CFG NINJA AUDITS

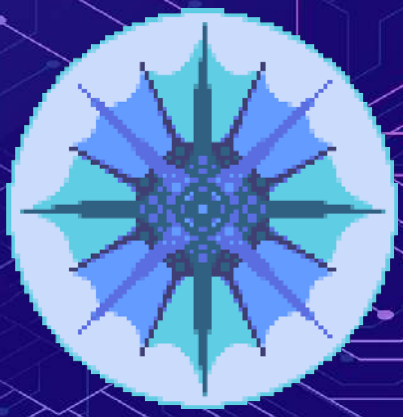
Security Assessment

Plankton Token

April 8, 2023

Audit Status: Pass

Audit Edition: Advance



POWERED BY BLADE POOL

Table of Contents

1 Assessment Summary

2 Project Overview

2.1 Token Summary

2.2 Risk Analysis Summary

2.3 Main Contract Assessed

3 Smart Contract Risk Checks

3.1 Mint Check

3.2 Fees Check

3.3 Blacklist Check

3.4 MaxTx Check

3.5 Pause Trade Check

3.6 Contract Ownership

3.7 Liquidity Ownership

3.8 KYC Check

4 Smart Contract Vulnerability Checks

4.1 Smart Contract Vulnerability Details

4.2 Smart Contract Inheritance Details

4.3 Smart Contract Privileged Functions

5 Technical Findings Details

6 Social Media Check(Informational)

7 Assessment Results and Notes(Important)

7.1 Score Results

8 Disclaimer

Assessment Summary

This report has been prepared for Plankton Token on the Arbitrium 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	0x04dA5E940911fE912FcD9Ac75B01CFE95BD7D65c
Name	Plankton
Token Tracker	Plankton (PLNKTON)
Decimals	18
Supply	10,000,000
Platform	Arbitrium
compiler	v0.8.4+commit.c7e474f2
Contract Name	BuybackBabyToken
Optimization	Yes with 200 runs
LicenseType	MIT
Language	Solidity
Codebase	https://arbiscan.io/token/0x04da5e940911fe912fcd9ac75b01cfe95bd7d65c#code
Payment Tx	0x7c01448176f2e9c940183803a4b648038cc99df24f0b796575b3ddf549ebe89f

Project Overview

Risk Analysis Summary

Parameter	Result
Buy Tax	10%
Sale Tax	10%
Is honeypot?	Clean
Is CoolDown?	No
Can edit tax?	Yes
Is anti whale?	No
Is blacklisted?	No
Is whitelisted?	No
Holders	26
Confidence Level	Medium

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.

Project Overview

Simulation Summary

Parameter	Result
Transfer From Owner	Pass
Transfer From Holder	Pass
Add Liquidity	Pass
Buy from Owner	Pass
Buy from Holder	Pass
Remove Liquidity	Pass
SwapAndLiquify	Pass
RemoveLiquidity	Pass
LaunchPad	PinkSale

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.

Main Contract Assessed
Contract Name

Name	Contract	Live
Plankton	0x04dA5E940911fE912FcD9Ac75B01CFE95BD7D65c	Yes

TestNet Contract Assessed
Contract Name

Name	Contract	Live
Plankton	0x3c0e473649633f656c66ae4ffdc5a94afba3975d	Yes

Solidity Code Provided

SolID	File Sha-1	FileName
BabyBuyBackToken	a03c6914d2248c3b4bd2a595e174fb044a57247f	BabyBuyBackToken.sol
BabyBuyBackToken		
BabyBuyBackToken		
BabyBuyBackToken		
BabyBuyBackToken		
BabyBuyBackToken		

Mint Check

The project owners of Plankton do 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.

Mint Notes:

Auditor Notes:

Project Owner Notes:

Owner can't mint new coins

Fees Check

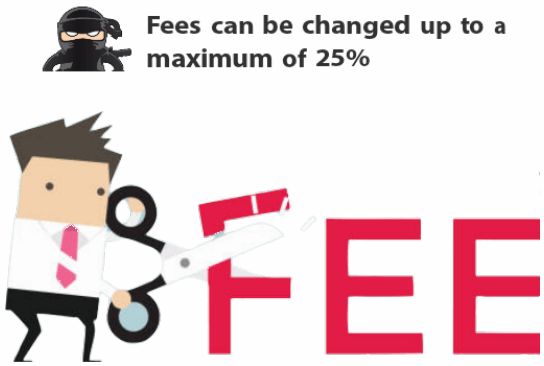
The project owners of Plankton do not have the ability to set fees higher than 25% .

The team May have fees defined; however, they can't set those fees higher than 25% or may not be able to configure the same.

Tax Fee Notes:

Auditor Notes: The contract currently has 10% buy and 10% sale taxes, and cannot be set higher than 25%.

