



SMART CONTRACT AUDIT REPORT

For
Airdrop



Prepared By: SFI Team

Prepared on: 27/11/2022

Prepared for: Card NFT Team

Contract address: Not deployed yet

Table of Content

- Disclaimer
- Scope of the audit
- Check Vulnerabilities
- Issue Categories
- Issues Found – Code Review
- Source Lines
- Risk Level
- Capabilities
- Testing proves
- Inheritance graph
- Call Graph
- Source Units In Scope
- Unified Modeling Language (UML)
- Functions signature
- Automatic general report
- Summary of the audit

- **Disclaimer**

This is a limited report on our findings based on our analysis, in accordance with good industry practice as of 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 the team on the basis of what it says or doesn't say, or how team produced it, and it is important for you to conduct your own independent investigations before making any decisions. team go into more detail on this in the below disclaimer below – please make sure to read it in full.

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 Saferico and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (SaferICO) owe no duty of care towards you or any other person, nor does Saferico 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 Saferico 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, Saferico hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against Saferico, 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.

• Scope of the audit

The scope of this audit was to analyze and document Airdrop smart contract codebase for quality, security, and correctness.

• Introduction

During the period of **November 25, 2022, to November 27, 2022**- SaferICO

Team performed a security audit for **Airdrop** smart contracts.

The project has 1 file. It contains approx 171 lines of Solidity code. Most of the functions and state variables are well commented on using the Nat spec documentation, but that does not create any vulnerability.

Source Code: it is a private code.

Check Vulnerabilities

In order to check for the security of the contract, we tested several attacks in order to make sure that the contract is secure and follows best practices automatically.

1. Unit tests passing.
2. Compiler warnings;
3. Race Conditions. Reentrancy. Cross-function Race Conditions. Pitfalls in Race Condition solutions;
4. Possible delays in data delivery;
5. Transaction-Ordering Dependence (front running);
6. Timestamp Dependence;

7. Integer Overflow and Underflow;

8. DoS with (unexpected) Revert;

9. DoS with Block Gas Limit

10. Call Depth Attack. Not relevant in modern Ethereum network

11. Methods execution permissions;

12. Oracles calls;

13. Economy model. It's important to forecast scenarios when a user is provided with additional economic motivation or faced with limitations. If application logic is based on incorrect economy model, the application will not function correctly and participants will incur financial losses. This type of issue is most often found in bonus rewards systems.

14. The impact of the exchange rate on the logic;

15. Private user data leaks.

• Issue Categories

Every issue in this report has been assigned to a severity level. There are four levels of severity, and each of them has been explained below.

Risk-level	Description
High	A high severity issue or vulnerability means that your smart contract can be exploited. Issues on this level are critical to the smart contract's performance or functionality, and we recommend these issues be fixed before moving to a live environment.
Medium	The issues marked as medium severity usually arise because of errors and deficiencies in the smart contract code. Issues on this level could potentially bring problems, and they should still be fixed.
Low	Low-level severity issues can cause minor impact and or are just warnings that can remain unfixed for now. It would be better to fix these issues at some point in the future.
Informational	These are severity issues that indicate an improvement request, a general question, a cosmetic or documentation error, or a request for information. There is low-to-no impact.

• Issues Found – Code Review

High severity issues

There are no High severity vulnerabilities found.

Medium severity issues

There are no Medium severity vulnerabilities found.

Low severity issues

#Missing zero address validation

Description

When the owner wants to add an admin, he has to check for the zero address, he didn't add the burn address as admin. Otherwise, he will lost the control forever .

```
function setAdmin(address _newAdmin)
    external
    onlyOwner
{
    admin = _newAdmin;
}
```

Remediation

Use the require statement to check for zero addresses.

Status: **Closed**. Fixed in version2.

#Pragam version not fixed

Description

It is a good practice to lock the solidity version for a live deployment (use 0.8.17 instead of ^0.8.7). contracts should be deployed with the same compiler version and flags that they have been tested the most with. Locking the pragma helps ensure that contracts do not accidentally get deployed using, for example, the latest compiler which may have higher risks of undiscovered bugs. Contracts may also be deployed by others and the pragma indicates the compiler version intended by the original authors.

Remediation

Remove the ^ sign to lock the pragma version.

