QANOVRA

WHITEPAPER v2.4.2

A security-first Layer-1 blockchain for verifiable digital infrastructure

Document status	Value
Version	2.4.2 - Publication Layout Final Candidate
Date	23 August 2026
Network baseline	Qanovra L1 v3.7.5 — Frozen L1
Native asset	QNV
Maximum supply	10,000,000,000 QNV
Genesis hash	`78cefe355c7fb55c53dd173c9ca9d340306054a7fd5718e70d1d3193be7b93a3`
Chain ID	qnv-78cefe355c7fb55c53dd173c
Classification	Final layout candidate derived from audit-approved v2.4 LogoFix and layout-audited v2.4.1; no protocol or policy change

Qanovra UG (haftungsbeschränkt) i. G. was initiated in Germany on 13 August 2026 and notarized/formed on 21 August 2026. This technical whitepaper is not a legal, regulatory or offering document and is not a public-mainnet approval.

1. Executive Summary

Qanovra is a purpose-built Layer-1 blockchain designed around a simple premise: critical digital infrastructure should be deterministic, independently verifiable, operationally resilient and usable without sacrificing security. The project combines a frozen L1 protocol baseline with a separately audited operational ecosystem containing wallet, explorer, SDKs, RPC infrastructure, operator tooling, key-ceremony orchestration, recovery controls and external verification mechanisms.

The current technical baseline is Qanovra L1 v3.7.5. Its network identity is cryptographically bound to the genesis configuration. The genesis hash is 78cefe355c7fb55c53dd173c9ca9d340306054a7fd5718e70d1d3193be7b93a3 and the derived Chain ID is qnv-78cefe355c7fb55c53dd173c. The native asset is QNV, with a fixed maximum supply of 10 billion QNV.

Qanovra deliberately distinguishes software readiness from real-world readiness. Passing internal and independent technical review does not substitute for external actions such as the real HSM/key ceremony, independent validator onboarding, geographic disaster-recovery rehearsal, formal independent security attestation and legal approval. Those gates remain explicit rather than being converted into software-only claims.

2. Mission and Design Philosophy

Qanovra is intended to provide a dependable base layer for value transfer, applications, machine-to-machine coordination and future digital infrastructure. Its design philosophy prioritizes verifiability over marketing claims and fail-closed behavior over optimistic assumptions.

- Security first: state-changing operations are authorized, bounded and evidence-oriented.
- Determinism: genesis, canonical encoding and cross-client behavior are treated as protocol invariants.
- Single source of truth: the account state is the authoritative ledger; tokenomics is policy over that ledger.
- Operational resilience: recovery, multi-region operation, incident evidence and chaos qualification are first-class concerns.
- Developer usability: SDKs, RPCs, explorer and operator tooling are maintained as a coherent parallel ecosystem.
- Conservative release governance: invite-testnet and production approvals remain false until their actual external gates are completed.

3. Network Identity and Frozen L1 Baseline

Parameter	Current canonical value
L1 version	v3.7.5
State	Frozen L1 baseline
Candidate archive SHA-256	`1c41b8e5e7f757de2a79937ab5e408021718a456e2eb29f9b1c596a6ccab2414`
Genesis hash	`78cefe355c7fb55c53dd173c9ca9d340306054a7fd5718e70d1d3193be7b93a3`
Chain ID	qnv-78cefe355c7fb55c53dd173c
Native unit	QNV
Base unit	qnv-atom
Decimals	5
1 QNV	100,000 qnv-atom
Maximum ledger supply	1,000,000,000,000,000 qnv-atom

Five decimal places were selected as the maximum precision compatible with the protocol's existing safe-integer canonicalization contract. This keeps the full 10 billion QNV supply within the canonical integer range while preserving practical divisibility.

4. Ledger, Genesis and Supply Integrity

Qanovra uses one authoritative AccountState ledger. Genesis allocations are loaded deterministically and the network Chain ID is derived from the genesis hash. Protocol-controlled vaults occupy the reserved qnv:system: namespace and are structurally separated from ordinary user accounts.

