



# CONTRACT WOLF

**Blockchain Security - Smart Contract Audits**



## **Security Assessment**

February 11, 2022

<b>Disclaimer</b>	<b>3</b>
<b>Scope of Work &amp; Engagement</b>	<b>3</b>
<b>Project Description</b>	<b>4</b>
<b>Risk Level Classification</b>	<b>5</b>
<b>Methodology</b>	<b>6</b>
<b>Used Code from other Frameworks / Smart Contracts (Imports)</b>	<b>7</b>
<b>Token Description</b>	<b>8</b>
<b>Inheritance Graph</b>	<b>9</b>
<b>Overall Checkup</b>	<b>10</b>
<b>Verify Claim</b>	<b>11</b>
<b>Write Functions of Contract</b>	<b>12</b>
<b>Call Graph</b>	<b>13</b>
<b>SWC Attacks</b>	<b>14</b>
<b>Audit Result</b>	<b>16</b>
<b>Findings</b>	<b>17</b>
<b>Audit Comments</b>	<b>18</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 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

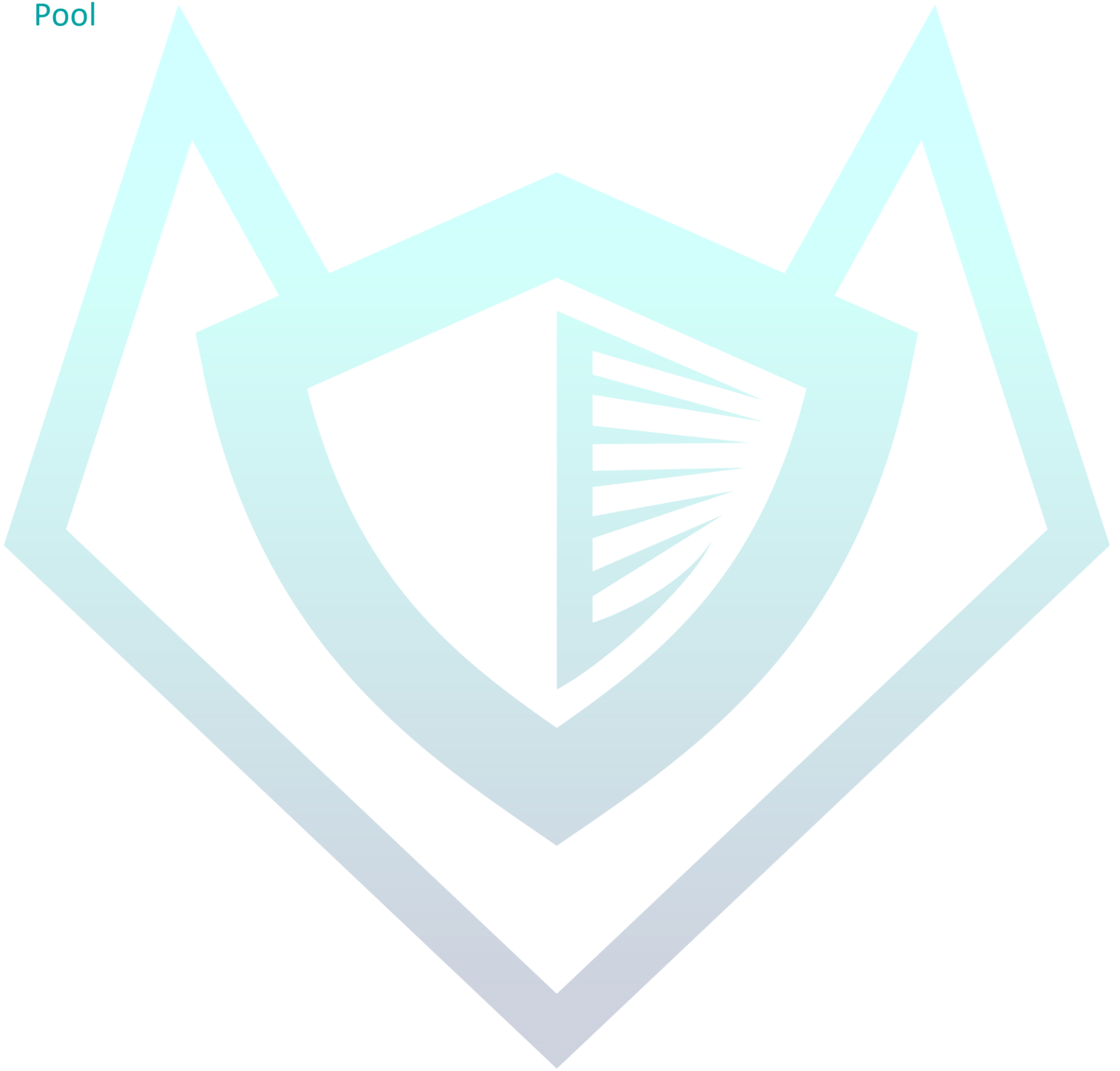
**Blue Lobster Money** team agreed and provided us with the files that needs to be tested (Github, Bscscan, Etherscan, files, etc.). The scope of the audit is the main contract.

