CFG NINJA AUDITS

Security Assessment

TokenWhistle Token

Token

May 27, 2023

Audit Status: Pass

Audit Edition: Advance

Token Whistle

POWERED BY BLADE POOL

Risk Analysis

Classifications of Manual Risk Results

Classification	Description
Critical	Danger or Potential Problems.
Major	Be Careful or Fail test.
Minor	Pass, Not-Detected or Safe Item.
Informational	Function Detected

Manual Code Review Risk Results

Contract Priviledge	Description
Buy Tax	9
Sale Tax	9
Cannot Sale	Pass
Cannot Sale	Pass
Max Tax	20
Modify Tax	Up to 20%
Fee Check	Pass
Is Honeypot?	Not Detected
Trading Cooldown	Not Detected
Can Pause Trade?	Pass
Pause Transfer?	Not Detected

Contract Priviledge	Description
Max Tx?	Fail
Is Anti Whale?	Detected
Is Anti Bot?	Not Detected
Is Blacklist?	Not Detected
Blacklist Check	Pass
is Whitelist?	Not Detected
Can Mint?	Pass
Is Proxy?	Not Detected
Can Take Ownership?	Not Detected
Hidden Owner?	Not Detected
Owner	0x00f7d7d05be230685f47bd9ace7cee9c25493e51
Self Destruct?	Not Detected
Other?	Detected
Other?	Not Detected
Holders	1
Auditor Confidence	Low

The following quick summary it's added to the project overview; however, there are more details about the audit and its results. Please read every detail.

Table of Contents

Assessment Summary

This report has been prepared for TokenWhistle Token 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.
- Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders
- Thorough line-by-line manual review of the entire codebase by industry experts.

Project Overview

Token Summary

Parameter	Result
Address	0xfC75C3a882a5bF53d55F75a0300aC309A1d63d25
Name	TokenWhistle Token
Token Tracker	TokenWhistle Token (Whistle)
Decimals	18
Supply	5,000,000
Platform	Binance Smart Chain
compiler	v0.8.18+commit.87f61d96
Contract Name	ReflectionTokenWithAntibot
Optimization	Yes with 200 runs
LicenseType	MIT
Language	Solidity
Codebase	https://bscscan.com/address/0xfC75C3a882a5bF53d55F75a0300aC309A1d63d25#code
Payment Tx	0x

Main Contract Assessed
Contract Name

Name	Contract	Live
TokenWhistle Token	0xfC75C3a882a5bF53d55F75a0300aC309A1d63d25	Yes

TestNet Contract was Not Assessed

Solidity Code Provided

SolID	File Sha-1	FileName
Whistle	0c44217d4e10c7fd3d2275a07bd4706e92dbac64	ReflectionTokenWithAntibot.sol
Whistle		
Whistle		
Whistle		

Mint Check

The project owners of TokenWhistle Token do not have a mint function in the contract, owner cannot mint tokens after initial deploy.

The Project has a Total Supply of 5,000,000 and cannot mint any more than the Max Supply.

Mint Notes:

Auditor Notes:

Project Owner Notes:

Fees Check

The project owners of TokenWhistle Token do not have the ability to set fees higher than 20 .

The team May have fees defined; however, they can't set those fees higher than 20 or may not be able to configure the same.

Tax Fee Notes:

Auditor Notes: The contract currently has 0% buy and 0% sale taxes.

Project Owner Notes:

Blacklist Check

The project owners of TokenWhistle Token do not have a blacklist function their contract.

The Project allow owners to transfer their tokens without any restrictions.

Token owner cannot blacklist the contract: Malicious or compromised owners can trap contracts relying on tokens with a blacklist.

Blacklist Notes:

Auditor Notes: .

Project Owner Notes:

MaxTx Check

The Project Owners of TokenWhistle Token can set max tx amount.

The ability to set MaxTx can be used as bad actor, this can limit the ability of investors to sale their tokens at any given time if is set too low..

We recommend the project to set MaxTx to Total Supply or simiar to avoid swap or transfer from failures

MaxTX Notes:

Auditor Notes:

Project Owner Notes:

Pause Trade Check

The Project Owners of TokenWhistle Token don't have the ability to stop or 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

Pause Trade Notes:

Auditor Notes:

Project Owner Notes: .

