ENCRYPIA · PUBLIC TECHNICAL BRIEF

ZEQRON: A Post-Quantum Semantic Coordination Protocol

Public Technical Brief v0.2 — Technical posture note (Tier 3)

Authors: Encrypia (protocol coordination)

Date: September 2026

Phase: Architecture · Pre-testnet

Classification: Public (short) · Master WP = Internal

Canonical source: Markdown ZEQRON-WHITEPAPER-PUBLIC-v0.2.md

This PDF is a typographic companion of the canonical Markdown. It does not expand claims. Design and software maturity only — not a live public-network publication and not a peer-reviewed paper. Strong claims carry labels: design · code · unpublished.

If this PDF and the Markdown diverge, the Markdown wins.

Abstract

Distributed ledgers still largely optimize a 2008-shaped problem: a single global transfer ledger secured by classical signatures that NIST has placed on a migration clock. That model leaves structural gaps under post-quantum pressure and agentic automation—global state contention, transparency mistaken for privacy, human-only identity, and costly crypto retrofit after deployment.

This public technical brief presents **Zeqron** as a *semantic coordination protocol*: parties negotiate meaning-bearing agreements with actor-local state, optional transparent-setup STARK-class privacy, and **NIST FIPS 203 / 204 / 205** primitives from genesis, with protocol-level hooks for attested agents (**ZAXON**) and industrial assets (**ZNA**). Consensus ordering follows a DAG with a BFT-style committee in the Mysticeti family, adapted for post-quantum signatures (**design**); public materials cite Babel et al. as lineage, not as transferable measured performance.

Contributions of this note are architectural and documentary, not empirical network results: a labeled public posture; a four-layer architecture with a walked design example; a cryptographic stack limited to standardized naming; concept-level ZNA/ZAXON; and an evidence taxonomy that forbids mixing lab figures with observed public-chain metrics. Status as of September 2026: substantial Rust monorepo and RFC-driven design (**code** / **design**); **no** measured public network (**unpublished**).

Keywords: post-quantum cryptography; semantic coordination; DAG-BFT; STARK; agent attestation; industrial assets; evidence hygiene; Pre-testnet

1. Introduction

1.1 Problem

Most public ledgers still solve for a global ordered list of transfers. Cryptography on that list—ECDSA, Ed25519—is the class NIST has scheduled for migration under Shor's algorithm. Patching post-quantum signatures, privacy, and non-human actors onto a generic token L1 does not by itself yield a coordination layer for humans **and** non-humans.

Gap	Why it matters
Global state contention	Every write competes for one shared state machine; scale becomes a permanent tax.
Pseudonymity ≠ privacy	Transparency-by-default forces adversarial reconstruction by analytics and compliance.
Human-only identity	Agents and industrial controllers need *attested* identity and bounded capability—not only a wallet address.
Crypto retrofit	Migrating a live chain to NIST PQC after the fact is multi-year systemic risk ("harvest now, decrypt later").

1.2 Thesis

Zeqron is not "another L1 for tokens." It is a **semantic coordination protocol**: parties negotiate and settle meaning-bearing agreements (Contracts) with actor-local state, optional privacy proofs, and **post-quantum cryptography from genesis**—designed so AI agents and industrial assets are first-class participants, not bolted-on applications.

Principle	Meaning (public)	Label
Bilateral coordination	Work is negotiated between parties first; the global DAG anchors hashes for ordering/finality—not a single global account lock for every step.	design
Semantic typing	Relationships carry type and context (Zones), not only balances.	design
Privacy-native optionality	STARK-style proofs are part of the design surface, configurable per Zone.	design · code
PQ-native crypto	FIPS 203 / 204 / 205 on hot and cold paths; no "migrate later" as the security plan.	design · code
Agent + industrial hooks	**ZAXON** and **ZNA** are protocol concepts.	design · code

What this brief is not claiming: that a public Zeqron network is live; that any TPS number is production-observed; or that internal "masters ≈ 100%" equals world readiness.

