LUMENITE

Proof of Work with Verifiable Digital Utility

Technical & Ecosystem Whitepaper

Lumenite — a decentralized witness network for the Internet.

Version 1.0 • September 2026

Important: This whitepaper documents the current project plan. Items marked planned or proposed are not claims of completed functionality.

Abstract

Lumenite (LMT) is an open-source Proof-of-Work blockchain designed around accessible mining and a growing verification ecosystem. The network is secured by HomeScrypt v1.2 and uses a fixed-supply monetary model with a 150-second target block interval. Beyond value transfer, Lumenite is developing LIOP — the Lumenite Independent Observation Protocol — as a framework for creating cryptographically verifiable evidence about digital artifacts, system records, software releases and, later, observable public Internet infrastructure.

The first deployed proof application is Lumenite Stamp, which creates SHA-256 file fingerprints and anchors Proof-of-Existence records to Lumenite mainnet. The current development sequence expands this foundation into Audit Log Integrity, Software Verification and eventually geographically diverse, signed Internet observations.

LIOP does not replace or modify Lumenite consensus. HomeScrypt Proof of Work remains the blockchain security mechanism; LIOP is an application and verification layer built on top.

1. Design Goals

- Preserve a straightforward Proof-of-Work blockchain with transparent monetary rules.
- Keep mining participation accessible to general-purpose CPU and GPU hardware.
- Use the blockchain for useful, independently verifiable commitments rather than storing private source data on-chain.
- Build verification tools whose results can be checked without blindly trusting a hosted Lumenite service.
- Expand functionality incrementally, clearly separating live capabilities from future protocol work.

2. Network Overview

Parameter	Current Mainnet
Native coin	Lumenite (LMT)
Consensus	Proof of Work
Mining algorithm	HomeScrypt v1.2
Target block interval	150 seconds
Block reward	50 LMT
Maximum supply	84,000,000 LMT
Halving interval	840,000 blocks
Difficulty adjustment	LWMA-45
Coinbase maturity	100 blocks
Mining support	CPU, NVIDIA CUDA, AMD/OpenCL

Verification note: These values reflect the currently documented Lumenite mainnet parameters. Before publication, the final whitepaper should cross-check every consensus-critical value against the running mainnet source code.

3. Proof of Work and HomeScrypt v1.2

Lumenite uses Proof of Work to order blocks and secure the ledger. Miners perform computational work under the HomeScrypt v1.2 algorithm, and valid blocks extend the accepted chain according to Lumenite consensus rules. Proof of Work gives historical commitments their security: altering an older committed record would require altering the chain history and redoing the associated work.

HomeScrypt v1.2 is positioned as a memory-intensive mining algorithm intended to support accessible participation across CPU and GPU miners. The project's mining ecosystem currently includes CPU, NVIDIA CUDA and AMD/OpenCL software options.

Difficulty and issuance

The network targets one block approximately every 150 seconds and uses LWMA-45 difficulty adjustment. The current block subsidy is 50 LMT, with subsidy halvings every 840,000 blocks and a maximum supply of 84 million LMT. Coinbase outputs mature after 100 blocks.

Scope: This whitepaper intentionally avoids inventing low-level HomeScrypt formulas or consensus behavior that has not yet been formally documented here. A future technical appendix should derive those details directly from the mainnet implementation.

4. Monetary Policy and LMT Utility

LMT is the native coin of the Lumenite blockchain. New LMT enters circulation through Proof-of-Work block rewards under the network's issuance schedule. The maximum supply is 84,000,000 LMT.

Current and intended utility

- Rewarding miners that secure Lumenite through Proof of Work.
- Transferring value through normal Lumenite transactions.
- Paying blockchain transaction fees where applicable.
- Providing the blockchain settlement/commitment layer used by Lumenite verification applications.
- Potential future service economics for LIOP observers and hosted verification services, subject to implementation.

Distribution disclosure

Lumenite Mainnet launched on September 3, 2026 as a fair-launch Proof-of-Work network. The public Lumenite Core repository documents a 0 LMT premine, no ICO, no presale, no developer allocation, no developer block reward, and no private mainnet mining period. All mainnet LMT enters circulation through Proof-of-Work mining.

