Aureon Labs — Cross-Chain Bridge Whitepaper (v0.9)

Seamlessly connect value and messages across every chain.

Aureon Labs • 2025-10-14

1) Abstract

Aureon Labs is a modular cross-chain bridge enabling secure token transfers and general message passing across heterogeneous blockchains (EVM and non-EVM). It combines a light-client-first security model with a unified liquidity layer and a fast-path relayer mesh to deliver transfers in seconds while preserving verifiability and liveness.

Design goals: Security-first verification (light clients/zk proofs) with circuit breakers; finality-aware speed via optimistic fast path; unified SDK for tokens, NFTs, calls, and intents; capital-efficient unified vaults and intent-based routing.

2) Problem

Fragmented security and liquidity, inconsistent developer interfaces, slow confirmations, and poor refund UX.

3) Solution Overview

Three layers:
• Aureon Messaging Layer (AML): verified message passing via light clients/zk, optimistic fast path, replay protection & rate limits.
• Aureon Liquidity Layer (ALL): unified vaults, intents, dynamic routing across pools/MMs/native bridges.
• Aureon Orchestration Network (AON): permissionless bonded relayers with slashing & QoS scoring.

4) Target Chains (initial)

Ethereum, BNB Chain, Base, Polygon, and Solana. Extensible to Optimism/Arbitrum, Aptos/Sui via proof adapters.

5) Architecture

Contracts: BridgeCore, LiquidityVault, TokenAdapter, RiskGuard, FeeManager.
Message flow: initiate → optional fast fill → proof verification → reconcile/repay → refund on timeout.
Security: proof-based as primary; rotating threshold committee only where proofs infeasible; rate limits, timelocks, replay protection.

6) Liquidity & Routing

Unified vaults; route types = canonical / pool swap / hybrid; intent router selects best route by fee, depth, risk, finality ETA; oracles via TWAP + cross-sources; MEV-aware protections.

7) Developer Experience

TypeScript/Rust SDK (transferToken, sendMessage, estimateRoute, hooks). REST: /v1/quote, /v1/submit, /v1/tx/:id. Wallets (Phantom/MetaMask), DEX/launchpad widgets, webhooks.

8) Fees & Treasury (no token)

Base gas passthrough + 0.05%–0.30% bridge fee + dynamic fast-path premium. Distribution of revenue: 60% LPs, 25% relayers, 10% treasury, 5% insurance (governance-tunable).

9) Security Program

≥2 audits pre-mainnet; continuous fuzzing/static; bug bounty; incident runbooks; timelocked upgrades or immutability post-maturity.

10) Risks

Relayer collusion, liquidity/oracle desync, reorgs, contract bugs, privileged key risks. Mitigations: proof-based settlement, slashing & caps, TWAP/circuit breakers, confirmations, audits, timelocks.

11) Compliance & Operations

UI/API sanction screening for hosted gateways; contracts & SDK permissionless and self-hostable.

12) Roadmap

Phase 0 (M1-2): EVM testnets + Solana devnet; token transfers; explorer; Audit #1.
Phase 1 (M3-4): General messaging; bonded fast path; dashboards; bug bounty; Audit #2.
Phase 2 (M5-6): Mainnet (ETH, BNB, Base, Polygon, Solana); limits + insurance; partial relayer decentralization.
Phase 3 (M7-12): Permissionless relayers; governance bootstrap (tokenless); zk-adapters; open intent marketplace.
Phase 4: Ecosystem integrations; SDK v2; fiat on/off-ramps.

13) KPIs & Transparency

Security: incidents & audit coverage. UX: median latency, success & refund rate. Economics: TVL, relayer QoS, LP APY. Distribution: route mix; % proof-verified vs fast-filled.

14) Governance (progressive)

Phase A: multisig + timelocks. Phase B: on-chain polls; signers execute. Phase C: DAO (tokenless) with quorum/thresholds, anti-whale voting-escrow.

15) User Experience

One-click bridge, transparent quotes (fees/ETA/trust level), explicit refund details, receipts with verifiable proofs.

16) Example Pseudocode

High-level functions xTransfer and reconcile describing fast-path & proof settlement.

17) Brand & Publishing

Brand: aureonlabs monogram (blue gradient) + wordmark. Sites: docs.aureonlabs, scan.aureonlabs, bridge.aureonlabs.

18) Conclusion

Aureon Labs delivers secure, fast, capital-efficient cross-chain value and message transfer with verifiable proofs, unified liquidity, and a developer-first stack.