DieFi™

Avoid Lost Crypto

Whitepaper

By

fortknoxster™

Table of contents

Introduction 3
What is DieFi? 4
DieFi Features 8
Why Use Blockchain? 9
DieFi Technology 10
Comparison 23
FKX Token Utility 24
Team 25

Introduction

FortKnoxster is a cyber-security company specializing in securing digital assets. FortKnoxster has developed filed patents and trademarks on a unique and innovative platform called DieFi.

DieFi is the first solution in the marketplace, which address a massive problem in the blockchain industry:

What happens to my digital assets if I die, have an accident, or lose my crypto keys?

According to analytics company Chainalysis, more than 200 Billion USD worth of Bitcoin is lost because of death or loss of keys. Including all other digital assets, this number is probably over a Trillion USD.

Administrating and securing digital assets and NFT's is not an easy task. Most users of digital assets have several wallets, both "hot" and "cold" wallets and often more are generated as time passes by. Securing the seed phrases and storing them in a safe place is a big challenge. Moreover, it is extremely important as the loss of these can have dire consequences because the digital assets will be locked and impossible to access.

The DieFi platform has been developed and engineered over several years and features the most secure technologies available to secure all platform content.

What is DieFi?

If you have ever wondered what would happen to your digital assets when you are no longer on this earth, you are not alone.

Who will take over your crypto & NFT portfolio?

Would a family member be able to find that piece of paper with your recovery key that you have hidden somewhere in the house? Will they know which crypto wallet you hold, and if you should have more than one, which recovery key/phrase is for which wallet?

With millions of crypto wallets, more than 100 million bitcoin owners and over 12,000 cryptocurrencies in circulation, anyone with a decent crypto / NFT portfolio should be thinking the same when digital estate planning– how can I safely pass my crypto assets to my loved ones.

The FortKnoxster DieFi platform is the solution. DieFi is an automated beneficiary platform for all digital asset owners.

DieFi allows you to set up a beneficiary testament, which will automatically be activated, when you fail to sign in to your FortKnoxster account for a period of 12 months or a period decided by yourself. A 'Dead man's switch' triggers this automation.

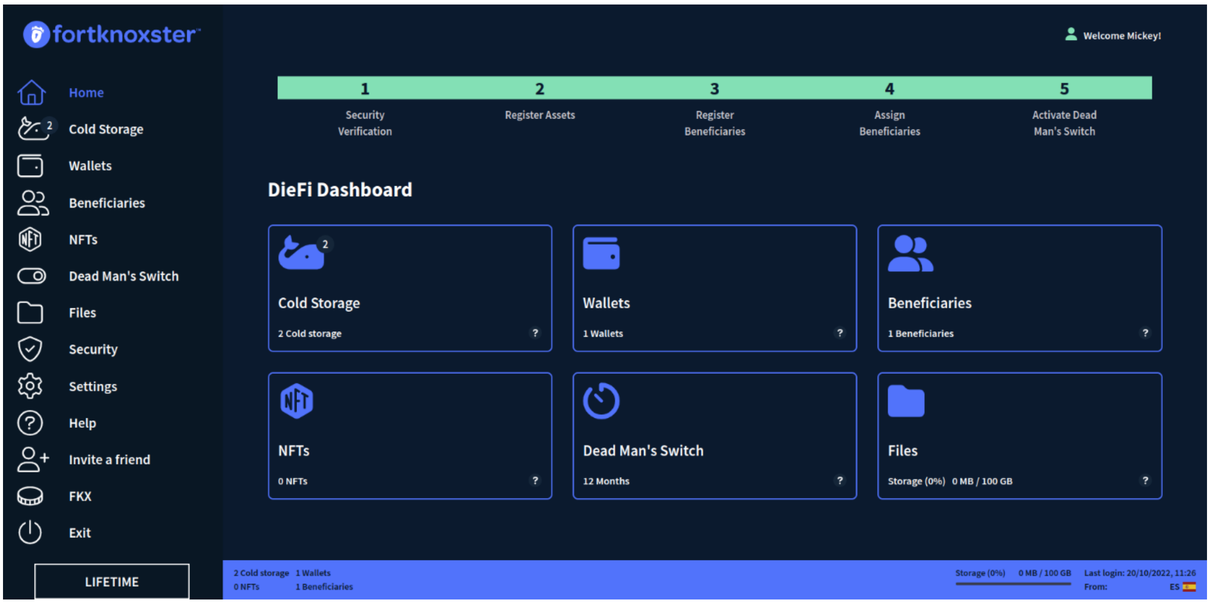
To register a beneficiary in the FortKnoxster DieFi platform, you must input your beneficiary's First name, Last name, date of birth, nationality, and email address. This information will be used to verify the beneficiary's identity with our ID verification partner.

An automated email notification is sent to your beneficiary when the dead man's switch timer is triggered and beneficiary can initiate the recovery process, which involves thorough ID verification steps.

The dead man's switch is reset and extended to 12 months every time a wallet owner login to their account. If the wallet owner has FortKnoxster Pro, Platinum or Lifetime, they can customize this timer.

All document and wallet registrations are encrypted and only accessible to the intended recipients. Once your beneficiary gets access to your account, they are able to read all information you have prepared and shared with them specifically. You can even upload videos and more.

DieFi Dashboard



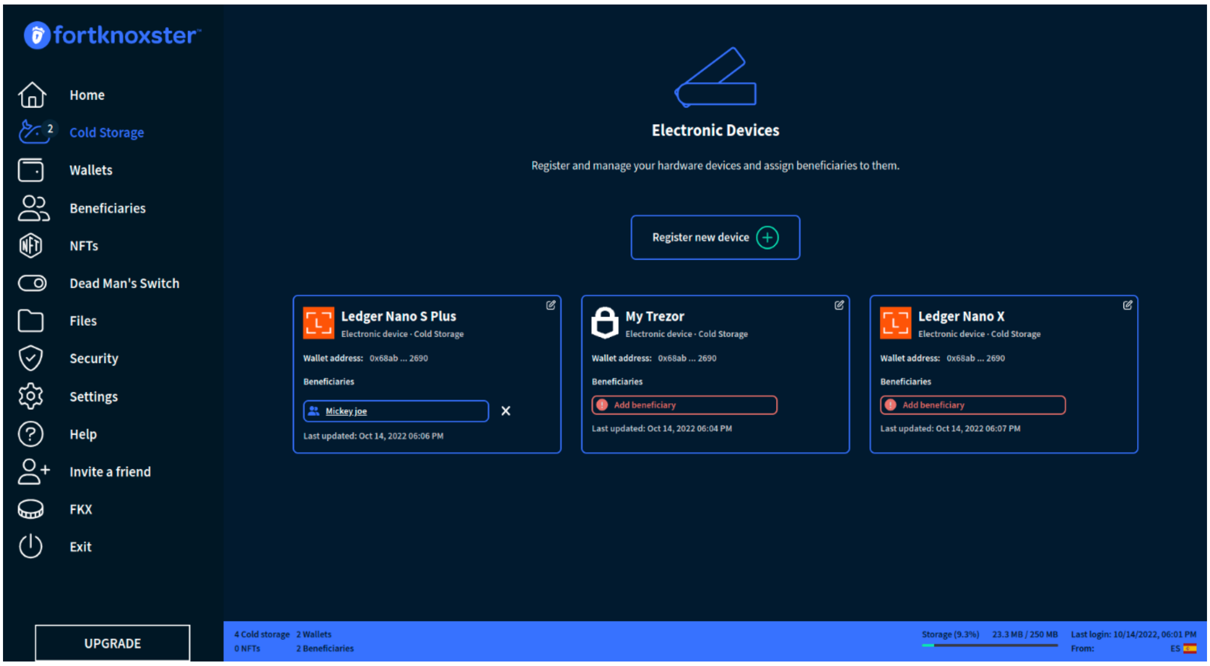
1 Security Verification
2 Register Assets
3 Register Beneficiaries
4 Assign Beneficiaries
5 Activate Dead Man's Switch

DieFi Dashboard

Cold Storage – 2 Cold storage
Wallets – 1 Wallets
Beneficiaries – 1 Beneficiaries
NFTs – 0 NFTs
Dead Man's Switch – 12 Months
Files – Storage (0%) 0 MB / 100 GB

2 Cold storage 1 Wallets
0 NFTs 1 Beneficiaries
Storage (0%) 0 MB / 100 GB
Last login: 20/10/2022, 11:26
From: ES

DieFi Cold Storage – Electronic Devices



Electronic Devices

Register and manage your hardware devices and assign beneficiaries to them.

