



# CONTRACT WOLF

**Blockchain Security - Smart Contract Audits**

## Security Assessment

March 1, 2022



<b>Disclaimer</b>	<b>4</b>
<b>Description</b>	<b>6</b>
<b>Engagement</b>	<b>6</b>
<b>Project Engagement</b>	<b>6</b>
<b>Logo</b>	<b>7</b>
<b>Contract Link</b>	<b>7</b>
<b>Risk Level Classification</b>	<b>8</b>
<b>Methodology</b>	<b>9</b>
<b>Used Code from other Frameworks / Smart Contracts (Imports)</b>	<b>10</b>
<b>Description</b>	<b>11</b>
<b>Scope of Work</b>	<b>13</b>
<b>Inheritance Graph</b>	<b>14</b>
<b>Verify Claim</b>	<b>15</b>
<b>Overall Checkup</b>	<b>18</b>
<b>Write Functions of Contract</b>	<b>19</b>
<b>SWC Attack</b>	<b>20</b>
<b>Audit Result</b>	<b>24</b>
<b>Audit Comments</b>	<b>25</b>

# Disclaimer

**ContractWolf.io** audits and reports should not be considered as a form of project's "advertisement" and does not cover any interaction and assessment from "project's contract" to "external contracts" such as Pancakeswap or similar.

**ContractWolf** does not provide any warranty on its released reports.

**ContractWolf** should not be used as a decision to invest into an audited project and is not affiliated nor partners to its audited contract projects.

**ContractWolf** provides transparent report to all its "clients" and to its "clients participants" and will not claim any guarantee of bug-free code within it's **SMART CONTRACT**.

**ContractWolf** presence is to analyze, audit and assess the client's smart contract's code.

Each company or projects should be liable to its security flaws and functionalities.

# Network

Binance Smart Chain (BEP20 Protocol)

## Website

<https://www.shibaimu.com/>



## Description

**Shiba IMU** will set the basis of Web 3.0 – The Meta Universe. The aim is to develop the Web 3.0 ecosystem which will be managed and run 100% by its community. Our founder Yoshi Nakamoto aims to give power back into the hands of internet users. The project is born to facilitate the handover of power back into the hands of the users. It is the ultimate roadmap to internet liberation.

**Shiba IMU** will create an ecosystem which will enable development of decentralized applications. At the heart of the ecosystem will be a search engine where consumers can opt in to sell their search data for a reward. The Shiba IMU token will be used to reward consumers. If the user does not wish to sell their data, then they will have complete privacy of their data in their hands.

## ContractWolf Engagement

1<sup>st</sup> of March 2022, **Shiba IMU** engaged and agrees to audit their smart contract's code by **ContractWolf**. The goal of this engagement was to identify if there is a possibility of security flaws in the implementation of the contract or system.

**ContractWolf** will be focusing on contract issues and functionalities along with the projects claims from smart contract to their website, whitepaper and repository which has been provided by **Shiba IMU**.

## LOGO



## Contract Link:

<https://www.bscscan.com/address/0xab8b2a83d7D14003d4fEa0477c3FD2CE31de110C>

# Risk Level Classification

Risk Level represents the classification or the probability that a certain function or threat that can exploit vulnerability and have an impact within the system or contract.

Risk Level is computed based on CVSS Version 3.0

Level	Value	Vulnerability
<b>Critical</b>	9 - 10	An exposure that can affect the contract functions in several events that can risk and disrupt the contract
<b>High</b>	7 - 8.9	An exposure that can affect the outcome when using the contract that can serve as an opening in manipulating the contract in an unwanted manner
<b>Medium</b>	4 - 6.9	An opening that could affect the outcome in executing the contract in a specific situation
<b>Low</b>	0.1 - 3.9	An opening but doesn't have an impact on the functionality of the contract
<b>Informational</b>	0	An opening that consists of information's but will not risk or affect the contract

# Auditing Approach

Every line of code along with its functionalities will undergo manual review to check its security issues, quality, and contract scope of inheritance. The manual review will be done by our team that will document any issues that there were discovered.

