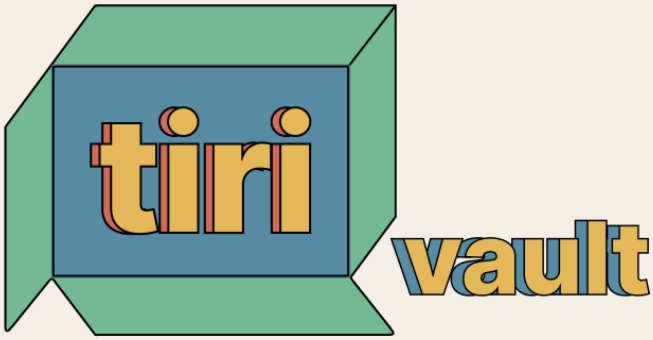


a decentralized data wallet

&

collaboration suite

Light paper

Boring Software Nation

2025

Abstract

Modern users have grown accustomed to the convenience of cloud-based workspaces: real-time synchronization, seamless file sharing, multi-device access, and integrated tools for managing personal data. However, this convenience often comes at the cost of privacy, vendor lock-in, and lack of control over where and how data is stored and accessed. In traditional systems, service providers retain access to user metadata, control authentication layers, and determine the lifecycle of user data, creating tension between usability and digital autonomy.

While decentralized storage networks promise a shift in ownership and control, they remain largely unsuitable for everyday workflows. Most function as low-level infrastructure: fragmented, difficult to onboard, and lacking workspace-level functionality. What users miss is a familiar, responsive experience without compromising on privacy or decentralization.

Tiri Vault is designed to bridge this gap. It is a gateway that turns decentralized file storage into a usable, privacy-first workspace. It enables secure file synchronization, encrypted sharing, password management, messaging, and more. Built on open standards, local encryption, and smart contract coordination, Tiri Vault offers users a familiar interface for working with decentralized data across devices, while keeping access under their sole control.

This lightpaper:

- Introduces the Tiri Vault concept and how it transforms decentralized storage into a Web3-native workspace;
- Outlines its trustless services for secure storage, collaboration and communication;
- Details the architecture and principles that allow privacy-first workflows in a decentralized environment.

Tiri Vault enables users to reclaim control over their digital interactions without giving up the simplicity they expect from modern cloud tools.

Contents

Background

In today's digital world, personal cloud file storage has become an essential tool for managing and securing digital assets. It offers users a convenient way to store, access, and share files across multiple devices while reducing the risk of data loss. The widespread adoption of cloud storage has made it a preferred choice for individuals who require seamless file synchronization, backup solutions, and remote access.

Most personal cloud storage services focus on four core functions:

- File Backup and Recovery: Regular cloud backups protect against data loss due to hardware failure, theft, or accidental deletion.
- Data Synchronization: Automated syncing ensures that users have the latest versions of their files across all linked devices, preventing inconsistencies.
- Remote Access & Mobility: Cloud storage allows users to access their files securely from any internet-connected device, making work and personal file management more flexible.
- Collaborative Sharing & Editing: Many services offer real-time collaboration tools, enabling users to share, edit, and manage access permissions for files seamlessly.

While cloud storage provides unmatched convenience, one of its biggest drawbacks is privacy. Users must trust third-party providers with their data, and while cloud companies implement security measures, risks remain. Data breaches, unauthorized access, and surveillance concerns have led many users to seek more privacy-focused alternatives.

Another growing challenge is cloud storage fragmentation—many individuals use multiple cloud providers for different needs (e.g., Google Drive for documents, Dropbox for collaboration, iCloud for photos). Managing files scattered across different platforms is inefficient, and a lack of interoperability between services complicates transfers and synchronization.

To solve these challenges, third-party data management applications have emerged, offering a centralized interface to manage files across multiple cloud platforms while enhancing security through client-side encryption. These solutions:

- ***Unify Storage Management*** – Allowing users to access and organize files from multiple cloud providers in one place.

- ***Enhance Privacy*** – Encrypting files locally before uploading them, ensuring that only users have access to their data (not the service provider or cloud platform).

However, this added privacy and convenience come at a cost—typically comparable to the price of the cloud storage itself.

Motivation

Decentralized file storage solutions have emerged as a promising alternative to traditional cloud platforms, offering stronger privacy, security, and cost-efficiency. Unlike centralized storage, Web3 solutions distribute data across a global network, preventing single points of failure and enhancing data resilience.

However, despite these advantages, most decentralized storage networks are designed primarily for infrastructure providers (IaaS) and corporate users, rather than private individuals. As a result, retail adoption remains low due to several usability challenges. To validate these challenges, we conducted a detailed examination of the top 10 Web3 storage services: Filecoin, Sia, Arweave, Storj, 0Chain, Crust Network, Swarm, DeNet, Jackal Protocol, FileFileGo.