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. Genesis Pool



# 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

- IOracle
- SafeMath8
- Math
- IERC20
- SafeMath
- Context
- Ownable
- Operator
- ERC20
- ERC20Burnable
- Blob

## Description

Optimization enabled: Yes

Decimal: 18

Symbol: BLOB

Max / Total Supply: 19,000

## Capabilities

### Components

Version	Contracts	Libraries	Interfaces	Abstract
1.0	3	3	2	3

### Exposed Functions

Version	Public	Private	External	Internal
1.0	24	0	11	36

### State Variables

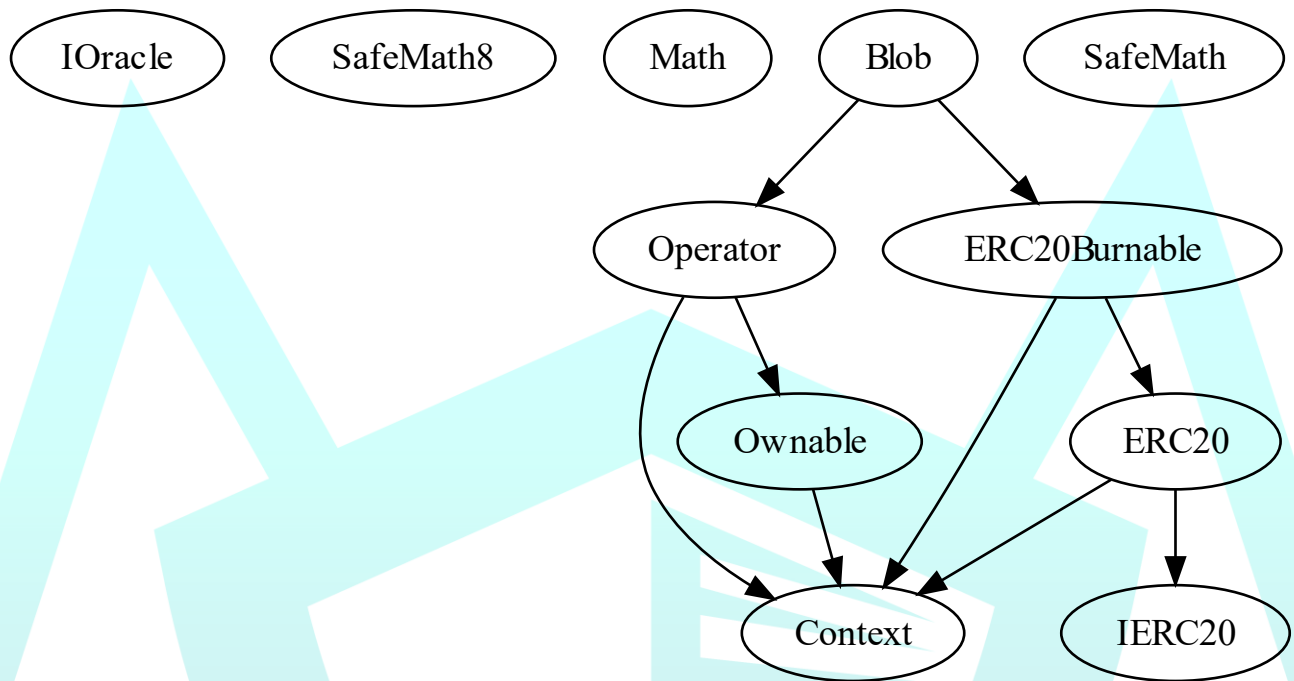
Version	Total	Public
1.0	12	4

### Capabilities

Version	Solidity Versions Observed	Experimental Features	Can Receive Funds	Uses Assembly	Has Destroyable Contracts
1.0	v0.6.12		Yes	No	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	X
Unverified / Not checked	🚩
Not Available	—

# Write Functions of Contract

1. approve (0x095ea7b3)

2. burn (0x42966c68)

3. burnFrom (0x79cc6790)

4. decreaseAllowance (0xa457c2d7)

