Solo Audit Report

Project Name: Birds of Space ERC20 Bulk Transfer

Introduction

The Birds of Space ERC20 project endeavors to establish a decentralized token on the Ethereum Virtual Machine blockchain, adhering to the ERC20 standard. This utility contract, denoted as “ERC20BulkSender,” is specifically crafted to streamline transactions within the Birds of Space platform’s ecosystem, focusing on facilitating bulk transfers efficiently.

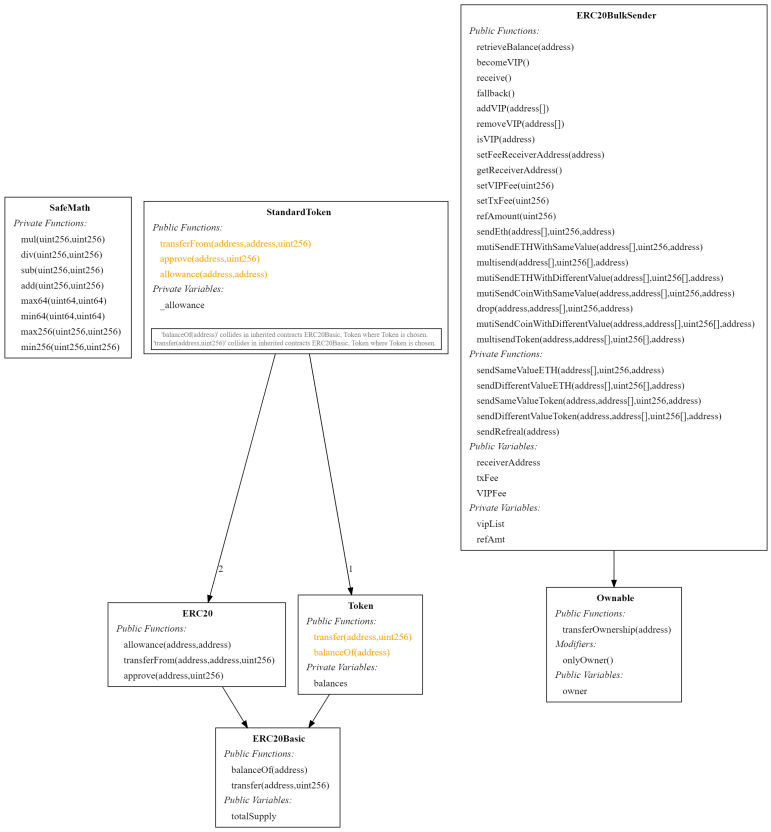
Audit Overview

The objective of this audit report is to evaluate the smart contract code and the comprehensive security measures integrated into the Birds of Space ERC20 Bulk Transfer project. The assessment involves scrutinizing the solidity codebase for potential vulnerabilities and verifying adherence to the industry’s best practices in smart contract development.

Conclusion

The audit report aims to provide insights into the security posture of the Birds of Space ERC20 Bulk Transfer project and identify areas for improvement. By conducting this audit, we aim to enhance the overall robustness and reliability of the smart contract codebase, thereby promoting trust and confidence among stakeholders.

Summary of Code Compilation and Quality Analysis



flow.png

- Compiled with solc
- Total number of contracts in source files: 7
- Source lines of code (SLOC) in source files: 355
- Number of assembly lines: 0
- Number of optimization issues: 1
- Number of informational issues: 63
- Number of low issues: 7
- Number of medium issues: 6
- Number of high issues: 1
- ERCs: ERC20

Name	Functions	ERCS	ERC20 info	Complex code	Features
SafeMath	8			No	
StandardToken	10	ERC20	No Minting	No	
			Approve Race Cond.		
ERC20BulkSender	28			No	Receive ETH
					Send ETH
					Tokens interaction

Contract SafeMath

Function	Modifiers
mul	[]
div	[]
sub	[]
add	[]
max64	[]
min64	[]
max256	[]
min256	[]

Contract StandardToken

Function	Modifiers
allowance	[]
transferFrom	[]
approve	[]
balanceOf	[]
transfer	[]
transfer	[]
balanceOf	[]
transferFrom	[]
approve	[]
allowance	[]

Contract ERC20BulkSender

Function	Modifiers
constructor	[]
transferOwnership	['onlyOwner']
retrieveBalance	['onlyOwner']
becomeVIP	[]
receive	[]
fallback	[]
addVIP	['onlyOwner']
removeVIP	['onlyOwner']
isVIP	[]
setFeeReceiverAddress	['onlyOwner']
getReceiverAddress	[]
setVIPFee	['onlyOwner']
setTxFee	['onlyOwner']
sendSameValueETH	[]
sendDifferentValueETH	[]
sendSameValueToken	[]
sendDifferentValueToken	[]
sendRefreal	[]
refAmount	['onlyOwner']
sendEth	[]
mutiSendETHWithSameValue	[]
multisend	[]
mutiSendETHWithDifferentValue	[]
mutiSendCoinWithSameValue	[]
drop	[]
mutiSendCoinWithDifferentValue	[]
multisendToken	[]
slitherConstructorVariables	[]

