SPYWOLF.CO

@SPYWOLFNETWORK

@SPYWOLFNETWORK

SPYWOLF

Security Audit Report

Audit prepared for

ReFi Protocol
(NFT Contract)

Completed on

September 18, 2024

OVERVIEW

This goal of this report is to review the main aspects of the project to help investors make an informative decision during their research process.

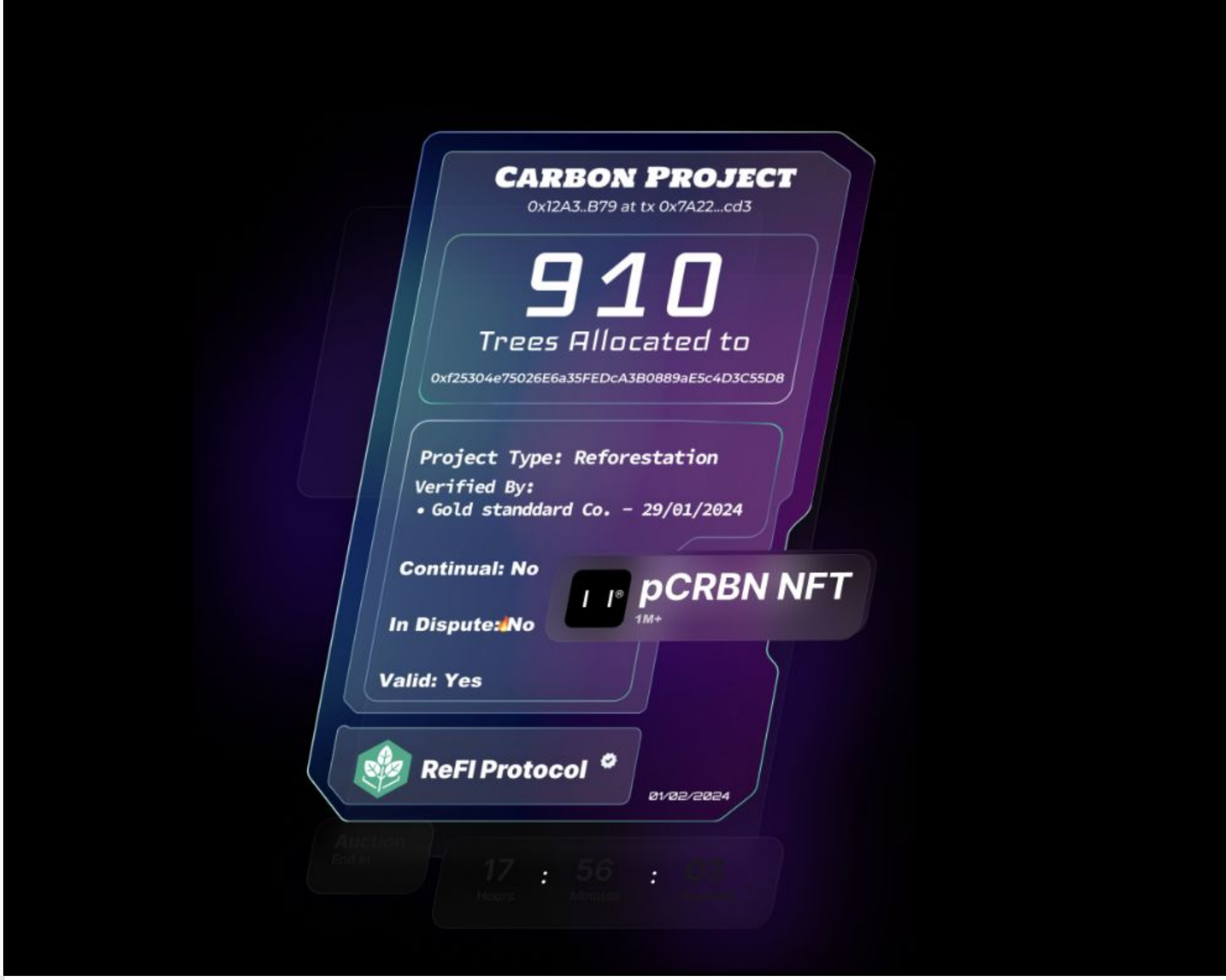
You will find a a summarized review of the following key points:

- ✓ Program’s source code
- ✓ Team transparency and goals
- ✓ Website's age, code, security and UX
- ✓ Whitepaper and roadmap
- ✓ Social media & online presence

> *The results of this audit are purely based on the team’s evaluation and does not guarantee nor reflect the projects outcome and goal*
>
> - SPYWOLF Team -

TABLE OF CONTENTS

ReFi Protocol



CARBON PROJECT

0x12A3..B79 at tx 0x7A22...cd3

910

Trees Allocated to

0xf25304e75026E6a35FEDcA3B0889aE5c4D3C55D8

Project Type: Reforestation

Verified By:

• Gold standdard Co. - 29/01/2024

Continual: No

In Dispute: No

Valid: Yes

Project Carbon NFTs

"Our carbon projects are tokenized into Project Carbon (pCRBN) NFTs, which store the project and ownership metadata. This innovative approach ensures that each NFT represents a verified portion of a carbon project, providing transparency and enhancing market trust."

Release Date: 16-09-2024

Category: NFTs Staking

PROGRAM INFO

Token Name ReFi Protocol Staking	Symbol -
Address A99rMhgutWBjPCAcbhoyknj2FqVQYUpBiu7srmonmnHy	
Network Solana	Language Rust
Deployment Date Sept 16, 2024	Type Staking NFT
Total Supply -	Status Launched

TAXES

Buy Tax	Sell Tax
0%	0%

*This is an NFT staking program and does not have any taxes

Our Program Review Process

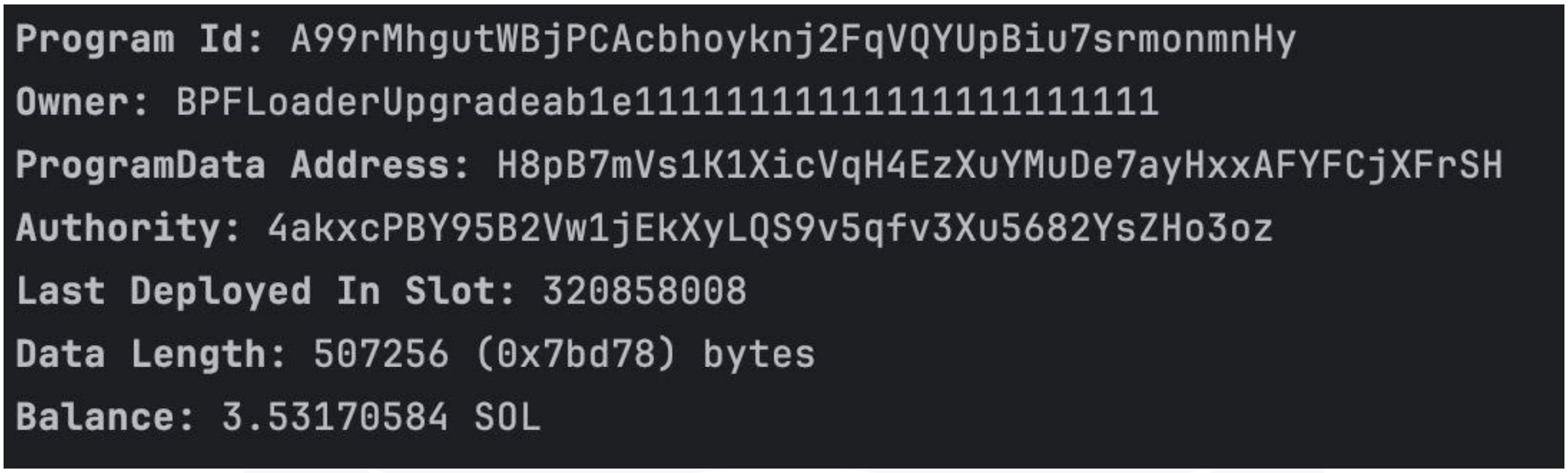
The contract review process pays special attention to the following:

- ✓ Testing the programs against both common and uncommon vulnerabilities
- ✓ Assessing the codebase to ensure compliance with current best practices and industry standards.
- ✓ Ensuring program logic meets the specifications and intentions of the client.
- ✓ Cross referencing program structure and implementation against similar programs produced by industry leaders.
- ✓ Thorough line-by-line manual review of the entire codebase by industry experts.

