes, monitored peer and consensus behavior, reliable time synchronization, tested backup and recovery, and separation between public API services and consensus-critical infrastructure. Operator runbooks should define startup, catch-up, maintenance, upgrade, archive, capacity, alert, and incident procedures.

Quorum changes are security changes. They should be reviewed, simulated or analyzed, staged, communicated, and monitored. A validator should not copy a quorum configuration without understanding its blocking sets and dependencies. The network should maintain an emergency communication path that does not itself grant a single party power to finalize ledger state.

## 11.5 Key management

Keys should be classified by consequence: validator keys, release-signing keys, treasury keys, issuer or credential keys, administrative credentials, customer keys, and routine service secrets require different controls. The highest-consequence keys should use hardware-backed protection or equivalent controls, threshold authorization where technically appropriate, geographic and organizational separation, documented generation, backup, rotation, revocation, recovery, and destruction.

Recovery mechanisms should be tested without exposing secrets. A recovery design that depends on one person’s memory, one device, or one vendor is not resilient. Transaction signing should include human-readable intent, destination verification, policy limits, and an independent out-of-band confirmation for material transfers. Logs should preserve evidence without logging secrets.

## 11.6 Incident response

| Phase | Required actions |
|---|---|
| Prepare | Roles, contact tree, severity, evidence handling, external counsel and specialists, backups, alternate communications, regulator and partner obligations, and exercise schedule. |
| Detect and assess | Validate the signal, preserve evidence, identify affected assets and trust boundaries, classify severity, and establish incident command. |
| Contain | Limit access, pause affected services or transfers, isolate systems, rotate credentials where safe, and protect users and ledger safety. |

| Phase | Required actions |
|---|---|
| Eradicate and recover | Remove the cause, rebuild from trusted sources, verify configuration and data, restore in stages, monitor, and document residual risk. |
| Notify | Provide accurate, timely notices to affected users, operators, partners, insurers, regulators, or the public as required; avoid speculation. |
| Learn | Conduct a blameless but accountable review, track corrective actions, update threat models and controls, and publish an appropriate incident summary. |

## 11.7 Privacy and data governance

A public or widely replicated ledger is generally inappropriate for raw personal, health, financial-account, precise-location, confidential business, export-controlled, or safety-sensitive data. Where a ledger is useful, applications should store the minimum necessary public commitment, identifier, status, or proof and keep sensitive source data in controlled systems. Hashing sensitive data does not automatically make publication safe; low-entropy or known data may be reidentified, and an immutable commitment can create long-lived linkage.

- Collect only data required for a defined purpose.
- Classify data by sensitivity, ownership, legal restriction, and operational consequence.
- Separate public ledger data, public API data, partner data, confidential business data, personal data, and restricted technical data.
- Define lawful basis or consent where required, and do not use broad language to authorize unrelated future use.
- Use role-based and attribute-based access, encryption in transit and at rest, logging, review, and time-bounded access.
- Set retention and deletion schedules; immutable ledgers require special design before personal data is written.
- Contractually control processors, vendors, partners, and cross-border data flows.
- Evaluate reidentification, model-training, location, and aggregation risks rather than relying only on direct identifiers.

## 11.8 Independent assurance

Independent review should be targeted to the risk. Code audit is useful for a defined release and scope but does not certify ongoing operations. Penetration testing is useful for exposed services but does not establish consensus safety. Financial audit addresses reported statements but does not prove treasury strategy is sound. Metriq should define the assurance question first, select qualified reviewers, publish scope and limitations where possible, track findings to closure, and avoid using an audit logo as an absolute security claim.

**SECURITY LANGUAGE**

Use “designed to,” “reviewed for,” or “tested against” with scope and date. Avoid “secure,” “unhackable,” “fully protected,” or similar absolute claims.

# Legal and Regulatory Workstreams

Metriq operates across nonprofit governance, digital assets, software, manufacturing, data, intellectual property, grants, commerce, and potentially regulated services. No single legal label resolves all of those obligations.

**NOT LEGAL ADVICE**

This section identifies workstreams for qualified counsel and responsible management. It is not a legal conclusion about any product, transaction, jurisdiction, or person.

## 12.1 Organizational and nonprofit governance

The Foundation should maintain current corporate records, board and officer authority, registered-agent and filing obligations, charitable or tax-exempt status records where applicable, conflict and compensation processes, related-party documentation, subsidiary oversight, donor or restricted-fund treatment, and accurate public statements about its legal status. Forming a nonprofit corporation does not by itself determine federal tax treatment or authorize every fundraising, investment, or commercial activity.

Commercial subsidiaries and investments should be reviewed for governance, tax, private-benefit, unrelated-business, transfer-pricing, and asset-use implications appropriate to the Foundation's status and jurisdictions. Agreements should define ownership, services, cost allocation, intellectual property, data, personnel, insurance, indemnity, profit distributions, and dissolution.