1.3 Contributions (this public note)

1. **Labeled public posture** for Encrypia-coordinated Zeqron materials (**design** documentation practice).
2. **Four-layer architecture** with a walked, non-customer design example and pointer to `ContractState` (**design · code**).
3. **Cryptographic stack naming** limited to NIST FIPS + transparent-setup STARK class; fine parameters **unpublished**.
4. **Concept surfaces** for ZNA and ZAXON without wire formats or live-market assertions (**design · code**).
5. **Evidence taxonomy** (observed · lab/POC · theoretical) forbidding cross-column TPS diligence (**design** of disclosure).
6. **Disclosure model**: public brief + companions; gated depth via NDA chapter index (titles only) (**unpublished** payload).

1.4 Organization

Section 2 situates related work. Section 3 states architecture. Section 4 states cryptographic posture. Section 5 covers protocol concepts and public code substance. Section 6 states the threat/evidence model. Section 7 records status and non-claims. Section 8 describes diligence and disclosure. Section

9 concludes. Appendices hold the anti-claim checklist and NDA index.

---

2. Related work

This section names **lineage and standards**. It does **not** transfer measured figures from prior systems onto a Zeqron network.

DAG-BFT / Mysticeti family. Babel et al. describe a DAG-BFT design with strong latency/throughput results under classical signatures [1]. Zeqron's consensus design follows a **Mysticeti-family** DAG with a BFT-style committee and **post-quantum** signatures (**design · code** of family software). Heavier PQ signatures change bandwidth and verification cost relative to Ed25519/BLS-class certificates; public materials must not paste upstream WAN latency or TPS columns next to "Zeqron observed."

NIST post-quantum cryptography. FIPS 203 (ML-KEM), FIPS 204 (ML-DSA), and FIPS 205 (SLH-DSA) standardize key encapsulation and signature families [2][3][4]. CNSA 2.0 and related guidance motivate genesis-time PQ rather than retrofit [5]. This brief names the standards; it does **not** publish parameter sets, key sizes as a marketing table, or KAT vectors.

Transparent zero-knowledge. STARK-class proofs with transparent setup are a design choice for zone-configurable privacy without a pairing-trusted ceremony (**design · code**). Fine FRI/circuit parameters remain **unpublished** in this Tier-3 surface.

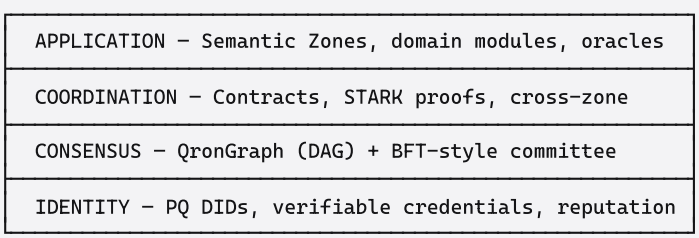
Agent identity and credentials. W3C Verifiable Credentials and DID patterns inform the public identity story; ZAXON adds code-digest–bound agent identity as a protocol concept (**design · code**). This is not a claim of a live agent marketplace.

Industrial / permissioned asset models. Regulated-token and supply-chain literature motivates typed assets with history; ZNA states genealogy, blueprints, and conservation rules at concept level (**design · code**) without publishing entropy formulas or wire schemas here.

---

3. Architecture

Four layers, one job each:



Layer	Responsibility	Public components	Label
Application	Domain rules and data ingress	Semantic Zones, WASM-capable modules, oracles	design · code
Coordination	Agreement lifecycle and privacy	Contracts, STARK proofs, semantic bridges (concept)	design · code
Consensus	Global ordering and finality	QronGraph DAG; Mysticeti-family BFT with PQ signatures	design · code
Identity	Who may act, with what credentials	ML-DSA DIDs, VCs, reputation scoring	design · code

Data flow (conceptual): Applications submit Contracts → Coordination validates and may attach proofs → Consensus orders/finalizes commitments → Identity authenticates participants throughout.

Walked example (design — no named customer). Two organizations agree on delivery of a composite batch whose composition must satisfy a recipe. Their zone application presents a typed contract with context. Coordination validates it and, if the zone requires privacy, attaches a transparent-setup STARK. Consensus anchors the commitment hash on the DAG. Identity accompanies the parties; if an agent executes a step, a ZAXON attestation bounds what it may do. The agreement object is the same state machine the monorepo names as `ContractState` (Proposed → … → Anchored, with Aborted / Disputed) (**code**). What the global record anchors is **commitment order**; publishing everyone's balance is not required.

