



CFG NINJA AUDITS

Security Assessment

Thoth Token

May 29, 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 Thoth 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	0xa232c1125602D44e2d51D6352b9a6B5e010f52c2
Name	Thoth
Token Tracker	Thoth (\$TOT)
Decimals	9
Supply	50,000,000,000
Platform	Binance Smart Chain
compiler	v0.8.19+commit.7dd6d404
Contract Name	Thoth
Optimization	Yes with 200 runs
LicenseType	Unlicensed
Language	Solidity
Codebase	https://etherscan.io/token/0xa232c1125602d44e2d51d6352b9a6b5e010f52c2#code
Payment Tx	Corporate



Project Overview

Risk Analysis Summary

Parameter	Result
Buy Tax	4%
Sale Tax	4%
Is honeypot?	Not Detected
Can edit tax?	No
Is anti whale?	Not Detected
Is blacklisted?	Not Detected
Is whitelisted?	Not Detected
Holders	1
Confidence Level	High

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
Thoth	0xa232c1125602D44e2d51D6352b9a6B5e010f52c2	Yes

TestNet Contract Assessed Contract Name

Name	Contract	Live
Thoth	0x38989BC8287D31b49b1450dd85fb1c8E233e28e8	Yes

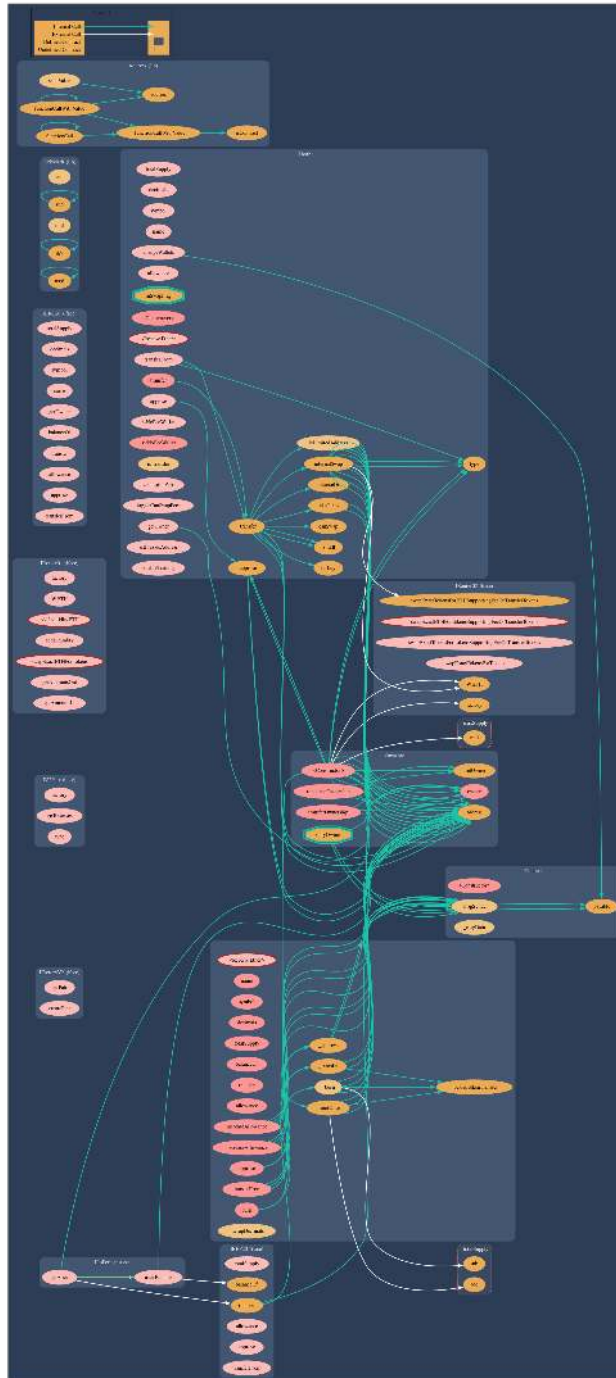
Solidity Code Provided

SolID	File Sha-1	FileName
Thoth	d78898e86fe47f7337d17592c1b2384ba2bd3c32	Thoth.sol
Thoth		
Thoth		



Call Graph

The contract for Thoth has the following call graph structure.