## 12.2 Digital-asset activity

MTRQ transfers, sales, grants, compensation, exchange access, custody, payment products, market support, and treasury transactions can implicate different legal regimes depending on jurisdiction and facts. Relevant areas may include securities, commodities, money transmission, payment services, consumer protection, sanctions, anti-money-laundering obligations, tax, accounting, advertising, unfair or deceptive practices, and recordkeeping. Metriq should map each activity rather than rely on a general "utility" label.

The Foundation should maintain approval controls over token-related public statements and agreements. Any exchange or market relationship should be documented, reviewed, and monitored. Metriq should not publish or endorse misleading volume, guaranteed liquidity, price targets, return expectations, or undisclosed paid promotion. Personnel with material nonpublic information should be subject to trading and confidentiality controls appropriate to their role.

## 12.3 Payments and financial services

A product that accepts, holds, converts, transmits, settles, or facilitates value for others may trigger licensing, registration, safeguarding, disclosure, fraud, error-resolution, privacy, sanctions, and consumer obligations. The analysis depends on custody, control, asset type, counterparties, geography, settlement flow, and who bears loss. A network transaction can be technically peer-to-peer while the surrounding product remains a regulated intermediary.

Before a public payment launch, Metriq should produce a jurisdiction and funds-flow map, legal entity analysis, banking and custody architecture, user terms, fee and spread disclosures, complaint and dispute process, transaction monitoring approach, reserve and reconciliation controls, fraud model, incident plan, and customer-support design.

## 12.4 Data, privacy, and cybersecurity law

Products that collect personal data must identify the controller or business, processor or service provider, purposes, categories, recipients, retention, security, user rights, cross-border transfers, and breach obligations. Sector-specific rules may apply to health, financial, employment, education, children, biometric, precise location, communications, or government data. Data recorded on an immutable or decentralized system requires special review before deployment because deletion, correction, localization, and controller identification may be difficult.

## 12.5 Manufacturing and physical products

Metriq Dynamics and any Foundation product program must comply with applicable customer, product, safety, quality, labeling, export-control, environmental, employment, and industry requirements. The required controls depend on the product and market. Aerospace, medical, pharmaceutical, automotive, defense, and consumer products can require distinct quality systems, traceability, validation, supplier, reporting, and record-retention obligations.

Autonomous or AI-assisted engineering does not transfer legal responsibility to the model. Qualified personnel must define when generated output is advisory, when it may enter a controlled workflow, and what review is required before production, release, or use. Public demos should state their limits and prohibit submission of sensitive or regulated data through uncontrolled channels.

## 12.6 Intellectual property and open source

Metriq's strategy combines open-source infrastructure with potentially proprietary inventions, trademarks, manufacturing processes, datasets, and commercial know-how. The Foundation should maintain an intellectual-property map showing owner, contributor agreements, licenses, third-party components, patent status, confidentiality, export restrictions, and permitted use by subsidiaries and partners. Public disclosure should be coordinated with patent strategy where applicable.

Forked software requires license compliance, preservation of notices, source obligations where applicable, and accurate attribution. Renaming should not obscure upstream origin. New contributions should be accepted under documented terms. The Foundation should separate a project's public license from trademark permission and from any service-level or warranty commitment.

## 12.7 Grants, investments, and cross-border programs

Funding recipients should be screened and contracted according to the transaction's risk. Relevant controls can include identity and authority verification, sanctions and restricted-party screening, purpose restrictions, anti-corruption terms, budget and milestone review, data and intellectual-property rules, local-law responsibility, tax reporting, audit rights, termination, return of unused funds, and prohibition on unlawful use. Cross-border programs require review of currency, exchange, charitable, export, tax, employment, and data constraints.

## 12.8 Publication checklist

| Statement or activity | Final-review question |
|---|---|
| “100% of profits” | What is the defined financial measure, which entities are covered, what reserves and exceptions apply, and how is compliance verified? |
| One trillion MTRQ supply | Does the authoritative genesis and current ledger reconciliation support the amount and allocation labels? |
| Centurial Fund | Is the fund legally and operationally constituted, or must it remain labeled Proposed? |
| Public validator and API services | Who operates them, what terms apply, what monitoring exists, and what is the current evidence window? |
| Performance or fee claims | Is the method current, reproducible, and appropriate to the context in which the claim appears? |
| Nonprofit status | Which corporate and tax statuses are accurate in each jurisdiction and at the publication date? |
| Product availability | Is the product actually available, to whom, under which terms, and with what safety or regulatory limits? |
| Patent or IP status | Has counsel approved the disclosure and exact status language? |

## 12.9 Release authority and correction duty

Final publication should be authorized through a named release record, not inferred from file circulation. The record should identify the approved version, owner, publication date, source package, evidence window, reviewers, unresolved qualifications, and the person or body with authority to publish. Legal, technical, financial, security, brand, and accessibility review should be scoped to the claims each reviewer is qualified to assess rather than treated as a generic approval.