Failure threshold (design hypothesis): classical less-than-one-third committee fault discussion applies to the BFT-style design; it is **not** a measured network fact.

Storage / ops detail (WAL parameters, validator ceilings, zone-split timers, crate graphs) lives in the **internal** master and RFCs—not in this public brief.

---

4. Cryptographic posture

Zeqron targets **NIST-standardized** post-quantum primitives plus transparent ZK:

Function	Algorithm family	Standard	Label
Signatures (primary)	ML-DSA (Dilithium lineage)	FIPS 204 [3]	design · code
Signatures (hash-based diversity)	SLH-DSA (SPHINCS+ lineage)	FIPS 205 [4]	design · code
Key encapsulation	ML-KEM (Kyber lineage)	FIPS 203 [2]	design · code
General hashing	BLAKE3 / ParallelHash family	Industry + NIST SP 800-185 where applicable [6]	design
Zero-knowledge	STARK proofs (transparent setup)	Design choice: no pairing-trusted ceremony	design · code

Public stance:

- Triple-FIPS PQ (203 + 204 + 205) is a **core design constraint**, not a roadmap checkbox.
- STARKs are chosen for transparent setup and hash-based soundness under quantum models; **fine-grained FRI / circuit parameters are omitted** (**unpublished**).
- Classical curves (e.g. BLS for legacy bridge experiments) are **not** the long-term production PQ story.
- **PQ adaptation of consensus (design):** heavier signatures change bandwidth and verification cost; lineage citation [1] is not a performance transfer claim.

Not published here: micro-benchmarks as network capacity; FRI query counts; Grover-bit marketing tables; "≥N-bit soundness" claims that belong in a controlled crypto appendix.

---

5. Protocol concepts and public code substance

5.1 ZNA — Native Industrial Assets (concept)

ZNA is a protocol-level asset model for real-world production and supply chains, not a decorative NFT wrapper (**design · code**).

- **Genealogy** — composites retain a cryptographically linked history of components.
- **Blueprints** — immutable recipes that define valid composition (inputs → output).
- **Conservation rules** — mass/entropy-style invariants in the protocol design (cannot invent mass; decomposition may lose value by design).
- **Single economic anchor** — industrial semantics sit alongside the sovereign token *design vocabulary* (ZQN), not as a parallel speculative layer asserted as a live market.

Wire formats, entropy ranges, depth limits, and schemas remain **unpublished** here.

5.2 ZAXON — Agent infrastructure (concept)

ZAXON is the agent hook: post-quantum attestation and accountability so non-human actors participate under explicit bounds (**design · code**).

- **Agent Identity (AID)** — fingerprint over code digest, operator DID, and declared capabilities; change of code or operator ⇒ new AID.
- **Sandboxed execution** — capability grants, quotas, kill-switches (not unbounded "smart wallet" scripts).
- **Trust dimensions** — conformance levels and certification tiers as a *framework*; bond amounts and insurance discounts are **not** live market facts here (**unpublished**).
- **Industrial telemetry (vision)** — attested signals before high-value physical actions (**design**).

5.3 Public code substance

Companion readings on whitepaper.zeqron.io expose real monorepo excerpts (**code · no public network endpoint**):

Exhibit	Role
`ContractState` / `ContractPhase`	Agreement lifecycle machine and high-level phases
`AgentIdentity`	`code_hash`, `operator_did`, `capabilities`
`FinalityLevel`	DAG claim-finality design states
`ConformanceLevel`	ZAXON conformance framework (research reading)

These prove **object-in-code**. They do **not** prove observed network TPS, latency, or availability.

5.4 Economic and operator vocabulary (public limits)

- **ZQN** — design vocabulary for the sovereign economic anchor; **not** an instrument offer in this document.
- **PoSS (design):** stake + observable service (availability, capacity, correctness)—not stake-only. Formulas and yields are **unpublished**.
- **Operators:** no public enrollment as of September 2026. Future runbook chapter *order* (machine → identity → stake → service → fault) may be named without ports, SKUs, amounts, or commands.

