ENCRYPIA

# ZEQRON

## Public Technical Brief v0.1

Architecture · Pre-testnet · September 2026

Companion PDF of the canonical Markdown — claims unchanged.

---

Audience: technical diligence, institutional evaluators, partners under NDA path
Date: September 2026
Status: Design + advanced implementation (codebase). Not a live public network publication.
Source of truth (internal): docs/ZEQRON-WHITEPAPER-v2.md (long-form master - not this document)

> Disclaimer (read first) This brief describes protocol *design* and *software maturity*. Proof-of-concept (POC) or lab measurements are not the same class of evidence as throughput, latency, or availability of a deployed public network. Zeqron does not currently publish measured public Devnet / Testnet / Mainnet performance. Any future network figures will be labeled by phase (Simulation / Devnet / Testnet / Mainnet) and sourced from that phase's instrumentation.

---

### 1. Problem

Most distributed ledgers still optimize for a 2008-shaped problem: a single global ledger of transfers, with cryptography that NIST has already put on a migration clock (ECDSA / Ed25519 under Shor).

That model leaves three gaps that matter under post-quantum pressure and agentic automation:

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

These are architectural constraints, not marketing slogans. Patching them onto a generic L1 does not yield a coordination layer for humans and non-humans.

---

### 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 apps.

- Principle - Meaning (public)
- 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.

- Semantic typing - Relationships carry type and context (Zones), not only balances.
- Privacy-native optionality - STARK-style proofs are part of the design surface, configurable per Zone-not an afterthought mixer.
- PQ-native crypto - NIST FIPS 203 / 204 / 205 primitives on the hot and cold paths; no "migrate later" story as the security plan.
- Agent + industrial hooks - ZAXON (agent attestation) and ZNA (native industrial assets) are protocol concepts, not side-chain demos.

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

## 3. Architecture (high level)

Four layers, one job each:

```
APPLICATION - Semantic Zones, domain modules, oracles

COORDINATION - Contracts, STARK proofs, cross-zone

CONSENSUS - QronGraph (DAG) + BFT-style committee

IDENTITY - PQ DIDs, verifiable credentials, reputation
```

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

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

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 stack (public)

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

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

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 here (internal / NDA).

- Classical curves (e.g. BLS for legacy bridge experiments) are not the long-term security story for production PQ posture.

```
Not published in this brief: micro-benchmarks presented as network capacity; FRI query counts;
Grover-bit marketing tables; "N-bit soundness" claims that belong in a crypto appendix under
controlled disclosure.
```

## 5. ZNA - Native Industrial Assets (concept)

ZNA is a protocol-level asset model for real-world production and supply chains, not a decorative NFT wrapper.

At concept level:

- Genealogy - composites retain a cryptographically linked history of components.
- Blueprints - immutable recipes that define valid composition (inputs -> output).
- Conservation rules - mass/entropy-style invariants enforced by the protocol design (cannot invent mass; decomposition may lose value by design).
- Single economic anchor - earlier "generated materials" experiments were retired; industrial semantics sit alongside the sovereign token model rather than a parallel speculative layer.

Depth (wire formats, entropy ranges, depth limits, protobuf schemas) remains in the internal master / RFCs.

## 6. ZAXON - Agent infrastructure (concept)

ZAXON is the AI / agent hook: a post-quantum attestation and accountability layer so non-human actors can participate under explicit bounds.

At concept level:

- Agent Identity (AID) - fingerprint over code digest, operator DID, and declared capability set; change of code or operator new AID.
- Sandboxed execution - agents run under capability grants, resource quotas, and kill-switches (not unbounded "smart wallet" scripts).
- Trust dimensions - conformance levels (technical controls) and certification tiers (operator assurance) as a *framework*; specific bond amounts and insurance discounts are not asserted as live market facts here.
- Industrial telemetry (vision) - attested signals before high-value actions in physical settings.

ZAXON is why Zeqron is framed as agent-native coordination, not "Web3-PQ only." Implementation detail, marketplace economics, and hardware-root wiring stay internal / NDA until deliberately published.

## 7. When not to choose Zeqron

Choose something else (or wait) if:

- You need a battle-tested public chain today - Zeqron has no measured public Devnet/Testnet/Mainnet offering SLA-grade performance claims.
- You only need a token L1 - if the product is a generic AMM / memecoin venue, a mature public chain is a better fit.
- You require full open-source of the core under OSI terms now - deep protocol access is gated (public surfaces: sites, this short brief, demos; core = NDA / partnership path).

- You need classical-only crypto compliance - Zeqron's direction is PQ-native; hybrid or classical-primary stacks may fit other mandates better in the short term.
- You cannot accept semantic / Zone complexity - if your team wants "accounts + Solidity and nothing else," the learning curve and model are misaligned.
- You need audited mainnet economics and bridges live - those are roadmap / diligence items, not present as public deployed fact in this brief.

---

## 8. Honest status (September 2026)

- Dimension - Reality
- Protocol software - Advanced: substantial Rust monorepo, extensive automated tests, RFC-driven design.
- Design maturity - Core architecture and crypto choices are specified and largely implemented in code.
- Public network - No public network with published, phase-labeled performance measurements.
- "Devnet Live" / "Production-Ready" - Do not use as public slogans for the network. Architecture and code != production network.
- POC / lab results - May exist internally; they are not interchangeable with deployed network TPS/latency.
- Mainnet - Planned as a future phase; no false dates in this brief.
- Disclosure - Public: short materials + demos. Deep dive / raw benchmarks / network access: NDA.

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

---

## 9. Comparability of performance claims

Public chains sometimes publish observed peak TPS (Bitcoin ~7, Ethereum tens of TPS, etc.). Those numbers describe deployed networks under real load.

Zeqron does not place lab/POC throughput in the same table column as those observed figures. Doing so conflates:

- Class - What it measures
- Observed network TPS - Live (or historically live) public systems
- POC / simulation / infra model - Controlled experiment or model under stated assumptions
- 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.

---

## 10. What this document deliberately omits

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

Those remain in the internal master, RFCs, and NDA packs.

## Appendix A - Anti-claim checklist (W0)

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

## Appendix B - Remains only in the internal master

- Full long-form narrative (~thousands of lines), adversarial-round history, and decision logs (D1-D13 / QRONCORD).
- Fine cryptographic parameters (FRI queries, Poseidon widths, soundness bit tables) and micro-benchmark grids.
- Ops/runtime detail: storage WAL, validator ceilings, zone-split timing, bridge fee formulas, crate refactor notes.
- Deep ZNA/ZAXON economics (bonds, insurance discounts, wire formats, schema bijections).
- Any POC throughput / multi-zone ceiling figures and tables that mix them with observed public-chain TPS.

## Document control

- Field - Value
- Version - v0.1 (W0 - publicable recorte anti-humo)
- Language - English (diligence default)
- Next (W1) - URL + PDF + brand application on whitepaper site - does not expand claims beyond this brief
- Owner - Encrypia / Zeqron protocol coordination
- Classification - Public (short). Master WP = Internal.

*End of Public Technical Brief v0.1*