## Methodology

The auditing process follows a routine series of steps:

1. Code review that includes the following:

- Review of the specifications, sources, and instructions provided to ContractWolf to make sure we understand the size, scope, and functionality of the smart contract.
- Manual review of code, our team will have a process of reading the code line-by-line with the intention of identifying potential vulnerabilities and security flaws.

2. Testing and automated analysis that includes:

- Testing the smart contract functions with common test cases and scenarios, to ensure that it returns the expected results.

3. Best practices review, the team will review the contract with the aim to improve efficiency, effectiveness, clarifications, maintainability, security, and control within the smart contract.

4. Recommendations to help the project take steps to secure the smart contract.



# Used Code from other Frameworks/Smart Contracts (Direct Imports)

## Imported Packages

- BurnableTaxToken
- Context
- ERC20
- ERC20Burnable
- IERC20
- IERC20Metadata
- Ownable

# Description

Optimization enabled: No

Version: v0.8.9

Decimal: 18

Symbol: SHIBA

## Capabilities

### Components

Version	Contracts	Libraries	Interfaces	Abstract
1.0	2	0	2	3

### Exposed Functions

Version	Public	Private
1.0	23	9

Version	External	Internal
1.0	9	10

### State Variables

Version	Total	Public
1.0	11	0

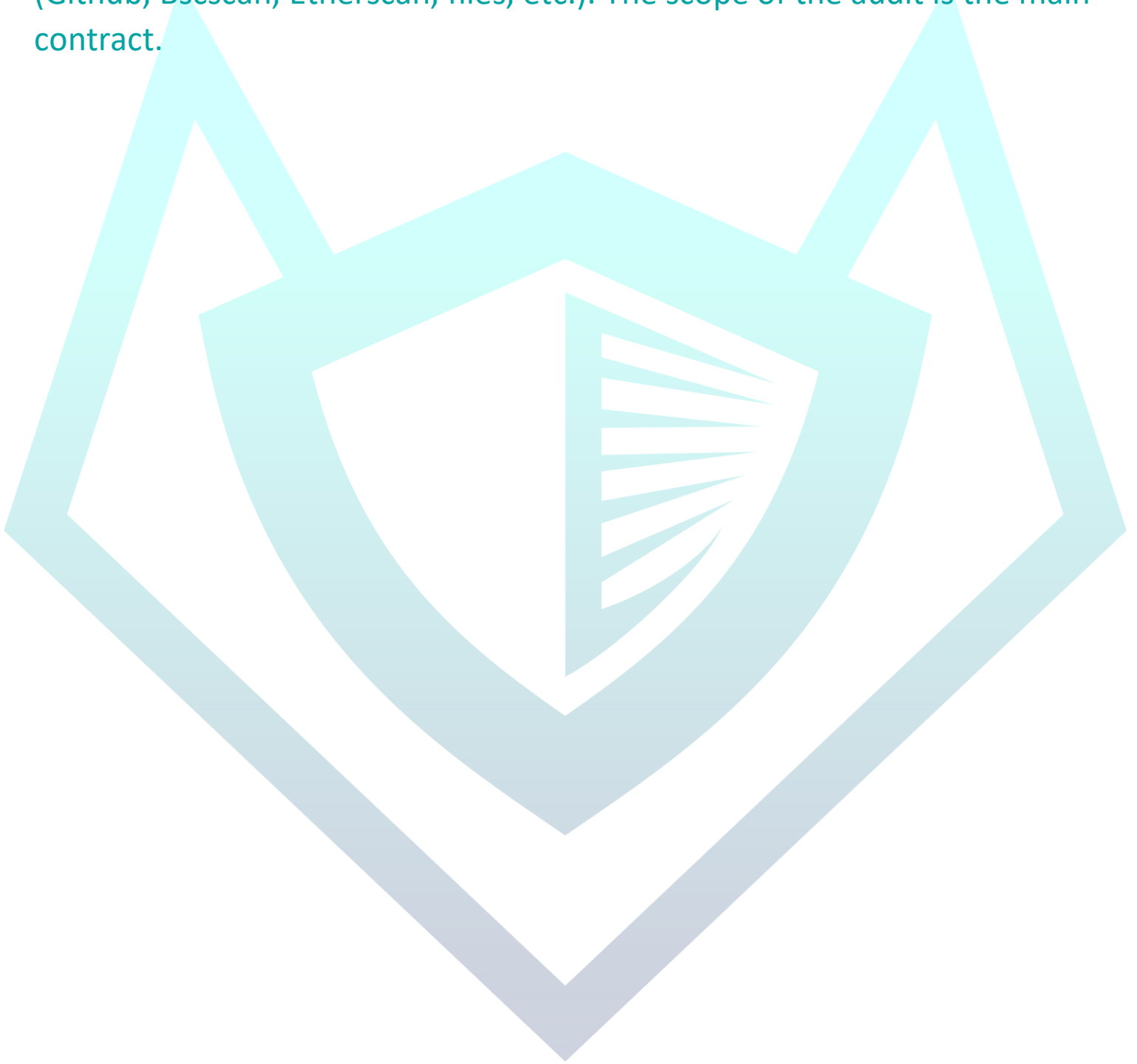
## Capabilities

Version	Solidity Versions Observed	Experimental Features	Can Receive Funds	Uses Assembly	Has Destroyable Contracts
1.0	v0.8.9		Yes	No	No

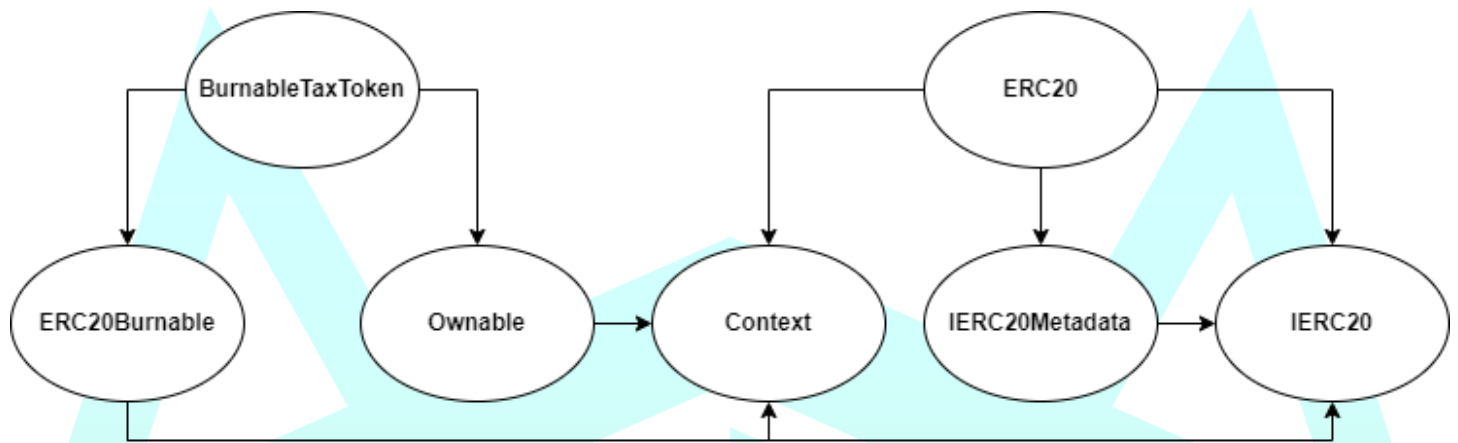


# Scope of Work

**Shiba IMU** team provided us with the files that needs to be tested (Github, Bscscan, Etherscan, files, etc.). The scope of the audit is the main contract.



