Enigmatic - L0: A Layer - 0 Communication Protocol

5. Security Model

5.1 Threat Model Definition

We define the global blockchain state as a tuple: $S = (\mathcal{U}, \mathcal{B}, T)$ where:

- $\mathcal{U}$ is the set of all UTXOs,
- $\mathcal{B}$ is the ordered set of DigiByte blocks,
- T is the mempool transaction graph.

Enigmatic - L0 assumes adversaries with the following capabilities:

- Full node access
- Chain analytics tooling
- Ability to reorder non - mined transactions via fee pressure
- Ability to observe address clustering heuristics

Adversaries cannot:

- Break modern symmetric encryption
- Predict witness randomness
- Modify already - mined blocks
- Violate DigiByte ’ s consensus rules

5.2 Confidentiality Guarantees

Message confidentiality derives from AES - GCM encryption:

$$ C = \text{AES\_GCM}_k(P, \text{nonce}) $$

where:

- P is plaintext
- k is a session key derived via:

$$ k = H(sk_{A} \cdot pk_{B}) $$

through elliptic - curve Diffie - Hellman over secp256k1.

UTXO encoding preserves ciphertext secrecy because:

$$ v_i = C_i \mod N $$

and recovering C_i from v_i without keys is equivalent to brute forcing the entire ciphertext space.

5.3 Integrity & Authenticity

Integrity is provided by:

1. AES - GCM authentication tags
2. Deterministic order constraints between UTXO frames
3. Transaction - level commitment: $h = H(v_1 || v_2 || ... || v_n || \text{fee})$

Authenticity derives from private - key ownership of the UTXO - spending address: $\text{sig} = \text{ECDSA}_{sk}(h)$

This forms an implicit sender identity without exposing metadata.

6. Threat Analysis

6.1 Chain Surveillance Resistance

Standard chain - analysis heuristics operate on:

- address reuse
- common input ownership
- clustering
- transaction fingerprinting

Enigmatic - L0 disrupts these heuristics due to:

- rotating address families
- symmetric UTXO - chunk structures
- fees mimicking organic variance
- entropy injected by ECDSA randomness

Formally, detectability is defined as:
$$ D = Pr[A(S) = 1] $$ where A is a classifier attempting to detect L0 traffic.

Our design aims to minimize:
$$ D \approx 0.50 $$ i.e., indistinguishable from random noise.

6.2 Transaction Pattern Obfuscation

The protocol introduces controlled randomness: $$ v'_i = (v_i + r_i) \mod N $$ where the jitter term r_i is derived from:
$$ r_i = H(\text{txid} || i) \mod N $$

This ensures no UTXO appears deterministically crafted.

6.3 Replay & Manipulation Protection

Replays are mitigated through:
$$ \text{nonce} = H(\text{prev\_txid}) $$

Manipulation is prevented because altering any UTXO amount changes: $$ H(\text{raw\_tx}) $$
breaking OP_RETURN checksums and AES - GCM tags simultaneously.