Publication creates an ongoing correction duty. Material facts can become stale when services move, repositories change, validators leave, policies are amended, products are withdrawn, or legal and technical conclusions evolve. Metriq should maintain a public correction and supersession process that preserves prior versions, states what changed, and removes or qualifies claims that are no longer supported.

# Roadmap and Release Gates

The roadmap is organized around evidence and control maturity. Dates may guide planning, but a gate is passed only when its required evidence exists.

## 13.1 Roadmap principles

- Do not activate a capability merely because a calendar date has arrived.
- Do not market a capability ahead of security, legal, operating, and support readiness.
- Prefer small, instrumented pilots to broad launches with weak observability.
- Retain rollback and exit options until production evidence justifies commitment.
- Publish what was learned, including missed targets and changed assumptions.
- Avoid bundling unrelated ambitions into one phase; each capability should have its own owner and gate.

## 13.2 Gate 1 - Institutional baseline

The first gate establishes the organization that will control later scale. Required evidence includes current entity and ownership records; board and delegated authority; conflict, treasury, claims, security oversight, records, and incident policies; subsidiary reporting; a defined profit-commitment policy; authoritative MTRQ supply and custody reconciliation; and a public document register that identifies current versus superseded materials.

| Deliverable | Pass condition |
|---|---|
| Entity map | All active entities, ownership, directors or managers, reserved powers, IP, bank and custody relationships, and reporting lines are current. |
| Policy baseline | Board-approved policies exist for treasury, conflicts, related parties, claims, grants/investment, security oversight, records, and whistleblowing. |
| Supply and custody report | Genesis allocation, current balances, historical movements, restrictions, signers, and reconciliation date are documented. |
| Public claim register | Material website, white-paper, token, network, product, and impact claims have owners, states, sources, and review dates. |

## 13.3 Gate 2 - Network evidence and release discipline

This gate converts public source code into a controlled network release process. Required evidence includes supported versions, documented build and test paths, signed releases, dependency inventory, security intake, operator runbooks, monitored validator and OrbitR services, quorum and blocking-set analysis, history verification, configuration control, and an incident exercise. Legacy naming and package references should be tracked and resolved according to a migration plan.

A benchmark may be published at this stage if its method and raw results are complete. It should remain labeled Simulated unless performed under defined production conditions. No smart-contract, bridge, or payment capability should be activated merely because related upstream code exists.

## 13.4 Gate 3 - Independent operator and developer readiness

The network should demonstrate that an independent party can build a supported release, operate a node, understand quorum configuration, publish or consume history, use OrbitR, submit and verify transactions, monitor the system, and recover from documented failure scenarios without private intervention by the original maintainers. At least one external security or architecture review should be completed for the defined release scope, with material findings resolved or transparently accepted.

Decentralization targets should be based on operator, key, hosting, geographic, and quorum independence. A credible target is not "more validators" in the abstract; it is reduction of common-mode failure and unilateral control.

## 13.5 Gate 4 - Product pilots

Each product pilot should have a charter, user, problem, architecture, legal and security review, data policy, budget, success and failure measures, support plan, incident owner, and exit criteria. Pilots should use noncritical or bounded value until reliability and control evidence supports expansion. The Foundation should not infer broad product-market fit from partner interest, memorandum signing, demo use, or subsidized transactions.

| Pilot evidence | Minimum question |
|---|---|
| User evidence | Does a defined user repeatedly choose the product when a real alternative exists? |
| Technical evidence | Does the system meet reliability, security, latency, accuracy, and operational requirements under the intended conditions? |
| Economic evidence | What is the full cost to acquire, deliver, support, comply, and maintain? Who pays and why? |
| Mission evidence | What measurable result advances abundance, wildlife conservation, or health, safety, and access? |
| Scale evidence | Which constraints become binding at 10x use, and what capital, staffing, infrastructure, and governance are required? |

## 13.6 Gate 5 - Centurial Fund operation

The proposed fund should not enter material operation until the board has adopted the treasury charter and allocation policies, signer and recovery controls are tested, legal and accounting treatment is reviewed, authoritative balances are reconciled, the first annual budget and liquidity plan are approved, conflicts are documented, and a reporting format is ready. Initial activity should use lower transaction limits and staged commitments while the control system is tested.

## 13.7 Gate 6 - Production validation and scale

Production validation requires evidence across a meaningful operating window. For the network, this includes version and configuration, uptime, ledger-close distribution, API availability, error and incident history, quorum health, operator diversity, security findings, and change history. For a product, it includes user retention, full unit economics, support burden, fraud or safety outcomes, compliance performance, and mission result. Scale should proceed only when the evidence supports the next risk level.

