# Litepaper

**Version:** One point One [1.1]

**Prepared:** March 2026

**Product:** Ciforus

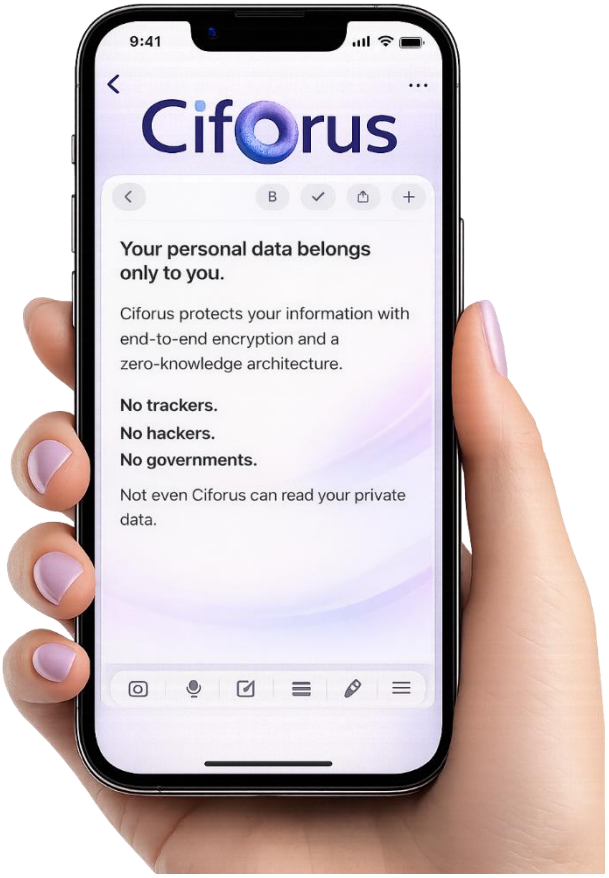
**Token:** CIFORUS (ERC-20 on Ethereum Mainnet)

**Contract Address:**
0x2D125Cba88516832AE1CDc1d39211fC259182c60

# Own your data. Control your identity

Ciforus is a privacy-focused workspace designed for secure communication, encrypted storage, and a premium digital identity with **@Ciforus.com** email address

Built for modern crypto-native users



# Ciforus Litepaper

## Important Notice

This litepaper is a concise strategic companion to the full Ciforus whitepaper. It summarizes the product thesis, privacy architecture, token utility, roadmap, and market positioning of Ciforus in a shorter and more investor-readable format. It is based on the current repository reference documents, current public product messaging, and the latest confirmed project information available as of March 30, 2026.

This document is not legal, tax, or investment advice. Some platform capabilities are live or near launch, while others remain roadmap items. To preserve platform security, the document intentionally avoids publishing sensitive implementation details that could materially increase attack risk.

## Table of Contents

Important Notice ..... 3
Table of Contents ..... 3
I. Executive Overview ..... 4
II. Why Ciforus Exists ..... 4
III. The Ciforus Platform ..... 6
IV. Privacy, Security, and Architecture ..... 8
V. Business Model and Tier Structure ..... 10
VI. Why the Token Matters ..... 11
VII. Token Utility and Tokenomics Snapshot ..... 12
VIII. Roadmap ..... 14
IX. Risk Factors ..... 16
X. Conclusion ..... 17
XI. References ..... 17

# I. Executive Overview

Ciforus is a privacy-first digital platform that unifies secure communication, encrypted storage, wallet-aware identity, account protection, and crypto-native payment workflows into one connected environment. It is built for users who need stronger privacy boundaries than conventional Web2 platforms can provide, with special relevance for crypto-native users, founders, operators, teams, and other high-sensitivity digital participants.

The problem Ciforus solves is fragmentation. Modern users are forced to split their identity, files, notes, communication, security settings, and payments across disconnected systems with conflicting privacy assumptions. Even when one tool is secure, another often reintroduces exposure through metadata, discovery models, provider control, or billing rails. Ciforus addresses this by applying one privacy and security philosophy across multiple modules instead of leaving users to assemble a fragile stack on their own.

