URUZ Protocol Whitepaper v0.2

Structural Graph Identity (SGI) and Post-Quantum Security for Permissionless DAG Finality

Status: Working Draft (internal)

Date: 2026-03-29

Network: URUZ (formerly referenced as AON in earlier drafts)

Abstract

URUZ is a permissionless DAG-based Layer 1 protocol that combines:

? work-weighted finality,

? staged reputation-based Sybil resistance (SGI),

? checkpoint-anchored history integrity,

? post-quantum trust anchors.

This document defines the URUZ security architecture at a level suitable for technical review while intentionally omitting sensitive operational constants and low-level defense tuning.

The central design choice is to treat SGI as a phased control system, not an all-at-once consensus switch.

1. Problem Statement

Permissionless networks must resist identity multiplication attacks without relying on centralized identity lists.

Traditional approaches externalize Sybil cost (capital, energy, or permissioning). URUZ explores a protocol-native alternative:

? reputation from verifiable graph behavior over time,

? bounded and staged influence,

? checkpoint-anchored safety against long-range manipulation.

URUZ does not assume that reputation alone is sufficient in all phases. Safety is enforced by layered controls and phased activation gates.

2. URUZ Architecture (High Level)

URUZ combines four security layers:

1. **DAG execution layer**

Parallel transaction propagation and conflict handling in a directed acyclic graph.

2. **Finality layer**

Work-weighted finality with bounded multi-factor policy.

3. **Checkpoint integrity layer**

Canonical history anchoring and controlled recovery.

4. **Identity and influence layer (SGI)**

Behavior-derived reputation with staged consensus influence.

This separation is intentional: execution, finality, checkpointing, and identity controls evolve on different timelines.

3. Finality Model (Conceptual)

URUZ finality is deterministic and policy-bounded.

A transaction moves through states (`PENDING`, `CONFIRMED`, `FINAL`) only when objective on-chain conditions are satisfied.

Key property: finality depends on verifiable graph evidence, not on a fixed validator committee.

This whitepaper intentionally avoids publishing production constants and internal guard thresholds.

4. SGI: Structural Graph Identity

SGI derives influence from durable, verifiable behavior in the DAG and checkpoint history.

At a conceptual level, SGI combines:

? contribution/work signals,

? diversity-aware referencing signals,

? consistency signals anchored to canonical history.

Important clarification

In URUZ, SGI is a phased mechanism:

? early phases: observation and bounded influence,

? later phases: increased influence only after objective maturity criteria,

? full influence: enabled only after stability and governance gates.

URUZ explicitly avoids claiming full SGI enforcement before those gates are met.

5. Long-Range and History-Rewrite Defense

Reputation systems are vulnerable if historical influence can be replayed against alternate histories.

URUZ addresses this with checkpoint anchoring:

? canonical checkpoint lineage defines the trusted history envelope,

? reputation influence is constrained by anchored history,

? recovery and re-sync operate under anchored integrity rules.

Residual risk between checkpoints is handled by bounded finality policy, staged controls, and continuous telemetry.

6. Bootstrap, Maturity, and Safety Gates

URUZ treats early network life as a distinct security regime:

? no unsafe “instant maturity” assumption,

? maturity requires multi-epoch evidence,

? concentration and quality signals are tracked before enabling stronger influence.

SGI activation depends on measurable network health, not calendar deadlines.

7. Post-Quantum Security Strategy

URUZ adopts post-quantum trust assumptions at protocol level and follows a crypto-agility strategy:

? no permanent lock-in to a single primitive forever,

? scheme/version governance by policy boundary,

? staged migration support where needed.

URUZ separates PQ domains:

1. transaction authentication,

2. consensus/checkpoint authority paths,

3. network session and node identity paths.

This separation reduces migration risk and avoids “partial PQ” blind spots.

8. Implementation Status (Truthful Snapshot)

Implemented (production/devnet paths)

? DAG execution and work-weighted finality core flow,

? checkpoint integrity and anchored recovery mechanisms,

? staged SGI observability paths and telemetry-driven operations,

? private multi-node devnet operations with automated monitoring.

In progress / staged rollout

? progressive SGI influence activation by policy gates,

? broader PQ coverage beyond trust anchors,

? key rotation/revocation hardening paths,

? continued adversarial and stability calibration.

Not claimed as complete in this draft

? full SGI consensus weighting in all phases,

? full-stack PQ enforcement across every protocol surface,

? final parameter set for public mainnet.

9. Security Posture and Disclosure Policy

URUZ uses defense-in-depth and staged activation.

Public documentation is intentionally constrained:

? no publication of sensitive operational thresholds,

? no publication of low-level adversarial tuning constants,

? no publication of internal incident response specifics.

This is a security and operational integrity decision, not a lack of formalism.

10. Research and Engineering Priorities

1. formal security analysis of staged reputation influence under adversarial models,
2. robust cross-node consistency semantics for advanced consistency signals,
3. full PQ rollout with crypto-agility policy and rotation safety,
4. long-horizon empirical calibration under stable multi-node operation.

11. Conclusion

URUZ proposes a pragmatic path for permissionless DAG security:

? deterministic graph-based finality,

? staged behavior-based Sybil resistance,

? checkpoint-anchored history integrity,

? post-quantum-forward architecture with cryptographic agility.

The protocol is designed to advance by verified gates rather than narrative milestones.

This v0.2 draft reflects that stance and supersedes earlier pre-rollout assumptions.

References (Selected)

1. Douceur, J.R. — The Sybil Attack (2002)

2. Kamvar et al. — EigenTrust (2003)

3. NIST FIPS 204 — ML-DSA (2024)

4. Public post-quantum migration discussions in major L1 ecosystems (including Ethereum PQ research track)