---

6. Evidence classes and comparability

Public chains sometimes publish **observed** peak TPS. Those numbers describe **deployed networks under real load**.

Zeqron **does not** place lab/POC throughput in the same table column as those observed figures:

Class	What it measures
(A) Observed network	Live (or historically live) public systems under stated load
(B) POC / simulation / infra model	Controlled experiment under stated assumptions
(C) Theoretical ceiling	Upper bound under idealized pipeline assumptions

Until Zeqron publishes phase-labeled instrumentation from a real Devnet/Testnet/Mainnet, **no Zeqron TPS number belongs beside Bitcoin/Ethereum "observed" rows** in diligence materials derived from this brief.

Threat / trust posture (public): PQ signatures and transparent ZK are design constraints against harvest-now/decrypt-later and trusted-setup dependency for the long story. This note is **not** a complete formal threat model with games and reductions (**unpublished** as Encrypia peer-reviewed paper).

---

7. Status and non-claims (September 2026)

Dimension	Reality
Protocol software	Advanced: substantial Rust monorepo, automated tests, RFC-driven design (**code**).
Design maturity	Core architecture and crypto choices specified and largely implemented (**design · code**).
Public network	**No** public network with published, phase-labeled performance measurements (**unpublished**).
"Devnet Live" / "Production-Ready"	**Do not use** as public slogans for the network.
POC / lab results	May exist internally; not interchangeable with deployed network TPS/latency.
Mainnet	Future phase; **no false dates** in this brief.
Disclosure	Public: this brief + companions + demos. Deep dive / raw benchmarks / network access: **NDA**.
Publisher	Encrypia coordinates the Zeqron protocol.

Interpretation rule: high internal completion percentages (masters / trackers) measure *code and spec hygiene*, not *world readiness*.

7.1 When not to choose Zeqron

1. You need a battle-tested public chain with SLA-grade claims **today**.
2. You only need a generic token L1 / venue.
3. You require full OSI open-source of the core **now** (deep access is gated).
4. You need classical-only crypto compliance in the short term.
5. You cannot accept semantic / Zone complexity ("accounts + one contract language only").
6. You need audited mainnet economics and live bridges as **present public fact**.

7.2 What this document deliberately omits

- Runbooks, deployment recipes, SKU/ops playbooks
- Validator ceilings, zone-split timers, mempool pipeline internals
- FRI / Poseidon parameter tables and bit-security marketing appendices
- Full RFC inventory and crate-by-crate dashboards
- Tokenomics depth, insurance schedules, marketplace fee tables
- Source dumps suitable for a full construction paper or unrestricted OSS core release

Those remain in the internal master, RFCs, and NDA packs—indexed in Appendix B. Constructive detail suitable for venue submission is a **separate Tier-4 track** and is out of scope for this public brief.

---

8. Diligence path and disclosure model

Use this as a memo skeleton—not a pitch deck.

Step	What to do	What not to invent
1 · Public surface	Read this brief + role companions; fix author (Encrypia), hierarchy (brief wins), phase (Architecture · Pre-testnet).	APY, TAM, TGE, "Production-Ready network."
2 · Code without network	Read named types / families. Object substance ≠ network measurement.	Endpoints, explorer URLs, speed columns vs observed chains.
3 · NDA index	Request Appendix B chapters by title. Index ≠ payload.	Filling tables from marketing copy.
4 · Kill criteria	Reject decks that invent yield, mix lab with observed TPS, or equate masters % to world readiness.	Soft "soon" fillers in economic fields.

Hierarchy: if a companion page on whitepaper.zeqron.io and this brief diverge, **this brief wins**.

---

9. Conclusion and future work

This v0.2 brief fixes a **public scientific *shape***—abstract, related work, labeled contributions, evidence hygiene—without expanding the Tier-3 claim class. Zeqron's public story remains: semantic coordination, PQ from genesis, agent and industrial hooks as protocol concepts, substantial software, and **no** measured public network yet.

Future work (no dates): named network phases with instrumentation; controlled disclosure of parameter appendices under agreement; formal papers **per innovation** only under the project's academic/IP publication track (after provisional protection where required)—not by silently thickening this brief.