5. distributeReward (0xf4fd47cf)

6. governanceRecoverUnsupported (0x54575af4)

7. increaseAllowance (0x39509351)

8. mint (0x40c10f19)

9. renounceOwnership (0x715018a6)

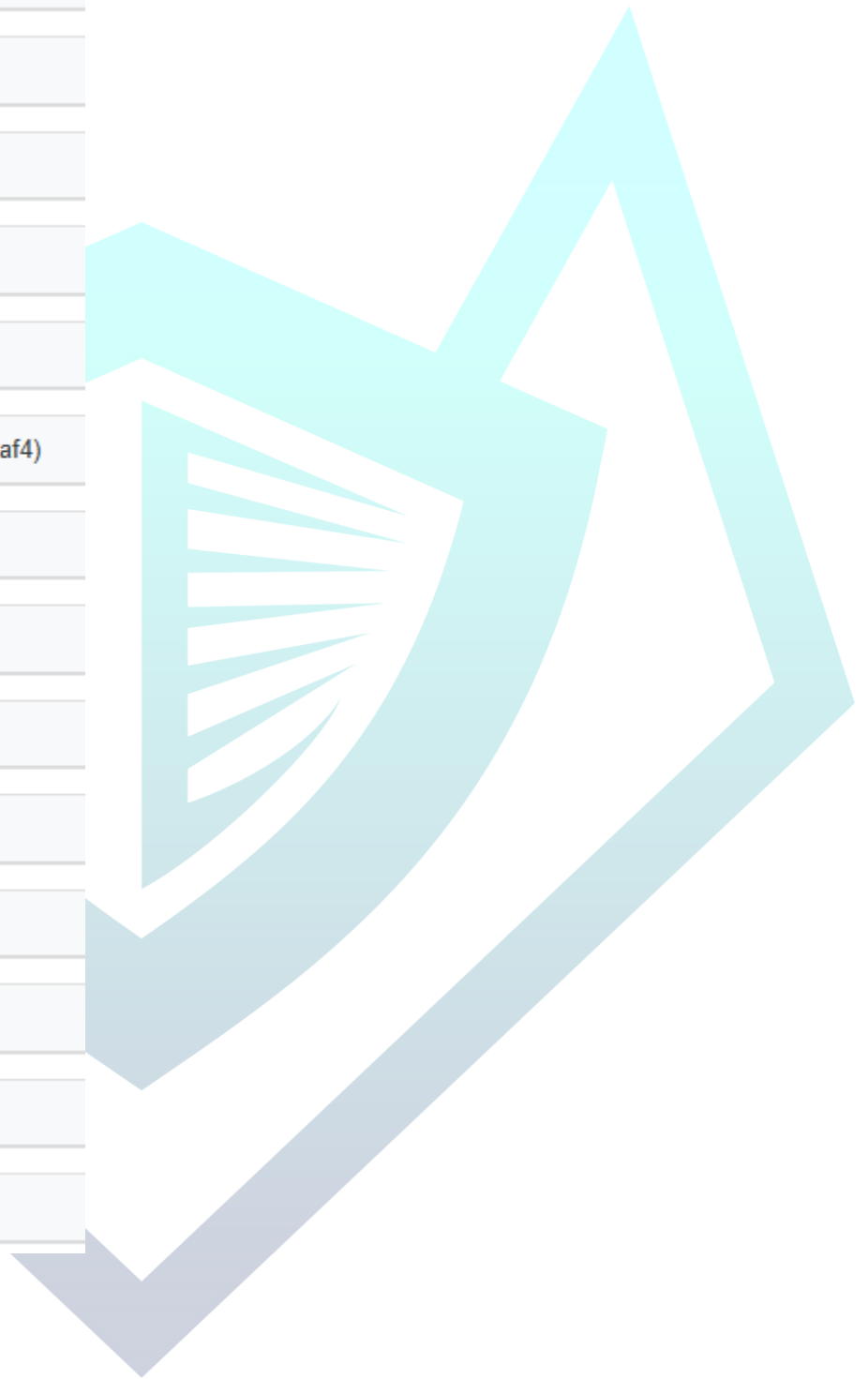
10. setBlobOracle (0x6247a113)

11. transfer (0xa9059cbb)