Project Owner Notes:



Blacklist Check

The project owners of Plankton 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 Plankton cannot set max tx amount

The Team allows any investors to swap, transfer or sell their total amount if needed.

MaxTX Notes:

Auditor Notes: ;

Project Owner Notes:

Project Has No MaxTX

Pause Trade Check

The Project Owners of Plankton 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 Plankton 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 0xbb000687721ddf851433187d842021004a731a9d 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.

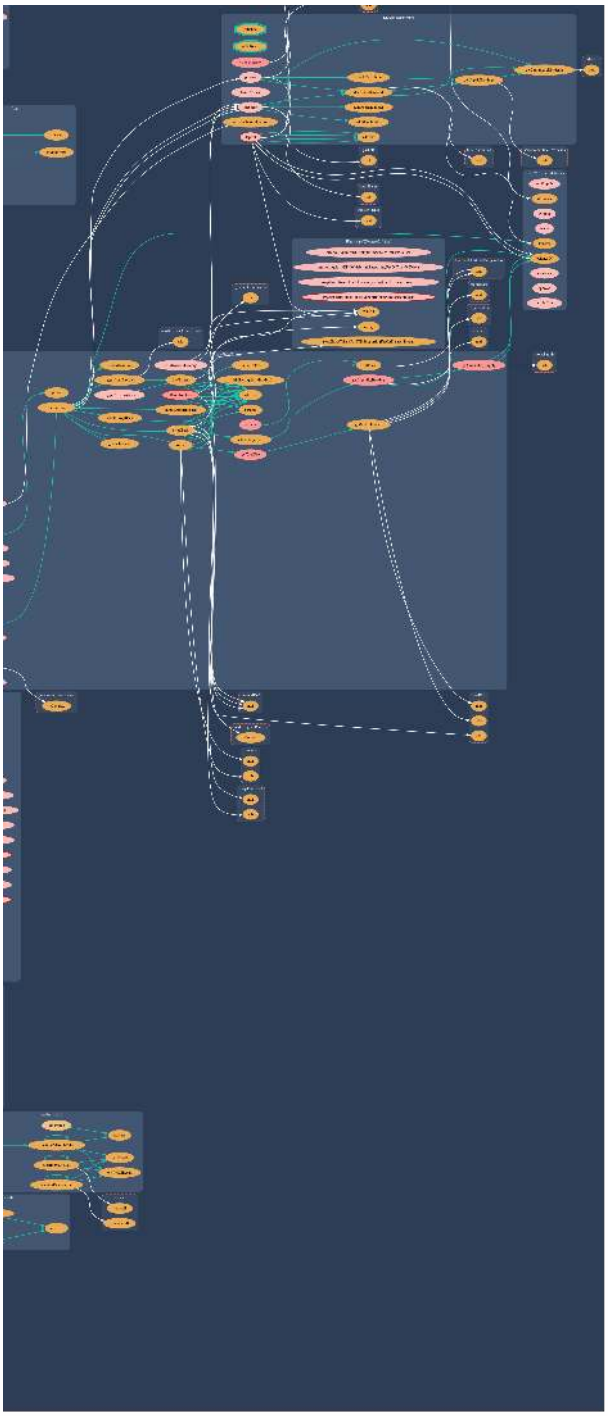
Liquidity Ownership

Most of the liquidity is currently locked; the lock can be seen here:

Liquidity Locker Link can be viewed from:
HERE

Call Graph

The contract for Plankton has the following call graph structure.



KYC Information

The Project Owners of Plankton is not KYC.

KYC Information Notes:

Auditor Notes:

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	BabyBuyBackToken.sol	L: 0 C: 0
SWC-101	Pass	Integer Overflow and Underflow.	BabyBuyBackToken.sol	L: 0 C: 0
SWC-102	Pass	Outdated Compiler Version file.	BabyBuyBackToken.sol	L: 0 C: 0
SWC-103	Pass	A floating pragma is set.	BabyBuyBackToken.sol	L: 0 C: 0
SWC-104	Pass	Unchecked Call Return Value.	BabyBuyBackToken.sol	L: 0 C: 0
SWC-105	Pass	Unprotected Ether Withdrawal.	BabyBuyBackToken.sol	L: 0 C: 0
SWC-106	Pass	Unprotected SELFDESTRUCT Instruction	BabyBuyBackToken.sol	L: 0 C: 0
SWC-107	Pass	Read of persistent state following external call.	BabyBuyBackToken.sol	L: 0 C: 0
SWC-108	Low	State variable visibility is not set..	BabyBuyBackToken.sol	L: 947 C: 12,L: 949 C: 9,L: 1230 C: 9
SWC-109	Pass	Uninitialized Storage Pointer.	BabyBuyBackToken.sol	L: 0 C: 0

