

The background of the slide features a complex network diagram. It consists of numerous small, light-gray circular nodes connected by thin, light-gray lines, creating a web-like structure. The nodes are distributed across the entire slide, with a higher density in the upper right and lower right areas. The overall color scheme is dark, with the network lines and nodes providing a subtle contrast against the black background.

**onweb3**

# Smart Contract Security Audit



# SHIBAFAM

ONWEB3 received the application for a smart contract security audit of SHIBAFAM on Feb 17, 2022. The following are the details and results of this smart contract security audit:

Token Name: SHIBAFAM (SHFM)

Contract address: [0xd099d86f862f42632bbfb8a64015f0a1f073dfed](https://www.onweb3.co/0xd099d86f862f42632bbfb8a64015f0a1f073dfed)

The audit items and results: (Other unknown security vulnerabilities are not included in the audit responsibility scope)

Audit Result: Passed

KYC Verification: Not verified

Audit Number: OW3029319112022

Audit Date: FEB 19, 2022

Audit Team: ONWEB3

<https://www.onweb3.co/>

## Table of Content

Introduction.....	4
Auditing Approach and Methodologies applied.....	4
Audit Details.....	4
Audit Goals.....	5
Security.....	5
Sound Architecture.....	5
Code Correctness and Quality .....	5
Security.....	5
High level severity issues.....	5
Medium level severity issues.....	5
Low level severity issues.....	6
Manual Audit .....	7
Critical level severity issues.....	7
High level severity issues.....	7
Medium level severity issues.....	7
Low level severity issues.....	7
Automated Audit.....	8
Remix Compiler Warnings.....	8
Disclaimer.....	9
Summary .....	10

## **Introduction**

This Audit Report mainly focuses on the overall security of SHIBAFAM Smart Contract. With this report, we have tried to ensure the reliability and correctness of their smart contract by complete and rigorous assessment of their system's architecture and the smart contract codebase.

## **Auditing Approach and Methodologies applied**

The ONWEB3 team has performed rigorous testing of the project starting with analyzing the code design patterns in which we reviewed the smart contract architecture to ensure it is structured and safe use of third-party smart contracts and libraries. Our team then performed a formal line by line inspection of the Smart Contract to find any potential issue like race conditions, transaction-ordering dependence, timestamp dependence, and denial of service attacks. In the Unit testing Phase, we coded/conducted custom unit tests written for each function in the contract to verify that each function works as expected. In Automated Testing, we tested the Smart Contract with our in-house developed tools to identify vulnerabilities and security flaws. The code was tested in collaboration of our multiple team members and this included -

- Testing the functionality of the Smart Contract to determine proper logic has been followed throughout the whole process.
- Analyzing the complexity of the code in depth and detailed, manual review of the code, lineby-line.
- Deploying the code on testnet using multiple clients to run live tests.
- Analyzing failure preparations to check how the Smart Contract performs in case of any bugs and vulnerabilities.
- Checking whether all the libraries used in the code are on the latest version.
- Analyzing the security of the on-chain data.

## **Audit Details**

Project Name: SHIBAFAM

Website: <https://shibafam.co/>

Platform: Binance Smart Chain

Type of Token: BEP20

Languages: Solidity (Smart contract) Platforms and Tools: Remix IDE, Truffle, Truffle Team, Ganache, Solhint, VScode, Mythril, Contract Library

## **Audit Goals**

The focus of the audit was to verify that the Smart Contract System is secure, resilient and working according to the specifications. The audit activities can be grouped in the following three categories:

**Security** Identifying security related issues within each contract and the system of contract.

**Sound Architecture** Evaluation of the architecture of this system through the lens of established smart contract best practices and general software best practices.

**Code Correctness and Quality** A full review of the contract source code. The primary areas of focus include:

- Accuracy
- Readability
- Sections of code with high complexity
- Quantity and quality of test coverage

**Issue Categories** Every issue in this report was assigned a severity level from the following:

**High level severity** issues Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

**Medium level severity issues** Issues on this level could potentially bring problems and should eventually be fixed.

**Low level severity issues** Issues on this level are minor details and warnings that can remain unfixed but would be better fixed at some point in the future.

Number of issues per severity

Level	High	Medium	Low
Note	0	0	0

Issues Checking Status

№	Issue description	Checking status
1	Compiler warnings.	passed
2	Race conditions and Reentrancy. Cross-function race conditions	passed
3	Possible delays in data delivery	passed
4	Oracle calls	passed
5	Front running	passed
6	Timestamp dependence	passed
7	Integer Overflow and Underflow	passed
8	DoS with Revert	passed
9	DoS with block gas limit	passed
10	Methods execution permissions	passed
11	Economy model	passed
12	The impact of the exchange rate on the logic	passed
13	Private user data leaks	passed
14	Malicious Event log	passed
15	Scoping and Declarations	passed
16	Uninitialized storage pointers	passed
17	Arithmetic accuracy	passed
18	Design Logic	passed
19	Cross-function race conditions	passed
20	Safe Zeppelin module	passed
21	Fallback function security	passed

**Manual Audit:** For this section the code was tested/read line by line by our developers. We also used Remix IDE's JavaScript VM and Kovan networks to test the contract functionality.

**Critical Severity Issues** No critical severity issues found.

**High Severity Issues** No high severity issues found.

**Medium Severity Issues** No medium severity issues found.

**Low Severity Issues** No low severity issues found.

## **Automated Audit**

### **Remix Compiler Warnings**

It throws warnings by Solidity's compiler. If it encounters any errors the contract cannot be compiled and deployed. No issues found.



**Disclaimer**

This is a limited report on our findings based on our analysis, in accordance with good industry practice as at the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, the details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report. While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the below disclaimer below – please make sure to read it in full. **DISCLAIMER:** By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice. No one shall have any right to rely on the report or its contents, and ONWEB3 and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (ONWEB3) owe no duty of care towards you or any other person, nor does ONWEB3 make any warranty or representation to any person on the accuracy or completeness of the report. The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and ONWEB3 hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, ONWEB3 hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against ONWEB3, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report. The analysis of the security is purely based on the smart contracts alone. No applications or operations were reviewed for security. No product code has been reviewed

**Summary**

*Smart contracts do not contain any high severity issues.*

Note: Please check the disclaimer above and note, the audit makes no statements or warranties on business model, investment attractiveness or code sustainability. The report is provided for the only contract mentioned in the report.