LITEPAPER V1.0

CPUNK

Post-Quantum Identity, Encrypted Messaging
& Multi-Chain Wallet

cpunk.io | March 2026 | Community-Driven & Open Source

Table of Contents

1. Introduction

CPUNK is a community-driven project building post-quantum, privacy-first infrastructure for digital identity, encrypted communication, and multi-chain asset management. The project is fully open source.

At its core is **DNA** (Decentralized Network Applications) — a single application that combines self-sovereign identity, end-to-end encrypted messaging, and a multi-chain cryptocurrency wallet. DNA runs on top of a custom-built, community-operated DHT network called **Nodus**, requiring zero centralized servers.

The **CPUNK token**, a CF20 token on the Cellframe blockchain, serves as the governance and utility token within the DNA ecosystem. All components are designed from the ground up to be resistant to quantum computing attacks using NIST-standardized post-quantum algorithms.

2. The Problem

Modern communication and identity systems share a common set of fundamental weaknesses:

- **Centralized control** — Identity providers (Google, Apple, Meta) can revoke access, censor users, and mine behavioral data at will.
- **Metadata exposure** — Even "encrypted" messengers leak metadata: who talks to whom, when, how often, and from where. Metadata alone is enough to reconstruct social graphs.
- **Quantum vulnerability** — RSA and elliptic-curve cryptography, used by virtually every messaging and wallet application today, will be broken by sufficiently powerful quantum computers. NIST has already published post-quantum standards (FIPS 203, 204, 205) as a direct response.
- **Fragmented identity** — Users maintain separate accounts, separate wallets, separate keys across dozens of platforms with no sovereign control over any of them.

> CPUNK's thesis: **privacy, self-sovereignty, and quantum resistance must be built into the foundation** — not bolted on later. DNA is that foundation.

3. DNA — Decentralized Network Applications

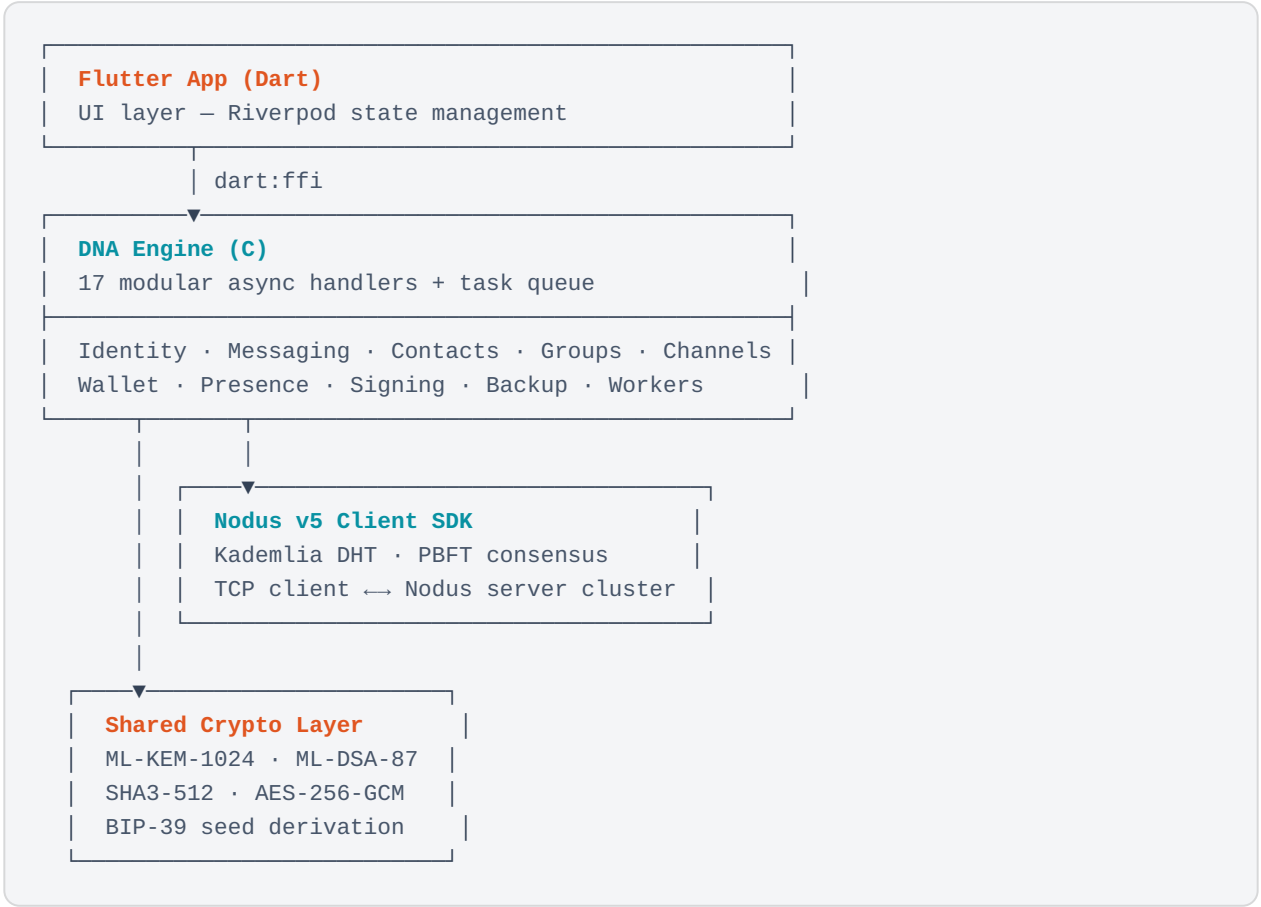
DNA is a single application built around three integrated pillars:

PILLAR	FUNCTION	KEY PROPERTY
DNA Identity	Self-sovereign, human-readable name tied to a post-quantum key pair	No phone, no email, no central authority
DNA Messenger	E2E encrypted peer-to-peer messaging with groups, channels, and feeds	Zero metadata, zero servers
DNA Wallet	Multi-chain wallet derived from the same seed as identity	One seed, four blockchains

All three pillars share a single BIP-39 seed phrase. One backup, one identity, one set of wallets — unified under one cryptographic root.

4. Architecture Overview

DNA is built as a native C library with a Flutter (Dart) UI layer communicating via FFI. The transport backbone is the Nodus network — a custom Kademlia DHT.



The C engine is modular: each domain (identity, messaging, wallet, etc.) is an independent handler that processes tasks from an async queue. This design allows concurrent operations, clean separation of concerns, and easy extensibility.

5. Cryptographic Primitives

All cryptographic operations use NIST-standardized post-quantum algorithms at the highest available security level (Category 5). No classical-only fallbacks are used.

ALGORITHM	STANDARD	PURPOSE	KEY SIZES
ML-KEM-1024 (Kyber1024)	FIPS 203	Key encapsulation (E2E key exchange)	Public: 1568 B Secret: 3168 B Ciphertext: 1568 B
ML-DSA-87 (Dilithium5)	FIPS 204	Digital signatures (identity, message auth)	Public: 2592 B Secret: 4896 B Signature: 4627 B
SHA3-512	FIPS 202	Hashing (DHT keys, integrity, addressing)	512-bit digest
AES-256-GCM	FIPS 197 / SP 800-38D	Symmetric encryption (message payloads)	256-bit key
BIP-39	Bitcoin standard	Seed phrase (12–24 words) for key derivation	128–256 bits of entropy

> **NIST Category 5** is the highest security level defined by NIST for post-quantum algorithms, providing security equivalent to AES-256 against both classical and quantum adversaries.

Key Derivation Flow

A single BIP-39 mnemonic is the root of all cryptographic material:

1. User generates (or restores) a 12–24 word seed phrase.
2. The seed derives the **Dilithium5 signing key pair** (identity).
3. The seed derives the **Kyber1024 key encapsulation pair** (messaging).
4. The seed derives **blockchain-specific wallet keys** for CF20, ERC20, SPL, and TRC20.