## 13.8 Future research

Metriq may investigate advanced smart-contract environments, interoperability, privacy-preserving credentials, autonomous manufacturing, artificial intelligence, robotics, conservation sensing, distributed identity, payment channels, and post-quantum migration. Research should be described as research. Each program requires a problem statement, technical hypothesis, owner, budget, threat model, intellectual-property position, experimental method, stopping rule, and path to deployment. Listing a technology in a roadmap is not evidence that it belongs in the architecture.

**ROADMAP STANDARD**

Progress is the accumulation of verified capability, not the passage of time or the number of announced initiatives.

## 13.9 Sequencing and operating cadence

The roadmap should recognize shared constraints. Network releases, treasury controls, product pilots, subsidiary oversight, security reviews, and mission programs compete for many of the same people, legal resources, data systems, and management attention. Starting each initiative independently can create a portfolio that is locally reasonable but collectively impossible. The Foundation should therefore maintain dependency maps, work-in-progress limits, accountable owners, and a consolidated capacity view before authorizing new material commitments.

A practical cadence is a quarterly gate review supported by monthly operating evidence for active high-risk work. The review should reconcile spend and MTRQ activity, update risks and dependencies, compare evidence with the next gate, identify stale assumptions, and make an explicit continue, expand, redesign, pause, transfer, or close decision. Annual planning should set portfolio limits and treasury capacity; it should not override failed gates.

# Risk Analysis

Metriq's model creates leverage: one technical or governance failure can affect the Foundation, network, treasury, operating companies, partners, and mission simultaneously.

## 14.1 Risk method

This section uses qualitative likelihood and impact rather than presenting false numerical precision. "High" does not mean certain; it means the exposure deserves active executive and board attention, defined controls, and evidence. Residual risk should be reassessed as implementation changes. Owners should record triggers, indicators, controls, contingency actions, and acceptance authority in a live risk register.

| Risk | Likelihood | Impact | Exposure | Primary controls |
|---|---|---|---|---|
| Key-person and governance concentration | High | High | Founder or small group controls strategy, information, keys, board decisions, and public claims. | Independent board capability, reserved powers, succession, threshold keys, delegated limits, records, and conflict controls. |
| Treasury concentration in MTRQ | High | High | Operating capacity falls with asset price or liquidity; sales affect market. | Liquidity reserve, stress testing, staged commitments, execution policy, diversification authority, and transparent reporting. |
| Validator and quorum concentration | High | High | Common operator, key, host, or quorum dependency undermines decentralization and resilience. | Independent operators, quorum analysis, infrastructure diversity, public configuration, and tested continuity. |
| Software fork and dependency drift | Medium-High | High | Security fixes or upstream changes are missed; custom changes become unmaintainable. | Upstream-delta register, supported versions, release engineering, dependency inventory, security advisories, and deprecation policy. |
| Unsupported public claims | High | High | Stakeholders rely on throughput, fee, compliance, impact, or availability statements lacking evidence. | Claim register, evidence states, legal/technical approval, expiration dates, and correction process. |
| Digital-asset regulatory change | High | High | Sales, custody, grants, payments, exchange access, or promotion become restricted or costly. | Activity-specific legal mapping, jurisdiction limits, contingency design, records, and controlled communications. |
| Security breach or key compromise | Medium | High | Loss of funds, service disruption, unsafe release, data exposure, or trust damage. | Threat models, threshold custody, secure development, monitoring, incident response, exercises, and independent review. |
| Product-market failure | High | Medium-High | Projects consume resources without recurring user demand or sustainable economics. | Staged pilots, user evidence, full unit economics, termination gates, and portfolio limits. |
| Mission drift | Medium | High | Commercial growth or token-market priorities displace intended outcomes. | Mission tests, board policy, profit commitment, program measurement, conflict rules, and public reporting. |

| Risk | Likelihood | Impact | Exposure | Primary controls |
|---|---|---|---|---|
| Overextension | High | High | Network, manufacturing, traceability, payments, AI, conservation, and other programs exceed management capacity. | Portfolio limits, sequencing, accountable owners, budgets, dependency mapping, and explicit closure decisions. |
| Subsidiary liability or quality failure | Medium | High | Physical product, contract, safety, quality, export, or customer failure affects Foundation assets and reputation. | Entity separation, insurance, QMS, contract review, safety and export controls, reporting, and board oversight. |
| Partner or counterparty failure | Medium | Medium-High | Partner misconduct, insolvency, security failure, poor data, or withdrawal disrupts a program. | Diligence, contracts, concentration limits, monitoring, audit rights, and alternate providers. |
| Reputational polarization | Medium | Medium-High | Mission language is interpreted as partisan, ideological, or inconsistent with technical execution. | Concrete outcomes, nonpartisan posture, disciplined claims, transparent decisions, and avoidance of performative language. |
| Data and privacy failure | Medium | High | Sensitive user, customer, health, location, or conservation data is exposed or immutably published. | Data minimization, classification, off-chain design, access controls, retention, privacy review, and incident response. |
| Market integrity and insider conduct | Medium | High | Undisclosed promotion, preferential transactions, manipulation, or insider dealing damages users and legal position. | Trading policy, disclosure, restricted lists, execution controls, related-party review, and independent oversight. |

