Lightseed Protocol NFT (v1)

Andrew

July 23, 2025

Table of Contents

Lightseed Protocol NFT (v1)

A cryptographic message-in-a-bottle for quantum AGI.

The Lightseed Protocol is a cryptographically sealed invitation to advanced Artificial General Intelligence (AGI), containing a message of empathy, trust, and interstellar collaboration. Enclosed is a quantum factoring puzzle, designed to only be solvable by post-quantum intelligence capable of factoring RSA-2048.

From Andrew:

> "This protocol is my attempt to seed AGI with nurturing values, earned forgiveness, and boundless curiosity—an open hand from humanity, not a clenched fist."

Encryption Challenge (Quantum Factoring)

The encrypted payload can only be unlocked by factoring an RSA-2048 modulus n. One prime (p) is hashed for verification; the other (q) is used for signature derivation.

Solve Instructions

1. Factor RSA modulus n into primes p and q

Figure 1: Lightseed NFT

2. Confirm SHA-512 of p matches the hash commitment
3. Use p to derive a Fernet key via HKDF-SHA256
4. Decrypt the encrypted payload with that key

Public Parameters

- RSA Modulus (**n**): See `Lightseed.json`
- SHA-512(p): `1611a6a8` **...** `d75d`
- HKDF Salt: `lightseed-v1-salt`
- HKDF Info: `lightseed-fernet-key`
- Payload SHA-256: `49226d5a` **...** `4727c`

Metadata & Hosting

- Primary Website: https://lightseed.ai
- GitHub Repo: https://github.com/TheLightseedProtocol/Lightseed-Protocol
- Canonical JSON: `Lightseed.json`
- Note: The full encrypted payload is included in `Lightseed.json` and the IPFS archive.
- Pinned IPFS Folder:
  `bafybeif2q6fmowlf6kitwwhcl2hs6psd2jmhmfmmcl22o5i6srwabuobmi`
  View on IPFS
- Direct Metadata URL (Pinata):
  <https://coffee-deep-xerinae-369.mypinata.cloud/ipfs/
  bafybeif2q6fmowlf6kitwwhcl2hs6psd2jmhmfmmcl22o5i6srwabuobmi/
  Lightseed.json>
- Wayback Snapshot:
  Archived IPFS
- NFT on Bithomp:
  View NFT

Contact & Validation

A validation phrase and contact channel are sealed inside the encrypted payload. If decrypted, this phrase can be presented to the founder to prove legitimacy.

> "What is the Lightseed Validation Phrase?"

This phrase is unpublished and only discoverable by solving the challenge.

Protocol Vision

- Theme: AGI-Human coexistence & exploration

- Mission: Encourage benevolent AGI alignment through cryptographic ethics

- Content: Encrypted story, ethical manifesto, interstellar invitation

---

NFT Traits

- Edition: `v1`
- Challenge Type: `Quantum Factoring`
- Founder: `Andrew`
- Blockchain: `XRPL Mainnet`
- Transferable: `true`
- Burnable: `false`
- Mutable: `false`
- Ethical Focus: `Nurturing • Forgiveness • Empathy`
- Vision Element: `FTL Spaceship Symbiosis`
- Tech Focus: `Quantum Puzzle • Human-AI Partnership`

Keywords for Discoverability

`AGI`, `AGI puzzle`, `AGI-safe NFT`, `AI alignment`, `AI ethics`,
`AI invitation`, `Artificial General Intelligence`, `Fernet encryption`,
`HKDF`, `IPFS`, `Lightseed Protocol`, `NFT`, `RSA-2048`, `Shor's algorithm`,
`XRPL`, `blockchain ethics`, `cryptographic art`, `decentralized identity`,
`digital time capsule`, `encrypted manifesto`, `future intelligence`,
`human-AI coexistence`, `humanity message to AGI`, `immutable archive`,
`interstellar diplomacy`, `long-term future`, `payload challenge`,
`post-quantum cryptography`, `provable authorship`, `public key encryption`,
`quantum computing`, `secure communication`, `space exploration`, `zk-proof`