# Inheritance Graph



# Verify Claims

## Correct implementation of Token Standard

Tested	Verified
✓	✗

Function	Description	Exist	Tested	Verified
TotalSupply	Information about the total coin or token supply	✓	✓	✓
BalanceOf	Details on the account balance from a specified address	✓	✓	✓
Transfer	An action that transfers a specified amount of coin or token to a specified address	✓	✓	✓
TransferFrom	An action that transfers a specified amount of coin or token from a specified address	✓	✓	✓
Approve	Provides permission to withdraw specified number of coin or token from a specified address	✓	✓	✓

## Optional implementation

Function	Description	Exist	Tested	Verified
renounceOwnership	Owner renounce ownership for more trust	✓	✓	✓

## Deployer cannot mint after initial deployment

Statement	Exist	Tested	Verified	File
Deployer cannot mint	✓	✓	✓	✓

Max / Total supply: 1,000,000,000,000,000

## Deployer can burn or lock user funds

Statement	Exist	Tested	Verified
Deployer can burn	✓	✓	✓

## Deployer cannot pause contract

Statement	Exist	Tested	Verified
Deployer cannot pause	—	—	—



# Overall Checkup (Smart Contract Security)

Tested	Verified
✓	✓

## Legend

Attribute	Symbol
Verified / Checked	✓
Partly Verified	X
Unverified / Not checked	🚩
Not Available	—

# Write Functions of Contract

1. approve

2. burn

3. burnFrom

4. decreaseAllowance

5. excludeFromFee

6. includeInFee

7. increaseAllowance

8. renounceOwnership

9. transfer

10. transferFrom

11. transferOwnership

# SWC Attacks

ID	Title	Relationships	Status
<a href="#"><u>SWC-136</u></a>	Unencrypted Private Data On-Chain	<a href="#"><u>CWE-767: Access to Critical Private Variable via Public Method</u></a>	PASSED
<a href="#"><u>SWC-135</u></a>	Code With No Effects	<a href="#"><u>CWE-1164: Irrelevant Code</u></a>	NOT PASSED
<a href="#"><u>SWC-134</u></a>	Message call with hardcoded gas amount	<a href="#"><u>CWE-655: Improper Initialization</u></a>	PASSED
<a href="#"><u>SWC-133</u></a>	Hash Collisions with Multiple Variable Length Arguments	<a href="#"><u>CWE-294: Authentication Bypass by Capture-replay</u></a>	PASSED
<a href="#"><u>SWC-132</u></a>	Unexpected Ether balance	<a href="#"><u>CWE-667: Improper Locking</u></a>	PASSED
<a href="#"><u>SWC-131</u></a>	Presence of unused variables	<a href="#"><u>CWE-1164: Irrelevant Code</u></a>	PASSED
<a href="#"><u>SWC-130</u></a>	Right-To Left Override control character (U+202E)	<a href="#"><u>CWE-451: User Interface (UI) Misrepresentation of Critical Information</u></a>	PASSED
<a href="#"><u>SWC-129</u></a>	Typographical Error	<a href="#"><u>CWE-480: Use of Incorrect Operator</u></a>	PASSED

<a href="#"><u>SWC-128</u></a>	DoS With Block Gas Limit	<a href="#"><u>CWE-400: Uncontrolled Resource Consumption</u></a>	<b>PASSED</b>
<a href="#"><u>SWC-127</u></a>	Arbitrary Jump with Function Type Variable	<a href="#"><u>CWE-695: Use of Low-Level Functionality</u></a>	<b>PASSED</b>
<a href="#"><u>SWC-125</u></a>	Incorrect Inheritance Order	<a href="#"><u>CWE-696: Incorrect Behavior Order</u></a>	<b>PASSED</b>
<a href="#"><u>SWC-124</u></a>	Write to Arbitrary Storage Location	<a href="#"><u>CWE-123: Write-what-where Condition</u></a>	<b>PASSED</b>
<a href="#"><u>SWC-123</u></a>	Requirement Violation	<a href="#"><u>CWE-573: Improper Following of Specification by Caller</u></a>	<b>PASSED</b>
<a href="#"><u>SWC-122</u></a>	Lack of Proper Signature Verification	<a href="#"><u>CWE-345: Insufficient Verification of Data Authenticity</u></a>	<b>PASSED</b>
<a href="#"><u>SWC-121</u></a>	Missing Protection against Signature Replay Attacks	<a href="#"><u>CWE-347: Improper Verification of Cryptographic Signature</u></a>	<b>PASSED</b>
<a href="#"><u>SWC-120</u></a>	Weak Sources of Randomness from Chain Attributes	<a href="#"><u>CWE-330: Use of Insufficiently Random Values</u></a>	<b>PASSED</b>
<a href="#"><u>SWC-119</u></a>	Shadowing State Variables	<a href="#"><u>CWE-710: Improper Adherence to Coding Standards</u></a>	<b>PASSED</b>