## 14.2 Systemic interactions

Risks are correlated. A decline in MTRQ may reduce treasury capacity, increase pressure to make promotional claims, weaken funding for security and operations, and create conflict around market support. A network incident can impair product adoption, asset liquidity, treasury value, and the Foundation's reputation at the same time. A governance failure can compromise treasury, subsidiaries, claims, and incident response. Stress testing should therefore model multi-factor scenarios rather than one risk at a time.

The Foundation should define minimum viable operations: the services, people, legal obligations, keys, infrastructure, records, and financial reserves that must survive a severe downturn or leadership transition. Noncritical projects should have orderly pause and closure plans so resources can be redirected without losing essential evidence or creating unmanaged obligations.

## 14.3 Risk appetite and acceptance

High technical ambition is compatible with bounded experimentation. Metriq can take substantial research and product risk when the downside is limited, users understand the status, sensitive data and funds are protected, and failure does not create unacceptable safety or legal consequences. It should have low tolerance for undisclosed conflicts, uncontrolled treasury authority, misleading claims, falsified records, avoidable exposure of sensitive data, unsafe production release, or circumvention of law and regulation.

Risk acceptance should identify the decision owner, rationale, evidence, duration, compensating controls, trigger for reassessment, and maximum exposure. Material accepted risks should be visible to the board. Repeated "temporary" exceptions should be treated as control failures rather than normal operations.

## 14.4 Early-warning indicators

- Material increase in undocumented or unreconciled treasury transactions.
- Critical operations dependent on one person, key, vendor, region, repository, or hosting provider.

- Public claims expanding faster than technical documentation or production evidence.
- Large growth in programs without corresponding growth in accountable owners and control capacity.
- Subsidized activity reported as adoption without retention after incentives.
- Repeated postponement of audits, reconciliations, security reviews, or policy approvals.
- Board materials that omit incidents, conflicts, subsidiary losses, treasury concentration, or failed projects.
- Legacy code and naming debt increasing without a supported migration plan.
- Mission allocations evaluated by dollars announced rather than verified outcomes and full cost.

**RISK POSTURE**

Metriq should be aggressive in research and conservative in claims, custody, safety, and authority.

## 14.5 Risk ownership and escalation

Every material risk should have one accountable owner even when controls are distributed across teams. The owner maintains the exposure statement, indicators, control evidence, open actions, due dates, dependencies, and escalation threshold. Committees may review risk, but collective review should not obscure who is responsible for obtaining evidence and acting when a threshold is crossed.

Escalation criteria should include control failure, missed reconciliation, unauthorized access or transfer, material incident, regulatory inquiry, repeated policy exception, deteriorating liquidity or concentration, validator or service dependency, safety concern, adverse user outcome, and evidence that a public claim is no longer accurate. Emergency action may require pausing a service, release, transfer, pilot, or communication before the full investigation is complete.

## 14.6 Residual risk and shutdown authority

Controls reduce risk; they do not eliminate it. Residual risk should be stated after controls and accepted by an authority proportionate to the potential loss. Acceptance should expire or trigger review when assumptions, scale, jurisdictions, counterparties, software, data, or operating conditions change. Material residual risks should appear in board reporting together with the rationale for continuing.

Critical systems and programs should have tested shutdown, rollback, key-recovery, data-preservation, user-notification, and continuity procedures. The authority to stop unsafe or unauthorized activity must be clear in advance. A system that can be launched but not safely paused, transferred, or retired is not operationally complete.

# Conclusion

Build what the future requires - and publish the evidence that shows what has actually been built.

Metriq's model is straightforward to state and difficult to execute. The Foundation intends to build infrastructure, products, and companies; place them into real use; and reinvest the value they create into long-term technology development and defined mission priorities. The Metriq Network, Gravity, OrbitR, MTRQ, Metriq Dynamics, the proposed Centurial Fund, and future Foundation programs are instruments within that model. None is the mission by itself.

The strongest part of the architecture is its potential alignment of technical execution and long-horizon purpose. Commercial capability can produce revenue, knowledge, distribution, manufacturing capacity, and institutional resilience. A century-scale allocation can support work that shorter cycles neglect. Open infrastructure can give users and operators a shared platform. The nonprofit structure can direct the destination of value away from conventional private extraction.

The same architecture creates material risks. Concentrated governance can undermine the nonprofit purpose. Concentrated validators can undermine decentralization. Concentrated treasury assets can undermine financial durability. Unsupported claims can undermine trust. An ambitious portfolio can outrun management and control capacity. A century-scale schedule can become a century-scale liability if custody, policy, and succession are weak.