Status: **Closed**. Fixed In version 2

#Use of block.timestamp for comparisons

Description

The value of block.timestamp can be manipulated by the miner.
And conditions with strict equality is difficult to achieve -
block.timestamp

Remediation

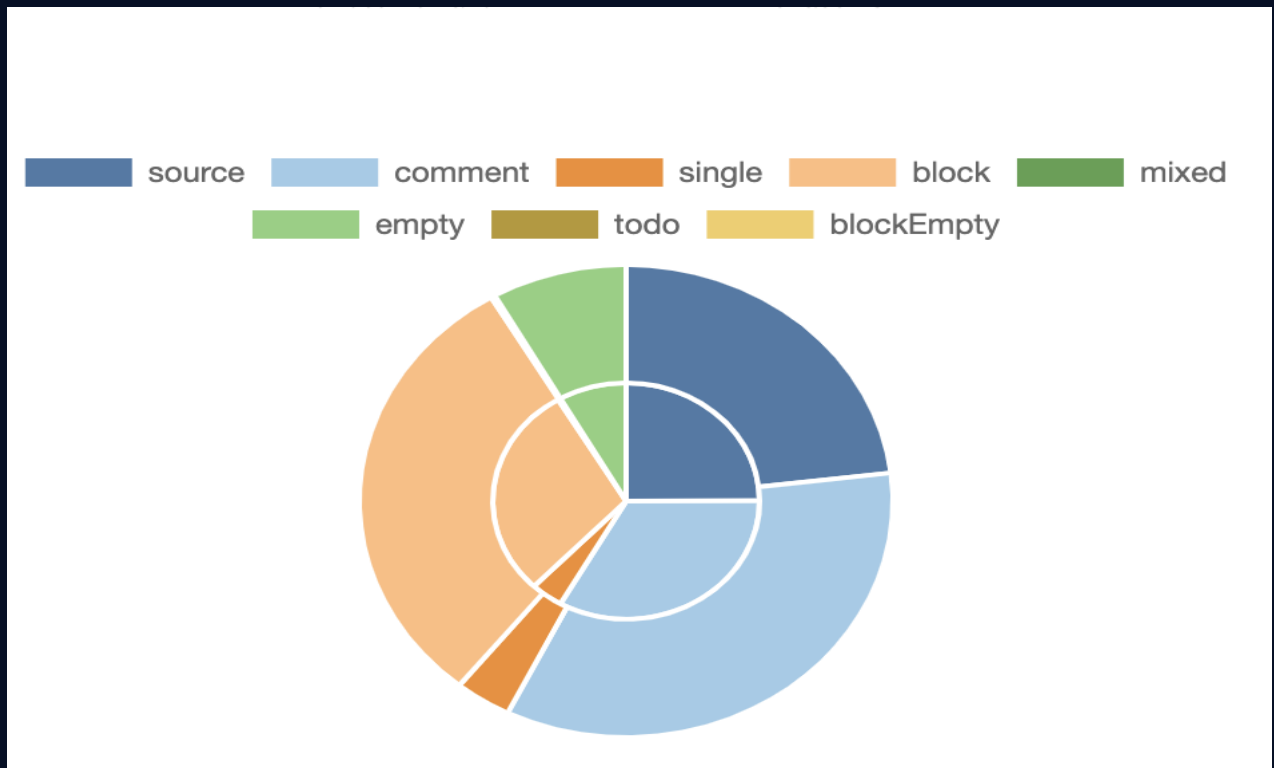
Avoid use of block.timestamp

Status: **Acknowledged**

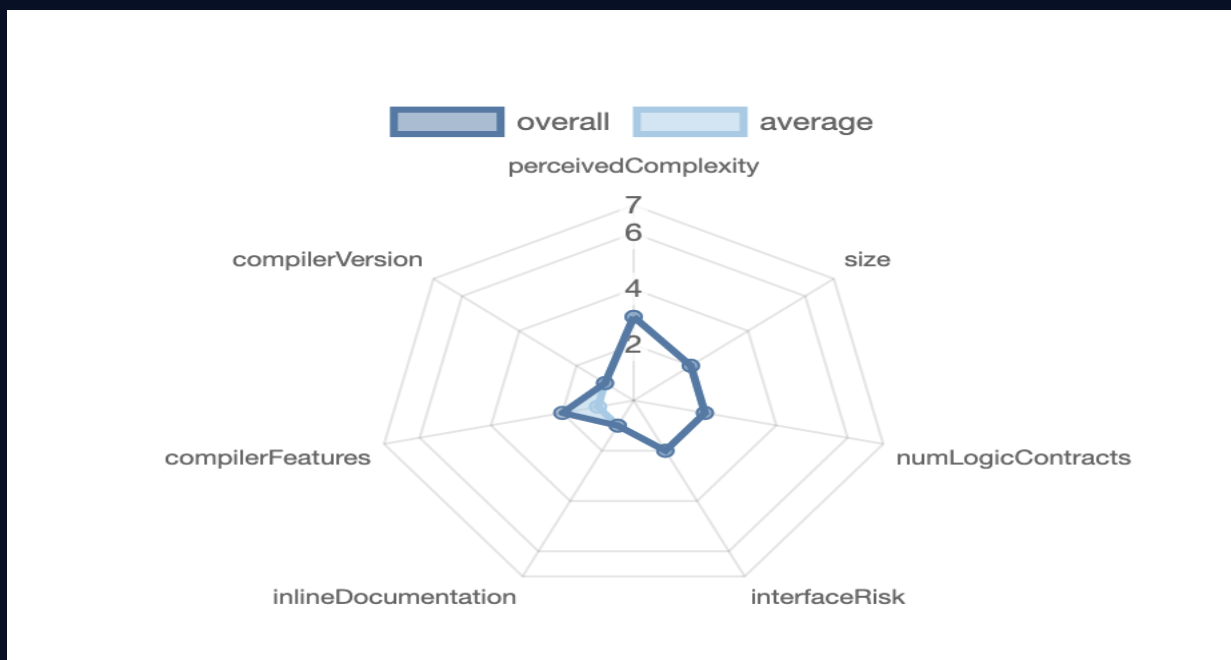
Informational issues

There are no Informational issues found.

- Source Lines




- Risk Level



- **Testing proves**
- **Check for security**

95859bf303970c952edbe7ff60e1e0cc20b0f95724717c419fc95584f1c975a6
File: Airdrop.... | Language: solidity | Size: 5500 bytes | Date: 2022-11-27T09:04:34.720Z

Critical	High	Medium	Low	Note
0	0	0	0	0



- **Solidity Static Analysis**

The image shows the Solidity Static Analysis tool interface, which is divided into two main panels. The left panel is titled 'SOLIDITY STATIC ANALYSIS' and