CONTRACT WOLF

Blockchain Security - Smart Contract Audits

Security Assessment

February 19, 2022

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 its **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.

Scope of Work

Blue Lobster Money team agreed and provided us with the files that needs to be tested (Github, Bscscan, Etherscan, files, etc.). The scope of the audit is the main contract.

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 **Blue Lobster Money**.

Description

Algo-stable asset via seigniorage on Arbitrum - first of its type.

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
Critical	9 - 10	An Exposure that can affect the contract functions in several events that can risk and disrupt the contract
High	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
Medium	4 - 6.9	An opening that could affect the outcome in executing the contract in a specific situation
Low	0.1 - 3.9	An opening but doesn't have an impact on the functionality of the contract
Informational	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

- IBoardroom
- IOracle
- IBasisAsset
- ContractGuard
- Context
- Ownable
- Operator
- Babylonian
- ReentrancyGuard
- IERC20
- Address
- SafeMath
- SafeERC20
- Math
- Treasury

Description

Optimization enabled: Yes

Capabilities

Components

Version	Contracts	Libraries	Interfaces	Abstract
1.0	3	5	4	2

Exposed Functions

Version	Public	Private	External	Internal
1.0	17	2	56	43

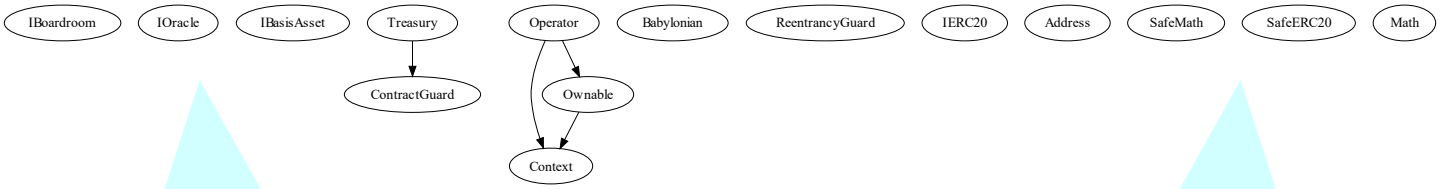
State Variables

Version	Total	Public
1.0	12	36

Capabilities

Version	Solidity Versions Observed	Experimental Features	Can Receive Funds	Uses Assembly	Has Destroyable Contracts
1.0	v0.6.12		Yes	Yes	No

Inheritance Graph



Correct implementation of Token Standard

Tested	Verified
✓	✓

Overall Checkup (Smart Contract Security)

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	✓	✓	✓

Verify Claims

Statement	Exist	Tested	Owner
Renounce Ownership	✓	✓	✓
Mint	✓	✓	✗
Burn	✓	✓	✗
Block	–	–	–
Pause	–	–	–

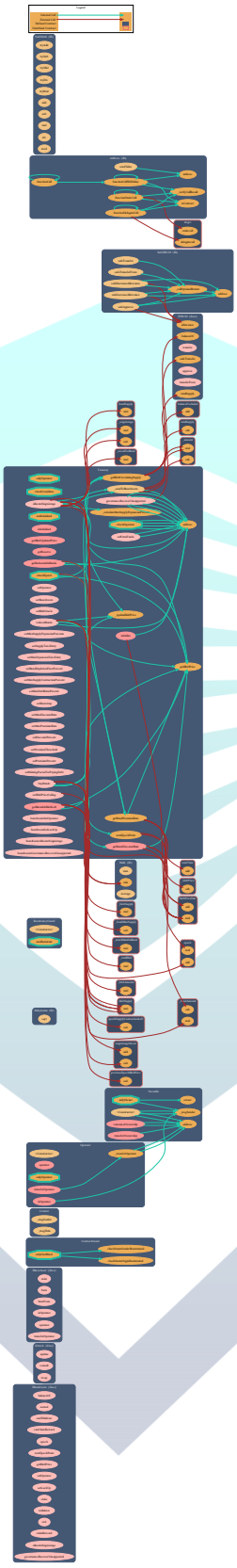
Legend

Attribute	Symbol
Verified / Can	✓
Verified / Cannot	✗
Unverified / Not checked	⚑
Not Available	–