One seed, one backup, full sovereignty over identity and assets.

6. The Nodus Network

Nodus is a purpose-built, pure-C Kademlia distributed hash table (DHT) that serves as the transport and storage backbone for all DNA operations. It replaces the need for centralized servers entirely.

Design Parameters

PARAMETER	VALUE	RATIONALE
Keyspace	512-bit (SHA3-512)	Post-quantum collision resistance
Replication factor (k)	8	High availability, survives node churn
Record TTL	7 days	Automatic garbage collection of stale data
Wire format	CBOR	Compact, schema-flexible binary encoding
Wire framing	7-byte header (magic 0x4E44 + version + length)	Fast parsing, version negotiation
Consensus	PBFT (Practical Byzantine Fault Tolerance)	Consistency for critical records

Two-Tier Protocol

Nodus separates server-to-server and client-to-server communication into distinct protocol tiers:

- **Tier 1 (UDP)** — Kademlia peer discovery between Nodus servers: `PING`, `FIND_NODE`, `PUT`, `GET`.
- **Tier 2 (TCP)** — Client connections from DNA apps: `AUTH`, `DHT_PUT`, `DHT_GET`, `LISTEN`, `CHANNELS`.

Clients authenticate to the nearest Nodus node, which then handles routing, replication, and delivery across the DHT on their behalf.

Core Functions

- **Peer discovery** — Clients find each other via DHT key lookups. No central directory.
- **Offline message delivery** — Encrypted messages are stored in distributed mailboxes replicated across the 8 closest nodes. Recipients retrieve them upon reconnection.
- **Identity resolution** — DNA names resolve to public keys and routing hints via DHT lookups.
- **Real-time subscriptions** — Clients subscribe to DHT key ranges for instant notification of new messages, presence changes, and group updates.

> Nodus nodes are community-operated. They store and forward only **encrypted blobs** — they cannot read message contents, identity data, or transaction details. Privacy is enforced by architecture, not policy.

7. DNA Identity

A DNA identity is a human-readable name (3–20 characters) cryptographically bound to a post-quantum key pair. Registration happens entirely on the Nodus DHT — no blockchain transaction, no central registrar, no fee.

Properties

- **Self-sovereign** — Ownership is defined by the private key. No entity can revoke, reassign, or censor a DNA name.
- **Pseudonymous** — No phone number, email, or real-world identity required.
- **Permanent** — Once registered, a DNA name is immutable and globally unique across the Nodus network.
- **Ecosystem-wide** — The same DNA name is used for messaging, wallet operations, governance, and all future CPUNK services.

Registration Flow

1. User creates or restores a wallet from a BIP-39 seed phrase inside the DNA app.
2. User chooses a unique DNA name. The app checks availability on the DHT.
3. The name is bound to the user's Dilithium5 public key and published to the Nodus network.
4. The identity is immediately usable for messaging, wallet, and all ecosystem interactions.

8. DNA Messenger

DNA Messenger is a fully decentralized, end-to-end encrypted messenger with no central servers, no phone number requirement, and no metadata collection. All message transport runs over the Nodus DHT.

Feature Set

FEATURE	DESCRIPTION
1:1 Messages	Direct encrypted messages between two DNA identities
Groups	Multi-party conversations with Group Encryption Key (GEK) rotation
Channels	One-to-many broadcast feeds with subscriber management
Public Feed	Global public timeline of signed posts
Personal Wall	Per-user public wall (posting requires CPUNK token burn)
Contacts	Contact requests, blocking, address book management
Presence	Online/offline status via DHT heartbeats
In-Chat Transfers	Send CPUNK tokens directly within a conversation

Message Delivery

- **Both online:** Messages are delivered instantly via direct TCP connections. Each client subscribes to its contacts' DHT keys for real-time push.
- **Recipient offline:** The ciphertext is written to distributed mailboxes across the 8 closest Nodus nodes. The sender can go offline immediately after — Nodus handles the rest.
- **Recipient returns:** The client queries the DHT, retrieves pending messages, and decrypts them locally.

