

# HEXNINJA AUDITS



Security Assessment

**Biwni Token**

July 19, 2022

# Table of Contents

## **1 Audit Summary**

## **2 Project Overview**

### 2.1 Token Summary

### 2.2 Main Contract Assessed

## **3 Smart Contract Vulnerability Checks**

### 3.1 Mint Check

### 3.2 Fees Check

### 3.3 MaxTx Check

### 3.4 Pause Trade Check

## **4 Contract Ownership**

## **5 Liquidity Ownership**

## **6 Important Notes To The Users**

## **7 Social Media Check(Informational)**

## **8 Disclaimer**



# Audit Summary

This report has been prepared for Biwni 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	0xeB1B8c185A6E0A0469020732e2C510bE0Aff6d9C
Name	Biwni
Token Tracker	Biwni (BIWNI)
Decimals	18
Supply	100,000,000
Platform	Binance Smart Chain
compiler	v0.8.4+commit.c7e474f2
Contract Name	StandardToken
Optimization	Yes with 200 runs
LicenseType	MIT
Language	Solidity
Codebase	<a href="https://bscscan.com/address/0xeB1B8c185A6E0A0469020732e2C510bE0Aff6d9C#code">https://bscscan.com/address/0xeB1B8c185A6E0A0469020732e2C510bE0Aff6d9C#code</a>
Payment Tx	0x662fa3959347c4a1b8fe3c699e5729ba060ef3d38f1ea83ce096a6872f83ec8e



# Project Overview

## Risk Analysis Summary

Parameter	Result
Buy Tax	0%
Sale Tax	0%
Is honeypot?	Clean
Can edit tax?	No
Is anti whale?	No
Is blacklisted?	No
Is whitelisted?	No
Holders	Clean
Security Score	90/100
Auditor Score	0/100
Confidence Level	Low

The following quick summary has been added to the project overview, however there are more details about the audit and their results please read every details.



## Main Contract Assessed Contract Name

Name	Contract	Live
Biwni	0xeB1B8c185A6E0A0469020732e2C510bE0Aff6d9C	Yes

## TestNet Contract Assessed Contract Name

Name	Contract	Live
Biwni	0x39Da7B170f7105E3a5EDc0fEb7de8f2AbB291C3C	Yes

## Solidity Code Provided

SolidID	File Sha-1	FileName
StandardToken	01a956d27494e8cdf0f7e8b707a1803e4f986168	StandardToken.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



# Mint Check

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

..

The Project has a Total Supply of 100,000,000 and cannot mint any more than the Max Supply.

.

**Mint Notes:**

**Auditor Notes:** A Mint Function was not found during the code review

**Project Owner Notes:**



**Owner can't mint new coins**





# Fees Check

The Project Owners of Biwni 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%.

**Tax Fee Notes:**

**Auditor Notes:** Contract has no tax.

**Project Owner Notes:** .



**Fees can be changed up to a maximum of 25%**



# MaxTx Check

The Project Onwers of Biwni 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.

MaxTX Notes:

Auditor Notes: No max tx found.

Project Owner Notes:

**Project Has No MaxTX**



# Pause Trade Check

The Project Owners of Biwni 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

**Pause Trade Notes:**

**Auditor Notes:** Not found.

**Project Owner Notes:**



**Owner can't pause trading**



# Contract Ownership

The contract ownership of Biwni 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 `0x5dA5D170464462E6cd93461799ED02Cf5F8cFE9b` which can be viewed from: [HERE](#)

The owner wallet has the power to call the functions displayed on the privileged 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.

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

**Ownership Notes:**

**Auditor Notes:** Owner Wallet received funds from ICCPad Owners Wallet.

**Project Owner Notes:**

# Liquidity Ownership

The token does not have liquidity at the moment of the audit, block 19670560



# KYC Information

The Project Owners of Biwni is not KYC. .

The owner wallet has the power to call the functions displayed on the privileged 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.

## KYC Information Notes:

**Auditor Notes:** Asked project owner about KYC or Doxxed

**Project Owner Notes:** Project owner has no plans to KYC



# Mythx Security Summary Checks

ID	Severity	Name	File	location
SWC-100	Pass	Function Default Visibility	StandardToken.sol	L: 0 C: 0
SWC-101	Pass	Integer Overflow and Underflow.	StandardToken.sol	L: 0 C: 0
SWC-102	Pass	Outdated Compiler Version file.	StandardToken.sol	L: 0 C: 0
SWC-103	Pass	A floating pragma is set.	StandardToken.sol	L: 5 C: 0
SWC-104	Pass	Unchecked Call Return Value.	StandardToken.sol	L: 0 C: 0
SWC-105	Pass	Unprotected Ether Withdrawal.	StandardToken.sol	L: 0 C: 0
SWC-106	Pass	Unprotected SELFDESTRUCT Instruction	StandardToken.sol	L: 0 C: 0
SWC-107	Pass	Read of persistent state following external call.	StandardToken.sol	L: 0 C: 0
SWC-108	Pass	State variable visibility is not set..	StandardToken.sol	L: 0 C: 0
SWC-109	Pass	Uninitialized Storage Pointer.	StandardToken.sol	L: 0 C: 0
SWC-110	Pass	Assert Violation.	StandardToken.sol	L: 0 C: 0
SWC-111	Pass	Use of Deprecated Solidity Functions.	StandardToken.sol	L: 0 C: 0
SWC-112	Pass	Delegate Call to Untrusted Callee.	StandardToken.sol	L: 0 C: 0
SWC-113	Pass	Multiple calls are executed in the same transaction.	StandardToken.sol	L: 0 C: 0



