# CFG NINJA AUDITS

## Security Assessment

# Crypto IRA Token

March 9, 2022

# Table of Contents

# Audit Summary

This report has been prepared for Crypto IRA Token on the Binance Smart Chain network. CFGNINJA provides both client-centered and user-centered examination of the smart contracts and their current status when applicable. This report represents the security assessment made to find issues and vulnerabilities on the source code along with the current liquidity and token holder statistics of the protocol.

A comprehensive examination has been performed, utilizing Cross Referencing, Static Analysis, In-House Security Tools, and line-by-line Manual Review.

The auditing process pays special attention to the following considerations:

- Testing the smart contracts against both common and uncommon attack vectors.
- Inspecting liquidity and holders statistics to inform the current status to both users and client when applicable.
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Verifying contract functions that allow trusted and/or untrusted actors to mint, lock, pause, and transfer assets.

# Project Overview

## Token Summary

| Parameter | Result |
| --- | --- |
| Address | 0xdd25e1955fd9f7b3abe83cc419070a7ace104dce |
| Name | Crypto IRA |
| Token Tracker | Crypto IRA (CIRA) |
| Decimals | 5 |
| Supply | 10,000,000 |
| Platform | Binance Smart Chain |
| compiler | v0.8.12+commit.f00d7308 |
| Optimization | Yes with 200 runs |
| LicenseType | Unlicense |
| Language | Solidity |
| Codebase | https://bscscan.com/token/0xdd25e1955fd9f7b3abe83cc419070a7ace104dce |
| Url | https://cryptoira.finance/ |

## Main Contract Assessed

| Name | Contract | Live |
| --- | --- | --- |
| Crypto IRA | 0xdd25e1955fd9f7b3abe83cc419070a7ace104dce | Yes |

## TestNet Contract Assessed

| Name | Contract | Live |
| --- | --- | --- |
| Crypto IRA | 0xF0d872671284E7ffeA3cb7aF1BE42Dc05e57f47b | Yes |

## Solidity Code Provided

| SolID | FileNameMD5 | FileName |
| --- | --- | --- |
| CIR101 | 74810a12d7a5d520236a2863f4abb5aa | cryptoirav2.sol |

# Smart Contract Vulnerability Checks

| Vulnerability | Automatic Scan | Manual Scan | Result |
|---|---|---|---|
| Unencrypted Private Data On-Chain | Complete | Complete | Low / No Risk |
| Code With No Effects | Complete | Complete | Low / No Risk |
| Message call with hardcoded gas amount | Complete | Complete | Low / No Risk |
| Hash Collisions With Multiple Variable Length Arguments | Complete | Complete | Low / No Risk |
| Unexpected Ether balance | Complete | Complete | Low / No Risk |
| Presence of unused variables | Complete | Complete | Low / No Risk |
| Right-To-Left-Override control character (U+202E) | Complete | Complete | Low / No Risk |
| Typographical Error | Complete | Complete | Low / No Risk |
| DoS With Block Gas Limit | Complete | Complete | Low / No Risk |
| Arbitrary Jump with Function Type Variable | Complete | Complete | Low / No Risk |
| Insufficient Gas Griefing | Complete | Complete | Low / No Risk |
| Incorrect Inheritance Order | Complete | Complete | Low / No Risk |
| Write to Arbitrary Storage Location | Complete | Complete | Low / No Risk |
| Requirement Violation | Complete | Complete | Low / No Risk |
| Missing Protection against Signature Replay Attacks | Complete | Complete | Low / No Risk |

| Vulnerability | Automatic Scan | Manual Scan | Result |
| --- | --- | --- | --- |
| Weak Sources of Randomness from Chain Attributes | Complete | Complete | Low / No Risk |

# Mint Check

The Project Owners of Crypto IRA does not have a mint function in the contract, owner cannot mint tokens after initial deploy

. .

The Project has a Total Supply of 10,000,000 and cannot mint any more than the Max Supply.

.

# Fees Check

The Project Owners of Crypto IRA does not have the ability to set fees higher than 25% .