Key Challenges in Existing Web3 Storage Networks

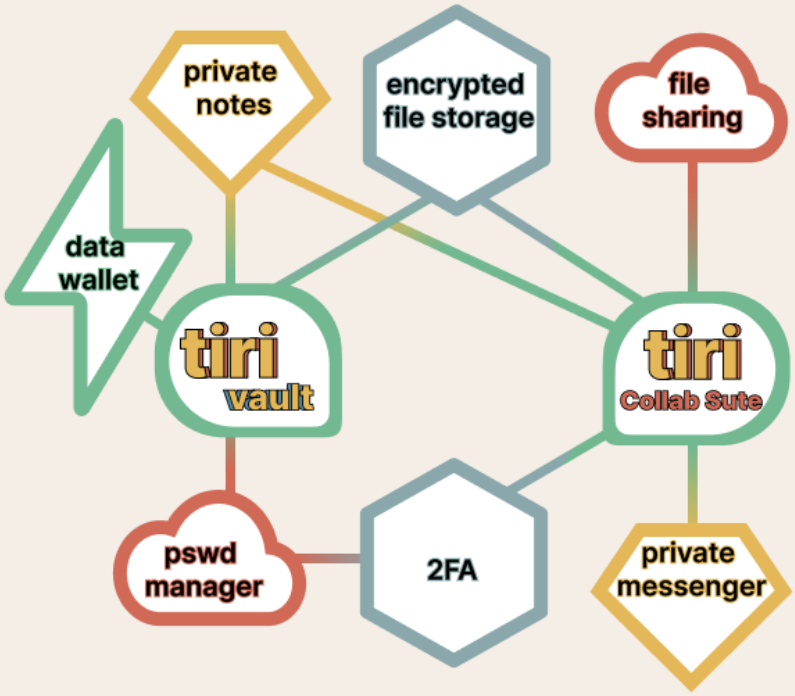
- ***Complex Onboarding Process*** – Nearly 50% of the top 10 Web3 storage services require users to navigate storage deals, contracts, staking requirements, and node setup, making onboarding too technical for the average user.
- ***Poor User Interfaces*** – Approximately 50% of the top 10 Web3 storage services lack a proper UI, relying on command-line interfaces (CLI) or minimal graphical dashboards.
- ***Complicated Storage Management*** – Around 40% of leading Web3 storage solutions use storage contracts, pay-per-deal models, or per-batch storage stamps, making it complicated to manage multiple files—especially for long-term storage.
- ***Limited or Complicated Multi-Device Access*** – About 60% of the top 10 Web3 storage services either lack support for accessing private storage from multiple devices or explicitly discourage such usage due to technical constraints. Among those that do support it, access is typically limited to alternate device usage rather than true parallel work. The architectural constraints of decentralized, blockchain-based networks inherently prevent real-time multi-device synchronization, making simultaneous access impractical.

- ***Lack of a Workspace Environment*** – About 70% of Web3 storage services provide only long-term archival storage, without file modification, deletion, or management tools. This limits use cases to static file hosting, public streaming, or cold storage—but not active file collaboration or daily work.

Tiri Vault was conceived as a solution that preserves decentralization and privacy while introducing familiar workflows and use cases that users expect. Our goal is to transform decentralized storage into a true workspace, simplifying onboarding and UX, unifying storage management across multiple Web3 platforms, and enabling privacy-first collaboration services. By bridging the gap between decentralized security and traditional usability, Tiri Vault redefines how Web3 storage can be used seamlessly and efficiently.

Tiri Vault concept

Tiri Vault is a next-generation Web3 storage platform designed to merge decentralization, privacy, and usability into a seamless and intuitive experience. Built for modern workflows, Tiri Vault enables real-time syncing, private collaboration, and smart contract integration, all while ensuring user sovereignty over their data.



Core Concepts of Tiri Vault:

Cross-Platform Web3 Workspace

Decentralized storage without disrupting existing workflows:

- Files are stored across distributed networks, ensuring redundancy and resilience against outages.
- Multi-device file access with instant updates — seamless real-time synchronization across all connected devices.
- Integrated with local folders — work from your PC or Mac just like with a traditional cloud storage solution.
- Unified access across Web3 storage networks — Tiri Vault acts as a single access point for managing and using storage from multiple decentralized networks.

Tiri Vault eliminates the friction of decentralized storage by making it work like a familiar Web2 cloud workspace while unifying Web3 storage across multiple platforms.

Privacy-First: Your Data, Your Control

User data remains completely private and inaccessible to service providers:

- End-to-end encryption at the front-end—all files are encrypted before leaving the device, ensuring zero-knowledge security.
- No third-party access, including Tiri Vault itself—users are the sole owners of their encryption keys.
- Additional privacy services, including secure vaults for passwords, notes, and credit card data, keeping sensitive information encrypted and protected.

Key Difference: Unlike centralized storage solutions, even Tiri Vault cannot access your files

Web Collaboration Without Compromising Privacy

Seamless collaboration, Web2 experience, but with full user control:

- End-to-end encrypted file sharing—users control access, with no intermediaries involved.
- No third-party control—all file permissions are cryptographically enforced.
- Crypto-backed, end-to-end encrypted, peer-to-peer messaging for teams and collaborators, ensuring private and secure communication.

Key Feature: Work with your team while maintaining full ownership and privacy over your data.

Tiri Vault Principles

Zero-Knowledge encryption

Tiri Vault is built on a zero-knowledge encryption model, ensuring that no third party, including a storage network, Tiri Vault itself, or any intermediary, can access user data. Tiri Vault encrypts all files and metadata client-side before they ever leave a user's device.