- Genesis loading is deterministic and bound to network identity.
- Protocol vault accounts are derived from their authorities rather than represented by arbitrary magic account names.
- Treasury is constrained to an exact 4-of-7 authorization model in the genesis policy.
- Supply invariants are checked against the authoritative ledger.
- Slashing is supply-accounted; reward accrual cannot silently create unbacked supply.
- Cross-client canonicalization and genesis-byte parity are treated as release-gate properties.

5. QNV Tokenomics

QNV is the native asset of Qanovra. The maximum supply is permanently defined as 10,000,000,000 QNV. The allocation model is designed to balance network security, ecosystem development, long-term treasury capacity, team incentives and founder alignment.

Allocation	Share	QNV
Community & network security	51.75%	5,175,000,000
Ambassador program	0.25%	25,000,000
Treasury & ecosystem	15.00%	1,500,000,000
Founder	15.00%	1,500,000,000
Core team	8.00%	800,000,000
Remaining canonical allocations	10.00%	1,000,000,000
TOTAL	100.00%	10,000,000,000

The final 10% is intentionally not relabeled in this whitepaper without the canonical genesis allocation schedule. The on-chain genesis configuration remains authoritative. This avoids inventing a category name merely to make a presentation table appear complete.

Allocation release policy (v2.4 publication update): The Founder allocation of 15% (1,500,000,000 QNV) is available from Genesis by design and is not represented as protocol-locked or vested. The absence of a protocol-enforced founder lock is therefore disclosed explicitly as a concentration and liquidity risk rather than obscured behind generic alignment language.

Core-team allocation policy: individual grants from the 8% Core Team allocation are subject to a 48-month vesting schedule measured from the applicable grant date, with a 12-month cliff followed by monthly linear vesting over the remaining 36 months. Ungranted balances remain within the designated allocation vault. This is a v2.4 launch-policy commitment and MUST be reflected in canonical vault/configuration evidence before broader network activation; this document does not claim that prose alone activates enforcement.

Treasury & ecosystem assets remain separately governed by the exact 4-of-7 authorization policy and its canonical timelock/cap controls. Founder, Core Team and Treasury allocations MUST NOT be presented as having identical liquidity or authorization conditions.

6. Staking and Validator Economics

Parameter	Policy
Minimum delegator stake	100 QNV
Minimum validator self-stake	100,000 QNV
Target staking ratio	55–70%
Target gross APR	approximately 8% at the 62.5% policy midpoint
Dynamic target corridor	6–10%, dependent on staking participation
Unbonding	Protocol value to be cited from the canonical configuration; not guessed in this document
Reward funding	Network-security protocol fees first; authorized Community & network security reserve covers a funded shortfall
Supply rule	No reward minting above the fixed 10,000,000,000 QNV maximum supply
APR target function	10% at <=55% staking; linear decline to 6% at >=70%; approximately 8% at 62.5%
Budget constraint	Effective rewards are capped by funded balances; target APR is not guaranteed

The staking model is intended to encourage broad participation while requiring meaningful validator alignment. Economic parameters are not treated as substitutes for cryptographic or operational security; validator identity, key custody, independent operation and evidence remain separate requirements.

Reward Funding & Emission Policy. QNV remains supply-capped at 10,000,000,000. Validator/delegator rewards MUST be paid only from already-funded AccountState balances: first from protocol fee revenue assigned to the network-security reward budget and, where required, from an explicitly authorized draw on the Community & network security allocation. Rewards MUST NOT mint unbacked QNV or increase the maximum supply.

For staking ratio s, the v2.4 target gross reward rate is r_target(s) = 10% for s <= 55%; it decreases linearly from 10% at 55% to 6% at 70%; and is 6% for s >= 70%. The midpoint s = 62.5% therefore corresponds to approximately 8%. This is a target, not a guaranteed return. If funded fee revenue plus authorized reward reserve is insufficient, the effective reward rate MUST fall below the target rather than create new supply.