Contract SafeMath

- Contract vars: []
- Inheritance:: []

Function	Visibility	Modifiers	Read	Write	Internal Calls	External Calls	Cyclomatic Complexity
mul(uint256,uint256)	internal	[]	[]	[]	['require(bool)']	[]	1
div(uint256,uint256)	internal	[]	[]	[]	['require(bool)']	[]	1
sub(uint256,uint256)	internal	[]	[]	[]	['require(bool)']	[]	1
add(uint256,uint256)	internal	[]	[]	[]	['require(bool)']	[]	1
max64(uint64,uint64)	internal	[]	[]	[]	[]	[]	1
min64(uint64,uint64)	internal	[]	[]	[]	[]	[]	1
max256(uint256,uint256)	internal	[]	[]	[]	[]	[]	1
min256(uint256,uint256)	internal	[]	[]	[]	[]	[]	1

Modifiers	Visibility	Read	Write	Internal Calls	External Calls	Cyclomatic Complexity

Contract ERC20Basic

- Contract vars: ['totalSupply']
- Inheritance:: []

Function	Visibility	Modifiers	Read	Write	Internal Calls	External Calls	Cyclomatic Complexity
balanceOf(address)	public	[]	[]	[]	[]	[]	2
transfer(address,uint256)	public	[]	[]	[]	[]	[]	2

Modifiers	Visibility	Read	Write	Internal Calls	External Calls	Cyclomatic Complexity

Contract ERC20

- Contract vars: ['totalSupply']
- Inheritance:: ['ERC20Basic']

Function	Visibility	Modifiers	Read	Write	Internal Calls	External Calls	Cyclomatic Complexity
balanceOf(address)	public	[]	[]	[]	[]	[]	2
transfer(address,uint256)	public	[]	[]	[]	[]	[]	2
allowance(address,address)	public	[]	[]	[]	[]	[]	2
transferFrom(address,address,uint256)	public	[]	[]	[]	[]	[]	2
approve(address,uint256)	public	[]	[]	[]	[]	[]	2

Modifiers	Visibility	Read	Write	Internal Calls	External Calls	Cyclomatic Complexity

Contract Token

- Contract vars: ['totalSupply', 'balances']
- Inheritance:: ['ERC20Basic']

Function	Visibility	Modifiers	Read	Write	Internal Calls	External Calls	Cyclomatic Complexity
balanceOf(address)	public	[]	[]	[]	[]	[]	2
transfer(address,uint256)	public	[]	[]	[]	[]	[]	2
transfer(address,uint256)	public	[]	['balances', 'msg.sender']	['balances']	[]	['balances[_to].add(_value)', 'balances[msg.sender].sub(_value)']	1
balanceOf(address)	public	[]	['balances']	[]	[]	[]	1

Modifiers	Visibility	Read	Write	Internal Calls	External Calls	Cyclomatic Complexity

Contract StandardToken

- Contract vars: ['totalSupply', 'balances', '_allowance']
- Inheritance:: ['ERC20', 'Token', 'ERC20Basic']

Function	Visibility	Modifiers	Read	Write	Internal Calls	External Calls	Cyclomatic Complexity
allowance(address,address)	public	[]	[]	[]	[]	[]	2
transferFrom(address,address,uint256)	public	[]	[]	[]	[]	[]	2
approve(address,uint256)	public	[]	[]	[]	[]	[]	2

Function	Visibility	Modifiers	Read	Write	Internal Calls	External Calls	Cyclomatic Complexity
balanceOf(address)	public	[]	[]	[]	[]	[]	2
transfer(address,uint256)	public	[]	[]	[]	[]	[]	2
transfer(address,uint256)	public	[]	['balances', 'msg.sender']	['balances']	[]	['balances[_to].add(_value)', 'balances[msg.sender].sub(_value)']	1
balanceOf(address)	public	[]	['balances']	[]	[]	[]	1
transferFrom(address,address,uint256)	public	[]	['_allowance', 'balances']	['_allowance', 'balances']	[]	['_allowance[_from][msg.sender].sub(_value)', 'balances[_from].sub(_value)']	1
			['msg.sender']			['balances[_to].add(_value)']	
approve(address,uint256)	public	[]	['_allowance', 'msg.sender']	['_allowance']	['require(bool)']	[]	1
allowance(address,address)	public	[]	['_allowance']	[]	[]	[]	1

Modifiers	Visibility	Read	Write	Internal Calls	External Calls	Cyclomatic Complexity

Contract Ownable

- Contract vars: ['owner']
- Inheritance:: []

Function	Visibility	Modifiers	Read	Write	Internal Calls	External Calls	Cyclomatic Complexity
constructor()	public	[]	['msg.sender']	['owner']	[]	[]	1
transferOwnership(address)	public	['onlyOwner']	[]	['owner']	['onlyOwner']	[]	2

Modifiers	Visibility	Read	Write	Internal Calls	External Calls	Cyclomatic Complexity
onlyOwner()	internal	['msg.sender', 'owner']	[]	['require(bool)']	[]	1