contains two sections: 'ERC' and 'Miscellaneous'. The right panel is also titled 'SOLIDITY STATIC ANALYSIS' and contains two sections: 'Security' and 'Gas & Economy'. Each section has a list of checks with checkboxes and a 'Run' button.

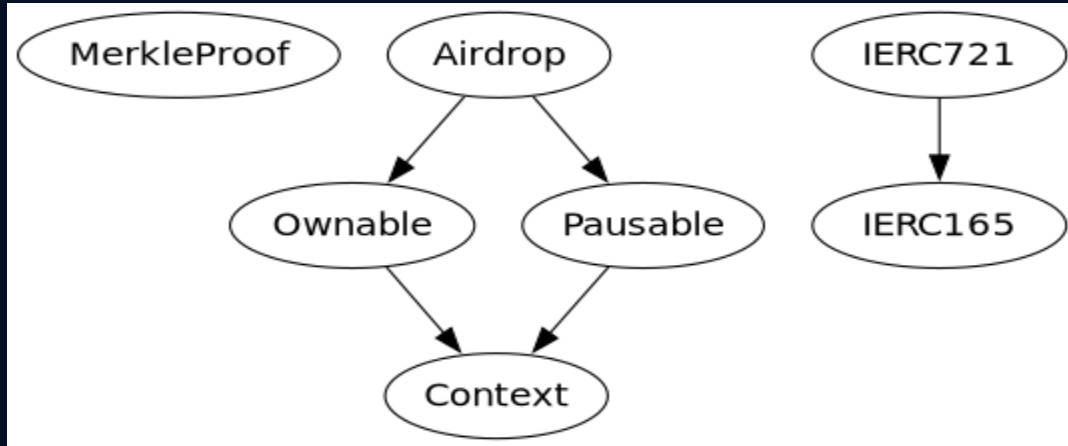
Left Panel: SOLIDITY STATIC ANALYSIS

- ERC**
 - ☒ Select ERC
 - ☒ ERC20:
'decimals' should be 'uint8'
- Miscellaneous**
 - ☒ Select Miscellaneous
 - ☒ Constant/View/Pure functions:
Potentially constant/view/pure functions
 - ☒ Similar variable names:
Variable names are too similar
 - ☒ No return:
Function with 'returns' not returning
 - ☒ Guard conditions:
Ensure appropriate use of require/assert
 - ☒ Result not used:
The result of an operation not used
 - ☒ String length:
Bytes length != String length
 - ☒ Delete from dynamic array:
'delete' leaves a gap in array
 - ☒ Data truncated:
Division on int/uint values truncates the result

