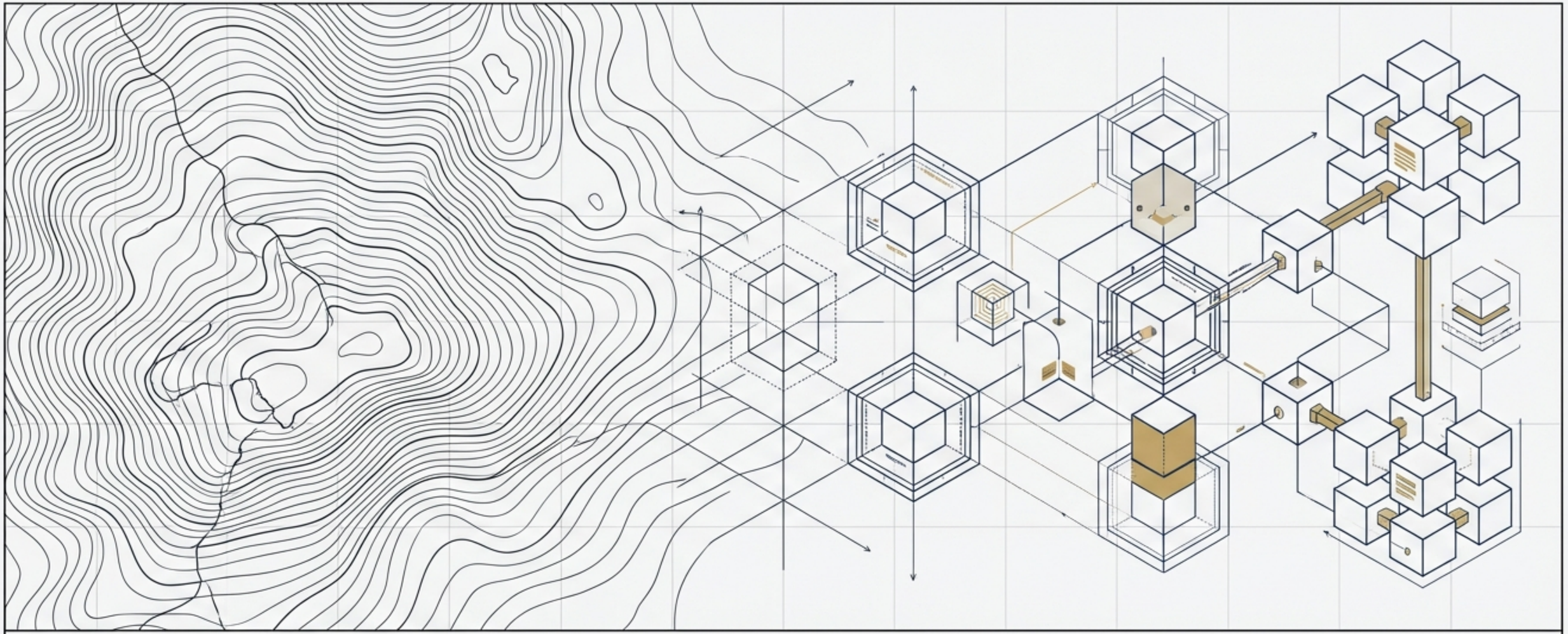


QXMP Oracle & Proof-of-Reserve System

Institutional-Grade Verification for Real-World Assets

ASSET VALUE:
$1.1 Trillion USD (Secured)

NETWORK:
QELT Mainnet (Chain ID 770)

STATUS:
Production-Ready (v2.1) | Live as of Jan 12, 2026

A Bespoke Solution for Static, In-Ground Assets

QXMP is a purpose-built oracle designed to ingest, validate, and continuously update valuations for large-scale resource assets. Unlike standard feed oracles, it provides a native on-chain Proof of Reserve for physical resources.