KYC Information

The Project Owners of Thoth 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	Thoth.sol	L: 0 C: 0
SWC-101	Pass	Integer Overflow and Underflow.	Thoth.sol	L: 0 C: 0
SWC-102	Pass	Outdated Compiler Version file.	Thoth.sol	L: 0 C: 0
SWC-103	Low	A floating pragma is set.	Thoth.sol	L: 3 C: 0
SWC-104	Pass	Unchecked Call Return Value.	Thoth.sol	L: 0 C: 0
SWC-105	Pass	Unprotected Ether Withdrawal.	Thoth.sol	L: 0 C: 0
SWC-106	Pass	Unprotected SELFDESTRUCT Instruction	Thoth.sol	L: 0 C: 0
SWC-107	Pass	Read of persistent state following external call.	Thoth.sol	L: 0 C: 0
SWC-108	Pass	State variable visibility is not set..	Thoth.sol	L: 0 C: 0
SWC-109	Pass	Uninitialized Storage Pointer.	Thoth.sol	L: 0 C: 0
SWC-110	Pass	Assert Violation.	Thoth.sol	L: 0 C: 0



ID	Severity	Name	File	location
SWC-111	Pass	Use of Deprecated Solidity Functions.	Thoth.sol	L: 0 C: 0
SWC-112	Pass	Delegate Call to Untrusted Callee.	Thoth.sol	L: 0 C: 0
SWC-113	Pass	Multiple calls are executed in the same transaction.	Thoth.sol	L: 0 C: 0
SWC-114	Pass	Transaction Order Dependence.	Thoth.sol	L: 0 C: 0
SWC-115	Pass	Authorization through tx.origin.	Thoth.sol	L: 0 C: 0
SWC-116	Pass	A control flow decision is made based on The block.timestamp environment variable.	Thoth.sol	L: 0 C: 0
SWC-117	Pass	Signature Malleability.	Thoth.sol	L: 0 C: 0
SWC-118	Pass	Incorrect Constructor Name.	Thoth.sol	L: 0 C: 0
SWC-119	Pass	Shadowing State Variables.	Thoth.sol	L: 0 C: 0
SWC-120	Pass	Potential use of block.number as source of randommness.	Thoth.sol	L: 0 C: 0
SWC-121	Pass	Missing Protection against Signature Replay Attacks.	Thoth.sol	L: 0 C: 0
SWC-122	Pass	Lack of Proper Signature Verification.	Thoth.sol	L: 0 C: 0
SWC-123	Pass	Requirement Violation.	Thoth.sol	L: 0 C: 0
SWC-124	Pass	Write to Arbitrary Storage Location.	Thoth.sol	L: 0 C: 0
SWC-125	Pass	Incorrect Inheritance Order.	Thoth.sol	L: 0 C: 0



ID	Severity	Name	File	location
SWC-126	Pass	Insufficient Gas Griefing.	Thoth.sol	L: 0 C: 0
SWC-127	Pass	Arbitrary Jump with Function Type Variable.	Thoth.sol	L: 0 C: 0
SWC-128	Pass	DoS With Block Gas Limit.	Thoth.sol	L: 0 C: 0
SWC-129	Pass	Typographical Error.	Thoth.sol	L: 0 C: 0
SWC-130	Pass	Right-To-Left-Override control character (U+202E).	Thoth.sol	L: 0 C: 0
SWC-131	Pass	Presence of unused variables.	Thoth.sol	L: 0 C: 0
SWC-132	Pass	Unexpected Ether balance.	Thoth.sol	L: 0 C: 0
SWC-133	Pass	Hash Collisions with Multiple Variable Length Arguments.	Thoth.sol	L: 0 C: 0
SWC-134	Pass	Message call with hardcoded gas amount.	Thoth.sol	L: 0 C: 0
SWC-135	Pass	Code With No Effects (Irrelevant/Dead Code).	Thoth.sol	L: 0 C: 0
SWC-136	Pass	Unencrypted Private Data On-Chain.	Thoth.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-103 - Floating Pragma.

CWE-664: Improper Control of a Resource Through its Lifetime.

References:

Description:

Contracts should be deployed with the same compiler version and flags that they have been tested with thoroughly. Locking the pragma helps to ensure that contracts do not accidentally get deployed using, for example, an outdated compiler version that might introduce bugs that affect the contract system negatively.

Remediation:

Lock the pragma version and also consider known bugs (<https://github.com/ethereum/solidity/releases>) for the compiler version that is chosen.