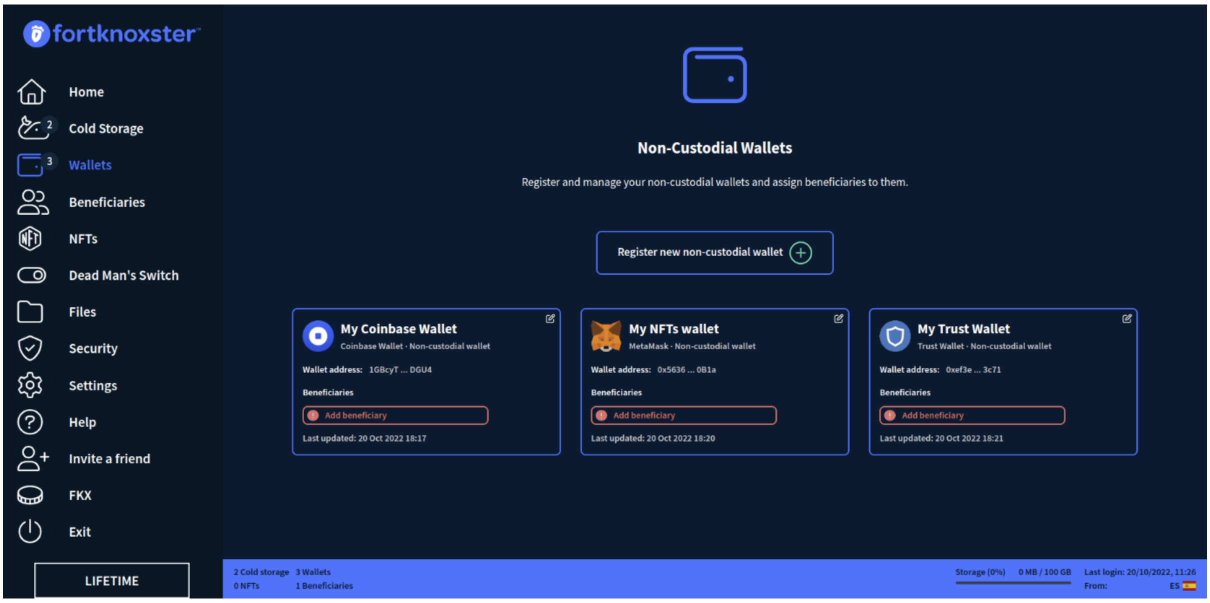
Ledger Nano S Plus
Electronic device · Cold Storage
Wallet address: 0x68ab ... 2690
Beneficiaries
Mickey joe
Last updated: Oct 14, 2022 06:06 PM

My Trezor
Electronic device · Cold Storage
Wallet address: 0x68ab ... 2690
Beneficiaries
Add beneficiary
Last updated: Oct 14, 2022 06:04 PM

Ledger Nano X
Electronic device · Cold Storage
Wallet address: 0x68ab ... 2690
Beneficiaries
Add beneficiary
Last updated: Oct 14, 2022 06:07 PM

4 Cold storage 2 Wallets
0 NFTs 2 Beneficiaries
Storage (9.3%) 23.3 MB / 250 MB
Last login: 10/14/2022, 06:01 PM
From: ES

DieFi Wallets – Non-custodial wallet



Non-Custodial Wallets

Register and manage your non-custodial wallets and assign beneficiaries to them.

Register new non-custodial wallet ⊕

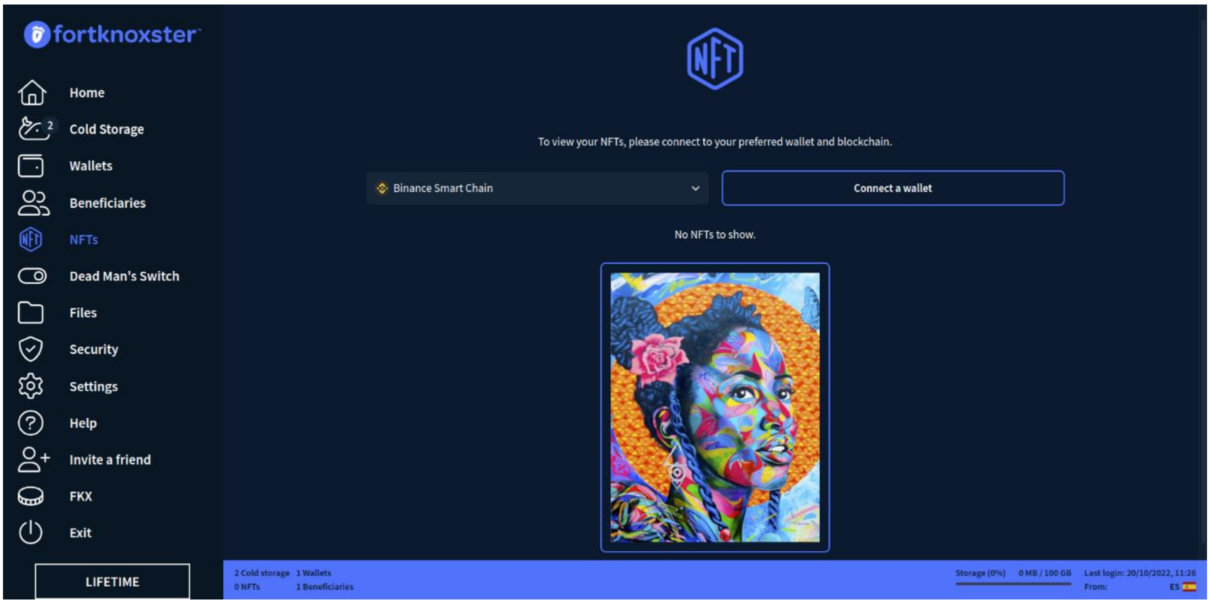
My Coinbase Wallet
Coinbase Wallet · Non-custodial wallet
Wallet address: 1GBcyT ... DGU4
Beneficiaries
Add beneficiary
Last updated: 20 Oct 2022 18:17

My NFTs wallet
MetaMask · Non-custodial wallet
Wallet address: 0x5636 ... 0B1a
Beneficiaries
Add beneficiary
Last updated: 20 Oct 2022 18:20

My Trust Wallet
Trust Wallet · Non-custodial wallet
Wallet address: 0xef3e ... 3c71
Beneficiaries
Add beneficiary
Last updated: 20 Oct 2022 18:21

2 Cold storage 3 Wallets
0 NFTs 1 Beneficiaries
Storage (0%) 0 MB / 100 GB
Last login: 20/10/2022, 11:26
From: ES

DieFi NFTs



To view your NFTs, please connect to your preferred wallet and blockchain.