Contract ERC20BulkSender

- Contract vars: ['owner', 'receiverAddress', 'txFee', 'VIPFee', 'vipList', 'refAmt']
  Inheritance:: ['Ownable']

Function	Visibility	Modifiers	Read	Write	Internal Calls	External Calls	Cyclomatic Complexity
constructor()	public	[]	['msg.sender']	['owner']	[]	[]	1
transferOwnership(address)	public	['onlyOwner']	[]	['owner']	['onlyOwner']	[]	2
retrieveBalance(address)	public	['onlyOwner']	['this']	[]	['balance(address)', 'getReceiverAddress']	['address(_receiverAddress).send(address(this).balance)', 'token.balanceOf(address(this))']	1
					['onlyOwner', 'require(bool,string)']	['token.transfer(_receiverAddress,balance)']	
becomeVIP()	public	[]	['VIPFee', 'msg.sender']	['vipList']	['getReceiverAddress', 'require(bool)']	['address(_receiverAddress).send(msg.value)']	1
			['msg.value']		['require(bool,string)']	[]	
receive()	external	[]	['msg.value']	[]	['getReceiverAddress']	['address(getReceiverAddress()).transfer(msg.value)']	1
fallback()	external	[]	['msg.value']	[]	['getReceiverAddress']	['address(getReceiverAddress()).transfer(msg.value)']	2
addVIP(address[])	public	['onlyOwner']	[]	['vipList']	['onlyOwner']	[]	2
removeVIP(address[])	public	['onlyOwner']	[]	['vipList']	['onlyOwner']	[]	2
isVIP(address)	public	[]	['owner', 'vipList']	[]	[]	[]	1
setFeeReceiverAddress(address)	public	['onlyOwner']	[]	['receiverAddress']	['onlyOwner', 'require(bool)']	[]	1
getReceiverAddress()	public	[]	['owner', 'receiverAddress']	[]	[]	[]	1
setVIPFee(uint256)	public	['onlyOwner']	[]	['VIPFee']	['onlyOwner']	[]	1
setTxFee(uint256)	public	['onlyOwner']	[]	['txFee']	['onlyOwner']	[]	1
sendSameValueETH(address[],uint256,address)	internal	[]	['msg.sender', 'msg.value']	[]	['isVIP', 'require(bool)']	['address(_to[i]).send(_value)']	4
			['txFee']		['require(bool,string)', 'sendRefreal']	['address(_to[i]).send(_value.add(txFee))']	
sendDifferentValueETH(address[],uint256[],address)	internal	[]	['msg.sender', 'msg.value']	[]	['isVIP', 'require(bool)']	['address(_to[i]).send(_value[i])']	4
			['txFee']		['require(bool,string)', 'sendRefreal']	['address(_to[i]).send(_value[i].add(txFee))']	
sendSameValueToken(address,address[],uint256,address)	internal	[]	['msg.sender', 'msg.value']	[]	['isVIP', 'require(bool)']	['address(msg.sender).transfer(msg.value)', 'token.transferFrom(from,_to[i],_value)']	5
sendDifferentValueToken(address,address[],uint256[],address)	internal	[]	['msg.sender', 'msg.value']	[]	['isVIP', 'require(bool)']	['address(msg.sender).transfer(msg.value)', 'token.transferFrom(msg.sender,_to[i],_value[i])']	5
sendRefreal(address)	internal	[]	['refAmt']	[]	[]	['address(_ref).transfer(refAmt)']	1
refAmount(uint256)	public	['onlyOwner']	[]	['refAmt']	['onlyOwner']	[]	1
sendEth(address[],uint256,address)	public	[]	[]	[]	['sendSameValueETH']	[]	1
mutiSendETHWithSameValue(address[],uint256,address)	public	[]	[]	[]	['sendSameValueETH']	[]	1
multisend(address[],uint256[],address)	public	[]	[]	[]	['sendDifferentValueETH']	[]	1
mutiSendETHWithDifferentValue(address[],uint256[],address)	public	[]	[]	[]	['sendDifferentValueETH']	[]	1
mutiSendCoinWithSameValue(address,address[],uint256,address)	public	[]	[]	[]	['sendSameValueToken']	[]	1
drop(address,address[],uint256,address)	public	[]	[]	[]	['sendSameValueToken']	[]	1
mutiSendCoinWithDifferentValue(address,address[],uint256[],address)	public	[]	[]	[]	['sendDifferentValueToken']	[]	1

Function	Visibility	Modifiers	Read	Write	Internal Calls	External Calls	Cyclomatic Complexity
multisendToken(address,address[],uint256[],address)	public	[]	[]	[]	['sendDifferentValueToken']	[]	1
slitherConstructorVariables()	internal	[]	['txFee']	['VIPFee', 'refAmt']	[]	[]	1
				['txFee']	['require(bool,string)', 'sendRefreal']	['sendAmount.add(txFee)']	

Modifiers	Visibility	Read	Write	Internal Calls	External Calls	Cyclomatic Complexity
onlyOwner()	internal	['msg.sender', 'owner']	[]	['require(bool)']	[]	1