LIGHTPAPER v1.4 · APRIL 2026

LAC

Light Anonymous Chain

Zero-History Privacy Blockchain Infrastructure

LAC introduces a fundamentally new class of blockchain infrastructure: the **Zero-History ledger**. Unlike all existing blockchains — including privacy coins — LAC does not store transaction history forever. It cryptographically verifies activity and then **physically deletes** historical data, retaining only compact state commitments.

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

"Monero hides data. Zcash encrypts data. LAC destroys it."

400,000+	~10s	Nov 2025	FIRST
Blocks Mined	Block Time	Genesis	Zero-History Chain

— THE PROBLEM —

Every blockchain stores history forever.

Modern blockchains suffer from a structural flaw that compounds over time: they store all history permanently. Even privacy-oriented blockchains retain transaction artifacts. While cryptography may protect data today, historical blockchains accumulate future liability:

- Chain analysis improves retroactively — past transactions become easier to trace over time
- Quantum computers will eventually decrypt encrypted historical data
- Storage requirements grow without bound — nodes become increasingly expensive
- Future cryptographic vulnerabilities expose transactions from years ago

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

The core problem is not insufficient encryption.

The core problem is permanent history.

— THE SOLUTION —

Zero-History: verify the past without storing it.

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 — without retaining the underlying transaction data. Once finalized and verified, historical data is physically deleted.

— ZERO-HISTORY THREE-TIER ARCHITECTURE —

TIER	DATA TYPE	RETENTION	CONTENT	FATE
L3	FULL DATA	30 days	**Complete blocks · all transactions & messages**	DELETED
L2	HASHES ONLY	90 days	**Block hashes · cryptographic proofs only**	DELETED
L1	COMMITMENTS	∞	**Merkle roots · validator-signed · permanent**	**KEPT**

After L1 commitment is validator-signed, L3 and L2 data are permanently removed from disk. There is nothing to decrypt in the future, because the past no longer exists.

— CORE FEATURES —

Full ecosystem, not just a coin.

■ VEIL Transfers

Anonymous transactions using Ring Signatures + Stealth Addresses. Every transaction hides the sender among 10+ decoys. Recipients use one-time addresses. Amount is encrypted. Post-quantum secure with Kyber-768. Monero-level anonymity built directly into the protocol — not a layer on top.

■ STASH Pool

Anonymous asset storage with fixed denominations (100 / 1K / 10K / 100K LAC). Deposit LAC → receive a 256-bit secret key → withdraw to any address from any device. Zero on-chain link between deposit and withdrawal. Built into protocol — not a smart contract.

■ Encrypted Messaging

End-to-end encrypted chats (Ed25519 + X25519 + XSalsa20-Poly1305). Ephemeral messages that self-destruct after 5 minutes. Burn-after-read messages destroyed the instant they are opened. Group channels (public / private / secret). Voice messages and images with automatic L2 cleanup.

■ Dead Man's Switch

If you do not check in for N days, automatic on-chain actions execute: transfer all funds to a designated address, send pre-written messages, burn STASH keys, wipe wallet. Everything recorded anonymously on L1. No other blockchain implements this natively.

■ Nagini Protocol

Geographic secret distribution using Shamir Secret Sharing. Split your seed into N shards, each encrypted with the GPS coordinates of a physical location. Recover only by visiting K locations in the real world. Quantum canary traps detect unauthorized recovery attempts.

■ Bitcoin SPV Wallet

Non-custodial Bitcoin wallet derived from your LAC seed via SHA256(SHA256("LAC-BTC-WALLET-v1:" + seed)). One seed phrase → two wallets. Keys derived locally, never transmitted. Native SegWit (bc1q...), full UTXO management, fee estimation.

■ Wraith Soul-bound NFT

Every wallet can mint a unique Wraith — a soul-bound token permanently linked to your address. Not transferable. Recorded on-chain. 5 equipment slots (Head/Core/Arms/Legs/Armor) take craftable items. Items upgrade to Level 5 (+25% bonus per level). Rare mutations drop randomly. Bonuses are real: block chance, fee discounts, shard drops.

■ LAC Mesh (WiFi Direct)

Offline peer-to-peer networking module for Android. Nodes form a mesh using WiFi Direct and relay encrypted messages without internet. Ed25519 encryption compatible with main chain. Store-and-forward routing with TTL. Foundation for the DePIN hardware layer.

— COMPETITIVE ANALYSIS —

Why existing blockchains cannot replicate this.