TOTAL VERIFIED VALUE

$1,090,958,787,645.94

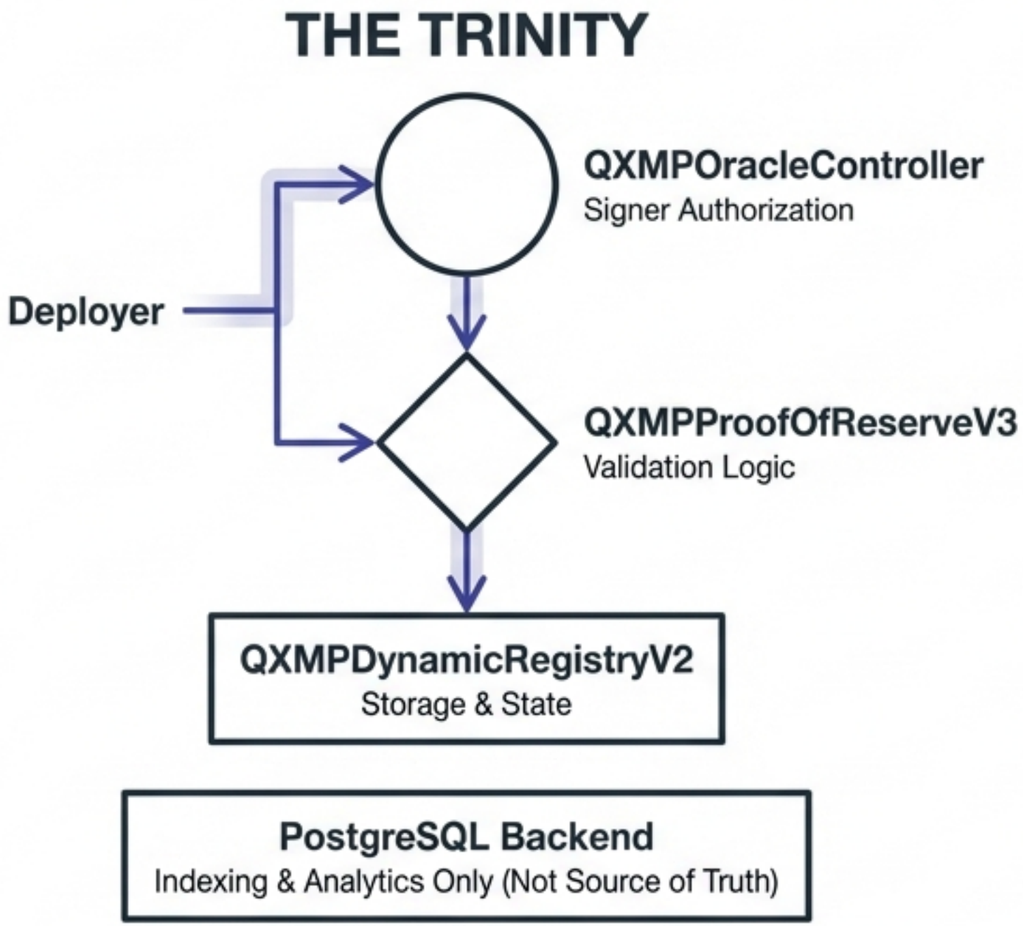
Across 12 distinct asset classes

Target: Diamonds, Gold, Lithium, Polymetallic Concessions.

Differentiation: Optimized for geological reporting, not high-frequency trading feeds (e.g., Chainlink/RedStone).

Core Promise: Native on-chain Proof of Reserve, not just off-chain attestations.

The Architecture of On-Chain Truth



Design Constraint: The registry cannot be mutated directly. All value updates must pass through the PoR contract and valid oracle signatures.

Smart Contract Responsibilities & Logic

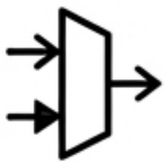
Governance

`QXMPOracleController`

- Manages authorized signers.
- Enforces EIP-191 prefixed message signing.
- Contains stateless verification logic.

The Gatekeeper

`QXMPProofOfReserveV3`



- Verifies Oracle signatures.
- Enforces freshness constraints (prevents stale data).
- Updates the registry atomically.
- Maintains an immutable historical audit trail.

The Vault

`QXMPDynamicRegistryV2`

- Canonical on-chain asset registry.
- Stores 8-decimal USD valuations.
- Holds IPFS document references.
- Supports soft-deleted historical fields for forensics.

The Oracle Mechanism: Identity & Signatures

Asset Identity

Assets are identified via deterministic bytes32 hashes.