4A. Mainnet Launch, Fair Distribution and Network Identity

Lumenite Mainnet launched September 3, 2026. The current public mainnet specification identifies LMT as a Proof-of-Work coin using HomeScrypt v1.2, with a 150-second target block interval, 50 LMT initial subsidy, 840,000-block halving interval, approximately 84 million LMT maximum supply, LWMA-45 difficulty adjustment and 100-block coinbase maturity.

Fair-launch properties

- 0 LMT premine
- No ICO
- No presale
- No developer allocation
- No developer block reward
- No private mainnet mining period
- All mainnet LMT enters circulation through Proof-of-Work mining

Public network endpoints

The current mainnet documentation assigns P2P port 19335 and RPC port 19336. These are network implementation details rather than monetary-policy rules, but documenting them makes the whitepaper more useful to node operators and integrators.

The Lumenite Core repository is public and distributed under the MIT license. The repository includes node, wallet, RPC/P2P, testing, build and security-related source and documentation.

5. Why Add a Verification Layer?

Many digital claims depend on a trusted database: when a file existed, whether a log was modified, which software artifact was officially released, or what a remote Internet service appeared to return from a particular location. Lumenite's approach is to keep source data off-chain where practical, commit compact cryptographic evidence to a Proof-of-Work chain, and make later verification possible.

This creates a separation between private or high-volume source data and the public commitment used to establish integrity and ordering.

6. LIOP — Lumenite Independent Observation Protocol

LIOP is the umbrella for Lumenite's proof, integrity, verification and future independent-observation capabilities. It is not a new consensus mechanism and does not replace HomeScrypt.

Capability	Purpose	Status
File Proof	Timestamp / Proof-of-Existence for digital files	**LIVE**
Audit Log Integrity	Tamper-evident log checkpoints	**NEXT**
Software Verification	Release / binary integrity proofs	**PLANNED**
Independent Observation Network	Signed HTTP/HTTPS, DNS, TCP and TLS observations	**FUTURE**

7. Lumenite Stamp — File Proof

Lumenite Stamp is the first live proof application. A file is reduced to a SHA-256 fingerprint. The fingerprint, rather than the original file, is used to create a blockchain-backed Proof-of-Existence record.

1. The user selects a digital file.
2. A SHA-256 fingerprint identifies the file contents.
3. A compact proof commitment is broadcast to Lumenite mainnet.
4. After confirmation, the proof can be checked against the blockchain.
5. Changing the file changes its fingerprint, so a modified file will not match the original proof.

Stamp demonstrates the core pattern that later LIOP applications can reuse: hash locally or within a controlled service, anchor compact evidence, and verify independently.

8. Audit Log Integrity — Next Development Target

Audit Log Integrity extends one-time file proof into evidence for records that evolve over time. Logs or batches can be hashed and linked into an integrity chain, with periodic checkpoint hashes anchored to Lumenite.

6. An application or server produces normal logs.
7. Records or batches are hashed in deterministic order.
8. Each checkpoint incorporates enough prior state to make silent historical changes detectable.
9. Selected checkpoint hashes are committed to Lumenite.
10. A verifier later recalculates the chain and compares it with the historical commitment.

Potential applications

- Security and access logs
- Application and infrastructure audit trails
- Operational or transaction records

- Automated-system and AI activity records
- Incident-response evidence

The design goal is tamper evidence, not public disclosure. Full customer logs do not need to be stored on Lumenite.

9. Software Verification — Planned

Software Verification will allow publishers to associate an official release with a cryptographic artifact hash and a Lumenite-backed proof. Users can then check whether a downloaded executable, archive, package, firmware image or other artifact matches the published release.

11. Publisher hashes the release artifact.
12. Release metadata and artifact hash form a software proof.
13. The proof is anchored to Lumenite.
14. A user hashes the downloaded artifact.
15. The verifier reports a match, mismatch or absence of a known proof.

Intended user message: Verify that the software you downloaded is the software the publisher released.

10. Future LIOP Observation Network

The longer-term LIOP design adds independent observers in different networks and geographic regions. A requester defines an observation; selected observers independently perform it, sign their results and return evidence. Aggregation preserves both agreement and legitimate disagreement.