Owner can't pause trading

Contract Ownership

The contract ownership of TokenWhistle Token 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 0x00f7d7d05be230685f47bd9ace7cee9c25493e51 which can be viewed:
HERE

The owner wallet has the power to call the functions displayed on the privileged functions chart below, if the owner's wallet is compromised, they could exploit these privileges.

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

We recommend the team use a Multisignature Wallet if the contract is not going to be renounced; this will give the team more control over the contract.

Liquidity Ownership

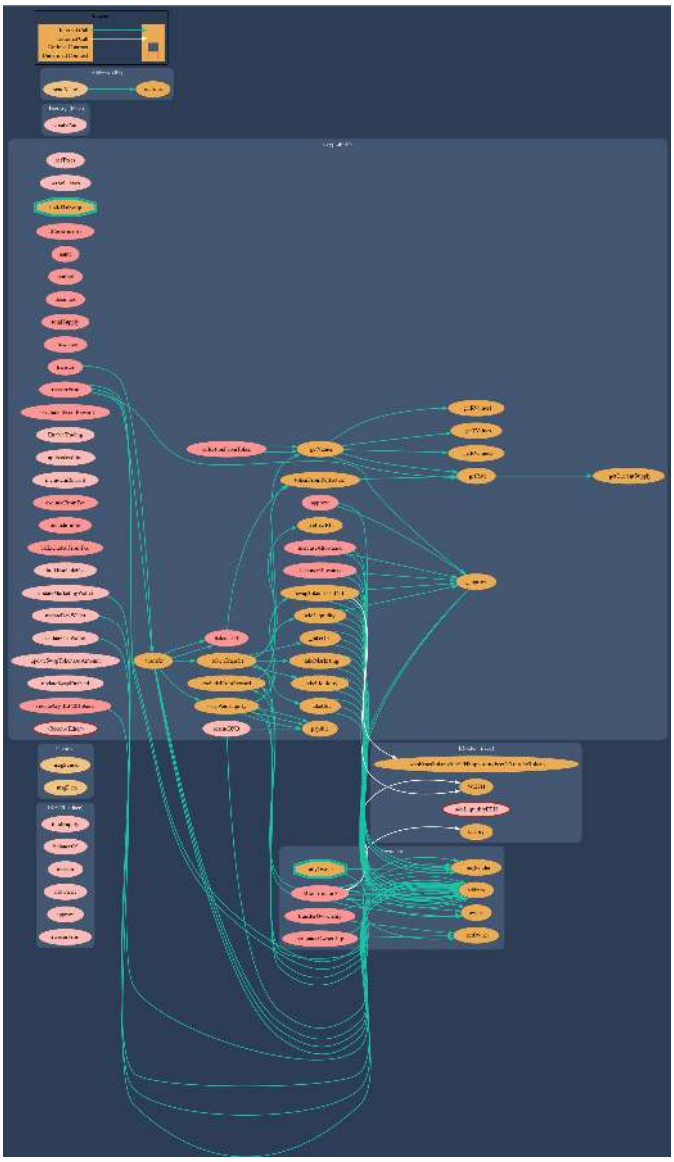
The token does not have liquidity at the moment of the audit, block 28530646

If liquidity is unlocked, then the token developers can do what is infamously known as 'rugpull'. Once investors start buying token from the exchange, the liquidity pool will accumulate more and more coins of established value (e.g., ETH or BNB or Tether). This is because investors are basically sending these tokens of value to the exchange, to get the new token. Developers can withdraw this liquidity from the exchange, cash in all the value and run off with it. Liquidity is locked by renouncing the ownership of liquidity pool (LP) tokens for a fixed time period, by sending them to a time-lock smart contract. Without ownership of LP tokens, developers cannot get liquidity pool funds back. This provides confidence to the investors that the token developers will not run away with the liquidity money. It is now a standard practice that all token developers follow, and this is what really differentiates a scam coin from a real one.

Read More

Call Graph

The contract for TokenWhistle Token has the following call graph structure.



KYC Information

The Project Owners of TokenWhistle Token is not KYC.