At the core of this encryption process is ChaCha20-Poly1305, a high-performance, authenticated encryption scheme that provides both fast encryption and robust integrity verification. Any data that leaves a client's device, as well as corresponding metadata, including file names, folder structures, and Content Identifiers (CIDs), is encrypted with a unique ChaCha20-Poly1305 key before being stored on the blockchain.

Encryption plays a critical role in decentralized storage, but not all encryption schemes offer the same balance of security, efficiency, and usability. AES (Advanced Encryption Standard), RSA, or hybrid models are widely used, but they present challenges that ChaCha20-Poly1305 overcomes.

Algorithm	Strengths	Weaknesses
AES-GCM	Highly Efficient with hardware acceleration	Relies on hardware for best performance, vulnerable to timing attacks if implemented improperly
RSA	Strong asymmetric encryption	Computationally expensive, impractical for large file encryption
ECIES (Elliptic Curve Integrated Encryption Scheme)	Compact key sizes, fast for public-key encryption	Not optimized for large-scale file encryption, mostly used for key exchange
ChaCha20-Poly1305	Faster in pure software, resistant to side-channel attacks, efficient in Web3 environments	Not as commonly hardware-accelerated as AES on some chipsets

While AES-GCM is common in Web2 cloud storage due to hardware acceleration, its performance drops significantly on platforms without dedicated AES instructions. ChaCha20-Poly1305, in contrast, operates with pure software efficiency, making it ideal for Web3 environments, including mobile, embedded, and decentralized platforms where hardware acceleration may not be available.

Unlike RSA and ECIES, which are primarily used for key exchanges rather than full file encryption, ChaCha20-Poly1305 enables scalable, high-speed encryption while ensuring message integrity with Poly1305 authentication.

ChaCha20-Poly1305's streaming capabilities enable on-the-fly encryption of files as they are being uploaded or modified, making it possible for Tiri Vault to support real-time file synchronization. This method makes Tiri Vault extremely scalable and practical for personal storage and collaboration.

By implementing ChaCha20-Poly1305 encryption on the client-side, Tiri Vault ensures that:

- User data remains completely private—no third party, including Tiri Vault, has access to files or metadata.
- Encryption performance is optimized for Web3, avoiding the reliance on hardware-accelerated AES.
- Metadata privacy is preserved.
- Streaming encryption allows real-time file synchronization, a key feature provided by Tiri Vault.

Tiri Vault's zero-knowledge encryption approach is designed for scalability, privacy, and efficiency, making it a next-generation solution for truly private decentralized storage.

Tiri Relay

Currently, no pure Web3 storage networks provide instant file synchronization similar to Web2 workspace services. Decentralized storage solutions prioritize security, redundancy, and immutability but lack the real-time access needed for collaborative workspaces. The primary challenges include delayed file retrieval, lack of in-place file modifications, and the need for frequent blockchain transactions to reflect updates.

Tiri Relay is a solution to integrate a hybrid architecture that combines decentralized blockchain-based storage with off-chain real-time synchronization mechanisms.

How Tiri Relay helps real-time file access in decentralized networks?

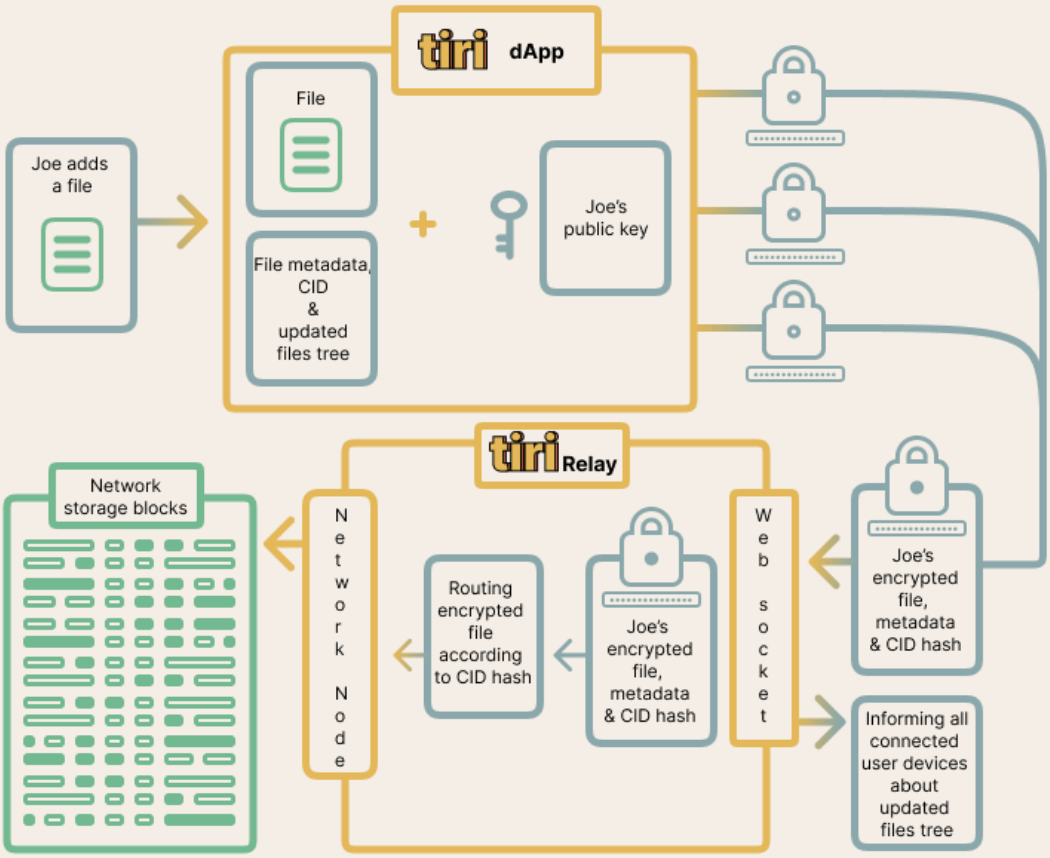
Zero-Knowledge Change Tracking: Tiri Relay maintains a user’s hierarchical file/folder tree structure, ensuring efficient navigation and organization of stored data. This tree structure is fully encrypted on the front-end side with a user’s public key, meaning that even Tiri Relay can not see filenames, paths, file structures, or contents. Changes to files or folders