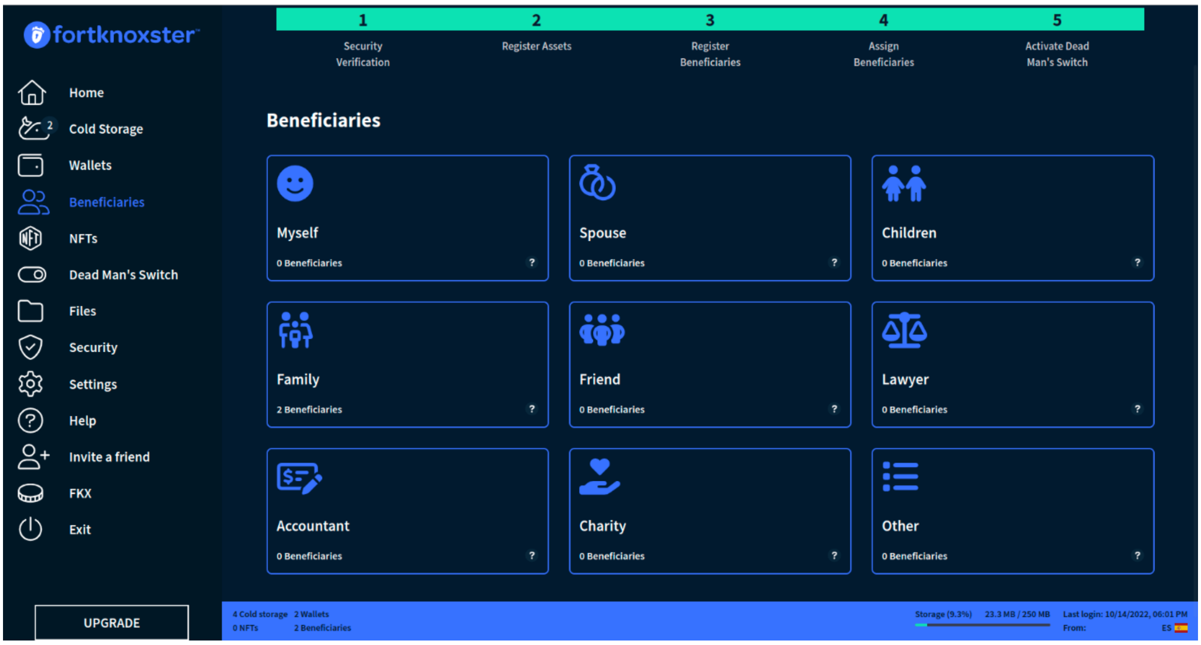
Binance Smart Chain

Connect a wallet

No NFTs to show.

2 Cold storage 1 Wallets
0 NFTs 1 Beneficiaries
Storage (0%) 0 MB / 100 GB
Last login: 20/10/2022, 11:26
From: ES

DieFi Beneficiaries



1 Security Verification

2 Register Assets

3 Register Beneficiaries

4 Assign Beneficiaries

5 Activate Dead Man's Switch

Beneficiaries

Myself
0 Beneficiaries ?

Spouse
0 Beneficiaries ?

Children
0 Beneficiaries ?

Family
2 Beneficiaries ?

Friend
0 Beneficiaries ?

Lawyer
0 Beneficiaries ?

Accountant
0 Beneficiaries ?

Charity
0 Beneficiaries ?

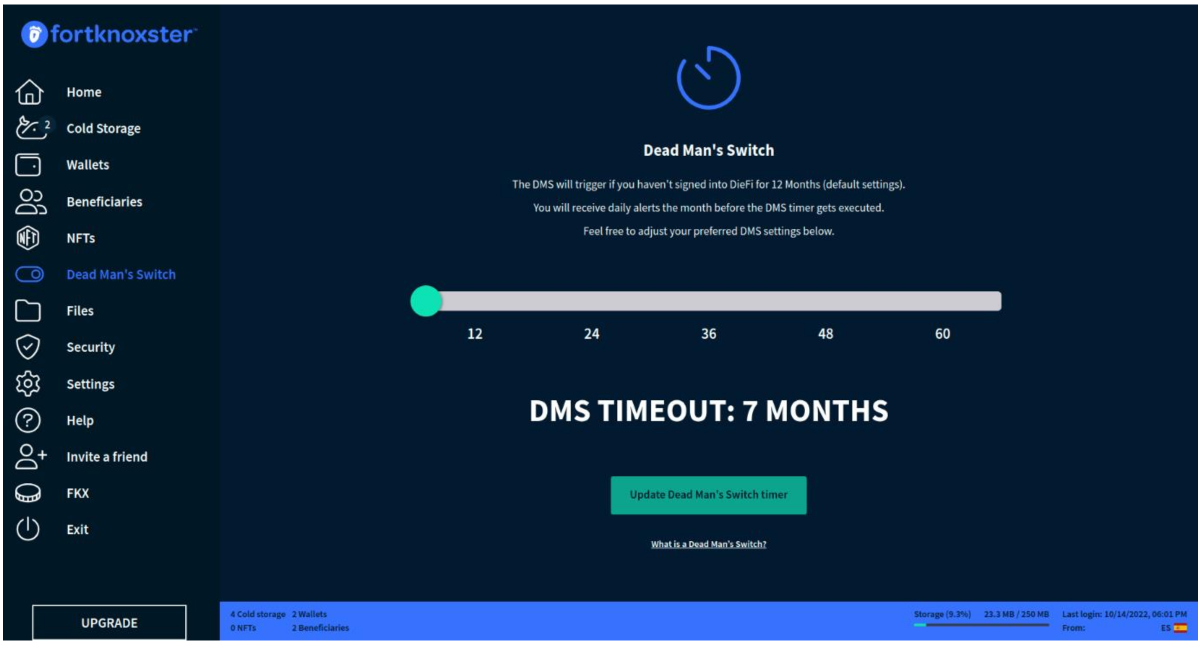
Other
0 Beneficiaries ?

4 Cold storage 2 Wallets
0 NFTs 2 Beneficiaries

Storage (9.3%) 23.3 MB / 250 MB

Last login: 10/14/2022, 06:01 PM
From: ES

DieFi Dead Man's Switch Timer



Dead Man's Switch

The DMS will trigger if you haven't signed into DieFi for 12 Months (default settings).
You will receive daily alerts the month before the DMS timer gets executed.
Feel free to adjust your preferred DMS settings below.

DMS TIMEOUT: 7 MONTHS

4 Cold storage 2 Wallets
0 NFTs 2 Beneficiaries

Storage (9.3%) 23.3 MB / 250 MB

Last login: 10/14/2022, 06:01 PM
From: ES

DieFi Features

DieFi™ safeguards Web3 and beyond. Store your digital assets, NFTs, ledgers, files, and other crypto information in one ultra-secure app.

Below are the main features of DieFi:

- **Store Any Crypto Information**

  Store all your crypto credentials in one safe place. Cold storage devices, ledgers, custodial, non-custodial wallets and trading account details. All is E2E-encrypted.

- **Manage NFTs**

  Manage, organize, and display your NFT portfolios across multiple blockchains. Enjoy the view of your collection at any time.

- **Crypto Beneficiaries & Testament**

  We make sure your family, friends, lawyer, or anybody you wish, can access your digital assets, when you are not able to anymore.

- **Dead Man's Switch Timer**

  Only you control when your beneficiaries are contacted. Default is 12 months after your last log-in. You can edit the timer as you wish.

- **Beneficiary ID Verification**

  Your beneficiaries will undergo strict real-time ID & face recognition scans incl. 100s of security checks. We use AI & machine learning to eliminate fraud.

- **File Storage**

  Store all your confidential crypto notes, documents and much more. Store separate folders to be accessed in the future by beneficiaries. All folders are segregated.

Why Use Blockchain?

A blockchain is a decentralized and open distributed ledger recording financial transactions (or virtually anything of value) between two parties on a peer-to-peer network. This continuously growing list of records is linked and secured with strong cryptography, making these transactions permanently verifiable and therefore incorruptible.

"Blockchain solves the problem of manipulation."

Quote: Vitalik Buterin, inventor of Ethereum

Since the blockchain is publicly verifiable, it provides security and transparency making it ideal for many types of security applications.

FortKnoxster takes advantage of these features, which the blockchain technology provides, by moving its centralized trust of digital identities to a decentralized one, specifically the Ethereum blockchain, using its smart contracts.

Trust is of vital importance and is the most important element in any crypto infrastructure. The current model of trust for digital identities in FortKnoxster is centralized. This centralized trust model is a common challenge today, as it becomes a single point of failure.

"Centralizing identity creates a single point of failure and builds a repository of high-value data that can attract hackers, and proper controls need to be in place to maintain integrity."