KYC Information Notes:

Auditor Notes: KYC to be completed by PinkSale, project will be a SAFU Project.

Project Owner Notes:

Smart Contract Vulnerability Checks

The Smart Contract Weakness Classification Registry (SWC Registry) is an implementation of the weakness classification scheme proposed in EIP-1470. It is loosely aligned to the terminologies and structure used in the Common Weakness Enumeration (CWE) while overlaying a wide range of weakness variants that are specific to smart contracts.

ID	Severity	Name	File	location
SWC-100	Pass	Function Default Visibility	ReflectionTokenWithAntibot.sol	L: 0 C: 0
SWC-101	Pass	Integer Overflow and Underflow.	ReflectionTokenWithAntibot.sol	L: 0 C: 0
SWC-102	Pass	Outdated Compiler Version file.	ReflectionTokenWithAntibot.sol	L: 0 C: 0
SWC-103	Pass	A floating pragma is set.	ReflectionTokenWithAntibot.sol	L: 0 C: 0
SWC-104	Pass	Unchecked Call Return Value.	ReflectionTokenWithAntibot.sol	L: 0 C: 0
SWC-105	Pass	Unprotected Ether Withdrawal.	ReflectionTokenWithAntibot.sol	L: 0 C: 0
SWC-106	Pass	Unprotected SELFDESTRUCT Instruction	ReflectionTokenWithAntibot.sol	L: 0 C: 0
SWC-107	Pass	Read of persistent state following external call.	ReflectionTokenWithAntibot.sol	L: 0 C: 0
SWC-108	Pass	State variable visibility is not set..	ReflectionTokenWithAntibot.sol	L: 0 C: 0
SWC-109	Pass	Uninitialized Storage Pointer.	ReflectionTokenWithAntibot.sol	L: 0 C: 0
SWC-110	Pass	Assert Violation.	ReflectionTokenWithAntibot.sol	L: 0 C: 0

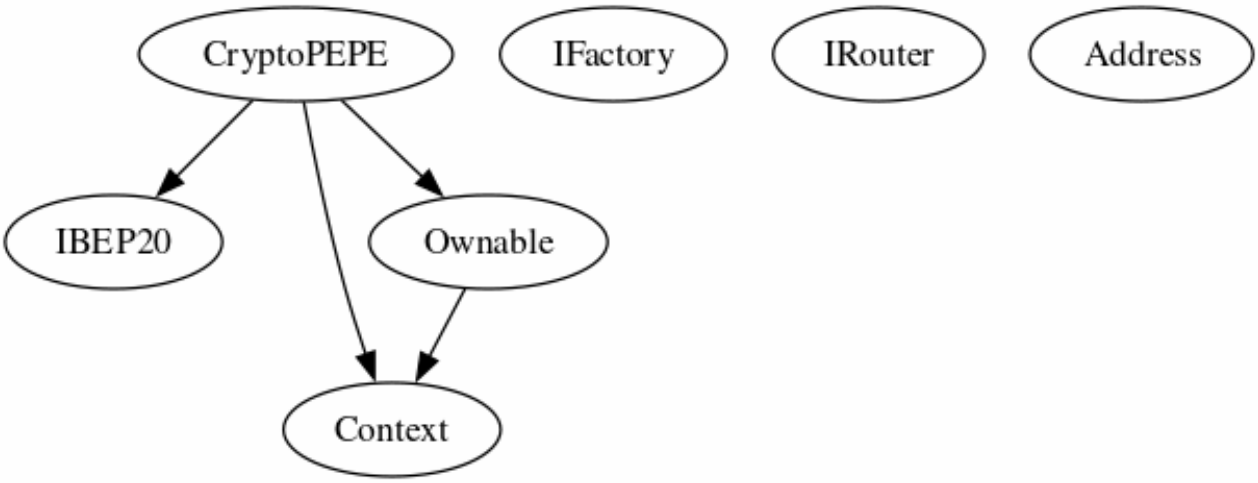
ID	Severity	Name	File	location
SWC-111	Pass	Use of Deprecated Solidity Functions.	ReflectionTokenWithAntibot.sol	L: 0 C: 0
SWC-112	Pass	Delegate Call to Untrusted Callee.	ReflectionTokenWithAntibot.sol	L: 0 C: 0
SWC-113	Pass	Multiple calls are executed in the same transaction.	ReflectionTokenWithAntibot.sol	L: 0 C: 0
SWC-114	Pass	Transaction Order Dependence.	ReflectionTokenWithAntibot.sol	L: 0 C: 0
SWC-115	Pass	Authorization through tx.origin.	ReflectionTokenWithAntibot.sol	L: 0 C: 0
SWC-116	Pass	A control flow decision is made based on The block.timestamp environment variable.	ReflectionTokenWithAntibot.sol	L: 0 C: 0
SWC-117	Pass	Signature Malleability.	ReflectionTokenWithAntibot.sol	L: 0 C: 0
SWC-118	Pass	Incorrect Constructor Name.	ReflectionTokenWithAntibot.sol	L: 0 C: 0
SWC-119	Pass	Shadowing State Variables.	ReflectionTokenWithAntibot.sol	L: 0 C: 0
SWC-120	Pass	Potential use of block.number as source of randonmness.	ReflectionTokenWithAntibot.sol	L: 0 C: 0
SWC-121	Pass	Missing Protection against Signature Replay Attacks.	ReflectionTokenWithAntibot.sol	L: 0 C: 0
SWC-122	Pass	Lack of Proper Signature Verification.	ReflectionTokenWithAntibot.sol	L: 0 C: 0
SWC-123	Pass	Requirement Violation.	ReflectionTokenWithAntibot.sol	L: 0 C: 0
SWC-124	Pass	Write to Arbitrary Storage Location.	ReflectionTokenWithAntibot.sol	L: 0 C: 0