QXMP:{PROJECT}-{STANDARD}-{JURISDICTION}

```
const id = "QXMP:ATKA2-NI43-ZA";
```

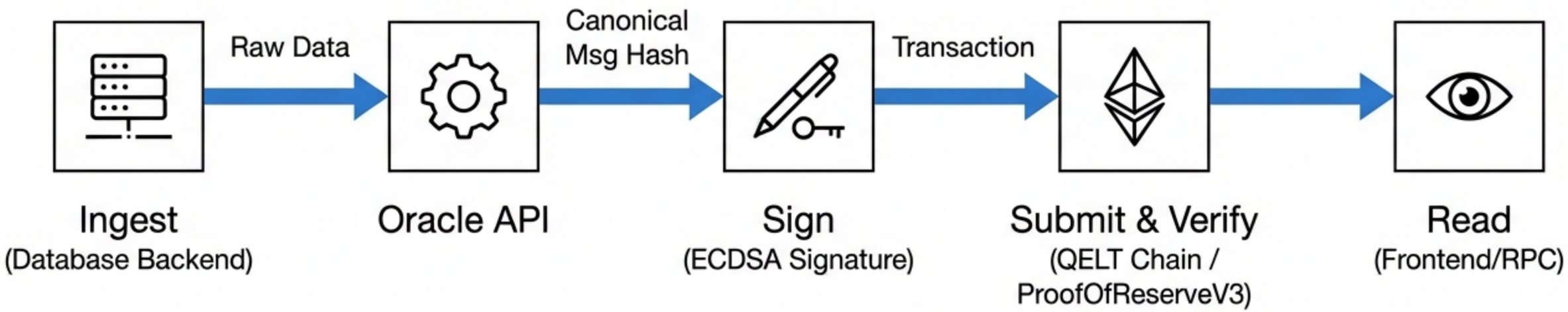
Cryptographic Guarantee

Uses custom ECDSA signatures (EIP-191). Guarantees 8-decimal USD precision for institutional accuracy.

Validation

No off-chain trust assumptions exist once the proof is submitted. Staleness protection enabled (default 24h).

Data Lifecycle & Verification Flow



Key Insight: Frontend reads are directly on-chain—no backend dependency for verification.

Registered Assets: The $1.1 Trillion Portfolio

Rank	Asset Name	Project Type	Verified Valuation (USD)
01	**SPMT Multi-Project**	**NI 43-101**	**$352,771,817,278.00**
02	Sperrgebiet HMS / Diamond / Gold	Mixed Resource	$237,500,000,000.00
03	AEM Gold Project (ATKA2)	Gold	$227,655,712,284.00
04	Rhenosterspruit / Syferfontein	Concession	$113,989,838,841.85
05	Chibuto HMS Project	Mineral Sands	$56,245,946,295.00
06	West Coast Diamond Projects	Diamonds	$41,488,859,999.80
07	Other Assets (Combined)	Various	~$61,000,000,000.00
	TOTAL REGISTERED VALUE		**$1,090,958,787,645.94**

Valuation Standards & Freshness

Geological Standards

Valuations derived from NI 43-101, JORC 2012, and SEC-compliant disclosures.

Cryptographic Signing

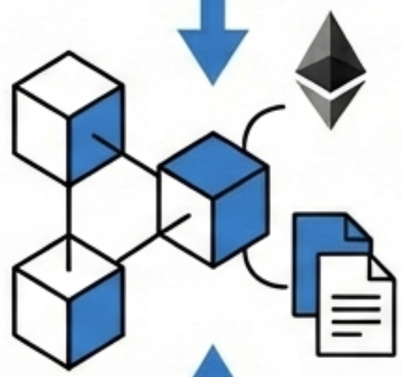
Reports are cryptographically signed and enforced on-chain.

Freshness Guarantee

System enforces staleness protection (default 24h) to ensure market relevance.

Auditability

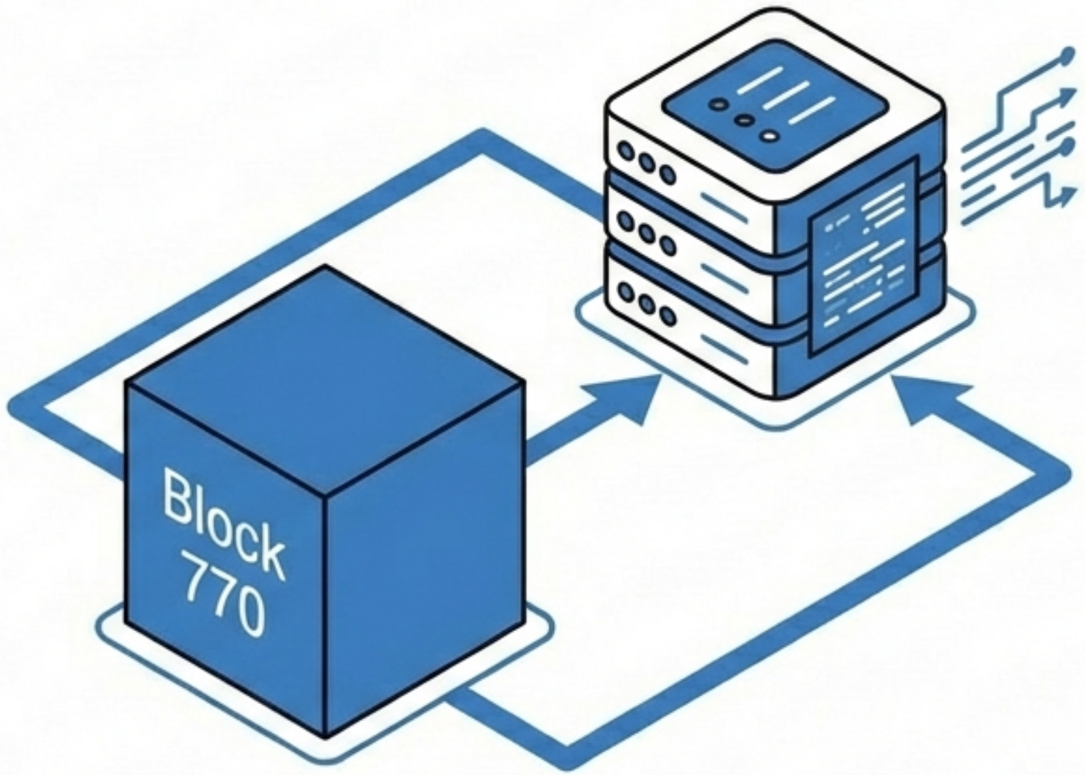
All valuations include IPFS document references linking to original geological surveys.