Blockchain security tools used:

- Solana Program Library (SPL)
- Manual Auditing / Sec3 / Neodyme
- Rust Compiler
- Anchor Framework

CURRENT STATS



```
Program Id: A99rMhgutWBjPCAcbhoyknj2FqVQYUpBiu7srmonmnHy
Owner: BPFLoaderUpgradeab1e11111111111111111111111
ProgramData Address: H8pB7mVs1K1XicVqH4EzXuYMuDe7ayHxxAFYFCjXFrSH
Authority: 4akxcPBY95B2Vw1jEkXyLQS9v5qfv3Xu5682YsZHo3oz
Last Deployed In Slot: 320858008
Data Length: 507256 (0x7bd78) bytes
Balance: 3.53170584 SOL
```

Verified Builds: VERIFIED ✔

The **Verified Builds** process has been thoroughly completed, ensuring that the deployed code exactly matches the audited version. This verification confirms that no unauthorized changes or vulnerabilities were introduced during deployment. As a result, the build is secure and fully aligns with the standards of integrity and trust required for the program.

VULNERABILITY ANALYSIS

Code	Title	
STPUPA	Update Authority	**Upgradable**
STPTFA	Transfer Fee Configuration Authority	**Passed**
STPMTA	Mint Authority	**Passed**
STPFRA	Freeze Authority	**Passed**

VULNERABILITY ANALYSIS

STPUPA: Update Authority

🟨 Upgradable

In a staking program, the Update Authority controls the ability to modify or update the program or its smart contracts. If this authority is not properly secured or managed, it could lead to:

- ✓ Unauthorized Updates: Attackers could alter program settings or code, affecting functionality, staking rules, or ownership.
- ✓ Security Exploits: A compromised update authority could introduce vulnerabilities or backdoors, compromising the security of the program and user assets.
- ✓ Trust Issues: Improperly handled updates could lead to a loss of user confidence in the platform, as unexpected or malicious changes might disrupt operations or compromise the integrity of the staking program.

The STPUPA: Update Authority is upgradable, meaning that modifications can be made when necessary. This flexibility allows for improvements and security updates while maintaining strict controls to ensure that only authorized updates are applied, ensuring the program's long-term integrity and security.

VULNERABILITY ANALYSIS

STPTFA: Transfer Fee Configuration Authority

🟩 Passed

In a staking program, the Transfer Fee Configuration Authority can set or modify fees when NFTs or tokens are transferred. If not properly secured, this could result in:

- ✓ Unauthorized Fee Modifications: Attackers could alter fees, making transactions costly or setting arbitrary fees.
- ✓ Fee Exploitation: A compromised authority could redirect a portion of transfers to malicious addresses, leading to financial loss.
- ✓ Trust Issues: Poor management of the authority could erode user trust due to unpredictable or malicious fee changes, reducing platform engagement.

Since this threat has been mitigated, it means the control over transfer fee configuration is likely well-secured, with proper access controls and monitoring to prevent unauthorized or malicious modifications.

Note: Even though this authority has currently passed the audit, an **upgradable Update Authority** means that these configurations could potentially change in the future.

VULNERABILITY ANALYSIS

STPMTA: Mint Authority

🟩 Passed

The Mint Authority controls the creation of new NFTs. If this authority is compromised or misused, it could lead to:

- ✓ Unauthorized Minting: Attackers could mint excess NFTs, diluting value or causing inflation.
- ✓ Token Exploits: A compromised mint authority could create tokens that bypass staking rules, leading to unfair advantages.
- ✓ Trust Issues: Mismanagement of minting could undermine user trust, as unchecked token creation affects the program's integrity and value.