ID	Severity	Name	File	location
SWC-125	Pass	Incorrect Inheritance Order.	ReflectionTokenWithAntibot.sol	L: 0 C: 0
SWC-126	Pass	Insufficient Gas Griefing.	ReflectionTokenWithAntibot.sol	L: 0 C: 0
SWC-127	Pass	Arbitrary Jump with Function Type Variable.	ReflectionTokenWithAntibot.sol	L: 0 C: 0
SWC-128	Pass	DoS With Block Gas Limit.	ReflectionTokenWithAntibot.sol	L: 0 C: 0
SWC-129	Pass	Typographical Error.	ReflectionTokenWithAntibot.sol	L: 0 C: 0
SWC-130	Pass	Right-To-Left-Override control character (U +202E).	ReflectionTokenWithAntibot.sol	L: 0 C: 0
SWC-131	Pass	Presence of unused variables.	ReflectionTokenWithAntibot.sol	L: 0 C: 0
SWC-132	Pass	Unexpected Ether balance.	ReflectionTokenWithAntibot.sol	L: 0 C: 0
SWC-133	Pass	Hash Collisions with Multiple Variable Length Arguments.	ReflectionTokenWithAntibot.sol	L: 0 C: 0
SWC-134	Pass	Message call with hardcoded gas amount.	ReflectionTokenWithAntibot.sol	L: 0 C: 0
SWC-135	Pass	Code With No Effects (Irrelevant/Dead Code).	ReflectionTokenWithAntibot.sol	L: 0 C: 0
SWC-136	Pass	Unencrypted Private Data On-Chain.	ReflectionTokenWithAntibot.sol	L: 0 C: 0

We scan the contract for additional security issues using MYTHX and industry-standard security scanning tools.

Inheritance

The contract for TokenWhistle Token has the following inheritance structure.



Privileged Functions (onlyOwner)

Please Note if the contract is Renounced none of this functions can be executed.