Zero-History is not an optimization — it is an architectural boundary. All existing blockchains, including privacy networks, share one core assumption: history must be stored forever. LAC operates under a different premise.

FEATURE	MONERO	ZCASH	SIGNAL	LAC
Physical data deletion	✗	✗	✗	✓
Ring Signatures	✓	✗	✗	✓
Encrypted messaging	✗	✗	✓	✓
Burn after read	✗	✗	✗	✓
Dead Man's Switch	✗	✗	✗	✓
Offline mesh networking	✗	✗	✗	✓
Built-in Bitcoin wallet	✗	✗	✗	✓
Post-quantum (Kyber-768)	✗	✗	✗	✓
Soul-bound NFT companions	✗	✗	✗	✓

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 —

Six structural 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. Nothing to decrypt when history doesn't exist.
- **4. Constant Storage Economics** — Node requirements remain bounded, enabling long-term decentralization and lower infrastructure costs. 50x storage reduction compared to full-history chains.
- **5. Regulatory Alignment** — Zero-History aligns naturally with data-minimization principles such as GDPR's "right to be forgotten," without compromising decentralization.
- **6. DePIN Infrastructure Layer** — LAC Mesh enables physical node deployment — privacy hotspots, offline relays, and edge compute validators earning rewards. Real hardware, real network resilience.

— TOKENOMICS —

Deflationary by design.

Every significant action on LAC burns tokens permanently. At scale, burn exceeds emission, creating a deflationary model. Burn mechanics are live in testnet — not theoretical.

PARAMETER	VALUE
Max Supply	~1,840,000,000 LAC (100-year emission)
Block Time	~10 seconds
Initial Reward	190 LAC / block
Winners / Block	19 (PoET fair distribution)
TX Fee	0.1 LAC (transfers) · 1.0 LAC (messages)
Username	50 LAC burned permanently
Level Upgrade	100 – 2,000,000 LAC burned
Wraith Mint	500 LAC
Level 7 ■ GOD	2× mining chance · 2× validator reward

— BURN MECHANICS —

Tokens are burned on: every message sent (1 LAC), username registration (50 LAC), every level upgrade (100–2,000,000 LAC), Wraith minting and item upgrades, STASH pool deposit fees. The network already burns more LAC than it mints per active user. At 10,000+ daily active users, net supply is deflationary.

— ROADMAP —

Built in the open. Verifiable on testnet.

	MILESTONE	STATUS
✓	**Zero-History blockchain (L1/L2/L3 deletion)**	Live · 400,000+ blocks

✓	**VEIL anonymous transfers + STASH pool**	Live in testnet
✓	**Encrypted messaging (regular / ephemeral / burn)**	Live in testnet
✓	**Dead Man's Switch + Nagini Protocol**	Live in testnet
✓	**Bitcoin SPV wallet (non-custodial)**	Live in testnet
✓	**Wraith soul-bound NFT system**	Core live · full in development
✓	**LAC Mesh WiFi Direct networking**	Live · open source
✓	**Zero-History validators with rewards/slashing**	Live in testnet
■	**Native iOS & Android apps**	In development · 2026
■	**Node Sale infrastructure (on-chain licenses)**	In development · Q3 2026
■	**Security audit**	Planned before mainnet
■	**Mainnet launch**	Target Q3–Q4 2026
■	**BTC ↔ LAC Atomic Swaps (HTLC)**	Planned
■	**DePIN hardware nodes (privacy hotspots)**	Roadmap 2026

— STATUS —

Live testnet. Open source. Community-driven.

LAC is in active beta testnet with 400,000+ blocks mined, real users, and real data deletion happening every day. All code is open source on GitHub. The project is built in Ukraine and funded through community support and planned node sale revenue.

■ Try it now — no installation required

Open lac-beta.uk in any browser. Create a wallet in 10 seconds.

— CONTACT & LINKS —

Get in touch.

CHANNEL	LINK / HANDLE
Testnet	https://lac-beta.uk
Website	https://lac-chain.com
GitHub	https://github.com/epidemiaya/LightAnonChain-
Telegram	@epidemia777 · channel: @lac_chain
X / Twitter	https://x.com/LAC_Chain
Medium	https://medium.com/@lanoesteban42
HackerNoon	https://hackernoon.com/blockchains-dont-have-a-privacy-problem-they-have-a-memory-problem

Email	fresrty@gmail.com
YouTube	https://youtu.be/-k5DKsVxjO0

LAC — Infrastructure for privacy-native applications. Lightpaper v1.4 · April 2026. Built in Ukraine

■■