Quote: IBM blockchain IDC report, "It Was Only a Matter of Time."

The distributed trust model, utilizing blockchain, is a new way of managing digital identities. Blockchain technology empowers users to control their own digital identity and share and communicate between trusted individuals with their consent. Therefore, no single entity can compromise a user's digital identity, and there is no single point of failure present.

DieFi Technology

The following is a technical explanation of FortKnoxster's end-to-end encryption and the DieFi architecture. It describes in detail the various cryptography designs and security using the Polygon blockchain with smart contracts and a decentralized network of threshold proxy re-encryption nodes.

At FortKnoxster, security and decentralization have the highest priority. Therefore, we have built the FortKnoxster encryption and technologies architectures by custom design.

FortKnoxster uses the strongest encryption algorithms and techniques available, combined with Blockchain and IA technologies. Our FIPS 140-2 compliant end-to-end encryption design ensures that only you have access to your data and no one else — not even FortKnoxster can access any data.

FortKnoxster's cryptography consists of AES-GCM 256-bit symmetric encryption, RSA-OAEP/RSA-PSS 4096-bit encryption with SHA-512 and Elliptic Curve ECDH/ECDSA P-521 encryption.

FortKnoxster Dead Man's Switch feature consists of strong end-to-end-encryption combined with a decentralized KMS approach using proxy re-encryption for secret key sharing with timed-based policy encryption through blockchain smart contracts.

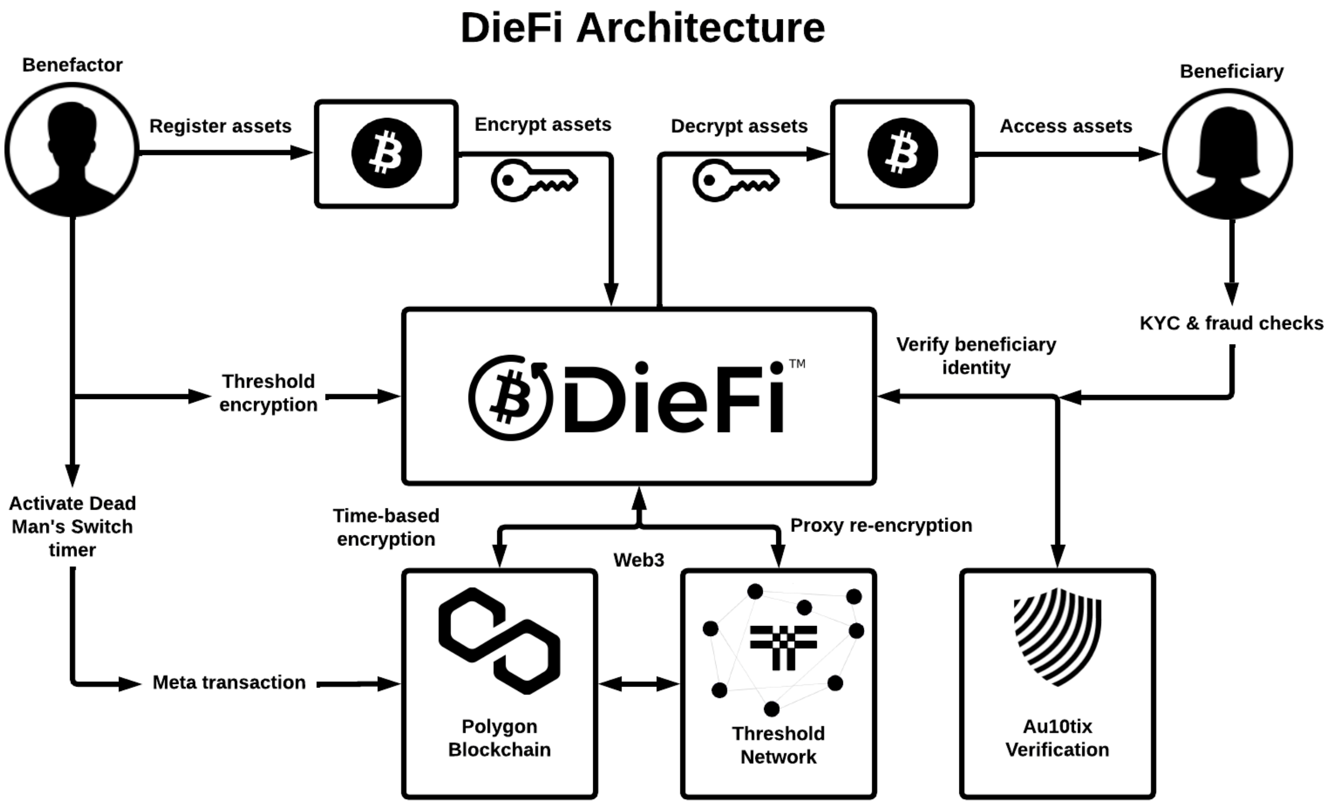


Figure 1

The diagram above describes in detail how the DieFi technology is designed.

Benefactor Encryption Keys

When a benefactor registers on FortKnoxster.com - 2 sets of RSA key-pairs are generated, 3 sets of elliptic curves (EC) key-pairs and 5 Key Protector(s) (one per private key) in the client's browser.

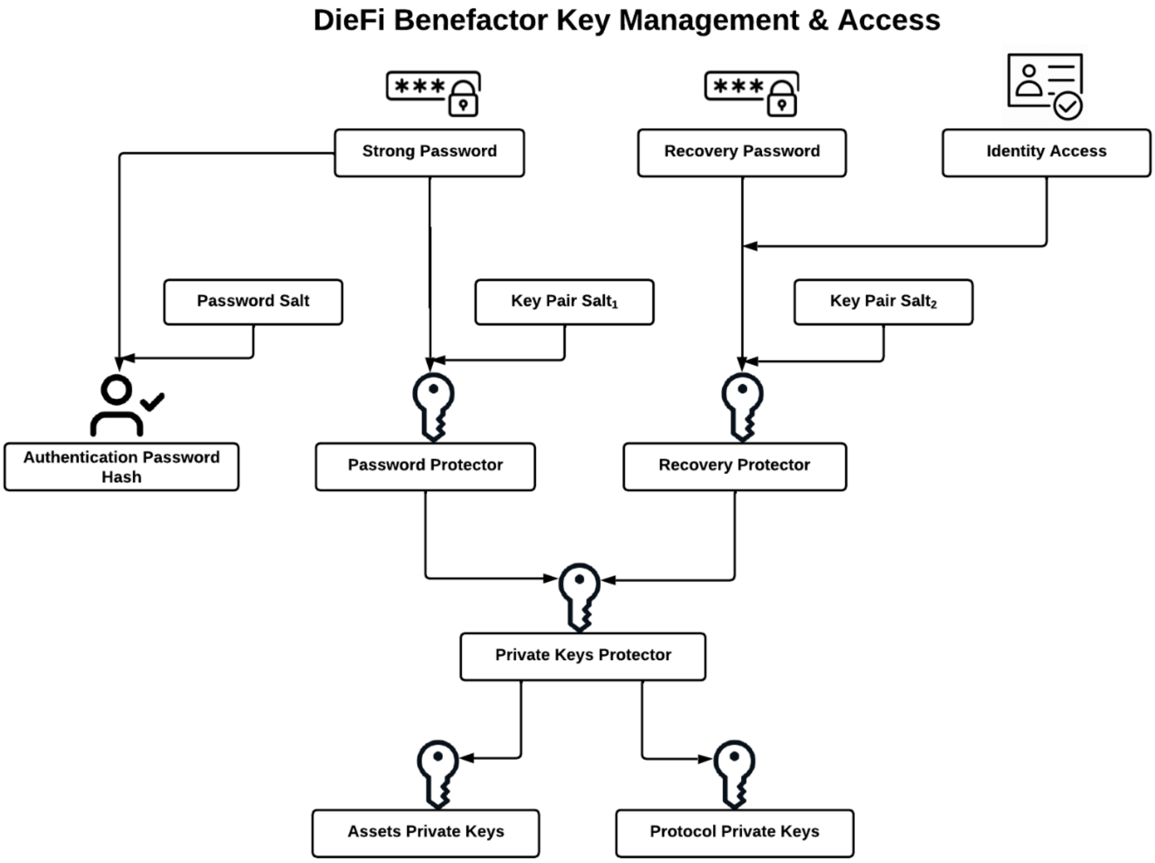


Fig. 2

Fig. 2 above is a schematic representation of DieFi's cryptography design for benefactor key management and recovery access. The various encryption keys and their function are described below:

- **Strong Password** – is created by the user during signup following a strong password policy. The password must be minimum 12 characters long and must contain uppercase characters, lowercase characters, numbers, and special characters.