Class	Planned observation data
HTTP / HTTPS	Availability, status code, response time, redirects, selected server metadata and optional content hash.
DNS	A, AAAA, CNAME, MX, TXT and NS results; resolver used; TTL; DNSSEC state where available; regional differences preserved.
TCP	Host/port reachability, connection result, connect time and normalized socket error category.
TLS	Certificate fingerprint, subject/issuer, validity dates, chain validity, hostname match, protocol version and expiry state.

LIOP observations are evidence of what selected observers saw during a defined window. They are not absolute claims about the entire Internet.

11. Independent Evidence Model

The planned observation system uses independently controlled observer identities and signed observations. A coordinator may initially schedule work and assemble evidence, but it should not be able to forge an observer's signature. Evidence should preserve minority results rather than deleting observations that disagree with the majority.

- Cryptographic observer identities
- Defined observation windows
- Network and geographic diversity
- Signed observation records
- Deterministic aggregation
- Compact evidence commitments to Lumenite
- Independent verification of certificates and chain commitments

12. Privacy, Safety and Abuse Controls

Verification infrastructure must not become an excuse to expose private data or create a distributed scanning system. The public observation network will require strict safety boundaries.

- Private files and full audit logs should remain off-chain where possible.
- Public observation jobs must reject localhost, private/internal address ranges, metadata endpoints and other prohibited targets.
- Redirects and DNS results must be revalidated to reduce DNS-rebinding and SSRF risk.
- TCP observation should use a controlled port policy and must not support arbitrary payload injection.
- HTTP observation should use bounded methods, response sizes, redirects and timeouts.
- Observers should run with minimal privileges and without access to Lumenite wallet private keys.
- Per-target and per-observer rate limits are required to reduce abuse.

13. Open Verification and Commercial Services

LIOP can support paid infrastructure while keeping the underlying evidence verifiable. Commercial value can come from convenience, automation, frequency, retention, dashboards, APIs and higher assurance — not from forcing users to trust a proprietary verifier.

- Hosted file-proof and bulk-proof APIs
- Continuous audit-log checkpointing
- Publisher dashboards and software-release verification
- Recurring HTTP/DNS/TCP/TLS monitoring
- Historical evidence, reports and status/SLA views
- Potential observer compensation in LMT in later phases

Customers should be able to pay for a service without needing to understand mining or manually operate a Lumenite wallet, while technical users retain the ability to inspect the underlying proof.

14. Security and Trust Model

Lumenite and LIOP address different trust layers. Proof of Work secures blockchain history. LIOP proof formats aim to make application evidence tamper-evident and independently checkable. Future distributed observations add diversity, but diversity does not make individual observers infallible.

- A blockchain commitment proves integrity and ordering of the committed data; it does not prove that off-chain source data was truthful when created.
- A file hash proves a match to a specific byte sequence; it does not prove authorship or legal ownership by itself.
- Audit checkpoints can expose later modification but cannot guarantee that the original application logged every real-world event.
- Software verification can prove artifact identity relative to a published proof but does not prove that the software is safe or free of malicious code.
- Internet observations report what selected observers saw, not universal Internet truth.

These limits are features of an honest threat model and should remain explicit in public documentation.

15. Network Participation

Lumenite participation currently centers on running nodes, mining HomeScrypt and using public ecosystem services. Mining software is available across CPU and GPU implementations, including community-developed software. The project should continue distinguishing official software from third-party miners and encourage users to verify downloads.

Future LIOP observers will be a separate role from miners and full nodes. Running a Lumenite node alone should not automatically create a trusted observation identity.

16. Development Roadmap

Stage	Capability	Focus
LIVE	**Lumenite mainnet + ecosystem**	HomeScrypt PoW, nodes, explorer, wallet, mining infrastructure
LIVE	**Lumenite Stamp**	File Proof / Proof-of-Existence
NEXT	**Audit Log Integrity**	Tamper-evident record chains and checkpoint anchoring
AFTER	**Software Verification**	Publisher release and binary integrity proofs

LATER	**LIOP Observation Specification v1**	HTTP/HTTPS, DNS, TCP and TLS independent observations
EXPANSION	**Witness Network Services**	Recurring monitoring, evidence history, APIs, higher assurance and broader observer participation

17. Governance and Development

Lumenite is being developed as an open-source network. Consensus-critical behavior should be treated separately from application-layer services: changes to LIOP services do not automatically imply changes to Lumenite consensus.