modify the Merkle tree hash, which serves as a cryptographic fingerprint of the entire file system. Zero-knowledge proofs allow user devices to verify that a change has occurred (e.g., a file was updated, renamed, or moved) without revealing the actual modifications and enable synchronization while maintaining full privacy.

WebSockets for Instant Synchronization: Tiri Vault employs an off-chain caching layer on a local user device that allows instant updates to files and uses Tiri Relay to commit the latest file versions to the decentralized storage network. Tiri Relay utilizes WebSockets to ensure real-time synchronization across multiple devices. Users see changes reflected instantly.

Hash Commitments for Integrity Checks: To maintain trust and verify file authenticity without storing every update on-chain, Tiri Vault uses hash commitments. This means that while the files remain mutable in the short term, their integrity is cryptographically verified before finalizing on decentralized storage.

Below is an overview of how a file is processed when added to a Tiri-synced local folder:



1. Detecting File Changes & Updating the FileTreeModel

When a user adds a new file to their Tiri-synced local folder, the Tiri Vault LocalFilesWatcher detects the change and updates the FileTreeModel, a structured representation of the user's files and folders.

2. Requesting the Last Saved FileTreeModel Hash from Tiri Relay

The Tiri App queries the Tiri Relay for the latest saved FileTreeModel hash to check for any changes. If this is the first synchronization, there is no stored FileTreeModel, so the newly generated model is set as the actual one. If a hash exists, the Tiri App compares the retrieved hash with the hash of the new FileTreeModel.

3. Resolving Differences Between Local and Stored File Trees

If the hashes don’t match, this means changes have occurred. The Tiri App then downloads the last stored FileTreeModel from Tiri Relay, decrypts it using the user’s private key, compares it to the new FileTreeModel and identifies four key differences (diffs):

Upload → Files that need to be uploaded to storage.

Remove → Files that need to be deleted from storage.

Download → Files that need to be downloaded to the local device.

LocalRemove → Files that need to be deleted from the local device.

Then it merges the changes and writes a new, updated FileTreeModel.

4. Processing File Synchronization

To ensure consistency and avoid conflicts, the Tiri App applies changes in a strict sequence: Remove → Upload → LocalRemove → Download.

5. Updating FileTreeModel on Tiri Relay

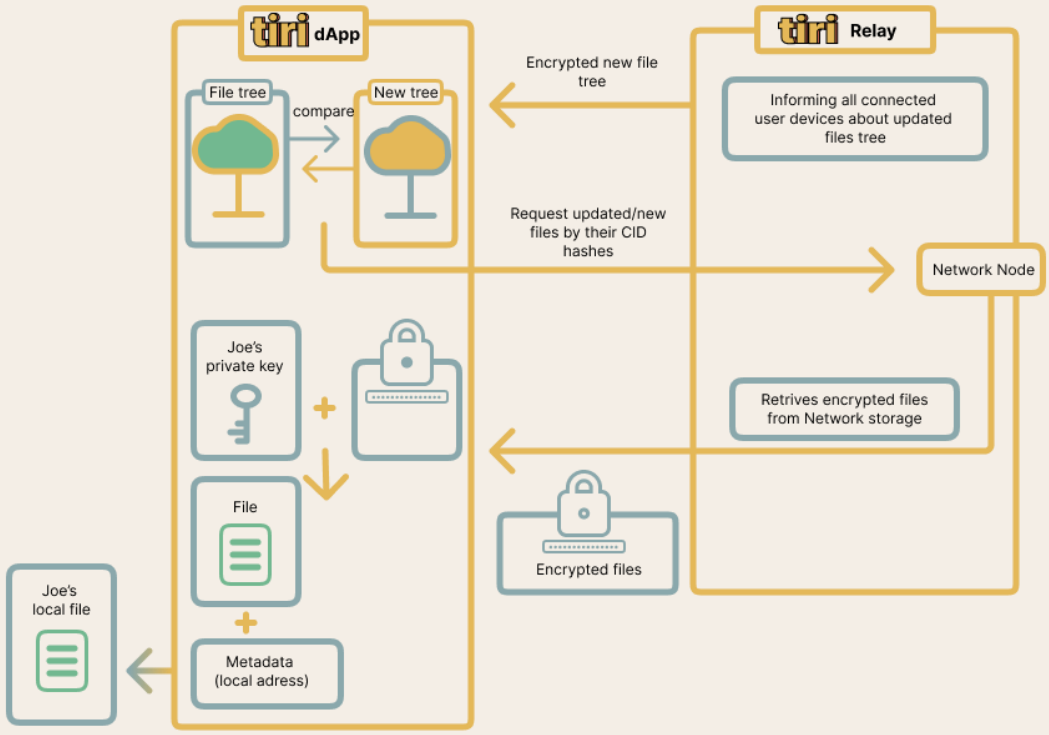
Once all file operations are successfully completed, the merged FileTreeModel is encrypted with the user’s public keyand uploaded to the Tiri Relay, replacing the previous version.