- **Authentication Password Hash** – NIST PBKDF2_SHA512 300,000 rounds derived hash from the users' password with a static salt, to authenticate a user without transmitting the users' password.

- **Recovery Password** – 32-byte random generated password by the users' browser/device when activating account recovery.

- **Identity Access** – is an additional account recovery feature in case of emergency. A user can register themselves as a beneficiary providing their identity details which are end-to-end encrypted and anonymous.

- **Key Pair Salt** - 32-byte random salt generated per key pair upon user signup.

- **Password Encryption Hash** – NIST PBKDF2_SHA256 100,000 rounds computed hash from the Strong Password and Key Pair Salt derives the Password Protector to encrypt assets and protocol key pairs

- **Recovery Encryption Hash** – NIST PBKDF2_SHA256 100,000 rounds computed hash from the Recovery Password and Key Pair Salt derives the Recovery Protector to encrypt assets and protocol key pairs.

- **Password Protector** – NIST AES_KW_256 key is derived from the Password Encryption Hash to wrap the Private Key Protector.

- **Recovery Protector** – NIST AES_KW_256 key is derived from the Recovery Encryption Hash to wrap the Private Key Protector.

- **Private Key Protector** – 256-bit random NIST AES_GCM_256 is generated for each Key Pair to wrap the Key Pairs private key

- **Asset Key Pairs** – NIST RSA_OAEP_4096_SHA512 and RSA_PSS_4096_SHA512 key pairs are generated in the user's browser/device and stored in encrypted form with the Private Key Protector.

- **Protocol Key Pairs** – NIST ECDH_P521 and ECDSA_P521 key pairs are generated in the user's browser/device and stored in encrypted form using Key Pair Encryption Hash.

Important: All private key material generated by the benefactor and any encryption/decryption operations involved are solely performed in the user's browser/device. The benefactor's personal password is only known to the benefactor and never transmitted. FortKnoxster has **zero-knowledge** of the benefactor's password, private keys and any crypto wallets/assets, files and any information end-to-end encrypted to the benefactor's private keys.

Crypto Wallets & Asset Registration

When a benefactor registers new crypto wallets and assets in the DieFi app, all asset details are end-to-end encrypted in a key container similar to the benefactor's private keys, as described before. The key container is encrypted with AES-GCM 256-bit, and its protector key is wrapped using RSA-OAEP 4096-bit encryption. The encrypted key container is finally signed with the RSA-PSS 4096 private key.

Beneficiaries Registration & Asset Assignment

For each new beneficiary registered by the benefactor, a unique encryption key is generated and kept safe in the end-to-end encrypted beneficiary details, which are encrypted the same way with wallet registrations described before. When wallets are assigned to a beneficiary, the unique beneficiary key is used to add an additional key protector to the assigned crypto assets' key container. Finally, the beneficiary key is the encryption key as described in Fig. 1.

Beneficiary Verification Process

DieFi activates the Dead Man's Switch timer (DMS) on the Polygon blockchain through a smart contract and encrypts a symmetric key through NuCypher proxy re-encryption, "The inheritance key."

When the DMS triggers, the beneficiaries are contacted via email with a secure link that initiates an ID verification (face scan and photo ID scan); the result of the ID and persona face-scan verification undergoes numerous checks for various fraud attempts through our verification partner Au10tix. Au10tix handles ID and face-scans in most airports worldwide and its customers represents among others; Binance, Coinbase, eToro, Kraken and PayPal.

After a successful verification/KYC, the node gets the result and computes an identity hash based on several values like full name, gender, date of birth and nationality, etc. and a security question.

In the enclaved node, the inheritance key is retrieved via NuCypher proxy re-encryption and the identity hash unlocks the beneficiary key to access the wallets/folder that was assigned/encrypted to this beneficiary key. The identity hash is the AAD to the AES-GCM algorithm, and therefore can't unwrap the beneficiary key if the identity is not correct.

If the identity is correct, the beneficiary key is unwrapped and re-wrapped to the beneficiary's newly created account public key, and the beneficiary now has access to all the shared information in DieFi.

If the beneficiary is not himself or herself, the beneficiaries might know nothing until the day the DMS is triggered in case of emergency or death. The benefactor registered all the beneficiary details beforehand in DieFi in order to re-compute the identity hash again in the future for the beneficiary key wrap/unwrap together with the inheritance key.

The beneficiary details are anonymous and end-to-end encrypted at all times – inaccessible to the node and only accessible to the benefactor. Nobody, including Fortknoxster, can access the DieFi platform, related notes, etc. DieFi is based on the zero-knowledge principles.

For more details, check the opensource E2EE code here: https://github.com/FortKnoxster/fortknoxster-crypto-web/blob/master/src/kryptos/wallets.js

Crypto Inheritance & Recovery Key Management

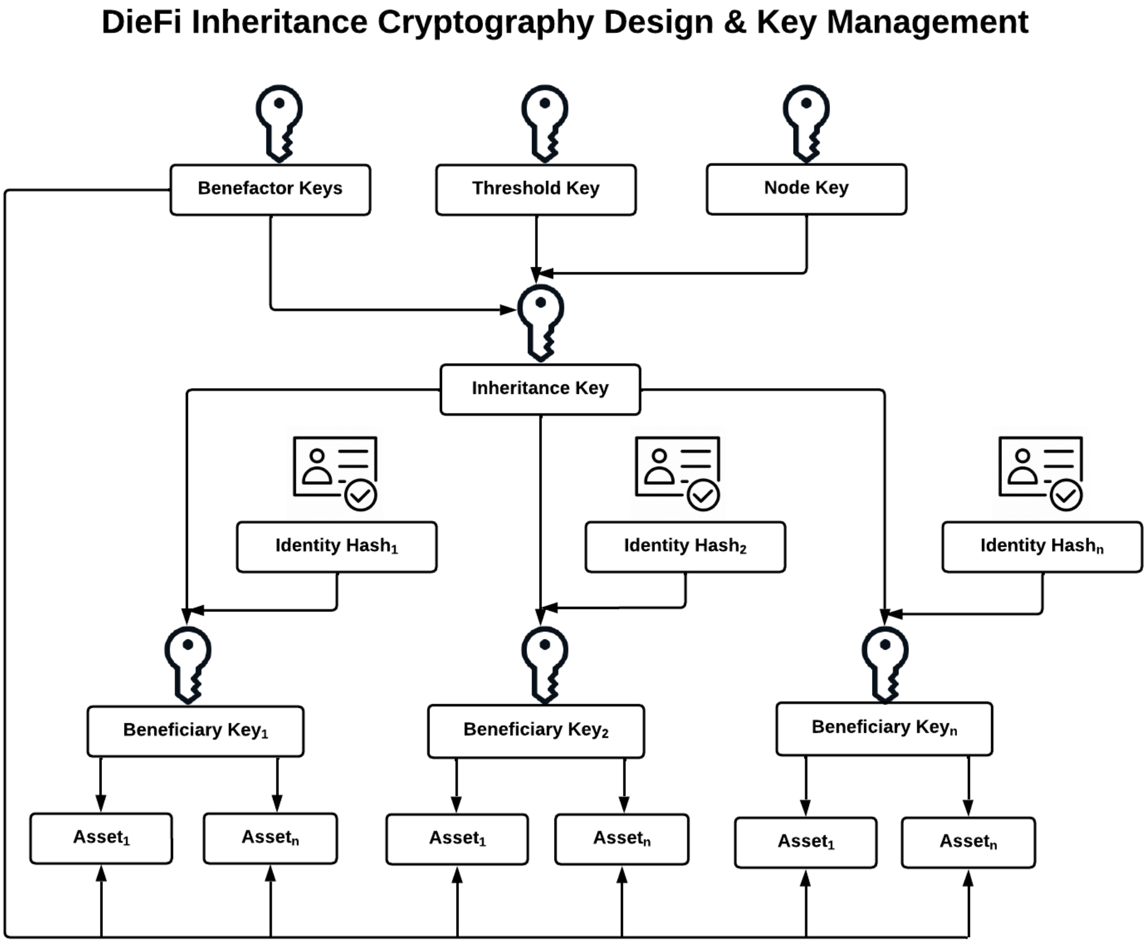


Fig. 3

Fig. 3 is a schematic representation of DieFi's cryptography key management system for crypto assets recovery to multiple beneficiaries or the benefactor itself. The various encryption keys and their function are described below:

- **Benefactor Keys** – are the Asset Key Pairs as Fig. 2. The asset public key is used to wrap the inheritance key and assets with an asymmetric protector and sign the encrypted Inheritance Key and encrypted assets.

- **Threshold Key** – is a symmetric encryption key used to wrap/unwrap the Inheritance Key. The Threshold key is generated by the Benefactor when the Dead Man's Switch timer is activated or renewed. The Threshold Key is then split using threshold encryption with 7 shares and threshold 3 or any other future shares/threshold combination. The 7 shares are distributed and proxy re-encrypted by decentralized threshold nodes. The Threshold Key can only be accessed and re-constructed once the Dead Man's Switch timer has triggered, as the threshold nodes enforce the time-based policy constraints activated by the benefactor in the blockchain smart contract.

- **Node Key** – is a unique access key generated by the benefactor every time the Dead Man's Switch is updated by the benefactor. The Node Key can retrieve the secret threshold shares from the threshold nodes only after the Dead Man's Switch has triggered and can then reconstruct the Inheritance Key.

- **Inheritance Key** – is a symmetric encryption key used to wrap/unwrap the beneficiary keys with the Identity Hash as AEAD input to the AES_GCM_256 encryption/decryption operation.

- **Identity Hash** – is computed from the anonymous beneficiary details and security questions when the benefactor registered a beneficiary. As described below. The Identity Hash is recomputed at the recovery event once a beneficiary has completed an identity verification, and acts as AEAD input to the AES_GCM_256 encryption/decryption operation. If the recomputed Identity Hash differs from the original computed Identity Hash, upon decryption, the decryption of the beneficiary key will fail even though the identity encryption/decryption key is correct. A successful decryption is therefore the cryptography proof of the beneficiary identity and access to the encrypted assets.

- **Beneficiary Key** – is a symmetric encryption key. For each registered beneficiary including oneself a unique beneficiary key is generated. The beneficiary key is encrypted with the other anonymous beneficiary details. When a benefactor assigns an asset to a beneficiary, the benefactor unlocks the encrypted assets asymmetric protector and encrypts the asset protector key with the beneficiary key, effectively adding a new access key to the asset.

- **Asset** – refers to the encrypted assets accessible only to the corresponding beneficiary encryption key and benefactor encryption key.

Web Crypto API

The web browsers implement the latest browser capabilities and use the Web Cryptography API (Web Crypto API), which is a web standard defined at the World Wide Web Consortium (W3C). The Web Crypto API allows for cryptographic operations in JavaScript web client applications.

"The Web Cryptography API defines a low-level interface to interacting with cryptographic key material that is managed or exposed by user agents. The API itself is agnostic of the underlying implementation of key storage but provides a common set of interfaces that allow rich web applications to perform operations such as signature generation and verification, hashing and verification, encryption and decryption, without requiring access to the raw keying material."

Source: (W3C) Web Cryptography API http://www.w3.org/TR/WebCryptoAPI

Using Web Crypto API makes the crypto design and its implementation highly stable and efficient when performing various crypto operations, as it leverages on the browser's own crypto stack implementation and which makes robust cryptographic algorithms available, compared to other pure JavaScript crypto implementations.

Web Crypto API is an interface made available for application developers to access various crypto operations enabling web application developments, with use cases such as encrypted messaging, encrypted cloud storage, document signing & sharing, data integrity protection among other use cases.

FortKnoxster uses the Web Crypto API in its advanced client end-to-end encryption design in combination with a strictly configured TLS and HTTPS.

Our code is served over HTTPS only from the https://diefi.fortknoxster.com origin and we DO NOT serve any external resources or cross-domain scripts unless they are specifically whitelisted.

Encryption Algorithms

Below is an overview of the encryption algorithms and crypto operations used in the DieFi end-to-end encryption design.

Algorithm	Encrypt	Decrypt	Sign	Verify	Derive	Digest	Wrap	Unwrap
RSA-PSS 4096			✓	✓				
RSA-OAEP 4096	✓	✓						
ECDSA P-521			✓	✓				
ECDH P-521					✓			
AES-GCM 256	✓	✓					✓	✓
AES-KW 256							✓	✓
HMAC			✓	✓				
PBKDF2					✓			
HKDF					✓			
BCRYPT					✓			
SHA-512						✓		
SHA-256						✓		

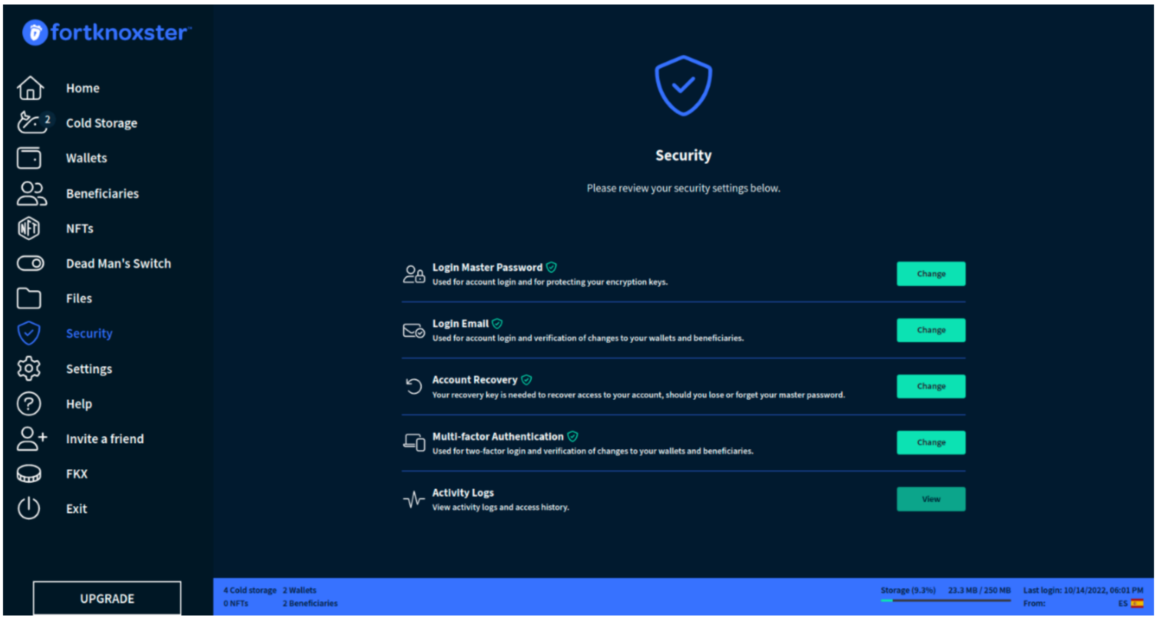
Peer-to-Peer Encryption Protocol

FortKnoxster has developed a unique peer-to-peer encryption message protocol between users' client devices and FortKnoxster's crypto nodes to protect against MITM attacks and prevent unauthorized account access beside the TLS layer.