Funding-horizon disclosure: if the 5,175,000,000 QNV Community & network security allocation were hypothetically used only for the policy-defined staking subsidy corridor, the indicative reserve life would be approximately 9.41 years at 55% total staking, approximately 10.35 years at 62.5% total staking, and approximately 12.32 years at 70% total staking. These values are calculated from the declared r_target(s) function and replace the earlier flat-8% illustration. They are not reserve-life promises: that allocation also serves broader network-security/community purposes, while protocol fees can reduce reserve draw. Once authorized subsidy funding is exhausted, rewards must be supported by funded fee revenue or another separately approved, already-funded source; no inflation backstop is implied.

Gross APR is stated before any operator commission. Validator commission is an operator-disclosed commercial parameter and is not represented here as consensus voting weight. The exact transaction-fee assessment formula remains implementation-authoritative until extracted from the canonical launch configuration; v2.4 does not invent a fee number.

7. Slashing Policy

Event / tier	Consequence / percentage
Normal / proportionate downtime	0% slash; reduced or lost rewards
Below 95% expected signatures in rolling 10,000-block window	0.10% slash + temporary jail
Repeated downtime	0.25% slash + temporary jail
Chronic downtime	up to 0.50% slash + temporary jail
Double-signing / equivocation	5% base slash + permanent tombstone of validator key
Consensus-threatening / Byzantine behavior	minimum 5% base slash
Correlated misconduct <1% of active validator count	5%
Correlated misconduct 1% to <5% of active validator count	10%
Correlated misconduct 5% to <10% of active validator count	20%
Correlated misconduct 10% to <20% of active validator count	50%
Correlated misconduct 20% to <1/3 of active validator count	75%
Systemic consensus-threatening participation >=1/3 of active validator count	100%

For correlated misconduct, the percentage is defined against the count of active admitted validators, not stake weight. Let c = involved_active_validators / active_validator_count. The slash principal base under the v2.4 publication-candidate policy is the validator's total bonded stake economically attributable to the offending validator at the time of slash evaluation, including validator self-stake and active delegated stake assigned to that validator. The effective principal slash is effective_slash = max(base_slash, correlated_slash(c)); base and correlation percentages are not added or multiplied. Slash principal is defined as burn in the v2.4 launch policy and must be reflected in burned_supply. A temporary jail lasts at least one complete 10,000-block observation window; this duration is intentionally normative in blocks, and no canonical real-time equivalent is published here until block-cadence extraction is complete. Unjail requires expiry of that window, a signed operator request, a non-tombstoned key and successful current eligibility/health checks. A tombstoned validator key can never be unjailed. These v2.4 semantics require implementation/conformance evidence before launch.

8. Security Architecture

Qanovra's security model is layered. Protocol safety, application authorization, operational custody, build reproducibility and evidence integrity are treated as different security domains rather than collapsed into one claim.

- Atomic ledger/state handling and restart reconciliation.
- Request authentication with body binding, freshness windows and replay protection.
- Reserved system-account namespace and policy-controlled vault movement.
- Bounded tokenomics message amounts and fail-closed validation.
- Pinned build/toolchain controls and supply-chain evidence.
- Offline verification of manifests, signatures, provenance and frozen-core bindings.
- Explicit separation between software evidence and independent real-world attestations.

9. Key Ceremony and Treasury Control

Qanovra's ceremony architecture is built around seven participants plus an independent observer and an exact 4-of-7 authorization threshold. The tooling supports offline coordination, role enforcement, signed and hash-chained transcripts, QR/USB air-gap transfer, abort/retry behavior and non-exporting provider adapters.

The ceremony layer orchestrates threshold authorization and evidence. It does not claim to implement a novel threshold-Ed25519/DKG protocol. Actual non-exportable signing must be provided by an audited HSM, KMS, Vault or established threshold-signature provider. The real ceremony remains an external execution gate until performed and attested.

10. Qanovra Wallet

The Qanovra Wallet is developed as a separate security-sensitive product surface. The audited frozen line reached v0.30.17 Final Freeze Evidence Closure. In that audit, all three findings from the preceding report were closed and no new finding was raised; the full test suite reported 664/664 passing.

The wallet nevertheless keeps external readiness conservative. Browser end-to-end evidence and real environment qualification are not replaced by internal flags. This distinction is central to Qanovra's release model.