6. Notifying All Devices for Synchronization

Tiri Relay operates a WebSocket server that actively notifies all connected user devices whenever a new FileTreeModel hash is saved. When a device receives this notification, it requests the updated FileTreeModel, decrypts it, and applies the necessary changes. This ensures

that all user devices remain in sync, providing a seamless and decentralized file collaboration experience.

When a file update occurs on another device, Tiri Relay ensures that all connected devices receive and apply changes efficiently while maintaining end-to-end encryption and zero-knowledge privacy. Below is a files update workflow:



1. Requesting the New FileTreeModel

The user's device receives an update notification from Tiri Relay's WebSocket server and requests the latest FileTreeModel from Tiri Relay.

2. Resolving Differences

The Tiri App decrypts the new FileTreeModel using the user's private key and compares the decrypted FileTreeModel with the previously saved local version. The Tiri App identifies and processes four key differences in the same strict sequence: Remove (files that need to be deleted from storage) → Upload (files that need to be uploaded to storage) → LocalRemove (files that need to be deleted from the local device) → Download (files that need to be downloaded to the local device).

3. Downloading Updated Files

New files required for synchronization are downloaded using their CID hashes through Tiri Relay. The files are then decrypted on the device using the user's private key. Once decrypted, the files are saved locally according to their decrypted CIDs, preserving their original file structure.

4. Saving the Updated FileTreeModel as the Actual Version

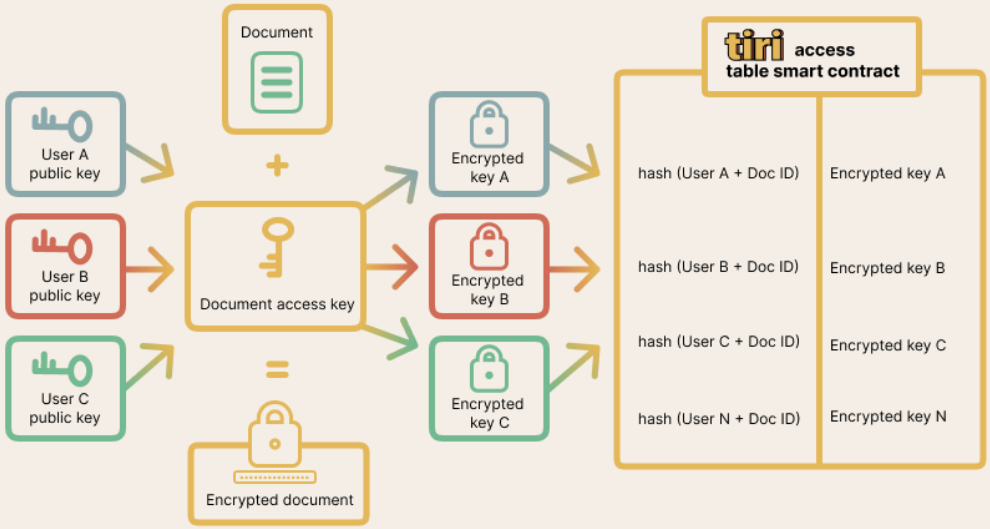
If all updates are processed successfully, the new FileTreeModel is saved locally as the current actual version.

This seamless synchronization workflow provided by Tiri Relay ensures that Tiri Vault users can work across multiple devices without data loss, conflicts, or security compromises.

Asymmetric Key Wrapping

Tiri Vault implements a decentralized, smart contract-based access control system to securely manage encrypted file sharing. Instead of re-encrypting entire files when access permissions change — an approach that would be computationally expensive and inefficient — Tiri Vault employs an asymmetric key-wrapping mechanism, where only the document access key is re-encrypted and stored on-chain.

This approach ensures that encrypted files stored in a decentralized storage network remain unchanged, while access to them is dynamically managed through the blockchain.



For documents to be shared with other users a special file type/group “collaboration suite” is set. Each file marked as a member of the Tiri Collaboration Suite is encrypted using the same ChaCha20-Poly1305 algorithm, but with a unique symmetric encryption key. Instead of encrypting files for multiple recipients, the system encrypts only the file’s encryption key for each user who is granted access.

When a user is granted access, their public key is used to encrypt the document’s access key, and this encrypted key is put to the Tiri Access List (TAL) smart contract. When a user retrieves the file, they first decrypt the access key using their private key, and then use it to decrypt the file itself.