All critical user actions such as registering, fetching, updating, and deleting wallets and beneficiaries and account settings (like account recovery, password change and two-factor authentication) are both encrypted and cryptographically signed bidirectionally between the user device and the crypto nodes. This node encryption protocol uses Elliptic Curve Diffie-Hellman (ECDH) for key generation and key agreement and Elliptic Curve Digital Signature Algorithm (ECDSA) for digital signing and verification of encrypted protocol messages.

Account Security

Several account security features and measures are built into the DieFi app.



Security

Please review your security settings below.

Login Master Password
Used for account login and for protecting your encryption keys.
Change

Login Email
Used for account login and verification of changes to your wallets and beneficiaries.
Change

Account Recovery
Your recovery key is needed to recover access to your account, should you lose or forget your master password.
Change

Multi-factor Authentication
Used for two-factor login and verification of changes to your wallets and beneficiaries.
Change

Activity Logs
View activity logs and access history.
View

4 Cold storage 2 Wallets
0 NFTs 2 Beneficiaries
Storage (9.3%) 23.3 MB / 250 MB
Last login: 10/14/2022, 06:01 PM
From: ES

To protect users from any kind of account attacks, FortKnoxster enforces various security measures and offers the following account security features:

- **Two-factor authentication** – adds an extra layer of protection to your account by entering both your password and also a security code (an OTP) during login.
- **Zero-knowledge authentication** – your password is never sent to the server.
- **Intelligent 4th generation CAPTCHA** – blocks malicious traffic to prevent account attacks and other threats and fraud attempts.
- **Web application firewall (WAF)** – filtering web requests with rate limits to protect against malicious attacks.
- **Automated account blocking** – when Brute Force attacks or other abuses are detected.
- **Account recovery** – regain access to your FortKnoxster account with your recovery key.
- **Digitally signed web requests** – prevents MITM attacks with private key and ensures only you can make changes to your account.
- **Change password** – protect your account by re-encrypting your private keys and locking out other devices.

- **Account authorization** – authorize critical account updates with password, email OTP and two-factor OTP.
- **Web security** – XSS protection, CSP, SRI and more as described next in Web Security.

Web Security

Cross-Site Scripting (XSS) attacks are probably the most widely spread type of attacks on web applications and happen when malicious scripts are injected into websites to target end-users.

The goal of an XSS attack is to make some browser script execute in the victim's browser on infected sites and to steal sensitive information such as a session cookie from an authenticated user and then send it back to the attacker's server. The attacker can then gain access to the victim's account on that specific website by using this session cookie. Such an attack can be done without the victim's knowledge.

This kind of attack has been performed on well-known services such as WhatsApp, where the attacker was able to completely hi-jack some victim's WhatsApp account and be able to control that victim's account.

Websites and web applications are vulnerable to XSS attacks typically when user inputs are not filtered correctly.

FortKnoxster implements several security measures to make sure our users are protected against any kind of XSS attacks, by making sure user inputs such as an inbox or chat message are escaped and sanitized before displaying it, in the receiver's browser. Furthermore, our web application and server configurations have been optimized to set the **HTTP Only** cookie flag, **X-XSS-Protection,** and **Content-Security-Policy** response headers.

Our research in **Content Security Policy (CSP)** has resulted in a very strict CSP configuration, by not allowing any kind of external sources to be loaded inside the FortKnoxster environment.

CSP is supported in all modern browsers and protects against XSS by whitelisting allowed sources of script, style, media, and other resources when you visit a website.

To have this kind of protection, the CSP configurations need to be done in the webserver configurations and is a special response header (Content-Security-Policy) sent from the server back to the browser, when a page is requested.

We have taken these extra security measures to make sure our CSP configurations are as strict as possible by whitelisting only internal resources, and thereby blacklisting any kind of external loading of resources in the client's browser when visiting our website and using our services, and therefore enforce our user's privacy.

Subresource Integrity (SRI) is a security feature that enables browsers to verify that resources such as Javascript code files are delivered to the browser without any manipulation or interception. By providing a cryptographic hash of the resource the browser can match the integrity of the resource with the hash and reject any malicious code injection attempts. FortKnoxster uses SRI on all Javascript resources to prevent such malicious attacks.

Cross Site Request Forgery (CSRF/XSRF) is a special kind of attack, where the attacker can trick the victim into performing unwanted actions, such as authorizing a bank transfer.

FortKnoxster prevents CSRF vulnerabilities by including a unique session token on each HTTP request and a special XSRF cookie.

Furthermore, the FortKnoxster session cookie is encrypted with AES-CBC 256bit and a mac using the HMAC function, taking a server key as input.

Phishing is a type of social engineering attack. The attacker masquerades as the trusted site, tricking the victim to perform unwanted actions, such as stealing login credentials, credit card details and other sensitive data.

FortKnoxster implements several security measures to also prevent these kinds of attacks.

Open Source

Our source codes are open sourced on GitHub and allow security researchers to fully evaluate our end-to-end encryption implementation and smart contracts in our desktop/mobile web app:

https://github.com/FortKnoxster

Security Audits

The FKX token smart contract has been security audited prior to deployment on the Ethereum and Binance Smart Chain blockchains.

To view the full report, visit:

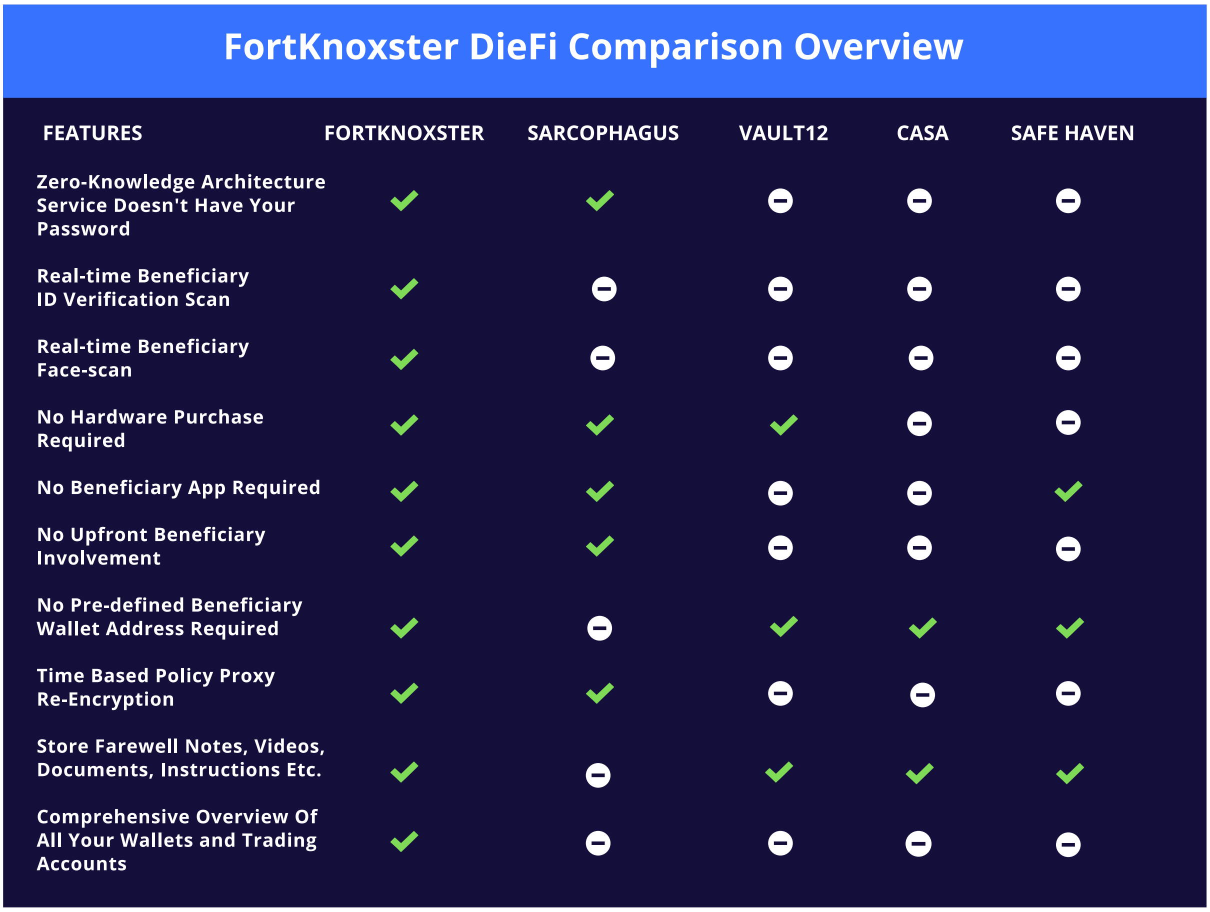
https://github.com/FortKnoxster/fkx-token/blob/master/audit/PeckShield-Audit-Report-FKX-1.0.pdf

The DieFi smart contracts on Polygon have been audited by Certik.

