LAC Lightpaper

Light Anonymous Chain

Zero-History Privacy Blockchain Infrastructure

Version 1.2
Updated: January 2026

Abstract

LAC (Light Anonymous Chain) is a next-generation privacy blockchain built around a novel **Zero-History (Non-Persistent Ledger)** architecture.

Unlike traditional blockchains — including privacy-focused networks — that permanently store transaction history, LAC cryptographically verifies activity and then physically deletes historical data, retaining only compact state commitments and proofs of validity. This eliminates retroactive chain analysis, reduces long-term attack surfaces, and delivers true forward secrecy — including resilience against future quantum decryption.

In existing blockchains, privacy degrades over time as historical data accumulates. LAC inverts this dynamic: **privacy improves with age**, because sensitive data no longer exists.

On top of its Zero-History core, LAC provides a privacy-native platform for anonymous messaging, identity, and application development, secured by Ring Signatures, Stealth Addresses, and post-quantum cryptography.

NEW in v1.2: Production-ready **VEIL Transfers** and **STASH Pool** — Monero-level anonymity meets Tornado Cash-style mixing, built directly into protocol.

A functional testnet is live with 10,300+ blocks, demonstrating the architecture in real network conditions.

LAC is not another messaging app on a blockchain.
It is foundational infrastructure for a world where data retention itself is the risk.

The Problem

Modern blockchains suffer from a structural flaw that compounds over time: **they store history forever**.

Even privacy-oriented blockchains permanently retain transaction artifacts. While cryptography may protect data today, historical blockchains accumulate future liability:

- Chain analysis improves retrospectively
- Correlation techniques evolve
- Quantum computing threatens legacy cryptography
- Storage requirements grow without bound

As a result, **privacy degrades with time**, rather than improves.

Privacy coins reduce visibility but still preserve historical structures — headers, commitments, UTXO sets, or encrypted payloads — creating a permanent attack surface. If cryptographic assumptions weaken years later, the past can be exposed.

Transparent smart-contract platforms prioritize composability at the cost of confidentiality, making all activity permanently public. Privacy solutions are bolted on as complex, fragile add-ons rather than embedded at the protocol level.

Centralized "secure" messaging platforms avoid blockchains altogether, but rely on servers, metadata retention, and legal trust assumptions that collapse under real-world pressure.

The core problem is not insufficient encryption.
The core problem is permanent history.

Solution: Zero-History Blockchain Architecture

LAC introduces a fundamentally different approach: a **Zero-History (Non-Persistent) blockchain**.

Instead of preserving full transaction history forever, LAC separates validation from retention.

The network periodically produces cryptographic state commitments that prove the correctness of all prior activity — balances, supply, and consensus — without retaining the underlying transaction data. Once finalized and verified, historical blocks are physically deleted from the network.

What remains:

- Compact state commitments
- Proofs of past validity
- The current blockchain state

What disappears:

- Transaction details
- Message contents
- Historical metadata
- Any data usable for retroactive analysis

There is nothing to decrypt in the future, because the past no longer exists.

This architecture delivers decisive advantages:

- **True forward secrecy** — past activity remains private even if future cryptography breaks
- **Quantum-resistant privacy** — not only by stronger algorithms, but by data absence
- **Constant storage growth** — the chain does not expand indefinitely
- **Fast node synchronization** — nodes verify commitments, not years of history
- **Lower regulatory exposure** — historical personal data is not retained by design

Zero-History is not a feature. It is a new ledger class.

Core Architecture Overview

LAC's architecture is designed around intentional data lifecycle management.

Zero-History Core

- Periodic cryptographic state commitments
- Verified transition proofs between states
- Safe deletion of obsolete historical data

Privacy-Native Cryptography

- **Ring Signatures** for sender anonymity
- **Stealth Addresses** for recipient unlinkability
- **Post-quantum encryption** (Kyber-768) for future resilience

Ephemeral Data Layers

- Short-lived messages and metadata
- Automatic expiration and deletion
- No recoverable forensic traces

Applications such as messaging, identity, governance, and DeFi are enabled by the architecture, not patched on afterward.

NEW: VEIL + STASH — Production-Ready Privacy Features

👻 VEIL TRANSFERS

Fully anonymous transactions with Monero-level privacy built directly into protocol.