Encryption Model

Every message is encrypted with **Kyber1024 + AES-256-GCM**. The message envelope carries only 20 bytes of routing header — no sender identity, no timestamps, no IP addresses. Group messages use a **Group Encryption Key (GEK)** that is rotated on membership changes and distributed to members via individual Kyber1024-encrypted channels.

9. DNA Wallet

DNA Wallet is a multi-chain cryptocurrency wallet built directly into the DNA app. It derives all blockchain-specific keys from the same BIP-39 seed phrase as the identity and messaging keys.

Supported Chains

CHAIN	TOKEN STANDARD	CAPABILITIES
Cellframe	CF20	Native CPUNK token, delegation, DEX trading
Ethereum	ERC20	Token transfers, balance tracking, DEX quotes (Uniswap)
Solana	SPL	Token transfers, balance tracking, DEX quotes (Jupiter)
TRON	TRC20	Token transfers, balance tracking

Key Properties

- **One seed, all chains** — A single mnemonic controls all wallets. No separate backups needed.
- **Non-custodial** — Private keys never leave the device. No server holds custody.
- **In-chat transfers** — CPUNK tokens can be sent directly within messenger conversations.
- **Integrated DEX** — Live swap quotes from Jupiter (SOL) and Uniswap (ETH) displayed natively.

10. CPUNK Token

CPUNK is a CF20 token on the Cellframe blockchain. It serves as the governance and utility token within the DNA ecosystem.

PROPERTY	VALUE
Standard	CF20 (Cellframe)
Total supply	1,000,000,000 (fixed, no additional minting possible)
Launch date	February 1, 2025
Distribution	100% unlocked at launch

Utility

- **Governance** — CPUNK holders vote on protocol decisions and improvement proposals.
- **Feed/Wall access** — Posting to the public feed or personal wall requires burning CPUNK, preventing spam and giving posts economic weight.
- **In-chat transfers** — CPUNK is the only token transferable directly within messenger conversations.
- **Ecosystem alignment** — Holding CPUNK signals commitment to the privacy and decentralization values of the project.

11. Platform Availability

PLATFORM	STATUS	NOTES
Linux (x64)	Available	Primary development platform, full feature set
Android (arm64)	Available	APK distribution, cross-compiled native libraries
Windows (x64)	Available	Cross-compiled builds
iOS	Planned	Architecture supports it, awaiting build pipeline

All builds are produced by CI/CD pipelines. The entire codebase — C engine, Flutter UI, Nodus server, and shared crypto layer — is **open source** and publicly auditable.

12. Roadmap

Completed

- Post-quantum identity system (Dilithium5 + Kyber1024)
- E2E encrypted 1:1 messaging, groups, channels, and feeds
- Multi-chain wallet (CF20, ERC20, SPL, TRC20)
- Nodus v5 DHT network with PBFT consensus
- In-chat CPUNK transfers
- DEX integration (Jupiter, Uniswap, Cellframe DEX)
- Linux, Android, and Windows builds

In Progress

- iOS build pipeline
- Enhanced group management and admin controls
- DHT backup and restore for identity portability
- Network monitoring and node operator tooling

Planned

- File and media sharing (encrypted attachments)
- Voice messaging
- Extended governance framework (on-chain proposals)
- Node operator incentive mechanisms
- Additional blockchain integrations

13. Community & Governance

CPUNK is a community-driven project with no corporate entity behind it. Development is coordinated openly, and all code is available for public review.

- **Open source** — Full source code is hosted on GitLab (gitlab.cpunk.io) and mirrored on GitHub.
- **Community governance** — CPUNK holders participate in decision-making through on-chain voting.
- **Node operators** — Community members run Nodus nodes that form the network backbone.
- **Contribution model** — Anyone can contribute code, documentation, translations, or infrastructure.

Links

RESOURCE	URL
Website	cpunk.io
Source Code	gitlab.cpunk.io/cpunk
Telegram	t.me/chippunk_official
X (Twitter)	x.com/OfficialCpunk
Exchange	bitcointry.com (CPUNK/USDT)