Ciforus is the product. CIFORUS is the economic engine of the product. The token is not meant to replace the platform thesis or overshadow it. Instead, it powers the economic coordination layer of the ecosystem through discounts, access incentives, staking-based tier activation, reward alignment, and usage-linked deflation.

In short, Ciforus aims to become a premium crypto-native privacy environment rather than just another software tool. Its long-term ambition is to evolve into a serious privacy infrastructure layer for users who treat digital sovereignty as a real requirement.

# II. Why Ciforus Exists

## 2.1 The structural problem

Digital life is fragmented. Email sits in one service, messaging in another, files in another, notes in another, billing in another, and wallet activity in public blockchain environments. These systems rarely share the same privacy model or trust assumptions.

That fragmentation produces several risks:

- identity is scattered across too many surfaces
- metadata remains visible even when content is partly protected
- platforms maintain too much power over access and recovery
- convenience features often depend on readable indexes and exposed infrastructure
- payment rails can reintroduce identity leakage even after privacy has been protected elsewhere

For crypto users, these risks are amplified. Wallets can represent money, governance rights, operational authority, and reputational history. When wallet-linked users rely on fragmented consumer tools, they become easier to profile, impersonate, target, and socially engineer.

## 2.2 Why this matters now

Privacy is no longer a niche preference. It is operational infrastructure. Public reporting from major security organizations continues to show that credential abuse, phishing, social engineering, identity compromise, fraud, and data breaches remain core threats. In crypto, those risks are even more severe because attackers often focus on users with asymmetric value, whether that value sits in capital, influence, early information, or access.

Ciforus is built on the belief that serious crypto users should not have to choose between usability and privacy every time they write a note, send a file, verify an identity, or accept a payment.

## 2.3 The Ciforus thesis

Ciforus treats privacy as infrastructure rather than a feature. That means:

- privacy should be built into architecture, not added later
- identity should be user-anchored, not provider-dictated
- communication, storage, notes, access, and billing should follow one coherent trust model
- free users should not be stripped of the core security standard
- crypto-native users need a usable identity environment, not just a wallet address

# III. The Ciforus Platform

Ciforus is organized as a modular ecosystem. The modules are distinct in function, but connected by shared privacy, identity, and security principles.


## 3.1 Core modules

### Email and the @ciforus.com identity pillar

**Email is a core product pillar of Ciforus.** The `@ciforus.com` identity is positioned as a premium, privacy-first digital identity rather than just another inbox. Ciforus Email supports private communication between Ciforus users, strong transport security for external interoperability, aliases, disposable addresses, and a future direction toward a fuller webmail experience.

### Wallet Messaging

Ciforus Messaging is built around wallet-based identity rather than usernames or phone numbers. Wallet ownership becomes the trust anchor for private communication. The system supports encrypted conversations, verified wallet identity, and pending encrypted delivery for recipient wallets that have not yet completed registration.

### Secure Storage

Ciforus Storage is a confidentiality-first vault for important digital files. It is not positioned as bulk media storage. It is designed for protected file handling, identity-linked sharing, and a stronger privacy posture around stored content.

### Notes

Ciforus Notes is an encrypted private writing environment for ideas, drafts, strategy, research, and records. Confirmed product direction includes encrypted notes, labels, pinning, and unlimited Secure Notes across all current tiers.

### Security Center

The Security Center is the account-protection layer of the ecosystem. It includes TOTP-based two-factor authentication, recovery email handling, a 12-word recovery phrase model, session management, and wallet verification support.

### Wallet Identity Layer

Wallet Identity connects verified wallet ownership to the rest of the platform. It allows the user to move through messaging, security, and payment features with a trust anchor rooted in cryptographic ownership rather than exposed social identity.

### Pay Links

Pay Links extend the platform into crypto-native payment requests. Users can create branded public-facing payment flows while keeping settlement direct-to-wallet rather than converting Ciforus into a custody wallet.