This approach allows files to remain static on decentralized storage, while permissions are managed dynamically on-chain, preventing redundant storage and excessive gas fees.

To revoke access to a file, the file owner removes the recipient’s encrypted access key from the TAL smart contract. Since the access key is no longer retrievable, the user loses access to the document—even though the file itself remains unchanged in storage. This method ensures that revoked users cannot decrypt files, even if they previously had access.

Trustless Framework

Tiri Vault extends beyond secure decentralized file storage, providing a suite of privacy-first, smart contract-based services that eliminate centralized control over sensitive data. By leveraging smart contracts, these services operate in a trustless, censorship-resistant manner, ensuring that users maintain full control over their information without reliance on intermediaries. Tiri Vault implements a zero-knowledge approach, encrypting data on the client side before committing it to the blockchain.

Tiri Vault’s trustless framework includes:

- Passwords and text data management (Rubeus);
- End-to-end encrypted peer-to-peer messaging (Diffy Chat);

Each of these services operates independently through dedicated smart contracts, ensuring self-sovereign control over personal data while eliminating the risks of traditional centralized services.

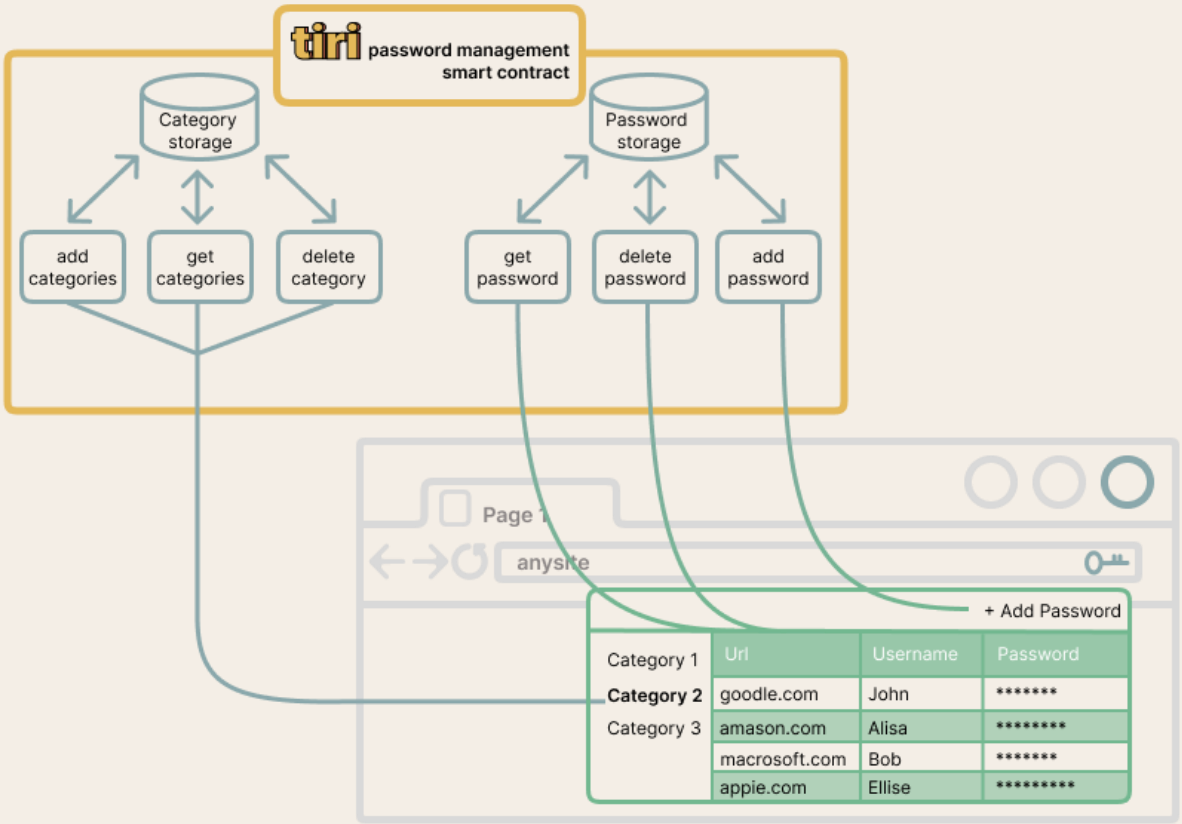
Passwords & Text Storage (Rubeus)

Beyond synced file storage, Tiri Vault provides a privacy-first vault for sensitive text-based information, including:

- *Passwords*
- *Credit card details*
- *Secret and seed phrases*
- *Personal notes*

Unlike conventional password managers, which store encrypted credentials on central servers, Tiri Vault ensures that all stored data is encrypted client-side before being committed to the blockchain. This guarantees zero-knowledge privacy, meaning that no entity, including Tiri Vault, has access to stored passwords or notes.

At the core of this system lies the Rubeus smart contract, which allows users to store and retrieve encrypted credentials using wallet authentication instead of master passwords. This approach eliminates risks of centralized server breaches, phishing attacks, and password leaks and provides a simple but flexible pricing model, where users can choose between paying for “put-to-contract” actions, monthly fees or quantity subscriptions.