11. Parallel Ecosystem

The Parallel Ecosystem surrounds the frozen L1 without silently modifying consensus, genesis, tokenomics or node runtime. Its role is to make the chain operable, observable, integrable and independently verifiable.

- Explorer with canonical/reorg/orphan awareness and QNV transparency surfaces.
- RPC infrastructure with geographic routing, read-only policy, quotas and bounded WebSockets.
- Python and TypeScript SDKs with security and determinism guards.
- Multi-operator control plane with RBAC, signed enrollment, mTLS, certificate lifecycle and tamper-evident audit.
- Recovery orchestration with deterministic archives, authenticated encryption, regional replication and state-root verification.
- Chaos/soak qualification for network, host, snapshot, validator and Byzantine failure scenarios.
- Standalone verification tooling covering hashes, manifests, signatures, provenance, SBOMs and frozen-L1 binding.
- Deployment examples for containerized and Kubernetes-based high-availability operation.

Parallel Ecosystem v0.13.0 RC12 reached a final software-freeze assessment with no open software remediation item in its audit. Invite-testnet and production approval remained deliberately false because external gates cannot be closed by software alone.

Explorer reorg/orphan awareness refers to competing or abandoned candidates before finalization. Under the documented finalization invariant, an already-finalized height cannot be finalized a second time; v2.4 does not claim post-finalization reorganization as normal network behavior.

12. Developer Experience

Developer adoption depends on predictable interfaces as much as raw protocol capability. Qanovra therefore treats SDK symmetry, deterministic serialization, typed parameters, installable packages, secure redirect behavior, API contracts and reproducible toolchains as product requirements.

The goal is a development path in which an application team can move from documentation to SDK to RPC to explorer without learning a different security model at every boundary.

13. Governance

Governance is designed to minimize unilateral control over protocol-controlled assets and high-impact operations. Treasury actions are subject to threshold authorization and policy constraints, while operational roles are separated through the multi-operator control plane.

The governance philosophy is deliberately evidence-driven: approvals, changes, recovery actions and ceremony events should leave verifiable artifacts. This supports accountability without requiring users to trust an opaque operator narrative.

14. Resilience and Disaster Recovery

Availability is approached as an engineering discipline rather than an absolute promise. Qanovra's operational stack includes encrypted multi-region backups, deterministic archives, empty-server restore workflows, state-root matching, validator restart evidence, safe-point rollback and chaos qualification.

No blockchain can truthfully promise literal 100% uptime under every physical, legal or network condition. Qanovra's objective is instead to maximize fault tolerance, make failure modes observable, and provide tested recovery paths with independent evidence.

15. Intended Use Cases

- Native digital value transfer and staking.
- Developer applications requiring deterministic settlement and verifiable state.
- Institutional integrations through controlled RPC/SDK surfaces.
- Machine-to-machine and future robot/agent coordination where autonomous actors require a shared verifiable ledger.
- Payments and programmable economic workflows.
- Long-lived digital ownership and inheritance-oriented applications built outside the frozen consensus boundary.
- Infrastructure requiring auditable operator actions and recovery evidence.

16. Release and Audit Model

Qanovra uses staged readiness. A software artifact may be technically closed while the network remains unauthorized for invite-testnet or production. This is intentional. Appendix C is the single current readiness snapshot for operational gates; this section defines the release model and does not duplicate volatile gate states.

17. Organizational Status

The formation of Qanovra UG (haftungsbeschränkt) was initiated on 13 August 2026 and notarized on 21 August 2026 in Germany. Until commercial-register registration is completed, public and institutional documents should describe the entity as 'Qanovra UG (haftungsbeschränkt) i. G.' or an equivalent German formation-status wording. Final legal form, registry status and mandatory disclosures remain subject to professional legal review.

18. Roadmap to Invite Testnet

- Complete formal independent L1 attestation against the v3.7.5 candidate and its bound genesis identity.
- Execute the real 4-of-7 key ceremony with the selected HSM/KMS provider(s) and independent observer.
- Onboard organizationally independent validator operators.
- Run and evidence a genuinely geographic recovery exercise.
- Complete remaining independent security and legal gates.
- Qualify wallet/browser and operational environments with real external evidence.
- Only then change invite-testnet authorization flags through the governed release process.