ID	Severity	Name	File	location
SWC-114	Pass	Transaction Order Dependence.	StandardToken.sol	L: 0 C: 0
SWC-115	Pass	Authorization through tx.origin.	StandardToken.sol	L: 474 C: 15
SWC-116	Pass	A control flow decision is made based on The block.timestamp environment variable.	StandardToken.sol	L: 0 C: 0
SWC-117	Pass	Signature Malleability.	StandardToken.sol	L: 0 C: 0
SWC-118	Pass	Incorrect Constructor Name.	StandardToken.sol	L: 0 C: 0
SWC-119	Pass	Shadowing State Variables.	StandardToken.sol	L: 0 C: 0
SWC-120	Pass	Potential use of block.number as source of randomness.	StandardToken.sol	L: 0 C: 0
SWC-121	Pass	Missing Protection against Signature Replay Attacks.	StandardToken.sol	L: 0 C: 0
SWC-122	Pass	Lack of Proper Signature Verification.	StandardToken.sol	L: 0 C: 0
SWC-123	Pass	Requirement Violation.	StandardToken.sol	L: 0 C: 0
SWC-124	Pass	Write to Arbitrary Storage Location.	StandardToken.sol	L: 0 C: 0
SWC-125	Pass	Incorrect Inheritance Order.	StandardToken.sol	L: 0 C: 0
SWC-126	Pass	Insufficient Gas Griefing.	StandardToken.sol	L: 0 C: 0
SWC-127	Pass	Arbitrary Jump with Function Type Variable.	StandardToken.sol	L: 0 C: 0
SWC-128	Pass	DoS With Block Gas Limit.	StandardToken.sol	L: 0 C: 0





ID	Severity	Name	File	location
SWC-129	Pass	Typographical Error.	StandardToken.sol	L: 0 C: 0
SWC-130	Pass	Right-To-Left-Override control character (U+202E).	StandardToken.sol	L: 0 C: 0
SWC-131	Pass	Presence of unused variables.	StandardToken.sol	L: 0 C: 0
SWC-132	Pass	Unexpected Ether balance.	StandardToken.sol	L: 0 C: 0
SWC-133	Pass	Hash Collisions with Multiple Variable Length Arguments.	StandardToken.sol	L: 0 C: 0
SWC-134	Pass	Message call with hardcoded gas amount.	StandardToken.sol	L: 0 C: 0
SWC-135	Pass	Code With No Effects (Irrelevant/Dead Code).	StandardToken.sol	L: 0 C: 0
SWC-136	Pass	Unencrypted Private Data On-Chain.	StandardToken.sol	L: 0 C: 0

We scan the contract for additional security issues using MYTHX and industry standard security scanning tool



# Security Check Details Page

## SWC Information Notes:

Auditor Notes: No Vulnerabilities were found during the security scan, however we did notice they used an older compiler version instead of latest of 0.8.14. Important to read about the bugs associated with 0.7.6 <https://docs.soliditylang.org/en/v0.7.6/bugs.html#>

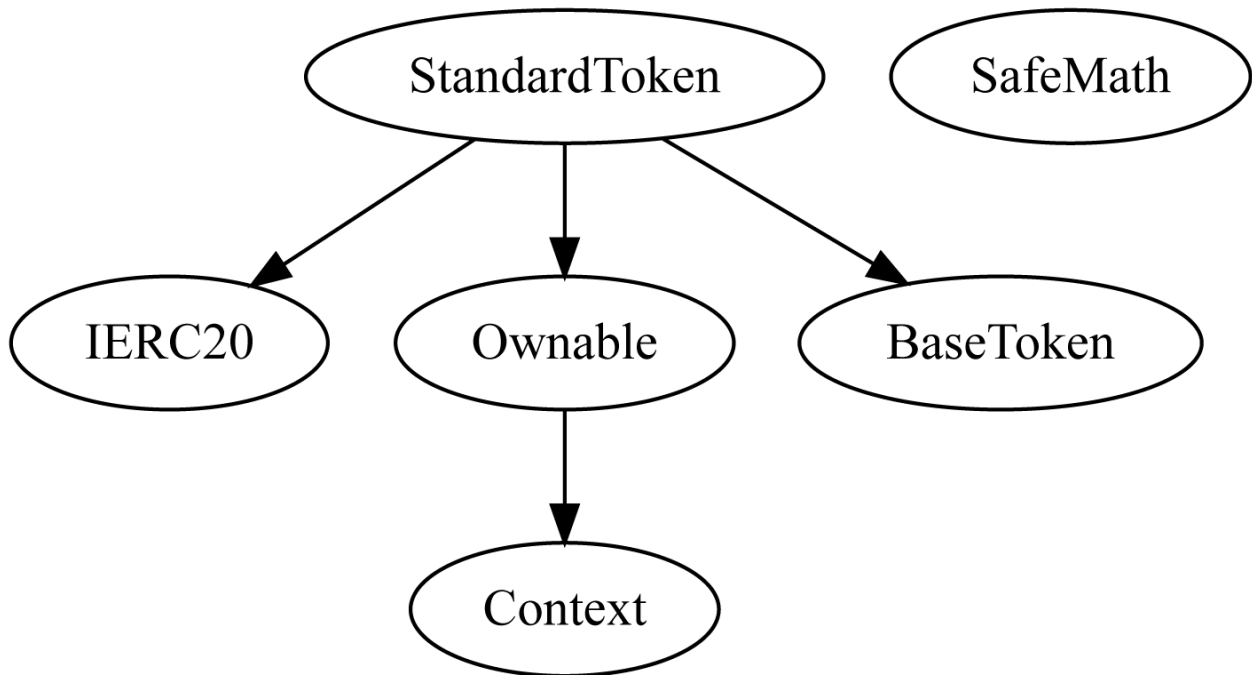
## Project Owner Notes:



# Call Graph and Inheritance

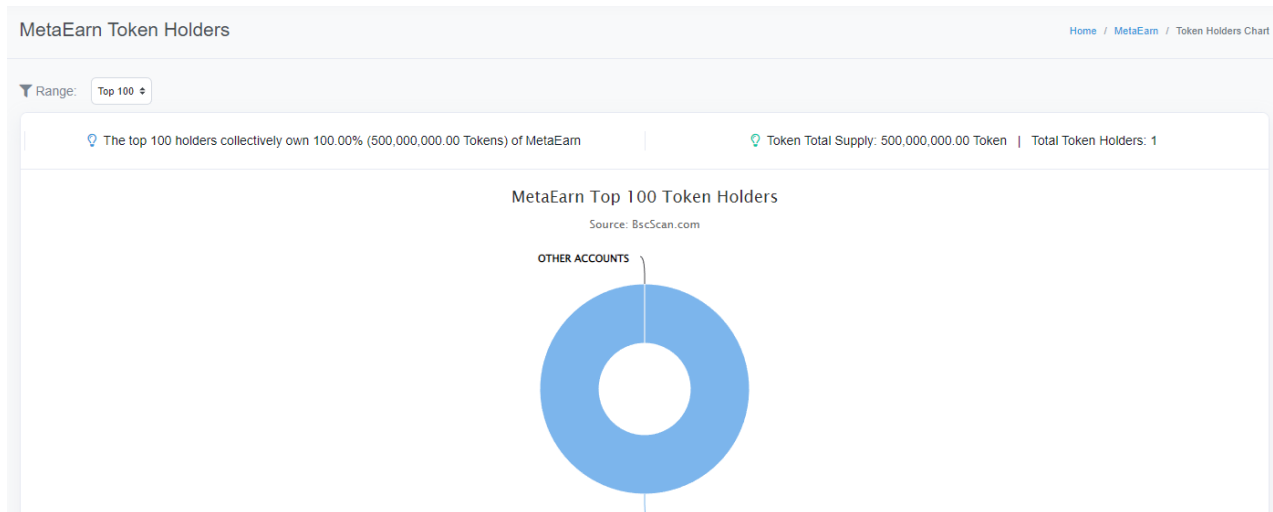
The contract for Biwni has the following call graph structure

The Project has a Total Supply of 100,000,000 and has the following inheritance



# Tokenomics

The contract for Biwni has the following tokenomics



## Privileged Functions (onlyOwner)

Function Name	Parameters	Visibility
<code>renounceOwnership</code>	<code>none</code>	<code>public</code>
<code>transferOwnership</code>	<code>address newOwner</code>	<code>public</code>



## Auditor Final Feedback.

### Important Notes To The Users:

- <https://biwni.com> is not up and running.
- Project Owner state over 500 tokens are listed on the exchange, I was not able to find any evidence of this.
- Owner can't charge 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.
- Customer want to sell 90% of the tokens and reserve 10% for the Team.
- Social media is not present and this can be a red flag during this time.
- Wallet was first seen 7/18/2022 and received funds from Kucoin Wallet, this may not be the project owner's primary wallet.
- We have determined this project may be a scam or scam likely to happen, we are going to fail the security assessment. To be clear there are no issues with the contract, our concerns are more about the lack of information from the project.

### Audit Status



# Social Media Checks

Social Media	URL	Result
Twitter	<a href="https://twitter.com/BiwniExchange">https://twitter.com/BiwniExchange</a>	Pass
Instagram		Fail
Website	<a href="https://biwni.com">https://biwni.com</a>	Fail
Telegram	<a href="https://t.me/BiwniExchange">https://t.me/BiwniExchange</a>	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:** Project Owner states they will have their site up and running soon.





# 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 advocacy 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.