The minting process is securely managed, preventing unauthorized token creation or exploitation. All controls are in place to ensure that only authorized actions can be taken, preserving the integrity and stability of the staking program. Users can trust that the minting authority operates safely and as intended.

Note: Even though this authority has currently passed the audit, an **upgradable Update Authority** means that these configurations could potentially change in the future.

VULNERABILITY ANALYSIS

STPFRA: Freeze Authority

🟩 Passed

The Freeze Authority controls the ability to pause or freeze NFT transfers. If this authority is compromised or misused, it could lead to:

- ✓ Unauthorized Freezing: Attackers could freeze legitimate users' assets, blocking transfers and disrupting staking or trading activities.
- ✓ Program Exploitation: A malicious actor with control of the freeze authority could selectively freeze assets to manipulate the market or gain an unfair advantage.
- ✓ Trust Issues: Misuse or unclear management of the freeze authority could undermine user trust, as unpredictable freezing actions would create uncertainty about asset liquidity and availability.

The freeze authority is securely managed, ensuring that only authorized actions can freeze NFT transfers. All necessary security measures are in place, and the program passed this aspect of the audit, confirming its stability and reliability for users.

Note: Even though this authority has currently passed the audit, an **upgradable Update Authority** means that these configurations could potentially change in the future.

NFT COLLECTION VERIFICATION

The Collection address (3r7vxPzmMVprd4RavPiVwZWtrySXpfm7pgHogDVTmMne) has been reviewed and confirmed to ensure that only NFTs from the designated collection are allowed for staking. This address plays a crucial role in the integrity of the staking program, ensuring that unrelated or unauthorized NFTs cannot be staked.

Key Verification Points:

- ✓ The Collection address (3r7vxPzmMVprd4RavPiVwZWtrySXpfm7pgHogDVTmMne) correctly restricts staking to NFTs that are part of the approved collection.
- ✓ Only approved NFTs within this collection can be staked, maintaining program integrity.
- ✓ No vulnerabilities or issues were identified in the way the staking program interacts with the Collection address.

VERIFIED CANDY MACHINE

Candy Machine address (33aG56J1qYV5KKDS8h2RGqauYTXdRLTJwWDXvE8FWtGJ) has been verified as the legitimate source for minting the NFTs in the staking collection. Ensuring that only NFTs minted by this authorized candy machine can be staked adds an additional layer of security to the program.

Key Verification Points:

✓ Candy Machine address (33aG56J1qYV5KKDS8h2RGqauYTXdRLTJwWDXvE8FWtGJ) was confirmed as the authorized source of NFT minting for the collection.

✓ No unauthorized NFTs can be minted or staked in the program, protecting against fraudulent additions.

✓ The interaction between the Candy Machine and the staking program is secure, with no vulnerabilities detected.