Pragma statements can be allowed to float when a contract is intended for consumption by other developers, as in the case with contracts in a library or EthPM package. Otherwise, the developer would need to manually update the pragma in order to compile locally.

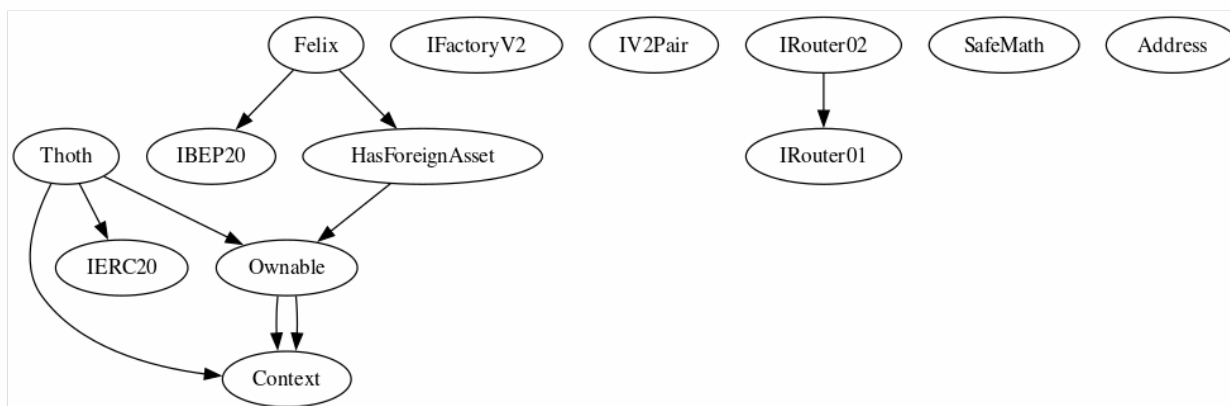
References:

Ethereum Smart Contract Best Practices - Lock pragmas to specific compiler version.



Inheritance

The contract for Thoth 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
setNoFeeWallet	address account, bool enabled	Public
changeLpPair	address newPair	External
toggleCanSwapFees	bool yesno	External
changeWallets	address marketing	External
setPresaleAddress	address presale, bool yesno	External
enableTrading		External



Smart Contract Advance Checks



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



ID	Severity	Name	Result	Status
\$TOT-16	Medium	Invalid collection of Taxes during Transfer.	Pass	Not-Found



\$TOT-02 | Function Visibility Optimization.

Category	Severity	Location	Status
Gas Optimization	 Minor	Thoth.sol: L: 737 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
setNoFeeWallet	address account, bool enabled	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.



\$TOT-03 | Lack of Input Validation.

Category	Severity	Location	Status
Volatile Code	 Major	Thoth.sol: L: 43 C: 14, L: 263 C: 14, L: 296 C: 14, L: 333 C: 14, L: C:	 Pending

Description

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

The given input is missing the check for the a few 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. a few onlyOwners are missing required function.








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	1	0	0
 Informational	1	0	0
Total	2	0	0



Social Media Checks

Social Media	URL	Result
Twitter	https://twitter.com/EduCode_Meta	Pass
Other	https://facebook.com/EduCodeAcademy/	Pass
Website	https://edubits.io/franchise-nfts	Pass
Telegram	https://t.me/edubitscommunity	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	94/100
Auditor Score	85/100
Review by Section	Score
Manual Scan Score	47/50
SWC Scan Score	36 /37
Advance Check Score	11/16

The Following Score System Has been Added to this page to help understand the value of the audit, the maximum score is 100, however to attain that value the project must 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:

- A few vulnerabilities or issues were found during our testing.
- Contract by Freddy.

Auditor Score =85
Audit Passed



Appendix

Finding Categories

Centralization / Privilege

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

Gas Optimization

Gas Optimization findings do not affect the functionality of the code but generate different, more optimal EVM 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 how block.timestamp works.

Control Flow

Control Flow findings concern the access control imposed on functions, such as owner-only functions being 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 may result in a vulnerability.

Coding Style

Coding Style findings usually do not affect the generated byte-code but rather comment on how to make the 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 requirements on the input variables than a setter function.

Coding Best Practices

ERC 20 Coding Standards are a set of rules that each developer should follow to ensure the code meets a set of criteria 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 advocacy 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.