19. Risk Disclosure and Non-Claims

This whitepaper is a technical and strategic description, not a guarantee of investment performance, legal status, regulatory approval, uninterrupted availability or immunity from defects. Cryptographic systems, software, hardware custody, network infrastructure and governance processes all carry residual risk. Under the v2.4 publication-candidate launch policy, slashing percentages apply to the offending validator's total bonded stake attributable to that validator, including delegated stake; delegators therefore bear proportional slashing exposure and should treat validator selection as a security decision rather than a passive-yield choice.

The words 'frozen', 'closed' and 'verified' refer only to the specifically identified technical baseline or audit scope. They must not be interpreted as a claim that all external operational, regulatory or security gates have already occurred.

Regulatory-document separation: this technical whitepaper is not intended to serve as an EU MiCA crypto-asset white paper or as a substitute for any offering, admission-to-trading, consumer-disclosure or regulatory filing that may be legally required. Any public offer or EEA market-access process requires a separate legal assessment and, where applicable, a dedicated compliant disclosure document. P0-09 remains fail-closed until written legal review exists. Cryptographic-migration posture: Qanovra v3.7.5 is not post-quantum secure. It is instead described as migration-prepared: any future move to successor signature suites such as ML-DSA and/or SLH-DSA requires a versioned protocol upgrade, updated conformance vectors, explicit validator/system-key rotation procedures and an authenticated user-account rebinding path for holders.

20. Canonical Technical References

Reference	Value / role
Qanovra L1	v3.7.5 Frozen L1
Genesis	`78cefe355c7fb55c53dd173c9ca9d340306054a7fd5718e70d1d3193be7b93a3`
Chain ID	qnv-78cefe355c7fb55c53dd173c
Asset	QNV
Base unit	qnv-atom, 5 decimals, 100,000 qnv-atom per QNV
Maximum supply	10,000,000,000 QNV
Wallet	v0.30.17 Final Freeze Evidence Closure
Parallel Ecosystem	v0.13.0 RC12 software freeze; operative v3.7.5 repin
Treasury/key policy	Exact 4-of-7 authorization; seven participants plus observer for real ceremony

21. Conclusion

Qanovra is being built as a security-first blockchain platform whose differentiator is not a single headline feature, but the combination of deterministic protocol identity, bounded economics, threshold-controlled system assets, independent verification, operational resilience and a developer-facing ecosystem that is held to the same release discipline.

The v2.4 whitepaper is a publication candidate based on the external v2.2 document audit and the v2.3 re-audit of 21 August 2026. It closes the three high-severity documentation findings by defining reward funding/emission policy, explicitly disclosing Founder liquidity and Core Team vesting, and completing slashing bands and combination semantics. It preserves Qanovra L1 v3.7.5 as the frozen technical baseline and keeps unresolved canonical-value extraction and all real-world launch gates explicit.

Appendix A — Evidence Snapshot

The v3.7.5 technical handoff records a 34/34 gate pass, 284 Python tests with zero failures, and three supply-fuzz seeds preserving the full ledger supply. The genesis hash and Chain ID above are unchanged across the v3.7.5 handoff.

The wallet v0.30.17 Final Freeze Evidence Closure audit records 1,072/1,072 checksum entries valid and 664/664 tests passing. The Parallel Ecosystem RC12 audit reports no new finding and no open software remediation item, while retaining external invite-testnet gates.

Appendix B — Document Control

Field	Value
Document	Qanovra Whitepaper
Version	2.4.2 - Publication Layout Final Candidate
Status	Publication Layout Final Candidate
Supersedes	Whitepaper v2.4.1 Publication Layout Revision (delta-audited, 23 August 2026)
Baseline date	21 August 2026 substantive baseline; layout revision 23 August 2026
Change discipline	Any change to consensus, genesis, tokenomics or frozen runtime requires explicit versioning and renewed evidence
Document history	v2.0 initial audit-candidate line; v2.2 readiness refresh and external document audit; v2.3 audit-remediation candidate; v2.4 publication-candidate closure of re-audit findings; v2.4.1 typography/pagination revision; v2.4.2 hash-cell typography micro-fix only
Audit basis	External Qanovra Papers v2.3 re-audit dated 21 August 2026

Appendix C - Current Readiness Snapshot

Baseline date: 21 August 2026. This appendix updates operational and release-readiness evidence without changing the frozen Qanovra L1 v3.7.5 protocol baseline.

