Appendix B – Glossary & Definitions

Author: Ahmad Hemmati | Website: https://www.twincodesworld.com

Status: Open Source – Technical Supplement | Version: v1.0

AEAD (Authenticated Encryption with Associated Data)
Encryption schemes (e.g., AES-GCM, XChaCha20-Poly1305) that provide confidentiality, integrity, and authenticity while allowing binding of external metadata (AAD).

Appendix
Supplementary section of the whitepaper providing technical modules, definitions, references, and threat models.

Bloom Filter
A probabilistic data structure used to detect duplicates with tunable false-positive probability (~1% in LHDNS gossip deduplication).

Compliance Gateway
Optional LHDNS nodes that bridge to regulated environments (e.g., enterprises, governments) under explicit opt-in logging, without weakening core privacy guarantees.

Cover Traffic
Artificial dummy entries or messages injected into the network to disguise actual communication and resist traffic analysis.

DAO Governance
A decentralized governance model where token holders vote on upgrades, fees, and protocol parameters, with anti-capture safeguards.

DLN (Distributed Ledger Network)
The ephemeral, peer-to-peer ledger layer that stores, validates, and gossips LHDNS resolution entries.

ECDH (Elliptic Curve Diffie–Hellman)
A key exchange protocol based on elliptic curves, enabling two parties to establish a shared secret securely (X25519 is used in LHDNS).

Enc_contact
An encrypted payload inside a ledger entry that carries client contact metadata (e.g., relay token, WebSocket endpoint). Encrypted via X25519 + HKDF + AEAD.

Ephemeral Key Exchange
Session-limited ECDH key agreement that provides forward secrecy. Keys are rotated frequently and discarded after TTL expiry.

Ephemeral Resolution
Mapping of a service_id to enc_contact data through short-lived ledger entries. Designed to prevent metadata accumulation.

Forward Secrecy
A cryptographic property ensuring that compromise of long-term keys does not reveal past session keys or communication.

Gossip Protocol
An epidemic-style peer-to-peer protocol for propagating ledger entries. Nodes forward entries to random subsets of peers until TTL expiry.

Hash-Token
A deterministic, short-lived identifier derived from eph_pub, service_id, nonce, and time_window. Prevents linkage and replay.

LHDNS (Ledger-based Hashed Decentralized Naming System)
A next-generation naming architecture combining hash-derived identifiers, ephemeral ledger entries, cryptographic proofs, and decentralized governance.

Merkle Digest
A cryptographic digest built from Merkle trees of ledger entries. Used for auditability and cross-validation of node behavior.

Micropayment Channels
Off-chain payment mechanisms for frequent small transfers (e.g., paying relays), minimizing blockchain congestion.

Nonce
A random, one-time-use value ensuring uniqueness of cryptographic operations. Used in hash-token and enc_contact derivations.

Onion Routing
Layered encryption of messages across multiple relays, so each relay only knows its predecessor and successor, not the full path.

PQC (Post-Quantum Cryptography)
Algorithms designed to resist attacks from quantum computers. Considered in LHDNS's long-term roadmap.

Service Descriptor
A signed metadata object published by services that contains ephemeral public keys, accepted transports, and nonce policies.

Service_id
Canonical identifier of a service, defined as `svc:sha256:<hex>` (32-byte raw SHA-256 digest). Used for lookup and cryptographic binding.

Slashing
The punitive mechanism by which staked nodes lose part of their collateral if found misbehaving (e.g., equivocation, censorship).

Staking
Locking LHD tokens as collateral to participate in validation, relay, or governance roles.

TTL (Time To Live)
The short validity window of a ledger entry (default: 30 seconds). Entries automatically expire and are pruned after TTL + grace.