Right Panel: SOLIDITY STATIC ANALYSIS

- ☒ Select all
- ☒ Autorun
- Run**
- Security**
 - ☒ Select Security
 - ☒ Transaction origin:
'tx.origin' used
 - ☒ Check-effects-interaction:
Potential reentrancy bugs
 - ☒ Inline assembly:
Inline assembly used
 - ☒ Block timestamp:
Can be influenced by miners
 - ☒ Low level calls:
Should only be used by experienced devs
 - ☒ Block hash:
Can be influenced by miners
 - ☒ Selfdestruct:
Contracts using destructed contract can be broken
- Gas & Economy**
 - ☒ Select Gas & Economy
 - ☒ Gas costs:
Too high gas requirement of functions
 - ☒ This on local calls:
Invocation of local functions via 'this'
 - ☒ Delete dynamic array:
Use require/assert to ensure complete deletion
 - ☒ For loop over dynamic array:
Iterations depend on dynamic array's size
 - ☒ Ether transfer in loop:
Transferring Ether in a for/while/do-while loop

- **Inheritance graph**



- **Solidity Unit Testing Code & Results**

```
// SPDX-License-Identifier: GPL-3.0
```

```
pragma solidity >=0.4.22 <0.9.0;
```

```
// This import is automatically injected by Remix
```

```
import "remix_tests.sol";
```

```
// This import is required to use custom transaction context
```

```
// Although it may fail compilation in 'Solidity Compiler' plugin
```

```
// But it will work fine in 'Solidity Unit Testing' plugin
```

```
import "remix_accounts.sol";
```

```
import "../Airdrop.sol";
```

```
// File name has to end with '_test.sol', this file can contain more than one testSuite contracts
```

```
contract testSuite {
```

```
    /// 'beforeAll' runs before all other tests
```

```
    /// More special functions are: 'beforeEach', 'beforeAll', 'afterEach' & 'afterAll'
```

```
    function beforeAll() public {
```

SOLIDITY UNIT TESTING



Test your smart contract in Solidity.

Select directory to load and generate test files.

Test directory:

tests

Create

Generate

How to use...

▶ Run

■ Stop

☒ Select all

☒ tests/Airdrop_test.sol

Progress: 1 finished (of 1)

PASS testSuite (tests/Airdrop_test.sol)