Metriq should therefore be evaluated by observable standards: whether the technology works; whether users choose it; whether security and failure are managed; whether economics are sustainable; whether authority and conflicts are controlled; whether claims match evidence; whether resources are reconciled; and whether measurable outcomes advance abundance, wildlife conservation, and health, safety, and access.

**Build. Deploy. Create value. Reinvest. Scale what works.**

This paper is a working architecture for that standard. The next step is not a larger promise. It is completion of the evidence and governance gates required to publish the final version with precision.

# Evidence-State Register

This register is the publication position of version 6.0. It should be updated immediately before final release.

| Capability or claim | Description | State | Release condition |
|---|---|---|---|
| Metriq Foundation, Inc. | Foundation organization and governance center. | Implemented | Confirm current corporate and tax-status language, board authority, and governing documents before final publication. |
| Metriq Dynamics, Inc. | Foundation-owned manufacturing and engineering subsidiary. | Implemented | Confirm current ownership, good standing, operational scope, insurance, QMS status, and intercompany agreements. |
| Gravity source code | Core/node implementation publicly available. | Implemented | Identify supported branch, release, commit, upstream delta, build provenance, tests, and security status. |
| OrbitR source code | Client-facing API and indexing service publicly available. | Implemented | Identify supported branch, release, endpoint configuration, tests, privacy, and service status. |
| Public OrbitR service | Endpoint identified at orbitr.metriq.org. | Implemented | Publish availability window, operator, terms, monitoring, version, limits, and incident contact. |
| Metriq-operated validators | Four endpoints listed in the public portal. | Implemented | Verify live status, keys, versions, regions, hosts, archives, quorum configuration, and monitoring. |
| Independent validator ecosystem | Material consensus participation by unaffiliated operators. | Unvalidated / target | Publish operator independence and quorum evidence before claiming decentralized operation beyond the software design. |
| Metriq Lab | Public learning and transaction tools. | Implemented | Verify current functionality, supported network, privacy, security, and maintenance owner. |
| MTRQ native coin | Native asset used by the Metriq Network. | Implemented | Verify authoritative asset and genesis identifiers, protocol functions, current configuration, and naming. |
| One trillion MTRQ genesis supply | Documented supply design. | Documented; reconciliation required | Publish authoritative genesis and current supply reconciliation. |
| 900B Centurial / 100B Seed allocation | Documented allocation design. | Documented; reconciliation required | Publish accounts, control labels, historical movements, remaining balances, and restrictions. |
| 9B annual century tranche | Arithmetic design. | Proposed operating schedule | Confirm release mechanics, authority, carryforward, custody, legal treatment, and reporting. |
| Centurial Fund | Long-horizon treasury and allocation institution. | Proposed | Adopt charter, custody, allocation policy, conflicts, reporting, audit, continuity, and first-year operating plan. |
| 100% profit commitment | Public organizational commitment. | Policy commitment; definition required | Approve exact covered entities, financial measure, reserves, exceptions, timing, and reporting. |
| Smart-contract capability | General programmable contract execution. | Proposed unless separately evidenced | Identify production release, protocol activation, documentation, audits, test and production evidence. |

| Capability or claim | Description | State | Release condition |
|---|---|---|---|
| Cross-network bridges | Interoperability with external networks. | Proposed | Define verification and custody model, threat analysis, audit, governance, limits, monitoring, and incident plan. |
| Zero-fee payment processing | User-facing payment service subsidizing fees. | Proposed | Define entity, licensing, funds flow, banking/custody, pricing, fraud, support, unit economics, and pilot evidence. |
| Metriq Trade Traceability | Pre-enrolled identity and evidence-conditioned traceability program. | Design / controlled R&D | Keep patent-sensitive details controlled; complete engineering, security, privacy, standards, legal, and pilot gates. |
| Autonomous manufacturing | Progressive automation from intent through production. | Implemented components; broader autonomy proposed | Publish autonomy levels, human authority, safety gates, production cases, quality evidence, and limitations. |
| Network throughput / finality / fees | Numeric performance profile. | Unvalidated for general public claims | Publish reproducible benchmark and production evidence; remove unsupported legacy numbers. |
| Mission programs | Direct abundance, wildlife, and health/safety/access work. | Program-specific | Each program requires its own charter, evidence state, partners, budget, metrics, and report. |

**REGISTER CONTROL**

The evidence state should be assigned by the accountable owner and reviewed by technical, legal, financial, security, and communications personnel appropriate to the claim. Unsupported status upgrades are control failures.

# Economic Design and Analytical Calculations

These calculations explain the documented design. They do not attest to current balances, market value, liquidity, or legal treatment.