Technical Features:

- **Ring Signatures** — hide sender among 10+ decoys
- **Stealth Addresses** — one-time addresses for each transaction
- **Amount Hiding** — encrypted transaction values
- **Post-Quantum Ready** — Kyber-768 integration

Comparison:

Feature	Monero	Zcash	LAC VEIL
Ring Signatures	✅	❌	✅
Stealth Addresses	✅	✅	✅
Mandatory Privacy	✅	❌	✅
Post-Quantum	❌	❌	✅
Zero-History	❌	❌	✅
Messaging Integration	❌	❌	✅

Fee: 1.0 LAC
Speed: 10-30 seconds
Finality: ~13 seconds per block

🎒 STASH POOL

Anonymous asset storage — a legal, protocol-native mixing service.

How it works:

1. **Deposit:** Choose nominal (100 / 1,000 / 10,000 / 100,000 LAC) → receive STASH Key
2. **Storage:** Tokens held in anonymous pool, no owner tracking
3. **Withdraw:** Use STASH Key once → receive tokens to any address → key burns

Comparison:

Feature	Tornado Cash	Zcash Shielded	LAC STASH
Mixing Pool	✅	❌	✅
Fixed Nominals	✅	❌	✅
No Time Lock	❌	✅	✅
Offline Key Backup	❌	❌	✅

Legal Status	⚠️ Sanctioned	✅	✅
Blockchain Native	❌ (Smart Contract)	✅	✅

Why STASH is safer:

- Built into protocol (not smart contract)
- No trusted setup required
- Simple UX without complex zk-proofs
- Legal status (not sanctioned)

STASH Key Format:

stash_{"v":1,"n":1,"s":"256bit_secret"}

Security:

- 256-bit entropy
- One-time use
- Offline storage (paper/metal backup)
- No accounts required

Fees:

- Deposit: 2.0 LAC
- Withdraw: 0 LAC

Why Existing Blockchains Cannot Replicate This

Zero-History is not an optimization — it is an **architectural boundary**.

All existing blockchains, including privacy networks, share a core assumption: **history must be stored forever**.

- Bitcoin and Ethereum preserve full transaction history indefinitely
- Privacy coins reduce visibility but retain historical artifacts
- Rollups, mixers, and ZK add-ons depend on permanent base layers

These systems can improve anonymity today, but they accumulate long-term risk.

LAC operates under a different premise: **if historical data does not exist, it cannot be analyzed, correlated, subpoenaed, or decrypted later**.

This creates a clear structural distinction:

- **Privacy coins focus on hiding data**
- **LAC focuses on not keeping data**

Zero-History cannot be "added later." It requires control over the full ledger lifecycle from genesis.

Competitive Advantages

1. Architectural Moat

Zero-History is a first-principles redesign of blockchain data retention. Replicating it requires abandoning deeply embedded assumptions in existing protocols.

2. Privacy That Improves Over Time

Most privacy systems weaken as data accumulates. LAC becomes more private as historical information is removed from the attack surface.

3. Quantum-Resilient by Design

Rather than relying solely on stronger cryptography, LAC removes the data future attackers would need.

4. Constant Storage Economics

Node requirements remain bounded, enabling long-term decentralization and lower infrastructure costs.

5. Regulatory & Enterprise Optionality

Zero-History aligns naturally with data-minimization principles such as GDPR's "right to be forgotten," without compromising decentralization.

6. Production-Ready Features

VEIL + STASH are live on testnet, fully functional and tested.

Applications Enabled by Zero-History

The messenger is a proof of feasibility, not the end goal.

Zero-History + VEIL + STASH enable:

- Anonymous messaging and coordination
- Privacy-native DeFi primitives
- Confidential governance and voting
- Anonymous identity and reputation systems
- Enterprise-grade secure communication

These use cases are unlocked by the ledger design itself.

Market Opportunity

The global demand for privacy-preserving infrastructure is accelerating across:

- Blockchain and DeFi
- Secure communications
- Enterprise governance
- Regulatory-constrained environments

As data retention increasingly represents financial and legal risk, non-persistent ledgers become a **structural necessity** rather than a niche feature.

Conclusion

LAC is not competing to be another privacy coin, messaging app, or smart-contract platform.

It introduces a **new category of blockchain infrastructure: the Zero-History ledger**.

By verifying the past without preserving it, LAC enables systems where privacy does not erode with time, scalability does not collapse under storage growth, and future technological advances cannot retroactively expose users.

VEIL + STASH demonstrate that Zero-History is not just theoretical — it enables production-ready privacy features that surpass existing solutions.

This is not an incremental improvement.
It is a structural shift in how blockchains relate to history itself.

Status

- ✅ Live testnet (20 000+ blocks)
- ✅ Functional Zero-History primitives
- ✅ VEIL + STASH production-ready
- 🔄 Mainnet launch: Q2 2026

Contact:

- Telegram: @epidemia777

LAC — Infrastructure for privacy-native applications
Version 1.2 • January 2026