ID	Severity	Name	File	location
SWC-110	Pass	Assert Violation.	BabyBuyBackToken.sol	L: 0 C: 0
SWC-111	Pass	Use of Deprecated Solidity Functions.	BabyBuyBackToken.sol	L: 0 C: 0
SWC-112	Pass	Delegate Call to Untrusted Callee.	BabyBuyBackToken.sol	L: 0 C: 0
SWC-113	Pass	Multiple calls are executed in the same transaction.	BabyBuyBackToken.sol	L: 0 C: 0
SWC-114	Pass	Transaction Order Dependence.	BabyBuyBackToken.sol	L: 0 C: 0
SWC-115	Pass	Authorization through tx.origin.	BabyBuyBackToken.sol	L: 0 C: 0
SWC-116	Pass	A control flow decision is made based on The block.timestamp environment variable.	BabyBuyBackToken.sol	L: 0 C: 0
SWC-117	Pass	Signature Malleability.	BabyBuyBackToken.sol	L: 0 C: 0
SWC-118	Pass	Incorrect Constructor Name.	BabyBuyBackToken.sol	L: 0 C: 0
SWC-119	Pass	Shadowing State Variables.	BabyBuyBackToken.sol	L: 0 C: 0
SWC-120	Low	Potential use of block.number as source of randonmness.	BabyBuyBackToken.sol	L: 1567 C: 61,L: 1588 C: 31,L: 1617 C: 31
SWC-121	Pass	Missing Protection against Signature Replay Attacks.	BabyBuyBackToken.sol	L: 0 C: 0
SWC-122	Pass	Lack of Proper Signature Verification.	BabyBuyBackToken.sol	L: 0 C: 0
SWC-123	Pass	Requirement Violation.	BabyBuyBackToken.sol	L: 0 C: 0

ID	Severity	Name	File	location
SWC-124	Pass	Write to Arbitrary Storage Location.	BabyBuyBackToken.sol	L: 0 C: 0
SWC-125	Pass	Incorrect Inheritance Order.	BabyBuyBackToken.sol	L: 0 C: 0
SWC-126	Pass	Insufficient Gas Griefing.	BabyBuyBackToken.sol	L: 0 C: 0
SWC-127	Pass	Arbitrary Jump with Function Type Variable.	BabyBuyBackToken.sol	L: 0 C: 0
SWC-128	Pass	DoS With Block Gas Limit.	BabyBuyBackToken.sol	L: 0 C: 0
SWC-129	Pass	Typographical Error.	BabyBuyBackToken.sol	L: 0 C: 0
SWC-130	Pass	Right-To-Left-Override control character (U +202E).	BabyBuyBackToken.sol	L: 0 C: 0
SWC-131	Pass	Presence of unused variables.	BabyBuyBackToken.sol	L: 0 C: 0
SWC-132	Pass	Unexpected Ether balance.	BabyBuyBackToken.sol	L: 0 C: 0
SWC-133	Pass	Hash Collisions with Multiple Variable Length Arguments.	BabyBuyBackToken.sol	L: 0 C: 0
SWC-134	Pass	Message call with hardcoded gas amount.	BabyBuyBackToken.sol	L: 0 C: 0
SWC-135	Pass	Code With No Effects (Irrelevant/Dead Code).	BabyBuyBackToken.sol	L: 0 C: 0
SWC-136	Pass	Unencrypted Private Data On-Chain.	BabyBuyBackToken.sol	L: 0 C: 0

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

Smart Contract Vulnerability Details

SWC-108 - State Variable Default Visibility

CWE-710: Improper Adherence to Coding Standards

Description:

Labeling the visibility explicitly makes it easier to catch incorrect assumptions about who can access the variable.

Remediation:

Variables can be specified as being public, internal or private. Explicitly define visibility for all state variables.

References:

Ethereum Smart Contract Best Practices - Explicitly mark visibility in functions and state variables

Smart Contract Vulnerability Details

SWC-120 - Weak Sources of Randomness from Chain Attributes

CWE-330: Use of Insufficiently Random Values

Description:

Solidity allows for ambiguous naming of state variables when inheritance is used. Contract A with a variable x could inherit contract B that also has a state variable x defined. This would result in two separate versions of x, one of them being accessed from contract A and the other one from contract B. In more complex contract systems this condition could go unnoticed and subsequently lead to security issues.

Shadowing state variables can also occur within a single contract when there are multiple definitions on the contract and function level.

Remediation:

Using commitment scheme, e.g. RANDAO. Using external sources of randomness via oracles, e.g. Oraclize. Note that this approach requires trusting in oracle, thus it may be reasonable to use multiple oracles. Using Bitcoin block hashes, as they are more expensive to mine.