### 3.2 Product tiers

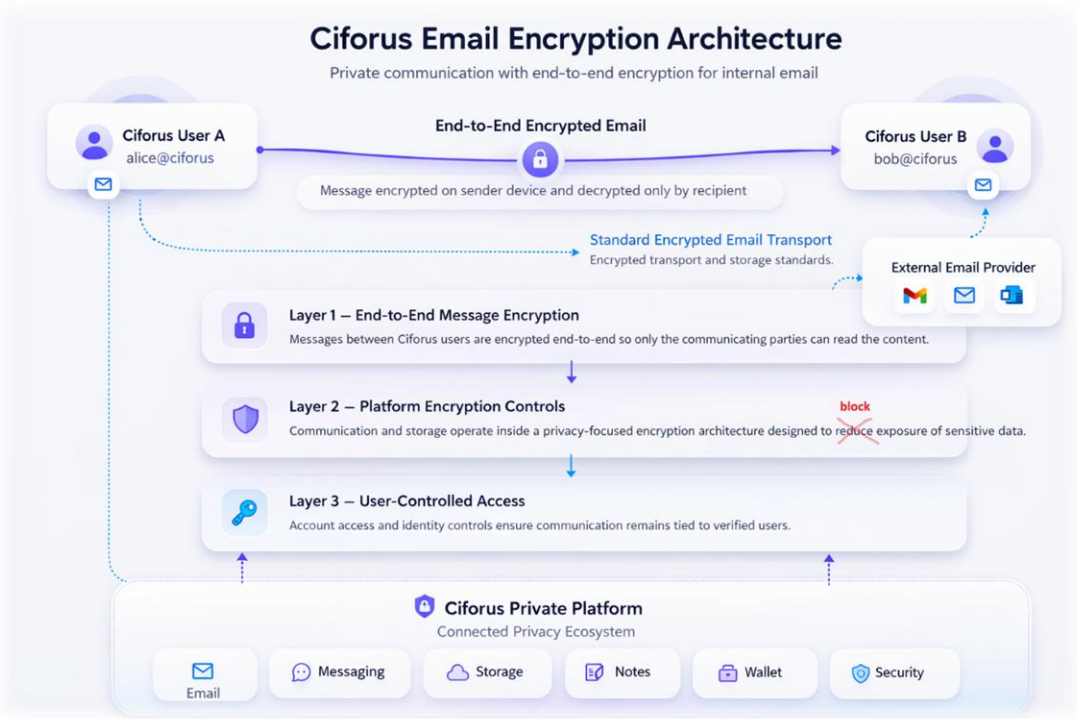
Ciforus currently presents three public tiers: Free, Pro, and Elite.

| Feature | Free | Pro | Elite |
|---|---|---|---|
| Secure Notes | Unlimited | Unlimited | Unlimited |
| `@ciforus.com` email | Included | Included | Included |
| Email aliases | 0 | 3 | 5 |
| Disposable addresses | 1 | 3 | 10 |
| Encrypted Storage | 100 MB | 500 MB | 1000 MB |
| Verified wallets | 2 | 4 | 10 |
| Public payment link | 1 | 1 | 1 |
| Active invoice Pay Links | 0 | 3 | 10 |
| Ciforus Rewards Program | Active | Active | Active |

A key product message should be preserved: security is not held back from free users. Paid tiers expand capacity and flexibility, but they do not redefine whether the user receives the platform's privacy-first foundation.

## IV. Privacy, Security, and Architecture

Privacy is the strongest strategic differentiator of Ciforus. The platform is not described as a set of isolated secure features. It is described as a coherent privacy architecture.



## 4.1 Security model at a glance

The public product and security references consistently point to:

- a custom engineered three-layer security model
- end-to-end encryption for native Ciforus communication paths
- zero-knowledge design principles
- user-controlled key access
- client-side or browser-side decryption boundaries where appropriate
- secure gateway mediation for the email environment
- AES-CTR plus HMAC file encryption in streaming contexts
- AES-256-GCM application-wide cryptographic protection for suitable protected data flows
- CSRF and session hardening
- recovery and wallet verification reinforcement

## 4.2 Zero-knowledge and privacy boundaries

Ciforus repeatedly emphasizes zero-knowledge principles. In practical terms, this means the system is designed to minimize infrastructure-level access to readable private content and to avoid convenience features that require broad readable indexes over sensitive user data.