WEBSITE

Website URL
refiprotocol.io/

Domain Registry
https://www.namecheap.com/

Domain Expiration
2025-07-15

Technical SEO Test
Passed

Security Test
Passed. SSL certificate present

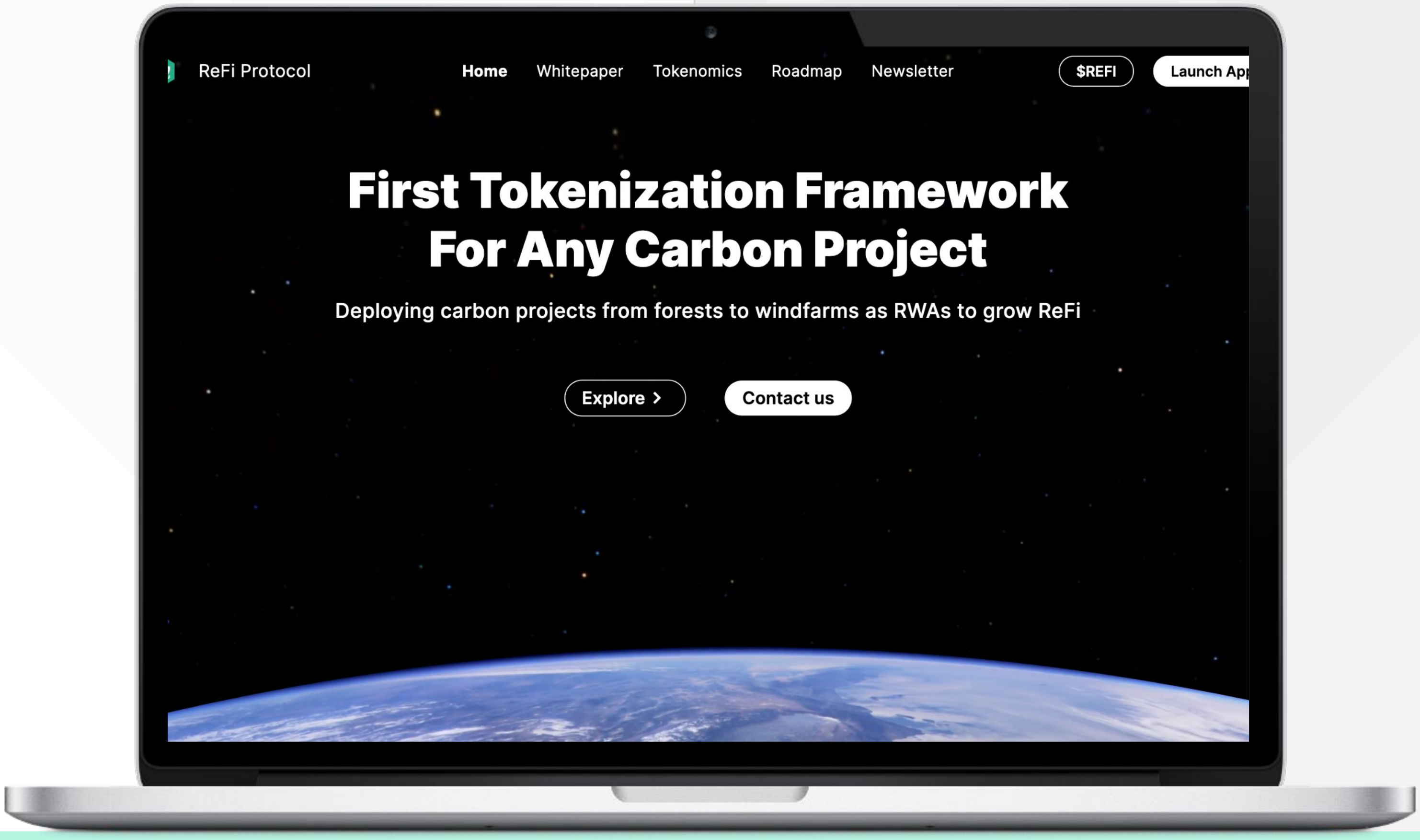
Design
Nice color scheme that goes with the theme of the project.

Content
VEry well written and has enough information for investors to know what the project is about.