Gate / area	Current status	Audit treatment
Frozen L1	Qanovra L1 v3.7.5 remains the operative frozen protocol baseline.	Treat as technical baseline; protocol changes require a new version and renewed evidence.
Wallet	Qanovra Wallet v0.30.17 remains the current audited/freeze line used by the readiness evidence set.	Reference only evidence tied to the exact v0.30.17 artifact set.
P1-02 Real Device Matrix	Windows, Android and iOS profiles have been exercised with real-device evidence; the project records the matrix as complete.	Attach the final central matrix, profile closures and hashes to the audit package.
P1-03 Reproducible Builds	Independent Windows/macOS rebuild comparison produced matching runtime and vendor trees with zero unexplained differences; technical result PASS.	Attach Builder A/B manifests and the signed/final observer attestation before representing the gate as formally closed.
P1-04 Runbooks	Operational runbooks have been executed/completed in the current project line.	Attach execution evidence, closure summary and hashes; distinguish rehearsals from production incidents.
P0-04 Production signing / live HSM	Live production-signing evidence is still fail-closed where only templates/example provider configurations exist.	Do not treat cloud/KMS examples or dry runs as production HSM evidence.
P0-05 Key ceremony	4-of-7 ceremony mechanics and negative controls have technical PASS evidence; production-qualified ceremony/HSM evidence remains a separate real-world requirement unless final signed ceremony evidence is supplied.	Audit the ceremony transcript, participant attestations, observer attestation and non-exportable key evidence.
P0-06 Independent validators	Five candidate slots and five onboarding packages are ready; real operators assigned: 0/5; operators admitted: 0/5; final state BLOCKED_REAL_INFRA.	Keep gate OPEN until independent organizations return evidence and are admitted fail-closed.
P0-07 Multi-region / DR	Software and runbook support exists; genuinely geographic production-grade qualification remains an external infrastructure gate.	Require real hosts/regions, failure-domain evidence and recovery drill artifacts.
P0-08 Independent security assessment	Separate external gate.	Do not infer completion from internal test/audit evidence.
P0-09 Legal / regulatory approval	Separate external gate for intended launch context.	Keep launch authorization fail-closed until written legal review is available.

Audit note: Only evidence-backed states are represented as complete. Prepared packages, internal rehearsals and technical prechecks are not treated as substitutes for independent real-world execution.

Appendix D - Audit Handoff Requirements

- Freeze the exact DOCX/PDF pair and generate SHA-256 hashes only after final formatting is complete.
- Include canonical L1 v3.7.5 genesis, Chain ID and release-evidence references used by both papers.
- Include the final P1-02 matrix closure, P1-03 Builder A/B evidence and observer attestation, and P1-04 runbook closure evidence.
- Include the P0-06 operator package index and five package hashes, while explicitly retaining 0/5 assigned and 0/5 admitted until that changes.
- Provide an evidence-to-claim matrix so every PASS/READY/CLOSED statement can be traced to a named artifact and hash.
- Treat any later change to consensus, genesis, tokenomics or the frozen runtime as requiring document versioning and renewed audit scope.
- Include evidence that the v2.4 Core Team vesting policy and v2.4 slashing/jail semantics are reflected in canonical launch configuration before representing them as enforced.
- Extract and cite exact unbonding, treasury timelock/cap, fee/resource-limit and ordinary account-derivation parameters from the canonical evidence set rather than guessing them.
- Heritari v1.1 remains separately audited against Qanovra L1 v3.6.9; do not claim v3.7.5 compatibility until a dedicated compatibility/repin review succeeds.