Team May have fees defined, however they dont have the ability to set those fees higher than 25%.

.

# MaxTx Check

The Project Onwers of Crypto IRA does not has the ability to set max tx amount

The Team allow any investors to swap, transfer or sale their total amount if needed.

# Pause Trade Check

The Project Onwers of Crypto IRA Owner can pause trading but he can't move tokens (Owner can't pause trading)

The Team has done a great job to avoid stop trading, and investors has the ability to trade at any given time without any problems

# Contract Ownership

The contract ownership of Crypto IRA is not currently renounced. The ownership of the contract grants special powers to the protocol creators, making them the sole addresses that can call sensible ownable functions that may alter the state of the protocol.

The current owner is the address 0xAe50A9404e79160c51e7266021B644B906972B3F which can be viewed from:
HERE

The owner wallet has the power to call the functions displayed on the priviliged functions chart below, if the owner wallet is compromised this privileges could be exploited.

We recommend the team to renounce ownership at the right timing if possible, or gradually migrate to a timelock with governing functionalities in respect of transparency and safety considerations.

# Liquidity Ownership

The token does not have liquity at the moment of the audit, block 17254423

# KYC Information

The Project Onwers of Crypto IRA has provided KYC Documentation.

KYC Certificated can be found on the Following:
KYC Data

# Priviliged Functions (onlyOwner)

| Function Name | Parameters | Visibility |
|---|---|---|
| renounceOwnership | none | public |
| transferOwnership | address newOwner | public |
| setMaxWalletPercent_base1000 | uint256 maxWallPercent_base1000 | external |
| manualBurn | uint256 burnAmount | external |
| set_sell_multiplier | uint256 Multiplier | external |
| setNumTokensSellToAddToLiquidity | uint256 numTokens | external |
| lock | uint256 time | external |
| tradingStatus | bool _status | external |
| cooldownEnabled | bool _status, uint8 _interval | external |
| manage_blacklist | address[] calldata addresses, bool status | external |
| enable_blacklist | bool _status | external |

## Important Notes To The Users:

- The team has provided a KYC Link during the time of assessment and can be found in the Audit.
- No mint function found, owner cannot mint tokens after initial deploy
- Owner can change fees up to 25%
- Owner can't set max tx amount
- Owner can't pause trading
- No high-risk Exploits/Vulnerabilities Were Found in the Source Code.
- Teams has show commitment to their project and is looking forward the features.

## Audit Passed

# Disclaimer

CFGNINJA has conducted an independent audit to verify the integrity of and highlight any vulnerabilities or errors, intentional or unintentional, that may be present in the codes that were provided for the scope of this audit. This audit report does not constitute agreement, acceptance or advocation for the Project that was audited, and users relying on this audit report should not consider this as having any merit for financial advice in any shape, form or nature. The contracts audited do not account for any economic developments that may be pursued by the Project in question, and that the veracity of the findings thus presented in this report relate solely to the proficiency, competence, aptitude and discretion of our independent auditors, who make no guarantees nor assurance that the contracts are completely free of exploits, bugs, vulnerabilities or deprecation of technologies.

All information provided in this report does not constitute financial or investment advice, nor should it be used to signal that any persons reading this report should invest their funds without sufficient individual due diligence regardless of the findings presented in this report. Information is provided 'as is', and CFGNINJA is under no covenant to the completeness, accuracy or solidity of the contracts audited. In no event will CFGNINJA or its partners, employees, agents or parties related to the provision of this audit report be liable to any parties for, or lack thereof, decisions and/or actions with regards to the information provided in this audit report.

The assessment services provided by CFGNINJA is subject to dependencies and under continuing development. You agree that your access and/or use, including but not limited to any services, reports, and materials, will be at your sole risk on an as-is, where-is, and as-available basis. Cryptographic tokens are emergent technologies and carry with them high levels of technical risk and uncertainty. The assessment reports could include false positives, false negatives, and other unpredictable results. The services may access, and depend upon, multiple layers of third-parties.