One of the clearest examples of this philosophy is the platform's deliberate avoidance of broad server-side full-text indexing of private notes, file contents, and message bodies. Ciforus treats that tradeoff as a privacy choice, not a missing feature disguised after the fact.

## 4.3 Email isolation and gateway architecture

The Email module is described as operating through a secure gateway layer that mediates mailbox actions, policy enforcement, and encryption-aware handling. This is why the email workspace is strategically distinct inside Ciforus. Email is not treated as a flat consumer mailbox surface. It is treated as a high-trust identity and communication layer.

## 4.4 Identity, recovery, and access hardening

Privacy is not credible without strong recovery and access design. That is why the product includes:

- TOTP-based 2FA

- recovery email setup and verification
- 12-word phrase handling with BIP39-compatible reinforcement
- session controls
- wallet verification flows
- account-level defense logic

### 4.5 Public standards and compatibility anchors

The current public security narrative references widely recognized standards and compatibility anchors, including AES, TLS 1.3, and OpenPGP-related interoperability concepts for relevant email contexts. These references help situate the product within a serious security conversation without disclosing implementation detail that should remain private.

## V. Business Model and Tier Structure

Ciforus is a product-first business with a crypto-native payment philosophy.

### 5.1 Public pricing snapshot

| Plan | Annual Equivalent Monthly Price | Monthly Price | Annual Total |
|---|---|---|---|
| Free | $0.00 | $0.00 | $0.00 |
| Pro | $4.99 | $6.99 | $59.88 |
| Elite | $9.99 | $13.99 | $119.88 |

Annual pricing is the default public comparison mode because it highlights the long-term rate advantage for paid users.

### 5.2 Privacy should not disappear at the payment step

Ciforus publicly states that billing should remain aligned with the same privacy philosophy as the product itself. For that reason, the platform currently favors crypto-native checkout and intentionally avoids card payments. The logic is straightforward: if communication and identity are being protected, the payment step should not casually reintroduce identity exposure.

Accepted and planned in-app payment assets include:

- USDT
- USDC

- ETH
- BNB
- CIFORUS, with an additional **20% discount** when selected in checkout

This reinforces a central message of the project: privacy is a system-level principle, not just a feature of the interface.

## VI. Why the Token Matters

The token should be understood correctly. It is not the reason Ciforus exists, but it is essential to how the Ciforus ecosystem matures economically.

### 6.1 Product first, token second

Ciforus solves a real product problem: fragmented privacy, weak digital ownership, wallet identity gaps, and exposed communication and payment flows. The platform thesis stands on its own. The token exists to deepen ecosystem alignment around that product.

### 6.2 Why fiat and stablecoins alone are not enough

Ciforus can accept non-native crypto assets such as USDT, USDC, ETH, and BNB for access and subscription flows. That is useful and practical, but it does not create a native economic loop.

Without a native token, the platform would lack:

- ecosystem-aligned discounts and incentives
- staking-based tier activation
- a usage-linked deflation mechanism
- a native reward and loyalty layer
- a direct bridge between platform adoption and ecosystem economics
- a future-ready asset for governance and deeper utility expansion

### 6.3 Truthful positioning

The most accurate way to position the token is this:

- CIFORUS is not mandatory for every paid action
- CIFORUS is required for the long-term economic architecture of the ecosystem

That distinction matters. Users can pay with other accepted crypto assets, but only CIFORUS can provide the native incentive and deflation structure that aligns the product with a growing ecosystem.