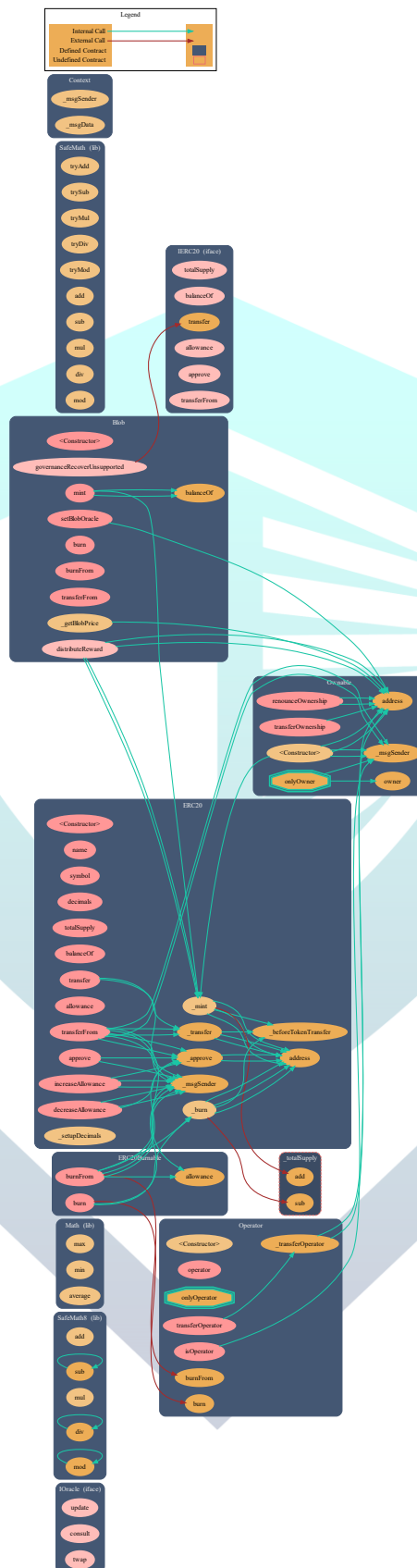
12. transferFrom (0x23b872dd)

13. transferOperator (0x29605e77)

14. transferOwnership (0xf2fde38b)



# Call Graph



# SWC Attacks

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

<a href="#"><u>SWC-110</u></a>	Assert Violation	<b>PASSED</b>
<a href="#"><u>SWC-109</u></a>	Uninitialized Storage Pointer	<b>PASSED</b>
<a href="#"><u>SWC-108</u></a>	State Variable Default Visibility	<b>PASSED</b>
<a href="#"><u>SWC-107</u></a>	Reentrancy	<b>PASSED</b>
<a href="#"><u>SWC-106</u></a>	Unprotected SELFDESTRUCT Instruction	<b>PASSED</b>
<a href="#"><u>SWC-105</u></a>	Unprotected Ether Withdrawal	<b>PASSED</b>
<a href="#"><u>SWC-104</u></a>	Unchecked Call Return Value	<b>PASSED</b>
<a href="#"><u>SWC-103</u></a>	Floating Pragma	<b>PASSED</b>
<a href="#"><u>SWC-102</u></a>	Outdated Compiler Version	<b>PASSED</b>
<a href="#"><u>SWC-101</u></a>	Integer Overflow and Underflow	<b>PASSED</b>
<a href="#"><u>SWC-100</u></a>	Function Default Visibility	<b>PASSED</b>

## 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



# Findings

## Operator can mint after initial deployment

```
function mint(address recipient_↑, uint256 amount_↑) public onlyOperator returns (bool) {  
    uint256 balanceBefore = balanceOf(recipient_↑);  
    mint(recipient_↑, amount_↑);  
    uint256 balanceAfter = balanceOf(recipient_↑);  
  
    return balanceAfter > balanceBefore;  
}
```

## Operator can burn tokens from own balance and allowed balances

```
function burn(uint256 amount↑) public override {  
    super.burn(amount↑);  
}  
  
ftrace | funcSig  
function burnFrom(address account↑, uint256 amount↑) public override onlyOperator {  
    super.burnFrom(account↑, amount↑);  
}
```

## Operator can withdraw BLOB and foreign tokens from contract

```
function governanceRecoverUnsupported(  
    IERC20 _token↑,  
    uint256 _amount↑,  
    address _to↑  
) external onlyOperator {  
    _token↑.transfer(_to↑, _amount↑);  
}
```

# Audit Comments

- Owner can renounce and transfer ownership
- Owner can change operator address
- Operator can change oracle address
- Operator can mint after initial deployment
- Operator can burn tokens from own balance and allowed balances
- Operator can distribute token rewards
- Operator can withdraw BLOB and foreign tokens from contract
- Owner cannot block users
- Owner cannot pause contract



# CONTRACTWOLF

Blockchain Security - Smart Contract Audits