## B.1 Supply arithmetic

| Calculation | Formula | Result |
|---|---|---|
| Centurial share | 900,000,000,000 / 1,000,000,000,000 | 90% |
| Seed share | 100,000,000,000 / 1,000,000,000,000 | 10% |
| Equal annual century tranche | 900,000,000,000 / 100 | 9,000,000,000 MTRQ |
| Annual tranche as share of genesis supply | 9,000,000,000 / 1,000,000,000,000 | 0.9% |
| Cumulative scheduled availability after 25 years | 9,000,000,000 x 25 | 225,000,000,000 MTRQ |
| Cumulative scheduled availability after 50 years | 9,000,000,000 x 50 | 450,000,000,000 MTRQ |
| Cumulative scheduled availability after 75 years | 9,000,000,000 x 75 | 675,000,000,000 MTRQ |
| Cumulative scheduled availability after 100 years | 9,000,000,000 x 100 | 900,000,000,000 MTRQ |

## B.2 Nominal tokens are not operating capacity

The number of MTRQ released in a year does not determine how much work the Foundation can fund. Operating capacity depends on the asset's lawful convertibility, realized price, market depth, execution cost, restrictions, taxes, custody, timing, and the availability of vendors or employees willing and able to accept the asset. A budget should therefore be denominated in the currency of the obligation and should state the conversion assumptions used.

For example, a nine billion MTRQ annual authority can support radically different operating budgets under different prices. More importantly, the amount that can be realized without unacceptable market impact may be much lower than the marked value of the balance. Treasury reporting should distinguish token quantity, accounting value, realizable liquidity at defined horizons, committed obligations, restricted amounts, and stress value.

## B.3 Scenario framework

| Variable | Base question | Stress question |
|---|---|---|
| Market price | What valuation basis is used for planning and reporting? | What happens at 75%, 90%, or near-total decline? |
| Market depth | What can be sold or transferred at acceptable cost? | What if primary venues suspend or depth disappears? |
| Operating burn | What fixed and variable obligations exist over 24-36 months? | Which costs cannot be reduced without impairing security, legal compliance, or core operations? |
| Release use | What portion is retained, granted, invested, or sold? | What if program capacity cannot responsibly use the available amount? |

| Variable | Base question | Stress question |
|---|---|---|
| Counterparty access | Which banks, custodians, exchanges, vendors, and partners are required? | What if a major counterparty freezes, exits, or becomes prohibited? |
| Regulatory treatment | Which activities are permitted under current analysis? | What if sale, custody, grant, or cross-border rules materially change? |

## B.4 Allocation decision model

A proposed allocation can be compared across expected mission result, probability of success, time to evidence, total cost, reversibility, operating burden, legal and safety exposure, strategic learning, correlation with the existing portfolio, and opportunity cost. Scores can structure discussion but should not replace judgment. The underlying assumptions and uncertainty matter more than a composite number.

| Factor | Illustrative review question |
|---|---|
| Mission result | What specific outcome is expected, for whom or what, and over what period? |
| Evidence strength | What prior technical, user, scientific, or operating evidence supports the thesis? |
| Cost effectiveness | What is the expected full cost per unit of outcome, including overhead and risk? |
| Additionality | What changes because Metriq participates that would not otherwise occur on similar terms? |
| Reversibility | Can the decision be paused, reduced, transferred, or terminated without unacceptable loss? |
| Strategic capability | Does the work create reusable code, data, equipment, distribution, knowledge, or partnerships? |
| Risk | What technical, legal, security, safety, market, governance, and reputation exposure is created? |
| Measurement | Can the result be observed with a credible baseline and attribution method? |

# Governance and Release-Control Checklist

A concise control baseline for the final publication and first operating phase.

| Control domain | Minimum release evidence |
|---|---|
| Corporate and authority | Current entity records; board and officer authority; subsidiary ownership; reserved powers; registered filings; current governing documents. |
| Profit commitment | Board-approved policy defining covered entities, financial measure, reserves, exceptions, timing, transfer path, and public reporting. |
| Treasury | Authoritative balances; signer map; threshold custody; recovery; transaction limits; reconciliation; valuation; liquidity; execution; related-party and counterparty controls. |
| Centurial Fund | Charter; annual availability rule; carryforward; allocation programs; conflicts; approval; milestones; audit; reporting; continuity; market-impact and legal review. |
| Network releases | Supported branches; commit and version; build provenance; tests; dependency inventory; signed artifacts; configuration; upgrade and rollback; vulnerability handling. |
| Validators | Operator identity and independence; keys; hosting; geography; versions; quorum sets; blocking sets; archives; monitoring; incidents; continuity. |
| OrbitR and public services | Owner; endpoint; version; capacity; privacy; security; rate limits; monitoring; availability; terms; support; incident contact. |
| Claims | Controlled register; exact wording; evidence state; owner; source; review date; expiry; limitations; correction path; superseded-material removal. |
| Products and pilots | Charter; user problem; architecture; budget; legal and security review; data policy; support; measures; adverse events; exit criteria. |
| Subsidiaries and investments | Diligence; capitalization; authority; conflicts; intercompany terms; IP; data; reporting; insurance; profit treatment; exit or dissolution. |
| Mission programs | Baseline; causal pathway; partner diligence; restrictions; full cost; outcome measures; attribution; reporting; continuation and closure thresholds. |
| Security and privacy | Threat models; key classification; secure development; access; logging; retention; incident response; exercises; external review; corrective actions. |
| Legal review | Nonprofit and tax status; MTRQ activities; treasury; payments; grants; investments; data; manufacturing; IP; sanctions; export; public claims. |
| Final publication | Board or delegated approval; current source check; brand compliance; accessibility; link validation; document metadata; PDF preflight; archived source package. |

