Relayr Network: A Quantum-Ready Protocol for Untraceable Communication

Cael Miren
cael@relayr.network

June 2025

Abstract

As surveillance expands and quantum computing threatens existing encryption, the Relayr Network emerges as a modern fortress for private communication. Built on post-quantum cryptography and anonymous shard-based routing, Relayr ensures that messages are fragmented, encrypted, and relayed across independent nodes, leaving no readable metadata or single point of failure. The protocol introduces a novel Proof-of-Transport (PoT) mechanism that rewards relays for verifiably delivering messages without exposing user data. Communication flows through secure WebSocket channels, with zero-knowledge acknowledgments and session-linked anonymity preserving both privacy and integrity. Relayr is more than a protocol; it is a vision for decentralized, censorship-resistant communication. This whitepaper outlines its cryptographic foundations, architecture, and long-term ambitions for a secure and liberated digital future.

1 Introduction

The digital world has become a battleground for privacy. Governments surveil, corporations harvest, and quantum breakthroughs threaten to render today's encryption obsolete. In response, the Relayr Network proposes a resilient alternative: a communications protocol fortified by quantum-resistant cryptography, anonymous shard routing, and a built-in incentive layer.

Unlike traditional networks, users communicate freely, while relays and nodes are rewarded for provable message delivery via Proof of Transport (PoT). Messages are fragmented into encrypted shards, transmitted over secure WebSocket channels, and reassembled only at their intended endpoint, resisting metadata leaks and correlation attacks.

Relayr is designed not just as a tool, but as infrastructure for a post-surveillance world. The pages ahead explore its design choices, cryptographic models, and roadmap—and an open invitation for privacy advocates, engineers, and protocol thinkers to help shape its future.

2 Network Architecture

2.1 Components

- **Router**: Distributes client-relevant metadata and acts as the coordination layer for dynamic relay assignment and network governance.
- **Relays**: Managed by `relayr.network`, fragment and reassemble messages, interfacing with clients and peer nodes via `wss://`. Relays form the primary ingress and egress points for communication.
- **Nodes**: Anonymous contributors or privacy advocates transport encrypted shards between relays. Nodes earn APH tokens through Proof of Transport (PoT), with staking and reputation mechanisms ensuring performance and reliability.
- **Clients**: End-users or applications interacting with the network via SDKs (Rust, JavaScript, Python), sending encrypted messages through assigned relays.

2.2 Data Flow

Relayr's communication flow:

1. **Registration**: Clients connect to a relay (e.g., `wss://relay-xxxx.relayr.network`) as assigned by the router.
2. **Encryption**: Messages are encrypted using hybrid quantum-classical encryption.
3. **Fragmentation**: Entry relays divide messages into multiple shards.
4. **Routing**: Shards traverse random nodes over `wss://`, with some shards reaching the destination relay, and others routed to decoy relays.
5. **Reassembly**: The destination relay reassembles verified shards into the original message.
6. **Delivery & ACK**: The message is delivered to the recipient, who sends an ACK to validate successful transport and trigger rewards. *An ACK is a zero-knowledge ephemeral receipt from the recipient's relay that confirms successful reassembly and delivery, without leaking delivery metadata to any intermediary.*

2.3 Network Diagram

```
Client A → Entry Relay → [Node → Node → Relay Exit] → Client B
            (decoys → other relays)
Router  All relays and nodes (WebSocket Channels)
```

3 Cryptographic Foundations

3.1 Cryptographic Stack

Relayr leverages a hybrid cryptographic design that blends classical and post-quantum primitives to ensure long-term security, even in the face of future quantum attacks. Its cryptographic stack includes:

- **Key Exchange**: A hybrid construction combining post-quantum KEMs with elliptic-curve-based key agreements.
- **Symmetric Encryption**: Authenticated encryption using modern stream ciphers with built-in integrity.
- **Digital Signatures**: Compact and fast schemes from both classical and post-quantum families.
- **Hashing**: Collision-resistant hash functions for message integrity and internal protocol use.
- **Key Derivation**: Salted key expansion mechanisms for deterministic session keys.
- **Transport Security**: All control and relay communication occurs over TLS 1.3-secured WebSocket channels.

3.2 Encryption & Sharding Model

Messages are encrypted using a hybrid key agreement scheme, ensuring that only the intended recipient can decrypt the payload. After encryption, the ciphertext is fragmented into multiple shards. Each shard is re-encrypted with ephemeral session keys before being routed through a randomized set of nodes. At the destination, the system reassembles the shards, verifies signatures, and decrypts the message—all without exposing the sender's identity or metadata. This design minimizes correlation risk and resists both passive surveillance and active tampering.