✓ Before all



✓ Check success



✓ Check success2



✓ Check failure



✓ Check sender and value



Result for tests/Airdrop_test.sol

Passed: 5

Failed: 0

Time Taken: 0.36s

```
// <instantiate contract>
Assert.equal(uint(1), uint(1), "1 should be equal to 1");
}

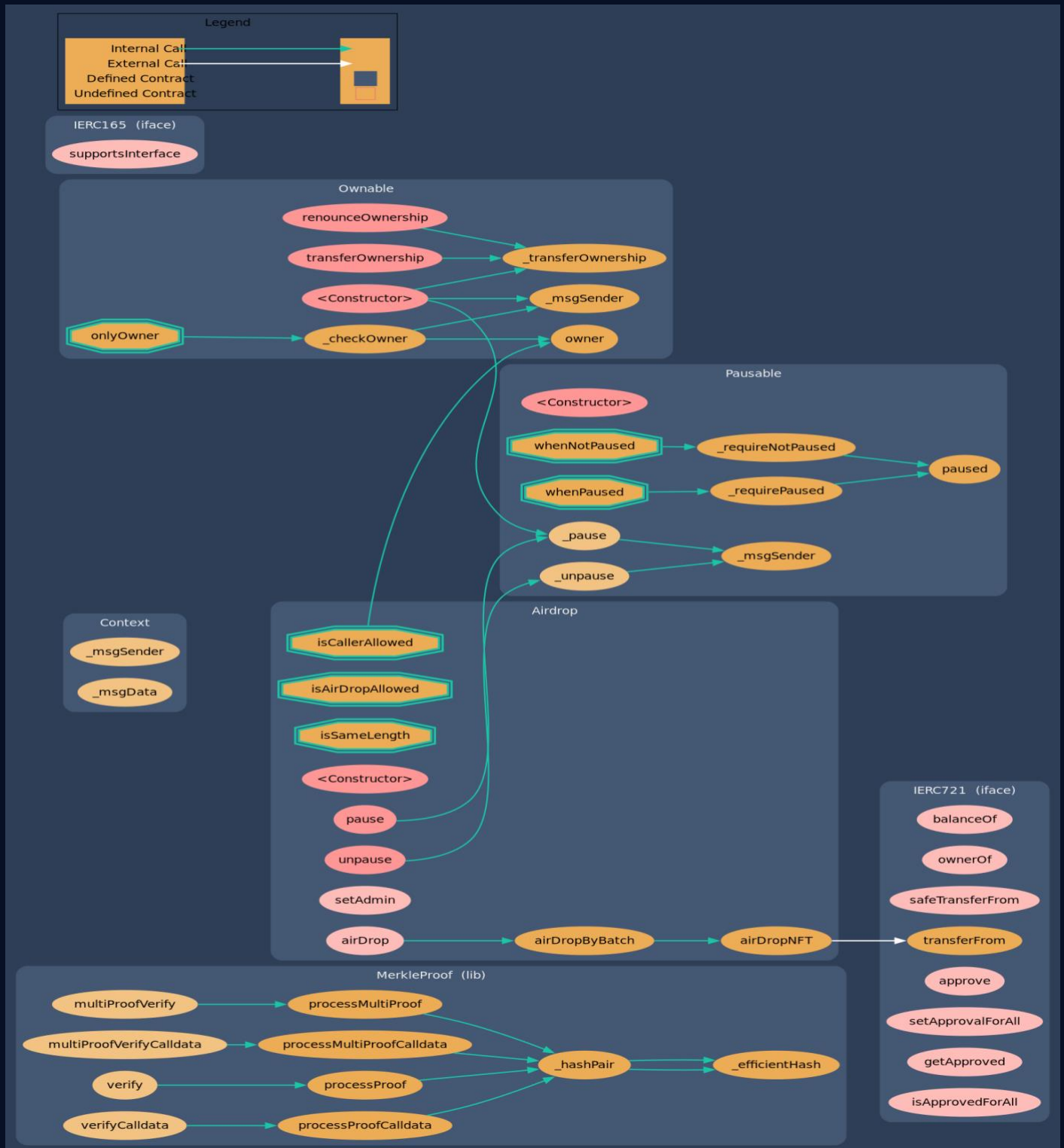
function checkSuccess() public {
    // Use 'Assert' methods: https://remix-
    ide.readthedocs.io/en/latest/assert_library.html
    Assert.ok(2 == 2, 'should be true');
    Assert.greaterThan(uint(2), uint(1), "2 should be greater than to
1");
    Assert.lessThan(uint(2), uint(3), "2 should be lesser than to
3");
}

function checkSuccess2() public pure returns (bool) {
    // Use the return value (true or false) to test the contract
    return true;
}

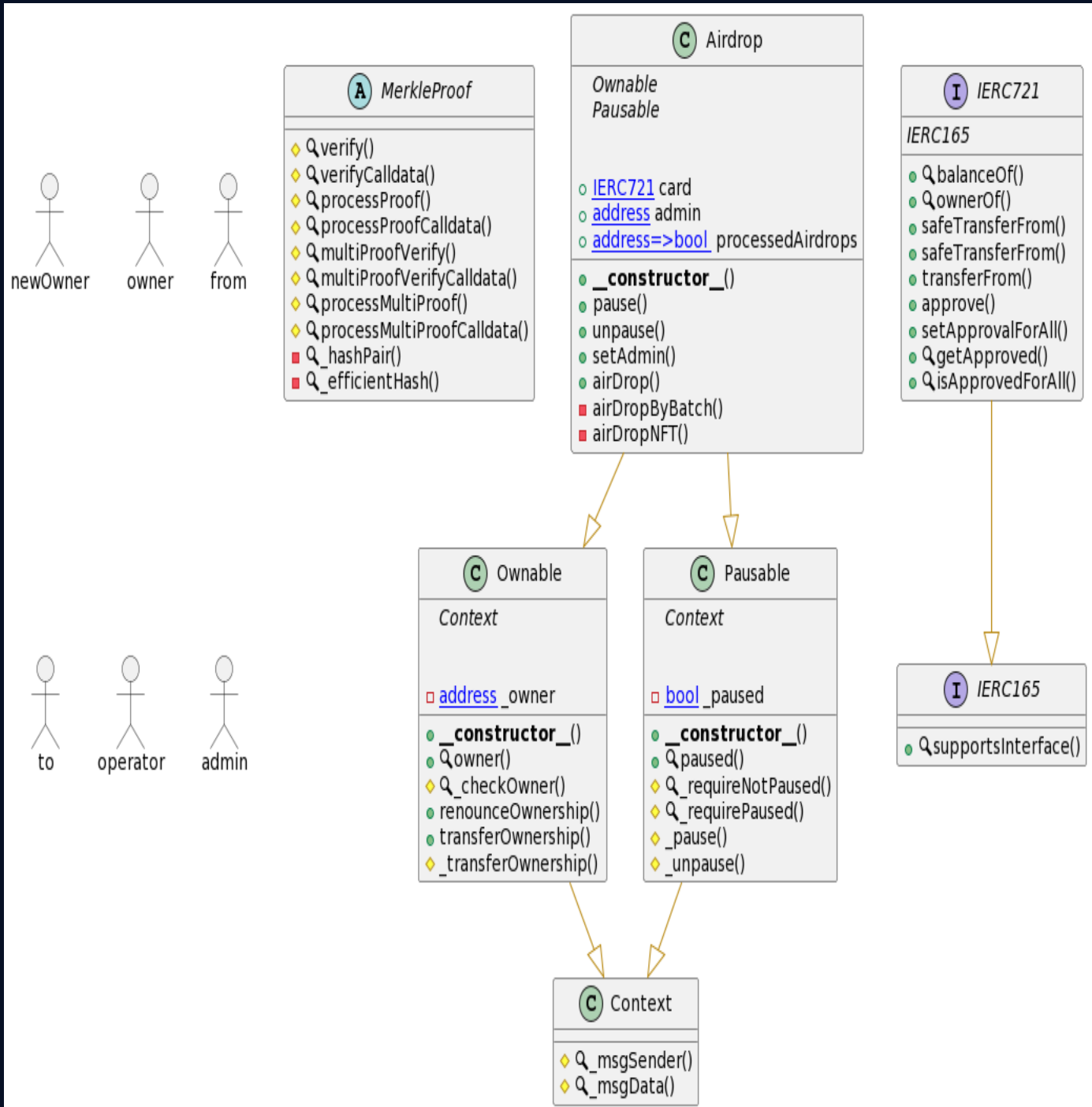
function checkFailure() public {
    Assert.notEqual(uint(1), uint(2), "1 should not be equal to 1");
}

/// Custom Transaction Context: https://remix-
ide.readthedocs.io/en/latest/unittesting.html#customization
/// #sender: account-1
/// #value: 100
function checkSenderAndValue() public payable {
    // account index varies 0-9, value is in wei
    Assert.equal(msg.sender, TestsAccounts.getAccount(1),
"Invalid sender");
    Assert.equal(msg.value, 100, "Invalid value");
}
}
```