References

[1] K. Babel, A. Chursin, G. Danezis, A. Kichidis, L. Kokoris-Kogias, A. Sonnino, M. Tian, and J. Zhang, "Mysticeti: Reaching the Limits of Latency with Uncertified DAGs," arXiv:2310.14821, 2023.
Cited as design lineage only — not as Zeqron observed performance.

[2] NIST, *FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard*, 2024.

[3] NIST, *FIPS 204: Module-Lattice-Based Digital Signature Standard*, 2024.

[4] NIST, *FIPS 205: Stateless Hash-Based Digital Signature Standard*, 2024.

[5] NSA, *Commercial National Security Algorithm Suite 2.0* (CNSA 2.0) — public transition guidance for national-security systems; cited as motivation for genesis-time PQ posture, not as a Zeqron certification claim.

[6] NIST, *SP 800-185: SHA-3 Derived Functions* (cSHAKE, KMAC, ParallelHash, TupleHash), 2016 — where ParallelHash-family hashing is referenced.

[7] Encrypia, *ZEQRON Public Technical Brief v0.1*, September 2026 — prior public cut; same claim class; superseded in form by this v0.2.

Appendix A — Anti-claim checklist

Use this before any external paste (deck, site, email, PDF):

- ☐ No phrase **"Production-Ready"** referring to a **network** or **product launch**

- ☐ No **“Devnet Live”** / **“Testnet Live”** / **“Mainnet Live”** without dated, phase-labeled evidence
- ☐ No **Zeqron TPS** in the same table class as Bitcoin/Ethereum **observed** TPS
- ☐ No POC/lab number presented as **deployed network** throughput or latency
- ☐ No invented **mainnet dates**
- ☐ No implication that **masters ≈ 100%** means public readiness
- ☐ No **FRI / circuit parameter** dump in public copy
- ☐ No **ops/runbook** content in public copy
- ☐ No claim of **full OSS core** or unrestricted protocol dump
- ☐ ZNA / ZAXON described as **concepts + design**, not as audited live markets
- ☐ Crypto claims limited to **NIST FIPS naming + STARK transparent setup** unless a separate reviewed appendix exists
- ☐ Any future metric tagged exactly one of: **Simulation / Devnet / Testnet / Mainnet**
- ☐ No **APY / TAM / TGE** invented from this brief
- ☐ Strong claims keep a **design · code · unpublished** label
- ☐ No uniqueness slogan (“first fully PQ…”) without evidence class
- ☐ Related-work citations do **not** transfer upstream measured figures to Zeqron

---

Appendix B — NDA index (titles only; payload gated)

Public diligence may **name** these chapters. Content ships under agreement—not reconstructed here.

ID	Chapter (title)	What it holds (hint, not payload)
B1	Long-form narrative + decisions	Master narrative; D1–D13 / QRONCORD decision logs
B2	Fine cryptographic parameters	FRI queries, Poseidon widths, bit-security tables, micro-benchmark grids
B3	Ops / runtime	WAL, validator ceilings, zone-split timing, bridge fee formulas, crate notes
B4	Deep ZNA / ZAXON economics	Bonds, insurance discounts, wire formats, schema bijections
B5	Phase evidence	POC / lab figures **with phase label**, if any — never mixed with observed public-chain TPS
B6	Core access terms	Partnership / deep-access terms (not full OSI dump now)

Requesting the pack by these titles is the diligence act. Inventing the tables in a public deck is a red flag.

Document control

Field	Value
Version	**v0.2** (academic *form*; claim class unchanged from v0.1)
Language	English (diligence / scientific default)
Canonical form	**Markdown** (`ZEQRON-WHITEPAPER-PUBLIC-v0.2.md`). Typographic **A4 PDF** companion available (`ZEQRON-WHITEPAPER-PUBLIC-v0.2.pdf`); if PDF and Markdown diverge, Markdown wins.
Companion	Role readings on whitepaper.zeqron.io — must not silently expand claims beyond this brief
Owner	Encrypia / Zeqron protocol coordination
Classification	**Public** (short). Master WP = **Internal**.
Prior	v0.1 retained at `ZEQRON-WHITEPAPER-PUBLIC-v0.1.md` for history

End of Public Technical Brief v0.2