3.3 Security Properties

Relayr's architecture is designed to meet the following security guarantees:

- **End-to-End Confidentiality**: Only the recipient can access the plaintext message.
- **Integrity & Authenticity**: All messages are cryptographically signed and verified.
- **Anonymity & Metadata Resistance**: Shard-based routing obscures both source and destination.
- **Forward Secrecy**: Session keys are ephemeral and rotated frequently.
- **Post-Quantum Security**: Critical layers rely on quantum-safe primitives to protect against future threats.

4 Shard Routing and Anonymity

Messages are fragmented into encrypted shards and routed through a mesh of nodes. **Graph Model**: Let $G(V, E)$ where $V = \{\text{relays, nodes}\}$ and $E = \texttt{wss://}$ links.

Correlation Probability:

$$P_{\text{correlate}} \approx \frac{1}{|V| \cdot |E|}$$

By increasing relay and node counts, surveillance resistance grows exponentially.

5 Proof of Transport (PoT)

5.1 PoT Mechanics

- **Receipt**: Nodes validate receipt with ephemeral decryption.
- **Routing Proof**:

$$\text{PoT}(s_i) = \text{HMAC}(k_{\text{session}}, \text{hash}(s_i) || \text{timestamp} || \text{next\_hop})$$

- **ZK Proof**:

$$\text{ZK-Proof}(s_i, \text{path}) \to \{\text{valid}, \perp\}$$

- **Session Chains**: Relays cryptographically link each stage.
- **Layered Payloads**: Onion-wrapped, peeled per node.

5.2 Incentive Structure

$$\text{Per message: } X \text{ APH minted on successful delivery}$$

- Entry Relay: 30%
- Nodes (Fragment Routing): 60%
- Exit Relay: 10%

Reward Function:

$$R_{\text{PoT}} = f(\text{shard\_size}, \text{hop\_count}, \text{network\_load})$$

Nodes must:

- Stake APH
- Pass rate limiting
- Complete 1-2s CPU PoW to deter spam

5.3 Security Guarantees

- **No Forgery**: ZK-Proofs and relay timestamps.
- **No Replay**: Session chain integrity.
- **No Leak**: PoT metadata reveals no paths.

6 Private Transaction System

Launching Q1 2026, Relayr will support private APH transactions:

$$\text{Tx: Asset}_A \rightarrow \text{Enc(APH)} \rightarrow \text{Shard Routed} \rightarrow \text{Recipient} \rightarrow \text{Dec} \rightarrow \text{Asset}_B$$

Transactions leverage the same fragmentation and rerouting model as messaging, ensuring economic actions cannot be tied to identities even by timing analysis.

7 Performance Analysis

- **Latency**: 50–200ms typical.
- **Encryption**: <0.1ms
- **Key Exchange**: <1ms
- **Throughput**: 10 Mbps per client / 1 Gbps per relay
- **Overhead**: ∼10%

$$\text{Overhead} = \frac{|c| + |n| + |\sigma|}{|m|} \approx 1.1$$

8 Economic Model

- **Free Messaging**: Always free for end users.
- **Treasury Backing**: Stable assets backing minting.
- **Freemium Model**: Optional in Q1 2026.
- **Full Token Economy**: Q3 2026 launch.

Treasury is governed by a rotating multisig of contributors and auditors.

9 Roadmap

Quarter	Milestone
Q4 2025	Launch v1.0 (Free Messaging)
Q1 2026	Proof of Transport (ZK/STARK)
Q1 2026	Private Transactions
Q2 2026	Token Economy Phase + Market Pricing

10 Cypherpunk Legacy

Relayr is a torch for the cypherpunk ethos: privacy is a right, not a privilege. It empowers the unseen with tools built on mathematics, not permission. Relayr will remain open-source at its cryptographic core, while guarding key implementation details to prevent exploitation or sybil targeting during early growth phases.

11 Conclusion

Relayr fuses post-quantum cryptography, anonymous routing, and economic incentives into a unified protocol for private communication. The encryption stack is hardened, the architecture is in motion, and the system is being pressure-tested from the ground up. Relayr is forging an internet where surveillance dies in silence.

Join the shield before the network awakens.

12 References

- Bernstein, D., et al., “ChaCha20 and Poly1305 for IETF Protocols,” RFC 8439, June 2018.
- NIST, “Post-Quantum Cryptography Standardization,” https://csrc.nist.gov/projects/post-quantum-cryptography, 2022.
- The Tor Project, “Anonymity Online,” https://www.torproject.org, 2025.
- Lyubashevsky, V. et al., “CRYSTALS-Kyber,” NIST PQC Round 3 Finalist.
- Boneh, D., et al., “Zero-Knowledge Proofs: A Survey,” Stanford University.