<a href="#"><u>SWC-118</u></a>	Incorrect Constructor Name	<a href="#"><u>CWE-665: Improper Initialization</u></a>	<b>PASSED</b>
<a href="#"><u>SWC-117</u></a>	Signature Malleability	<a href="#"><u>CWE-347: Improper Verification of Cryptographic Signature</u></a>	<b>PASSED</b>
<a href="#"><u>SWC-116</u></a>	Timestamp Dependence	<a href="#"><u>CWE-829: Inclusion of Functionality from Untrusted Control Sphere</u></a>	<b>PASSED</b>
<a href="#"><u>SWC-115</u></a>	Authorization through tx.origin	<a href="#"><u>CWE-477: Use of Obsolete Function</u></a>	<b>PASSED</b>
<a href="#"><u>SWC-114</u></a>	Transaction Order Dependence	<a href="#"><u>CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')</u></a>	<b>PASSED</b>
<a href="#"><u>SWC-113</u></a>	DoS with Failed Call	<a href="#"><u>CWE-703: Improper Check or Handling of Exceptional Conditions</u></a>	<b>PASSED</b>
<a href="#"><u>SWC-112</u></a>	Delegate call to Untrusted Callee	<a href="#"><u>CWE-829: Inclusion of Functionality from Untrusted Control Sphere</u></a>	<b>PASSED</b>
<a href="#"><u>SWC-110</u></a>	Assert Violation	<a href="#"><u>CWE-670: Always-Incorrect Control Flow Implementation</u></a>	<b>PASSED</b>

<a href="#"><u>SWC-109</u></a>	Uninitialized Storage Pointer	<a href="#"><u>CWE-824: Access of Uninitialized Pointer</u></a>	<b>PASSED</b>
<a href="#"><u>SWC-108</u></a>	State Variable Default Visibility	<a href="#"><u>CWE-710: Improper Adherence to Coding Standards</u></a>	<b>PASSED</b>
<a href="#"><u>SWC-107</u></a>	Reentrancy	<a href="#"><u>CWE-841: Improper Enforcement of Behavioral Workflow</u></a>	<b>PASSED</b>
<a href="#"><u>SWC-106</u></a>	Unprotected SELFDESTRUCT Instruction	<a href="#"><u>CWE-284: Improper Access Control</u></a>	<b>PASSED</b>
<a href="#"><u>SWC-105</u></a>	Unprotected Ether Withdrawal	<a href="#"><u>CWE-284: Improper Access Control</u></a>	<b>PASSED</b>
<a href="#"><u>SWC-104</u></a>	Unchecked Call Return Value	<a href="#"><u>CWE-252: Unchecked Return Value</u></a>	<b>PASSED</b>
<a href="#"><u>SWC-103</u></a>	Floating Pragma	<a href="#"><u>CWE-664: Improper Control of a Resource Through its Lifetime</u></a>	<b>PASSED</b>
<a href="#"><u>SWC-102</u></a>	Outdated Compiler Version	<a href="#"><u>CWE-937: Using Components with Known Vulnerabilities</u></a>	<b>PASSED</b>
<a href="#"><u>SWC-101</u></a>	Integer Overflow and Underflow	<a href="#"><u>CWE-682: Incorrect Calculation</u></a>	<b>PASSED</b>
<a href="#"><u>SWC-100</u></a>	Function Default Visibility	<a href="#"><u>CWE-710: Improper Adherence to Coding Standards</u></a>	<b>PASSED</b>

# AUDIT PASSED

## **Critical Issues**

No critical issues found

## **High Issues**

No high issues found

## **Medium Issues**

No medium issues found

## **Low Issues**

No medium issues found

## **Informational Issues**

No informational issues found

## **Function Issues**

No informational issues found

# Audit Comments

- Deployer can renounce ownership
- Deployer cannot pause the contract
- Deployer cannot mint after initial deployment
- Deployer can burn