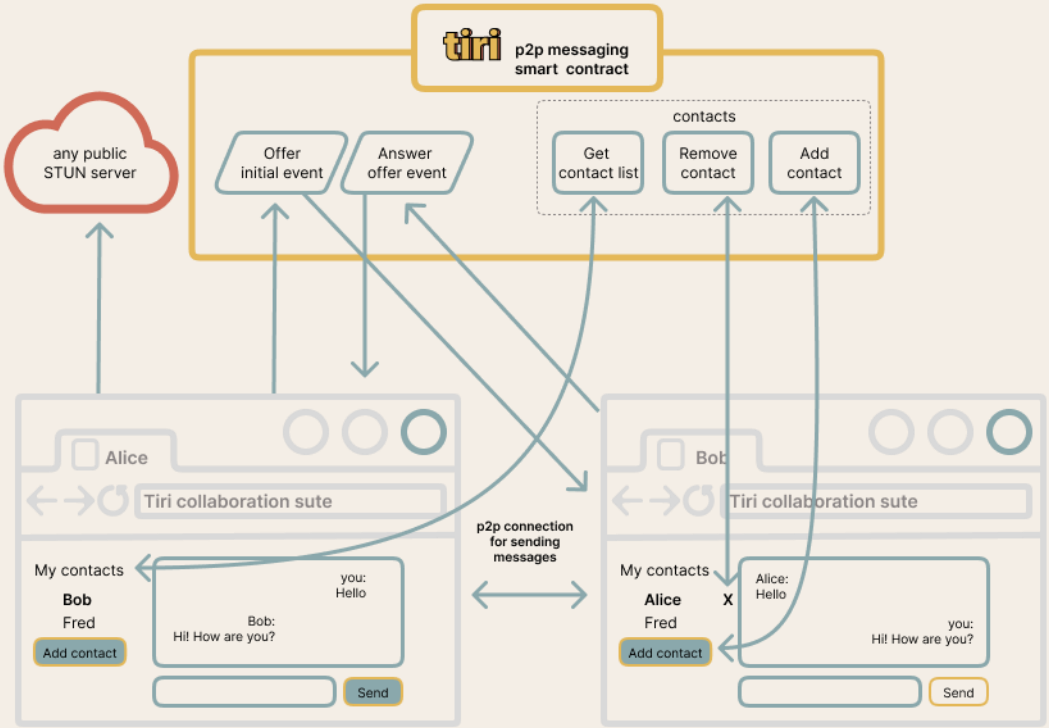


The data sent to the smart contract is encrypted using the ChaCha20-Poly1305 streaming algorithm with message authentication. This secures

transferred data from unauthorized interception and decryption as well as malicious data substitution by a node or any intermediary. The Rubeus Smart contract enables saved passwords, credit cards or other sensitive data to be automatically inserted into appropriate web forms, ensuring secure and seamless authentication with unprecedented convenience and functionality, it allows users to store any form of sensitive text, ensuring a secure, decentralized alternative to a set of traditional applications: password managers, payment wallets, online notebooks and etc.

Decentralized Encrypted Messaging (Diffy Chat)

Collaboration in a decentralized workspace requires more than just file sharing—users also need secure communication channels to exchange sensitive data. To address this, Tiri Collaboration Suite includes Diffy Chat, a decentralized, end-to-end encrypted messaging system designed for secure peer-to-peer communication. It is built upon a smart contract:



- *Wallet-based authentication → Users initiate chats and verify identities using their personal wallet credentials, eliminating reliance on usernames and passwords.*
- *End-to-end encryption → Messages are encrypted with a receiver's public key, ensuring that only the intended recipient can decrypt incoming messages.*
- *WebRTC-based peer-to-peer communication → Messages are exchanged directly between users without passing through centralized servers (except the first hello-message).*

- *Smart contract-based session negotiation → Diffy Chat uses a smart contract to store public keys, handle chat initiation and enable secure contact discovery.*
- *Public STUN servers for NAT traversal → Allowing users behind firewalls or private networks to establish direct communication.*

This approach ensures that all messages remain private, censorship-resistant, and untouchable by intermediaries, making Diffy Chat a secure alternative to mainstream messaging platforms—suitable for individuals, corporations, and industries requiring strict confidentiality (e.g., medical, financial, legal sectors).

The TIRI token

Utility

The launch of the TIRI token is a core element of our strategy to enable decentralized storage and access control across the Tiri Vault ecosystem. Our approach to token issuance is grounded in the careful selection of blockchain networks with strong adoption metrics—specifically, networks with a high number of unique wallets and active daily transactions. This ensures broad accessibility, enhanced visibility, and better integration with existing digital infrastructure.

TIRI tokens will be used as the native payment method for decentralized features within the Tiri Vault, including:

- *Discounted Storage Payments:* Users who pay for storage using TIRI will receive a discount compared to those paying directly in native coins of the underlying storage networks (e.g., SC). These transactions will be facilitated through atomic swaps via the Tiri Relay, enabling smooth and trustless conversions.
- *Smart Contract Features:* TIRI will be the medium for accessing advanced smart contract-driven features such as decentralized access control, p2p messaging or password manager.
- *Staking-Based Feature Access:* Users and organizations will be able to stake TIRI tokens to unlock additional functionality, such as synchronization logs storage, files versioning, 2FA and etc.