Call Graph



- Unified Modeling Language (UML)



• Capabilities

Components

 Contracts	 Libraries	 Interfaces	 Abstract
1	1	2	3

Exposed Functions

This section lists functions that are explicitly declared public or payable. Please note that getter methods for public stateVars are not included.













 Public	 Payable
18	0

External	Internal	Private	Pure	View
12	35	4	10	12

StateVariables

Total	 Public
5	3

Capabilities

Solidity Versions observed	 Experimental Features	 Can Receive Funds	 Uses Assembly	 Has Destroyable Contracts	
<div>^0.8.0</div> <div>^0.8.7</div>			<div>yes</div> <div>(1 asm blocks)</div>		
 Transfers ETH	 Low-Level Calls	 DelegateCall	 Uses Hash Functions	 ECRecover	 New/Create/Create2
 TryCatch	 Unchecked				

• Source Units In Scope

Source Units in Scope

Source Units Analyzed: 1
Source Units in Scope: 1 (100%)

Type	File	Logic Contracts	Interfaces	Lines	nLines	nSLOC	Comment Lines	Complex. Score	Capabilities
	Airdrop.sol	5	2	780	636	240	409	185	
	Totals	5	2	780	636	240	409	185	

Legend: [—]

- **Lines:** total lines of the source unit
- **nLines:** normalized lines of the source unit (e.g. normalizes functions spanning multiple lines)
- **nSLOC:** normalized source lines of code (only source-code lines; no comments, no blank lines)
- **Comment Lines:** lines containing single or block comments
- **Complexity Score:** a custom complexity score derived from code statements that are known to introduce code complexity (branches, loops, calls, external interfaces, ...)