To view the full report, visit:

https://www.certik.com/projects/fortknoxster-diefi

Comparison

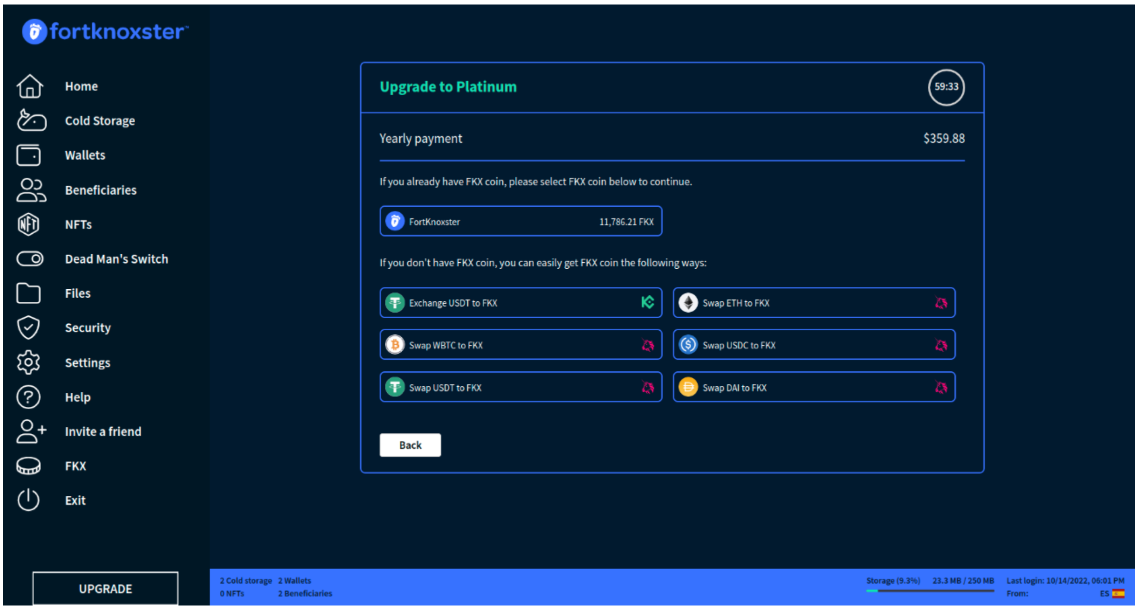


FortKnoxster DieFi Comparison Overview

FEATURES	FORTKNOXSTER	SARCOPHAGUS	VAULT12	CASA	SAFE HAVEN
Zero-Knowledge Architecture Service Doesn't Have Your Password	✓	✓	⊖	⊖	⊖
Real-time Beneficiary ID Verification Scan	✓	⊖	⊖	⊖	⊖
Real-time Beneficiary Face-scan	✓	⊖	⊖	⊖	⊖
No Hardware Purchase Required	✓	✓	✓	⊖	⊖
No Beneficiary App Required	✓	✓	⊖	⊖	✓
No Upfront Beneficiary Involvement	✓	✓	⊖	⊖	⊖
No Pre-defined Beneficiary Wallet Address Required	✓	⊖	✓	✓	✓
Time Based Policy Proxy Re-Encryption	✓	✓	⊖	⊖	⊖
Store Farewell Notes, Videos, Documents, Instructions Etc.	✓	⊖	✓	✓	✓
Comprehensive Overview Of All Your Wallets and Trading Accounts	✓	⊖	⊖	⊖	⊖

FKX Token Utility

The FortKnoxster utility token ($FKX) is used to purchase various upgrade services and incentivize users for different rewards.



Upgrade to Platinum

59:33

Yearly payment $359.88

If you already have FKX coin, please select FKX coin below to continue.

FortKnoxster 11,786.21 FKX

If you don't have FKX coin, you can easily get FKX coin the following ways:

- Exchange USDT to FKX
- Swap ETH to FKX
- Swap WBTC to FKX
- Swap USDC to FKX
- Swap USDT to FKX
- Swap DAI to FKX

2 Cold storage 2 Wallets
0 NFTs 2 Beneficiaries

Storage (9.3%) 23.3 MB / 250 MB

Last login: 10/14/2022, 06:01 PM
From: ES

The FKX utility token has a clear and important usage in our application as a means of both incentivizing further development and securing our ability to run and market FortKnoxster worldwide. The FKX token serves the purpose of being required to use FortKnoxster's DieFi Pro, Platinum and Lifetime DieFi features.

A fixed supply of 150 Mill. FKX was generated during the token distribution. A ledger on the blockchain was created, maintaining the FKX token, following the ERC-20 standard and allowing a secure mechanism for transferring FKX to other participants.

Our tokenomics and FKX ecosystem design: All paid plan features are charged in FKX. In other words, paid users will have to buy FKX on the exchanges, hereby creating the perfect utility ecosystem and FKX demand. (FKX has a total supply and circulation supply of 150 Million FKX.

For more information, please visit http://fortknoxster.com/fkx-coin.

Total/max & circulating supply

150.000.000 FKX

Current exchanges

KuCoin, Changelly PRO & Uniswap

Trading pairs

USDT, BTC, ETH, WETH

ERC-20 smart contract

0x16484d73ac08d2355f466d448d2b79d2039f6ebb

BEP-20 smart contract

0x5539e65b1e4854d28db16ba4d0873d11a9949c94

Team

FortKnoxster is founded by Danish entrepreneurs & IT-security specialists, who all share a great passion for cyber-security, blockchain, cryptography and privacy for all. Our core expertise is developing innovative platforms, based on the latest encryption, AI & blockchain technologies available.

Our vision statement:

To safeguard everybody's digital assets in cyberspace by offering the world's most secure crypto beneficiary and administration platform.

Niels Klitsgaard

CEO & Co-Founder

Niels is Danish and based in Dubai. Niels has been an entrepreneur most of his life. His original background is from banking and he holds an MBA in International Marketing. He is a strong, but informal leader, with great communication skills.

Niels has an innovative mindset and a "Nothing is impossible" attitude. experience in scaling and growing companies.

Susanne Firouzbakhsh

COO

A compliance professional with 25+ years of experience in Investment banking. Working in various operational roles in Copenhagen and New York, but mainly in London where she has spent most of her life.

She has strong commercial and analytical awareness. Works effectively across geographies,

Mickey Joe Nathan Johnnysson

CEO & Co-Founder

Mickey is Danish and has spent most of his adult life playing with computers and developing software. Mickey has a master in computer science and is a great leader and team player.

His major passions are computer engineering, crypto and Blockchain, and he enjoys any technical challenge, especially if it's the cutting-edge technology and innovative kind.

Rasmus Birger Christiansen

CPO & Co-Founder

A digital and telecommunications executive with 20+ years of international experience holding multiple senior management roles.

Passionate about digitization and the transformation of the digital landscape across industries with particular attention to secure communications and privacy.

Solid background and wealth of knowledge in management of mobile networks both from a functional and security perspective.