All smart contract functionality will be deployed on a network selected for its high adoption and developer ecosystem. While Polygon is currently our leading choice—due to its low fees, strong Ethereum compatibility,

DePIN engagement and large user base — we are also evaluating other popular networks or sidechains, including:

- *Arbitrum:* Offers low-cost transactions with high throughput, backed by Ethereum's security layer.
- *Optimism:* Focused on scalability and supports the broader Ethereum tooling.
- *Solana:* A high-performance Layer 1 blockchain known for extremely fast and low-cost transactions, with a rapidly growing developer and user community.
- *Secret Network (SCRT):* A privacy-focused smart contract platform where contract inputs, outputs, and states can remain encrypted. Particularly suitable for access control, private audit logs, and encrypted sharing logic.

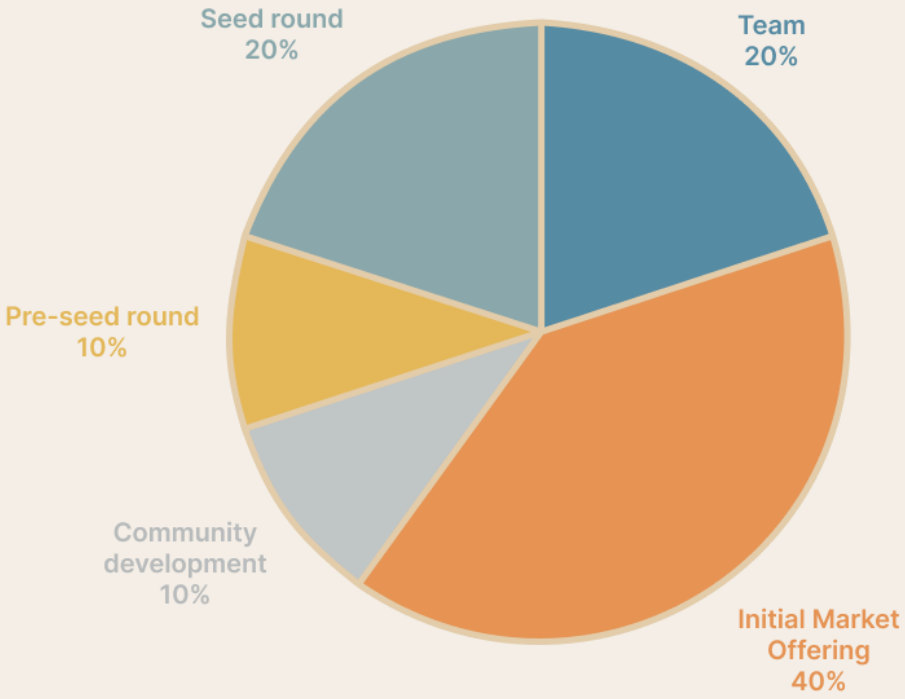
The final decision will balance transaction costs, ecosystem maturity, security, and ease of integration.

By anchoring the token in high-adoption networks and ensuring practical utility through meaningful incentives and smart contracts, we aim to make TIRI a functional and valuable component of the decentralized storage ecosystem.

Tokenomics

The total supply of the TIRI token is fixed at 1,000,000,000 coins, with a minimal unit of 0.001. The token distribution is structured to ensure a balanced and sustainable ecosystem, as outlined below:

Allocation	Percentage	Tokens Allocated
Initial Market Offering	40%	400 000 000 TIRI
Team	20%	200 000 000 TIRI
Presale (Seed Round)	20%	200 000 000 TIRI
Early Investors (Pre-Seed Round)	10%	100 000 000 TIRI
Community Development	10%	100 000 000 TIRI



Pre-ICO and ICO Details

To secure early funding and strategic partnerships, the Tiri Vault project will run a two-phase pre-sale before launching the public ICO. These early contributors will be onboarded through SAFT agreements with defined lock-up periods.

Pre-Seed Round

- Token Allocation: 10% of total supply = 100,000,000 TIRI
- Target Raise: US$300,000
- Token Price: US$0.003 per TIRI
- Lockup: 12-month lock from the date of token issuance
- SAFT Terms: Simple Agreement for Future Tokens (SAFT)

Seed Round

- Token Allocation: 20% of total supply = 200,000,000 TIRI
- Target Raise: US$1,200,000
- Token Price: US$0.006 per TIRI
- Lockup: 12-month lock from the date of token issuance
- SAFT Terms: As above

Initial Coin Offering (ICO)

- Token Allocation: 40% of total supply = 400,000,000 TIRI

- ICO Token Price = Total Pre-ICO Funds Raised / 400,000,000
- Vesting: Public tokens will be fully unlocked on distribution.

Post-ICO Distribution

An additional 10% of the supply (100,000,000 TIRI) will be released over 36 months following the ICO, primarily allocated toward:

- Global marketing campaigns
- Ecosystem incentives
- Strategic partnership grants

This phased release ensures continued network growth and token visibility while avoiding excessive early supply inflation.

Our project token is positioned to be a key player in the decentralized economy, offering a flexible, secure, and widely adopted solution for service payments across multiple blockchain networks. With a robust tokenomics structure, strategic network selection, and a carefully planned ICO, we are committed to driving mass adoption and creating value for all participants in the ecosystem.