Infrastructure: QELT Blockchain Integration

NETWORK:	QELT Mainnet
CONSENSUS:	QBFT (Proof of Authority) - Hyperledger Besu
CHAIN ID:	770
RPC ENDPOINT:	https://mainnet.qelt.ai
EXPLORER:	https://qeltscan.ai

Verification Status: All contracts are deployed, verified, and publicly accessible on the QELT explorer.



Security Model & Trust Assumptions

Key Management

Private keys are never exposed client-side. Signer rotation is fully supported by the Controller contract.

Replay Protection

Enforced via timestamps and staleness checks; old signatures cannot be reused.

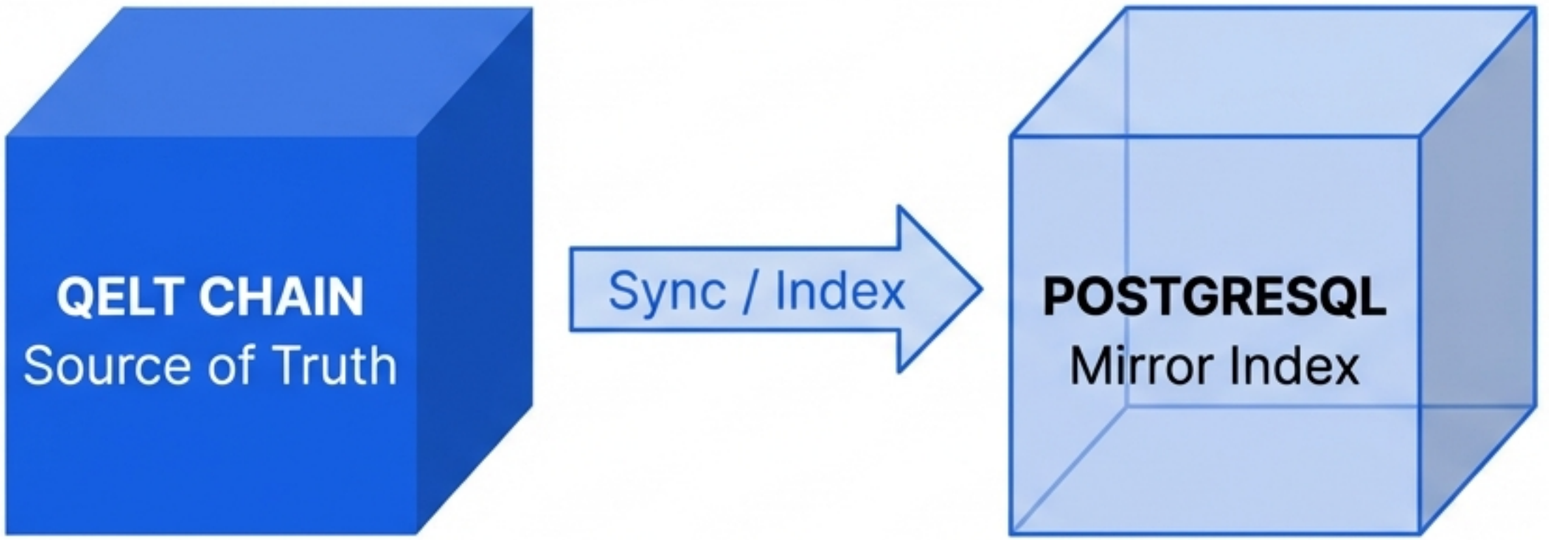
Forensics

The “Soft-Delete” feature in the Registry preserves forensic traceability. Nothing is ever truly erased, only deprecated.