Write Functions of Contract

1. allocateSeigniorage (0x5b756179)
2. boardroomAllocateSeigniorage (0x01a93783)
3. boardroomGovernanceRecoverUnsupported (0xa3ec30fe)
4. boardroomSetLockUp (0xf8cd4d72)
5. boardroomSetOperator (0xb06ce14a)
6. buyBonds (0x54f04a11)
7. governanceRecoverUnsupported (0x54575af4)
8. initialize (0x95b6ef0c)
9. redeemBonds (0x118ebbf9)
10. setBlobOracle (0x6247a113)
11. setBlobPriceCeiling (0xd06cdfe9)
12. setBoardroom (0xb3ffc777)
13. setBondDepletionFloorPercent (0x8c664db6)
14. setBootstrap (0x91bbfed5)
15. setDiscountPercent (0x154ec2db)
16. setExtraFunds (0xbcc81f19)
17. setMaxDebtRatioPercent (0x591663e1)
18. setMaxDiscountRate (0x98b762a1)
19. setMaxExpansionTiersEntry (0xd4b14944)
20. setMaxPremiumRate (0xa204452b)
21. setMaxSupplyContractionPercent (0xcecce38e)
22. setMaxSupplyExpansionPercents (0x0b5bcec7)
23. setMintingFactorForPayingDebt (0x499f3f19)
24. setOperator (0xb3ab15fb)
25. setPremiumPercent (0x40af7ba5)
26. setPremiumThreshold (0x04e5c7b1)
27. setSupplyTiersEntry (0x940e6064)

Call Graph



SWC Attacks

ID	Title	Status
SWC-136	Unencrypted Private Data On-Chain	PASSED
SWC-135	Code With No Effects	PASSED
SWC-134	Message call with hardcoded gas amount	PASSED
SWC-133	Hash Collisions with Multiple Variable Length Arguments	PASSED
SWC-132	Unexpected Ether balance	PASSED
SWC-131	Presence of unused variables	PASSED
SWC-130	Right-To Left Override control character (U+202E)	PASSED
SWC-129	Typographical Error	PASSED
SWC-128	DoS With Block Gas Limit	PASSED
SWC-127	Arbitrary Jump with Function Type Variable	PASSED
SWC-126	Insufficient Gas Griefing	PASSED
SWC-125	Incorrect Inheritance Order	PASSED
SWC-124	Write to Arbitrary Storage Location	PASSED
SWC-123	Requirement Violation	PASSED
SWC-122	Lack of Proper Signature Verification	PASSED
SWC-121	Missing Protection against Signature Replay Attacks	PASSED
SWC-120	Weak Sources of Randomness from Chain Attributes	PASSED
SWC-119	Shadowing State Variables	PASSED
SWC-118	Incorrect Constructor Name	PASSED
SWC-117	Signature Malleability	PASSED
SWC-116	Block values as a proxy for time	PASSED
SWC-115	Authorization through tx.origin	PASSED
SWC-114	Transaction Order Dependence	PASSED
SWC-113	DoS with Failed Call	PASSED
SWC-112	Delegate call to Untrusted Callee	PASSED
SWC-111	Use of Deprecated Solidity Functions	PASSED

SWC-110	Assert Violation	**PASSED**
SWC-109	Uninitialized Storage Pointer	**PASSED**
SWC-108	State Variable Default Visibility	**PASSED**
SWC-107	Reentrancy	**PASSED**
SWC-106	Unprotected SELFDESTRUCT Instruction	**PASSED**
SWC-105	Unprotected Ether Withdrawal	**PASSED**
SWC-104	Unchecked Call Return Value	**PASSED**
SWC-103	Floating Pragma	**PASSED**
SWC-102	Outdated Compiler Version	**PASSED**
SWC-101	Integer Overflow and Underflow	**PASSED**
SWC-100	Function Default Visibility	**PASSED**

Audit Result

AUDIT PASSED

Critical Issues

No critical issues found

High Issues

No high issues found

Medium Issues

No medium issues found

Low Issues

No low issues found

Informational Issues

No informational issues found

Function Issues

No informational issues found

Audit Comments

- Owner can renounce and transfer ownership
- Owner can change operator address
- Operator can transfer operator role
- Operator can change boardroom address
- Operator can change oracle address
- Operator can change BLOB price ceiling amount
- Operator can change max supply expansion percentage between .1% and 10%
- Operator can update supply tier entry
- Operator can update max expansion tier entry
- Operator can update bond depletion floor percentage between 5% and 100%
- Operator can change max supply contraction percentage between .1% and 15%
- Operator can change max debt ratio percentage between 10% and 100%
- Operator can update bootstrap settings
- Operator can update extra funds settings
- Operator can update max discount rate amount
- Operator can update max premium rate amount
- Operator can update premium threshold not higher than 1.5
- Operator can update premium percentage not higher than 200%
- Operator can update minting factor for paying debt between 100% and 200%
- Operator can collect foreign tokens from contract
- Operator can update boardroom operator address
- Operator can update boardroom set lock up settings
- Operator can allocate seignorage from boardroom
- Owner cannot mint after initial deployment
- Owner cannot burn tokens
- Owner cannot block users
- Owner cannot pause contract

CONTRACTWOLF

Blockchain Security - Smart Contract Audits