Appendix E - v2.4 Audit & Re-Audit Closure Matrix

This appendix maps the external v2.2 audit findings and the v2.3 re-audit findings to the v2.4 publication-candidate state. CLOSED_DOC means the ambiguity or policy omission is resolved in the documents. IMPLEMENTATION_EVIDENCE_REQUIRED means the policy is now explicit but MUST NOT be represented as enforced until canonical configuration/code evidence and tests confirm it. CANONICAL_EXTRACTION_REQUIRED means the document intentionally refuses to invent a frozen-runtime value that was not recovered from the evidence set.

ID	v2.4 status	Remediation	Required next evidence
PAP-H1	CLOSED_DOC / IMPLEMENTATION_EVIDENCE_REQUIRED	Fixed-supply reward funding, fee-first funded model, APR function and policy-consistent funding-horizon disclosure defined.	Bind policy to canonical launch configuration and reward-account evidence.
PAP-H2	CLOSED_DOC / IMPLEMENTATION_EVIDENCE_REQUIRED	Founder Genesis liquidity explicitly disclosed; Core Team 48-month / 12-month-cliff policy defined.	Evidence Core Team vault/grant enforcement before launch.
PAP-H3	CLOSED_DOC / IMPLEMENTATION_EVIDENCE_REQUIRED	20%-1/3 band added; validator-count unit, slash-principal basis, max() combination, burn and jail/unjail semantics defined.	Conformance-test canonical slashing implementation.
PAP-M1	OPEN_CANONICAL_EXTRACTION	No values guessed.	Extract unbonding, treasury timelock and annual cap.
PAP-M2	CLOSED_DOC	Count-based quorum makes controlled admission the Sybil boundary.	Cross-check P0-06 admission policy/evidence.
PAP-M3/M4/M5/M6	PARTIAL / CANONICAL_EXTRACTION	No unsupported liveness, network-limit, fee-number or account-derivation claims added.	Recover exact mechanisms/values and cite them in re-audit.
PAP-M7/M8/M9	CLOSED_DOC	Threat scope, crypto-agility/no-PQ claim, migration-prepared posture and finality terminology are addressed in the companion Yellow Paper.	Keep all external marketing aligned.
PAP-M10	PARTIAL	Document history added; Heritari v3.6.9 binding retained as a separate review item.	Detailed L1 changelog + dedicated Heritari v3.7.5 compatibility/repin audit.
PAP-M11	CLOSED_DOC / LEGAL_REVIEW_OPEN	Formation wording normalized and technical-paper/MiCA separation stated.	Written legal review remains P0-09.
PAP-N1/N3/N4	CLOSED_ARTIFACT	Exact v2.4 filenames, single readiness snapshot, normalized metadata and post-render hash workflow.	None beyond final handoff verification.
PAP-N2	PARTIAL	10% label unified across WP/YP; no category invented.	Attach canonical genesis-allocation schedule as evidence artifact.

ID	v2.4 status	Remediation	Required next evidence
REA-M1	CLOSED_DOC	Funding-horizon illustration recalculated from the declared APR function (55%: 9.41y; 62.5%: 10.35y; 70%: 12.32y).	Bind reward-funding policy to canonical reward accounts/config and tests.
REA-M2	CLOSED_DOC / IMPLEMENTATION_EVIDENCE_REQUIRED	Slash-principal basis defined as total bonded stake attributable to the offending validator, including delegated stake; delegator-risk disclosure added.	Conformance-test slashing base and delegator accounting.
REA-M3	CLOSED_DOC / FUTURE_PROTOCOL_REQUIRED	Migration design note adds target PQ successor families, versioned activation concept, and authenticated user-account rebinding requirement.	Future protocol-version artifact, vectors and implementation evidence before any suite migration.
REA-N1	CLOSED_DOC	Formation timeline now distinguishes initiation (13 August 2026) and notarized formation (21 August 2026).	Update commercial-register status when available.
REA-N2	CLOSED_ARTIFACT	Final filenames aligned with the manifest; PDF handoff included in the v2.4 package.	None beyond final handoff verification.
REA-N3	PARTIAL / CANONICAL_EXTRACTION	Jail duration remains normatively block-based; a real-time equivalent is intentionally not guessed until block-cadence extraction is complete.	Extract canonical block/resource cadence and update descriptive real-time guidance.