# VII. Token Utility and Tokenomics Snapshot

## 7.1 Current and near-term utility

The token's current and near-term utility model includes:

- tier upgrades across Free, Pro, and Elite
- discounted in-app payments when CIFORUS is selected
- staking-based tier activation
- ecosystem rewards and upgrade-credit style incentive programs
- future feature expansion around storage, messaging, and premium identity
- future governance exploration after TGE and community growth

## 7.2 Deployed token status

| Item | Specification |
|---|---|
| Token Name | Ciforus |
| Token Symbol | CIFORUS |
| Standard | ERC-20 |
| Network | Ethereum Mainnet |
| Total Supply | 100,000,000 |
| Decimals | 18 |
| Mintable | No |
| Inflation | None |
| Upgradeable | No |
| Contract Address | `0x2D125Cba88516832AE1CDc1d39211fC259182c60` |

The token is already deployed and publicly verifiable on Ethereum mainnet.

## 7.3 Supply allocation

| Allocation Category | Percentage | Tokens |
|---|---|---|
| Presale | 35% | 35,000,000 |
| Ecosystem and Rewards | 20% | 20,000,000 |
| Treasury / Operations | 20% | 20,000,000 |
| Team | 15% | 15,000,000 |
| Liquidity Provision | 10% | 10,000,000 |
| Total | 100% | 100,000,000 |

## 7.4 Presale summary

| Stage | Allocation | Price | Maximum Raise | Implied FDV |
|---|---|---|---|---|
| Stage 1 - Seed Round | 8,000,000 | $0.025 | $200,000 | $2.5M |
| Stage 2 - Growth Round | 15,000,000 | $0.035 | $525,000 | $3.5M |
| Stage 3 - Final Round | 12,000,000 | $0.05 | $600,000 | $5.0M |
| Total | 35,000,000 | Weighted by round | $1,325,000 | Final reference $5.0M |

## 7.5 Vesting summary

Presale vesting:

- 20% unlocked at TGE
- 10% unlocked one month after TGE
- remaining 70% released linearly over 12 months

Team vesting:

- 6-month cliff
- no tokens unlocked at TGE
- linear vesting over 24 months after cliff

## 7.6 Deflation model snapshot

The token follows a usage-linked deflation model rather than a purely narrative one. When CIFORUS is used for eligible platform services under the current policy direction:

- 40% is permanently removed from circulation
- 40% is allocated to treasury
- 20% is reserved for liquidity support

Burns are intended to occur through transfer to a public dead wallet rather than through a privileged contract burn function. This approach is meant to keep the contract simpler and the burn process more transparent.

# VIII. Roadmap

Ciforus can be framed through both a categorized delivery roadmap and an investor-focused phased roadmap.

## 8.1 Categorized roadmap snapshot

Completed or materially completed:

- platform concept, architecture, and core module development
- Notes, Secure Storage, Wallet Messaging, and Security Center implementation
- wallet verification direction and feature gating systems
- pricing architecture across Free, Pro, and Elite
- token deployment on Ethereum mainnet
- landing and ecosystem web presence

In progress:

- launch-readiness hardening and final refinement
- presale preparation and public launch operations
- broader in-app checkout and token utility activation
- ongoing performance, UX, and release polish

Future:

- expanded email capability and fuller webmail direction
- broader token utility and staking refinement
- deeper Pay Links, messaging, and ecosystem features
- governance exploration after ecosystem maturity

## 8.2 Investor-focused phased roadmap

### Phase 1: Q4 2024 and 2025 - Foundation

- core vision and product architecture defined
- privacy-first infrastructure and encryption model designed
- modular system structure finalized across Email, Messaging, Storage, Notes, and Identity
- token utility framework and ecosystem model initiated

Investor positioning:

- not an idea, but a fully planned system ready to build

### Phase 2: Q1 2026 - Product Build (Major Milestone)

- full platform development across all core modules
- advanced encryption systems and secure architecture implemented
- wallet-based identity and access control system developed
- email infrastructure integrated via secure gateway with JMAP-based backend direction
- landing platform and ecosystem websites launched
- token deployed on Ethereum mainnet and verified
- presale infrastructure prepared

Investor positioning:

- a fully built, multi-module product, not a prototype

### Phase 3: Q2 2026 - Public Launch and Presale

- official launch of the Ciforus platform
- token presale goes live
- token utility activated inside the platform through tier upgrades and access
- deployment and refinement of remaining launch modules such as Pay Links and wallet verification support
- continuous platform refinement and performance optimization