# Glossary

Terms are used narrowly to prevent the organization, network, coin, software, and evidence states from being conflated.

| Term | Definition |
|---|---|
| Blocking set | A set of nodes whose nonparticipation can prevent a validator from reaching its threshold for agreement. |
| Centurial Fund | The proposed century-scale treasury and allocation architecture associated with the documented 900 billion MTRQ allocation. |
| Claim register | A controlled record of material public claims, including exact wording, owner, evidence state, source, date, limitations, and review status. |
| Federated Byzantine Agreement (FBA) | A consensus model in which participants select their own trust relationships rather than relying on protocol-defined mining power or stake weight. |
| Gravity | The Metriq core and node implementation derived from Stellar Core. |
| Implemented | An evidence state indicating that a codebase, service, policy, or operation exists in working form and can be inspected. |
| Metriq | The master brand and primary public identity. |
| Metriq Dynamics | A distinct Foundation-owned manufacturing and engineering subsidiary. |
| Metriq Foundation | The nonprofit organizational and governance entity; not a separate improvised logo. |
| Metriq Network | The decentralized ledger and transaction environment operated by compatible nodes. |
| MTRQ | The native coin of the Metriq Network. Always uppercase. |
| OrbitR | The client-facing API and indexing layer derived from Horizon. Preserve the capital R. |
| Production validated | An evidence state indicating that a capability or claim has been demonstrated under defined production conditions with a published method and limitations. |
| Proposed | An evidence state indicating that an architecture, policy, product, or capability is defined but not yet delivered. |
| Quorum | A set of validators sufficient to reach agreement in which each member contains a quorum slice within the set. |
| Quorum set | The set of nodes a validator selects as relevant to reaching agreement. |
| Quorum slice | A subset of a validator's quorum set sufficient for that validator to advance under its configured threshold. |
| Simulated | An evidence state indicating that a result was produced in a bounded test, model, or laboratory environment with stated assumptions. |
| Stellar Consensus Protocol (SCP) | The federated consensus protocol on which Gravity's consensus design is based. |
| Treasury | Assets, accounts, custody arrangements, policies, authority, processes, and records used to fund and protect organizational operations. |

# References and Source Basis

Public web sources were accessed 15 July 2026. Repositories, standards, services, and guidance can change; verify the current version before claiming conformance or availability.

**[1] Metriq Foundation - official website.** Source

**[2] Metriq Foundation - About, mission, network, MTRQ, and legacy Century Fund descriptions.** Source

**[3] Metriq Portal - public Gravity validators, OrbitR endpoint, Lab, and history archives.** Source

**[4] MetriqOrg/Gravity - public source repository, prod branch.** Source

**[5] MetriqOrg/go - OrbitR service source and documentation.** Source

**[6] Stellar Development Foundation - Stellar Consensus Protocol overview.** Source

**[7] Metriq Dynamics - operating capabilities and Foundation ownership statement.** Source

**[8] Metriq Whitepaper, October 2025 - superseded public version.** Source

**[9] NIST SP 800-218 - Secure Software Development Framework (SSDF).** Source

**[10] NIST SP 800-57 Part 1 Revision 5 - Recommendation for Key Management.** Source

**[11] NIST SP 800-207 - Zero Trust Architecture.** Source

**[12] Metriq Brand Standards, version 3.2 - controlled brand package supplied by Metriq Foundation.** Internal controlled source, 2026

**[13] Metriq Trade Traceability technical white paper and patent-review materials.** Internal controlled sources, 2026

**[14] Metriq Dynamics Quality Management System manual, revision 1.0.** Internal controlled source, 2026

## Internal source controls

Internal materials should be cited in the final publication only to the extent that disclosure is authorized and does not compromise patent rights, confidential business information, security, personal data, customer obligations, or controlled technical data. The public paper should state when a conclusion depends on internal evidence that is available only to qualified reviewers.

**FINAL PUBLICATION GATE**

Before public release, reconcile the MTRQ supply and custody records; approve the profit commitment language; determine the Centurial Fund evidence state; verify live network and service details; complete legal and security review; validate all links; and remove or redirect superseded public copies.