Function Name	Parameters	Visibility
renounceOwnership		Public
transferOwnership	address newOwner	Public
withdrawToken		Public
withdrawETH		External
excludeFromMaxTransactionAmount		External
setAutomatedMarketMakerPair		External
updateMinAmountToTakeFee		External
updateMarketingWallet		External
updateRewardFee		External
updateMarketingFee		External
updateLiquidityFee		External

Function Name	Parameters	Visibility
includeInReward		External
excludeFromReward		External
updateMaxTransactionAmount		External
updateMaxWallet		External
updateUniswapV2Router		External
updateUniswapV2Pair		External
setUsingAntiBot		External

Smart Contract Advance Checks

ID	Severity	Name	Result	Status
Whistle-01	Minor	Potential Sandwich Attacks.	Pass	Not-Found
Whistle-02	Minor	Function Visibility Optimization	Fail	Pending
Whistle-03	Minor	Lack of Input Validation.	Fail	Pending
Whistle-04	Major	Centralized Risk In addLiquidity.	Pass	Not-Found
Whistle-05	Minor	Missing Event Emission.	Fail	Pending
Whistle-06	Minor	Conformance with Solidity Naming Conventions.	Pass	Not-Found
Whistle-07	Minor	State Variables could be Declared Constant.	Pass	Not-Found
Whistle-08	Minor	Dead Code Elimination.	Pass	Not-Found
Whistle-09	Major	Third Party Dependencies.	Pass	Not-Found
Whistle-10	Major	Initial Token Distribution.	Pass	Not-Found
Whistle-11	Minor	AntiBot is present on the transfer.	Fail	Pending
Whistle-12	Major	Centralization Risks In The X Role	Pass	Not-Found
Whistle-13	Informational	Extra Gas Cost For User..	Pass	Not-Found
Whistle-14	Medium	Unnecessary Use Of SafeMath	Pass	Not-Found
Whistle-15	Medium	Symbol Length Limitation due to Solidity Naming Standards.	Pass	Not-Found

ID	Severity	Name	Result	Status
Whistle-16	Medium	Invalid collection of Taxes during Transfer.	Pass	Not-Found
Whistle-17	Informational	Conformance to numeric notation best practice.	Pass	Not-Found
Whistle-18	Informational	Enable Trade and Exclude Exist to create a whitelist.	Pass	Not-found

Whistle-02 | Function Visibility Optimization.

Category	Severity	Location	Status
Gas Optimization	Minor	ReflectionTokenWithAntibot.sol: L: 586 C: 11	Pending

Description

The following functions are declared as public and are not invoked in any of the contracts contained within the projects scope:

Function Name	Parameters	Visibility
updateUniswapV2Router		public
excludeFromReward		public
includeInReward		public
setAutomatedMarketMakerPair		public

The functions that are never called internally within the contract should have external visibility

Remediation

We advise that the function's visibility specifiers are set to external, and the array-based arguments change their data location from memory to calldata, optimizing the gas cost of the function.

References:

external vs public best practices.

Whistle-03 | Lack of Input Validation.

Category	Severity	Location	Status
Volatile Code	Minor	ReflectionTokenWithAntibot.sol: 566,14,1146,14	Pending

Description

The given input is missing the check for the non-zero address.

The given input is missing the check for the setUsingAntiBot,setAutomatedMarketMakerPair onlyOwners are missing required function.

Remediation

We advise the client to add the check for the passed-in values to prevent unexpected errors as below:

```
...
 require(receiver != address(0), "Receiver is the zero address");
...
...
require(value X limitation, "Your not able to do this function");
...
```

We also recommend customer to review the following function that is missing a required validation. setUsingAntiBot,setAutomatedMarketMakerPair onlyOwners are missing required function.

Whistle-05 | Missing Event Emission.

Category	Severity	Location	Status
Volatile Code	Minor	ReflectionTokenWithAntibot.sol: 566, 14,569,14,1146,14	Pending

Description

Detected missing events for critical arithmetic parameters. There are functions that have no event emitted, so it is difficult to track off-chain changes.The linked code does not create an event for the transfer.

Remediation

Emit an event for critical parameter changes. It is recommended emitting events for the sensitive functions that are controlled by centralization roles.

Whistle-11 | AntiBot is present on the transfer..

Category	Severity	Location	Status
Optimization	Minor	ReflectionTokenWithAntibot.sol: 571,14	Pending

Description

During the transfer it sends the transaction to an external contract 'IGemAntiBot(gemAntiBot).onPreTransferCheck(from, to, amount)'

Remediation

Ensure the IGemAntiBot library is audited and the process is clean during the transfer.