Investor positioning:

- transition from product to live ecosystem

### Phase 4: Q3 2026 - Growth and Optimization

- real-time messaging improvements and system enhancements
- expansion of storage and email capabilities
- UX refinement and feature polishing
- early community scaling and adoption growth

Investor positioning:

- product maturity and user growth acceleration

### Phase 5: Q4 2026 - Expansion and Integrations

- strategic partnerships across crypto and privacy ecosystems
- Pay Links expansion and broader utility use cases
- exchange listing initiatives and liquidity expansion
- strengthening of the wallet-based identity layer

Investor positioning:

- ecosystem expansion and market presence

### Phase 6: 2027 - Scale and Ecosystem Evolution

- advanced token utility and deeper platform integration
- multi-chain expansion
- developer ecosystem and API layer
- exploration of governance mechanisms
- global scaling of infrastructure and user base

Investor positioning:

- Ciforus evolves into a core privacy infrastructure layer

## IX. Risk Factors

A credible litepaper should acknowledge the major risk categories clearly.

### 9.1 Product and infrastructure risk

Ciforus is a real application platform, which means it carries normal software and infrastructure risk categories including deployment issues, availability incidents, scaling complexity, abuse attempts against account flows, and integration risk.

### 9.2 Smart contract and token market risk

Although the token contract is intentionally simple, all tokens and smart contracts carry some residual technical and operational risk. Token value is also influenced by adoption, liquidity depth, execution quality, and wider market conditions.

### 9.3 Regulatory risk

The regulatory treatment of token sales, utility tokens, crypto-native services, and global digital products continues to evolve. Public communication, presale structure, and jurisdictional participation all require ongoing legal discipline.

### 9.4 User responsibility

A privacy-first platform can reduce exposure, but it cannot replace user discipline. Wallet security, recovery handling, phishing resistance, and basic operational security remain important responsibilities for every user.

## X. Conclusion

Ciforus is being built for a digital environment in which privacy, identity, communication, storage, recovery, and payments increasingly overlap. For serious crypto-native users, these are not separate categories. They are one operational surface.

The platform's strength is not one feature. It is consistency. Ciforus applies one privacy-first philosophy across email, messaging, notes, storage, wallet identity, security controls, and crypto-native billing. That makes it more than a collection of tools. It makes it a unified digital environment.

The token extends that environment into economics. Ciforus is the product. CIFORUS is the economic engine. Together, they create a product-and-economy model designed for long-term privacy infrastructure rather than short-term token speculation.

## XI. References

### Product and token verification


- Etherscan token page: <https://etherscan.io/token/0x2D125Cba88516832AE1CDc1d39211fC259182c60>
- Etherscan code: <https://etherscan.io/address/0x2D125Cba88516832AE1CDc1d39211fC259182c60#code>
- Blockscout verification: <https://eth.blockscout.com/address/0x2D125Cba88516832AE1CDc1d39211fC259182c60?tab=contract>
- Sourcify verification: <https://repo.sourcify.dev/1/0x2D125Cba88516832AE1CDc1d39211fC259182c60>
- Routescan verification: <https://routescan.io/address/0x2D125Cba88516832AE1CDc1d39211fC259182c60/contract/1/code>


### Current-time public references


- Proton Mail encryption documentation: <https://proton.me/support/mail/email-encryption>
- Telegram FAQ: <https://telegram.org/faq>
- Signal transparency and support materials: <https://signal.org/bigbrother/> and <https://support.signal.org/>

- Google Workspace client-side encryption documentation: <https://support.google.com/a/answer/10741897?hl=en-419>
- Apple privacy overview: <https://www.apple.com/privacy>
- IBM Cost of a Data Breach Report: <https://www.ibm.com/reports/data-breach>
- Microsoft Digital Defense Report 2025: <https://www.microsoft.com/en-us/security/security-insider/threat-landscape/microsoft-digital-defense-report-2025>
- Chainalysis 2026 crypto scam reporting: <https://www.chainalysis.com/blog/crypto-scams-2026/>

## END OF DOCUMENT

**March 2026**

Ciforus