Whitepaper
Yes. Well written

Roadmap
Yes

Mobile-friendly?
Yes



First Tokenization Framework For Any Carbon Project

Deploying carbon projects from forests to windfarms as RWAs to grow ReFi

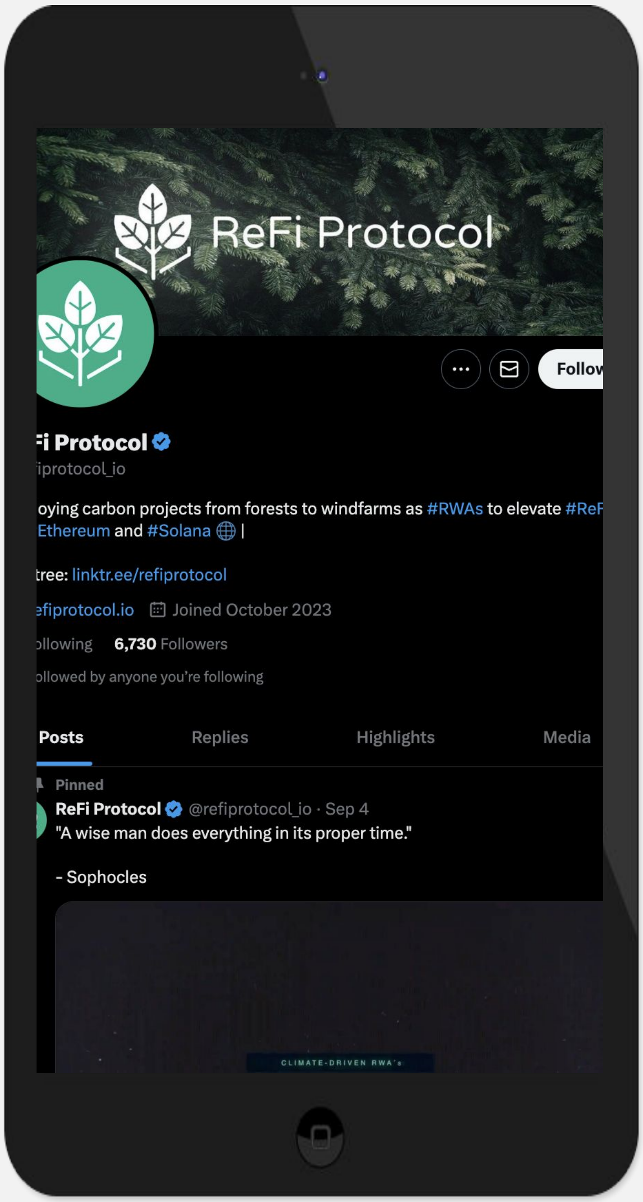
refiprotocol.io

SOCIAL MEDIA

& ONLINE PRESENCE

ANALYSIS

Project team is very active on socials and responds to comments.



Fi Protocol
iprotocol_io

oying carbon projects from forests to windfarms as #RWAs to elevate #ReF
Ethereum and #Solana 🌐 |

tree: linktr.ee/refiprotocol

efiprotocol.io Joined October 2023

ollowing 6,730 Followers

ollowed by anyone you're following

Pinned
ReFi Protocol @refiprotocol_io · Sep 4
"A wise man does everything in its proper time."

- Sophocles

Twitter's X

@refiprotocol_io

- 6,730 Followers
- Responds to comments
- Daily posts

Discord

- Not available

Telegram

@refiprotocolcommunity

- 1916 members
- Active mods and devs
- Daily announcements

Medium

refiprotocol.medium.com

- 15 posts
- VEry informative

SPYWOLF

CRYPTO SECURITY

Audits | KYCs | dApps
Contract Development

ABOUT US

We are a growing crypto security agency offering audits, KYCs and consulting services for some of the top names in the crypto industry.

- ✓ OVER 700 SUCCESSFUL CLIENTS
- ✓ MORE THAN 1000 SCAMS EXPOSED
- ✓ MILLIONS SAVED IN POTENTIAL FRAUD
- ✓ PARTNERSHIPS WITH TOP LAUNCHPADS, INFLUENCERS AND CRYPTO PROJECTS
- ✓ CONSTANTLY BUILDING TOOLS TO HELP INVESTORS DO BETTER RESEARCH

To hire us, reach out to
contact@spywolf.co or
t.me/joe_SpyWolf

FIND US ONLINE

SPYWOLF.CO

@SPYWOLFNETWORK

@SPYWOLFNETWORK

Disclaimer

This report shows findings based on our limited project analysis, following good industry practice from the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, overall social media and website presence and team transparency details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report.

While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the disclaimer below – please make sure to read it in full.

DISCLAIMER:

By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice.

No one shall have any right to rely on the report or its contents, and SpyWolf and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (SpyWolf) owe no duty of care towards you or any other person, nor does SpyWolf make any warranty or representation to any person on the accuracy or completeness of the report.

The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and SpyWolf hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, SpyWolf hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against SpyWolf, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report. The analysis of the security is purely based on the smart contracts, website, social media and team.

No applications were reviewed for security. No product code has been reviewed.