# PierNet: Technical Overview & Implementation

Version 1.0 | Technical Whitepaper | February 2025

## 1. Network Architecture

✅ \*\*User Devices as Nodes\*\* – Phones, tablets, Raspberry Pi devices form the core mesh.

✅ \*\*Long-Range & Fixed Nodes\*\* – LoRa, CBRS, and antennas extend rural coverage.

✅ \*\*Nodes That Act as Gateways Can Earn Connectivity Tokens\*\* – Devices that provide internet access to the network receive token rewards based on demand and usage.

## 2. Proof-of-Connectivity (PoC) Token Model

Nodes earn tokens based on:

✅ \*\*Reliability (Uptime & Stability).\*\*

✅ \*\*Geographic Expansion (Adding new coverage areas).\*\*

✅ \*\*Traffic Volume (Data Relayed).\*\*

Harbors (Internet Gateways) receive additional rewards for providing external access.

## 3. Dynamic Pricing & Priority-Based Token Spending

Data transmission costs are based on:

✅ \*\*Low Priority (Cheapest)\*\* – Background transfers, batch downloads.

✅ \*\*Standard Priority (Balanced Cost)\*\* – Normal browsing and messaging.

✅ \*\*High Priority (Most Expensive)\*\* – Real-time video, VoIP calls, emergency data.

Prices fluctuate based on network congestion and node availability.

\*\*Dynamic Pricing Model (Example Costs in Tokens per MB)\*\*

|  |  |  |  |
| --- | --- | --- | --- |
| Network Load | Low Priority (Tokens/MB) | Standard Priority (Tokens/MB) | High Priority (Tokens/MB) |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
| Low Traffic (Late Night) | 0.2 | 0.5 | 1 |
| Normal Traffic (Daytime) | 0.5 | 1 | 2 |
| High Traffic (Peak Hours) | 1 | 2 | 4 |

💡 These values dynamically adjust based on real-time demand. Higher congestion leads to increased costs for priority access.

## 4. DAO Governance & Network Reserve

✅ \*\*Hybrid DAO Model\*\* – A mix of token holders and active network contributors make governance decisions.

✅ \*\*Algorithm-Driven Pricing\*\* – The system automatically adjusts pricing; the DAO can intervene only in extreme cases.

✅ \*\*DAO Override Threshold\*\* – Requires a percentage of active participants to trigger a governance vote.

## 5. Security & Trust Mechanisms

✅ \*\*End-to-End Encryption\*\* – Prevents unauthorized data interception.

✅ \*\*Reputation-Based Trust\*\* – Nodes earn credibility based on uptime and reliability.

✅ \*\*Mitigation Against Malicious Nodes\*\* – Bad actors can be flagged and blacklisted.