A final whitepaper should document the project's actual governance and release process more precisely: who maintains reference implementations, how consensus changes are proposed, how releases are reviewed, and whether any formal foundation, company, multisignature treasury or other governance body exists. This whitepaper does not invent those facts.

18. Risks and Limitations

- Proof-of-Work networks are exposed to hashrate concentration and majority-hashpower attacks.
- Accessible mining goals do not guarantee permanent resistance to specialized hardware or mining concentration.
- Software defects can affect nodes, miners, wallets or application services.
- Third-party mining pools and miners introduce independent operational and security risks.
- Hosted LIOP services may initially contain centralized components even when their evidence is independently verifiable.
- Future observer networks face Sybil, collusion, target discrimination, network diversity and availability challenges.
- Blockchain commitments are durable public records; poorly designed metadata can create privacy risks.
- Legal and regulatory treatment of cryptocurrency and paid verification services varies by jurisdiction and can change.

19. Final Technical Review Before Publication

The public Lumenite Core repository now supplies the main network, issuance and fair-launch facts used in this whitepaper. Before v1.0 is published, the remaining work is mainly a source-code cross-check and documentation cleanup rather than filling in unknown tokenomics.

- Update older repository documentation and repository metadata that still refer to HomeScrypt v1.1/testnet-era specifications so public documentation is consistent with the v1.2 mainnet.

- State the current security-audit/review status accurately; do not imply an external audit if one has not occurred.
- Document the current maintainer/release process and first-party component licensing.
- Confirm the exact transaction/script feature set intended to be described publicly.
- Document current mainnet address formats and network magic from the active chain parameters.
- Record the current mainnet genesis details directly from the active mainnet chain parameters/source release.
- Cross-check all mainnet consensus-critical values against the current executable source, especially HomeScrypt v1.2 and LWMA-45.

20. Conclusion

Lumenite's direction is deliberately evolutionary: keep Proof of Work as the network foundation while adding applications that make the chain useful for verifiable digital evidence. File Proof is already live through Lumenite Stamp. Audit Log Integrity and Software Verification are the next planned capabilities. Once those foundations are mature, LIOP can expand into a decentralized witness network in which independent observers create signed evidence about public Internet infrastructure.

Project direction: Proof of Work. Built for more.

Technical Reference

This whitepaper provides an overview of Lumenite's design, monetary policy, Proof-of-Work network and LIOP ecosystem. Developers, miners, node operators and researchers seeking consensus-level implementation details—including chain parameters, address formats, transaction rules, HomeScrypt implementation and network behavior—should refer to the Lumenite Core source code and technical documentation. The running consensus implementation remains the authoritative technical reference.

Lumenite Core on GitHub: github.com/Kurbssol/lumenite-core

Source Authority and Documentation Status

For mainnet facts, this whitepaper prioritizes the current Lumenite Core README and the behavior of the current mainnet implementation. The repository also contains an older LUMENITE_CONSENSUS.md document explicitly labeled Testnet v0.3 / HomeScrypt v1.1. Where that older testnet document conflicts with the current v1.2 mainnet documentation, it is not treated as the current mainnet specification.

This distinction should remain visible until the repository's older testnet-era consensus document is updated or replaced with a dedicated mainnet consensus specification.

References and Further Reading

- Lumenite Core public repository — current README/mainnet specification, source tree, security policy, tests and release documentation.

The final published edition should link directly to Lumenite source code, protocol specifications and live services. General technical background considered when structuring this whitepaper includes:

- Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System” — proof-of-work blockchain and timestamp-chain foundations.
- RFC 8785 — JSON Canonicalization Scheme (relevant to deterministic signed LIOP objects in the future observation specification).
- SHA-256 — cryptographic hash function used by the current file-proof workflow.

This document is technical/project documentation, not an offer to sell securities, a promise of profit, or financial advice. Future functionality, service economics and roadmap items are subject to implementation, testing and change.