References:

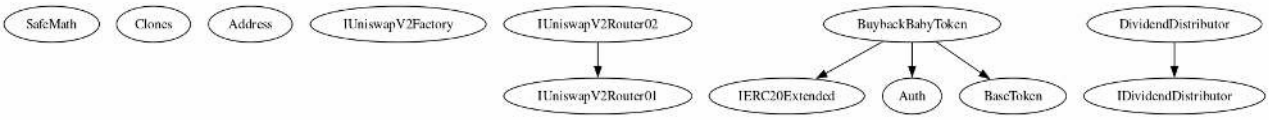
How can I securely generate a random number in my smart contract?)

When can BLOCKHASH be safely used for a random number? When would it be unsafe?

The Run smart contract.

Inheritance

The contract for Plankton 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
transferOwnership	newOwner (address)	public
authorize	address adr	public
unauthorize	address adr	public
triggerZeusBuyback	uint256 amount, bool triggerBuybackMultiplier	external
clearBuybackMultiplier		external
setAutoBuybackSettings	bool _enabled,uint256 _cap,uint256 _amount,uint256 _period	external
setBuybackMultiplierSettings	uint256 numerator,uint256 denominator,uint256 length	external
setIsDividendExempt	address holder, bool exempt	external

Function Name	Parameters	Visibility
setIsFeeExempt	address holder	external
setBuyBacker	address acc, bool add	external
setFees		public
setFeeReceivers	address _marketing FeeReceiver	external
setSwapBackSettings	bool _enabled, uint256 _amount	external
setTargetLiquidity	uint256 _target, uint256 _denominator	external
setDistributionCriteria	uint256 _minPeriod,uint256 _minDistribution	external
setDistributorSettings	uint256 gas	external

Smart Contract Advance Checks

ID	Severity	Name	Result	Status
PLNKTON-01	Minor	Potential Sandwich Attacks.	Pass	Not-Found
PLNKTON-02	Informational	Function Visibility Optimization	Fail	Pending
PLNKTON-03	Minor	Lack of Input Validation.	Fail	Pending
PLNKTON-04	Major	Centralized Risk In addLiquidity.	Pass	Not-Found
PLNKTON-05	Major	Missing Event Emission.	Fail	Pending
PLNKTON-06	Minor	Conformance with Solidity Naming Conventions.	Pass	Not-Found
PLNKTON-07	Minor	State Variables could be Declared Constant.	Pass	Not-Found
PLNKTON-08	Major	Dead Code Elimination.	Pass	Not-Found
PLNKTON-09	Major	Third Party Dependencies.	Pass	Not Found
PLNKTON-10	Major	Initial Token Distribution.	Pass	Not-Found
PLNKTON-11	Critical	distributeTokensBetween Holders is a multisender of tokens from contract.	Pass	Not-Found
PLNKTON-12	Major	Centralization Risks In The X Role	Pass	Not Found
PLNKTON-13	Informational	Extra Gas Cost For User..	Pass	Not-Found

ID	Severity	Name	Result	Status
PLNKTON-14	Medium	Unnecessary Use Of SafeMath	Pass	Not-Found
PLNKTON-15	Medium	Symbol Length Limitation due to Solidity Naming Standards.	Pass	Not-Found
PLNKTON-16	Medium	Invalid collection of Taxes during Transfer.	Pass	Not-Found

PLNKTON-02 | Function Visibility Optimization.

Category	Severity	Location	Status
Gas Optimization	Informational	BabyBuyBackToken.sol: 686,21, 687,21	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
currentIndex		internal
initialized		internal
inSwap		internal
setFees		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.

PLNKTON-03 | Lack of Input Validation.

Category	Severity	Location	Status
Volatile Code	Minor	BabyBuyBackToken.sol: 1582,14	Pending

Description

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

The given input is missing the check for the clearBuybackMultiplier, setIsFeeExempt, setBuyBacker and setDistributionCriteria is 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. clearBuybackMultiplier, setIsFeeExempt, setBuyBacker and setDistributionCriteria is missing required function.

PLNKTON-05 | Missing Event Emission.

Category	Severity	Location	Status
Volatile Code	Major	BabyBuyBackToken.sol: 659, 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.

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	1	0	0
Medium	0	0	0
Minor	1	0	0
Informational	1	0	0
Total	3	0	0

Social Media Checks

Social Media	URL	Result
Twitter	https://twitter.com/CWS_Community	Pass
Other	https://psychophilosophy.gitbook.io/crypto-whale-sharks/	Pass
Website	https://alpha.cryptowhalesharks.com/	Pass
Telegram	https://t.me/+p7YJs5wlf441YWRh	Pass

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	87/100
Auditor Score	85/100
Review by Section	**Score**
Manual Scan Score	37/51
SWC Scan Score	35 /37
Advance Check Score	15 /18

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.
- Project seems to be related to AI.
- Project Owner have experience building and developing projects.
- This is an Ethereum based project, always DYOR, from an Audit perspective it has some limitations and controls.

Auditor Score =85
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.