Project Action

Technical Findings Summary

Classification of Risk

Severity	Description
Critical	Risks are those that impact the safe functioning of a platform and must be addressed before launch. Users should not invest in any project with outstanding critical risks.
Major	Risks can include centralization issues and logical errors. Under specific circumstances, these major risks can lead to loss of funds and/or control of the project.
Medium	Risks may not pose a direct risk to users' funds, but they can affect the overall functioning of a platform
Minor	Risks can be any of the above but on a smaller scale. They generally do not compromise the overall integrity of the Project, but they may be less efficient than other solutions.
Informational	Errors are often recommended to improve the code's style or certain operations to fall within industry best practices. They usually do not affect the overall functioning of the code.

Findings

Severity	Found	Pending	Resolved
Critical	0	0	0
Major	0	0	0
Medium	0	0	0
Minor	3	0	0
Informational	1	0	0
Total	4	0	0

Social Media Checks

Social Media	URL	Result
Twitter	https://twitter.com/tokenwhistle	Pass
Other	https://www.facebook.com/tokenwhistle	Pass
Website	http://www.tokenwhistle.com	Pass
Telegram	https://t.me/tokenwhistle	Fail

We recommend to have 3 or more social media sources including a completed working websites.

Social Media Information Notes:

Auditor Notes: undefined

Project Owner Notes:

Assessment Results

Score Results

Review	Score
Overall Score	85/100
Auditor Score	80/100
Review by Section	**Score**
Manual Scan Score	32/53
SWC Scan Score	37 /37
Advance Check Score	16 /19

The Following Score System Has been Added to this page to help understand the value of the audit, the maximun score is 100, however to attain that value the project most pass and provide all the data needed for the assessment. Our Passing Score has been changed to 80 Points, if a project does not attain 80% is an automatic failure. Read our notes and final assessment below.

Audit Passed

Assessment Results

Important Notes:

- No issues or vulnerabilities were found.
- The Contract is a GemPad Generated Token.
- The Contract is fully functional, there are a few best practices that can be improved.
- This contract has an anti-bot function, is important to understand what the anti-bot is doing during the transfer.

Auditor Score =80
Audit Passed

Appendix

Finding Categories

Centralization / Privilege

Centralization / Privilege findings refer to either feature logic or implementation of components that actagainst the nature of decentralization, such as explicit ownership or specialized access roles incombination with a mechanism to relocate funds.

Gas Optimization

Gas Optimization findings do not affect the functionality of the code but generate different, more optimalEVM opcodes resulting in a reduction on the total gas cost of a transaction.

Logical Issue

Logical Issue findings detail a fault in the logic of the linked code, such as an incorrect notion on howblock.timestamp works.

Control Flow

Control Flow findings concern the access control imposed on functions, such as owner-only functionsbeing invoke-able by anyone under certain circumstances.

Volatile Code

Volatile Code findings refer to segments of code that behave unexpectedly on certain edge cases that mayresult in a vulnerability.

Coding Style

Coding Style findings usually do not affect the generated byte-code but rather comment on how to makethe codebase more legible and, as a result, easily maintainable.

Inconsistency

Inconsistency findings refer to functions that should seemingly behave similarly yet contain different code,such as a constructor assignment imposing different require statements on the input variables than a setterfunction.

Coding Best Practices

ERC 20 Conding Standards are a set of rules that each developer should follow to ensure the code meet a set of creterias and is readable by all the developers.

Disclaimer

CFGNINJA has conducted an independent security assessment to verify the integrity of and highlight any vulnerabilities or errors, intentional or unintentional, that may be present in the reviewed code for the scope of this assessment. This report does not constitute agreement, acceptance, or advocation for the Project, and users relying on this 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 the Project in question may pursue, and 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 entirely 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. Information is provided 'as is, and CFGNINJA is under no covenant to audited completeness, accuracy, or solidity of the contracts. 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 or actions with regards to the information provided in this audit report.

The assessment services provided by CFGNINJA are subject to dependencies and are under continuing development. You agree that your access 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 with high levels of technical risk and uncertainty. The assessment reports could include false positives, negatives, and unpredictable results. The services may access, and depend upon, multiple layers of third parties.