Immutable History

Every proof submission is append-only and permanently auditable.

The Role of Off-Chain Infrastructure



- The Database is a Mirror, not the Master.
- Tables (`assets`, `oracle_proofs`) map 1:1 with on-chain identifiers.
- API is restricted to admin injection and read-only aggregation.
- **Crucial Distinction:** If the database is destroyed, the value and **proof history** remain intact on the QELT chain.

Deployment & Migration Status

LAUNCH DATE

January 12, 2026

MIGRATION

Ethereum → QELT Complete

GAS CONSUMED

~6.4 Million

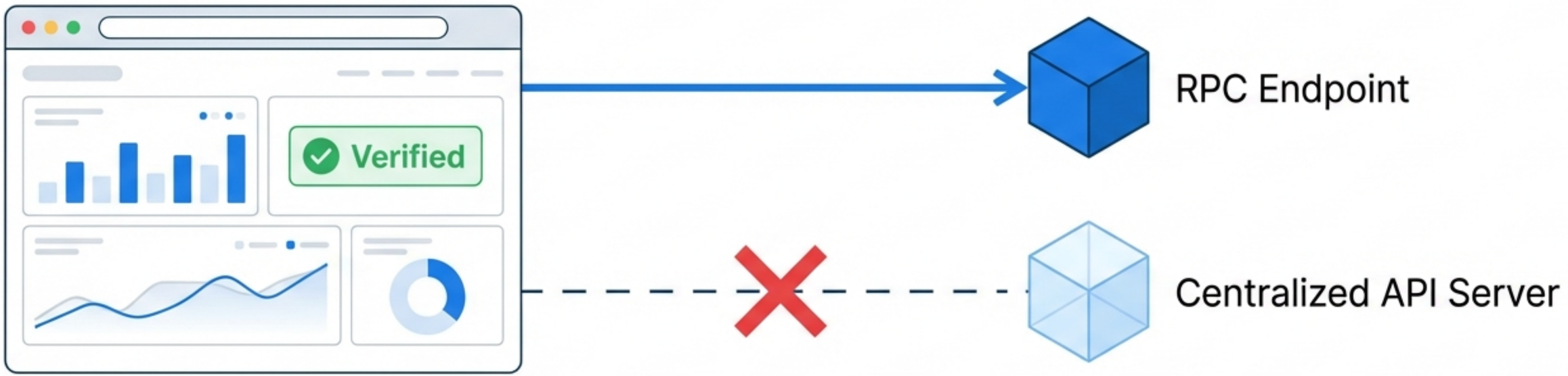
Complex deployment logic

SYSTEM STATUS

NOMINAL

Legacy oracle references removed. Registry ownership enforced. Assets re-verified on new chain.

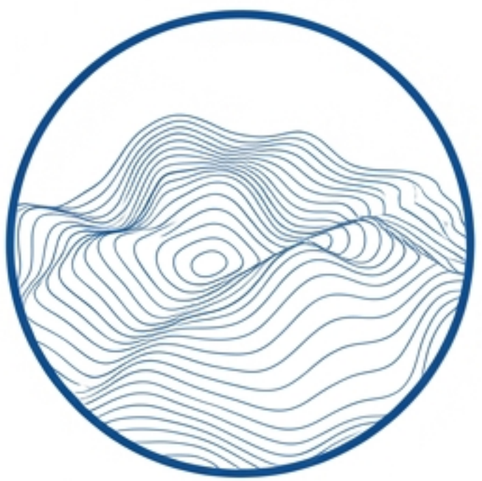
User Experience & Verification



- **Direct RPC Reads:** Frontend fetches data directly from blockchain nodes.
- **Explorer Integration:** Deep-links provided for every transaction and asset.
- **Visual Proof:** Users view Proof History and Registry State directly from smart contracts.
- **No Middleman:** Interface functions independently of centralized APIs.

A New Standard for Real-World Assets

QXMP delivers a production-grade, fully dynamic Proof-of-Reserve system capable of securing in-ground assets at a trillion-dollar scale. By combining deterministic oracle signatures, immutable on-chain proofs, and the QELT Layer-1, we provide a continuously verifiable reserve system that does not exist elsewhere in the market.



VERIFY THE PROOFS ON QELTSCAN.AI