• Function Signature

Sighash | Function Signature

=====

```
86333816 => multiProofVerify(bytes32[],bool[],bytes32,bytes32[])
5a9a49c7 => verify(bytes32[],bytes32,bytes32)
7ffe9d8c => verifyCalldata(bytes32[],bytes32,bytes32)
62702a6b => processProof(bytes32[],bytes32)
53b0f85f => processProofCalldata(bytes32[],bytes32)
862aac96 => multiProofVerifyCalldata(bytes32[],bool[],bytes32,bytes32[])
ea5d3eb6 => processMultiProof(bytes32[],bool[],bytes32[])
32712d22 => processMultiProofCalldata(bytes32[],bool[],bytes32[])
00a4cf28 => _hashPair(bytes32,bytes32)
41ed615b => _efficientHash(bytes32,bytes32)
119df25f => _msgSender()
8b49d47e => _msgData()
8da5cb5b => owner()
53a72975 => _checkOwner()
715018a6 => renounceOwnership()
f2fde38b => transferOwnership(address)
d29d44ee => _transferOwnership(address)
5c975abb => paused()
abb87a6f => _requireNotPaused()
4a994e05 => _requirePaused()
320b2ad9 => _pause()
fc8234cb => _unpause()
01ffc9a7 => supportsInterface(bytes4)
70a08231 => balanceOf(address)
6352211e => ownerOf(uint256)
b88d4fde => safeTransferFrom(address,address,uint256,bytes)
42842e0e => safeTransferFrom(address,address,uint256)
23b872dd => transferFrom(address,address,uint256)
095ea7b3 => approve(address,uint256)
a22cb465 => setApprovalForAll(address,bool)
081812fc => getApproved(uint256)
e985e9c5 => isApprovedForAll(address,address)
8456cb59 => pause()
```


3f4ba83a => unpause()

704b6c02 => setAdmin(address)

e0882af8 => airDrop(address,address[],uint256[])

c3aa0bb4 => airDropByBatch(address,address[],uint256[])

f0620391 => airDropNFT(address,address,uint256)

• Automatic General Report

Files Description Table


File Name	SHA-1 Hash
/Users/macbook/Desktop/smart contracts/Airdrop.sol	40d5eff1d7ad4d1b128bb88993288a83727da8eb


Contracts Description Table


Contract	Type	Bases		
↳	**Function Name**	**Visibility**	**Mutability**	**Modifiers**


|||||

| **MerkleProof** | Library | |||

| ↳ | verify | Internal  | ||


| ↳ | verifyCalldata | Internal  | ||

| ↳ | processProof | Internal  | ||


| ↳ | processProofCalldata | Internal  | ||


| ↳ | multiProofVerify | Internal  | ||

| ↳ | multiProofVerifyCalldata | Internal  | ||

| ↳ | processMultiProof | Internal  | ||


| ↳ | processMultiProofCalldata | Internal  | ||


| ↳ | _hashPair | Private  | ||

| ↳ | _efficientHash | Private  | ||

|||||

| **Context** | Implementation | |||



| ↳ | _msgSender | Internal  | ||


| ↳ | _msgData | Internal  | ||



|||||



| **Ownable** | Implementation | Context |||



| ↳ | <Constructor> | Public  |  | NO  |

| ↳ | owner | Public  | NO  |

| ↳ | _checkOwner | Internal  | ||

| ↳ | renounceOwnership | Public  |  | onlyOwner |

| ↳ | transferOwnership | Public  |  | onlyOwner |

| ↳ | _transferOwnership | Internal  |  | ||

|||||

| **Pausable** | Implementation | Context |||

| ↳ | <Constructor> | Public  |  | NO  |

```

|  | paused | Public  | |NO|
|  | _requireNotPaused | Internal  | |
|  | _requirePaused | Internal  | |
|  | _pause | Internal  |  | whenNotPaused |
|  | _unpause | Internal  |  | whenPaused |
|||||
| **IERC165** | Interface | |||
|  | supportsInterface | External  | |NO|
|||||
| **IERC721** | Interface | IERC165 |||
|  | balanceOf | External  | |NO|
|  | ownerOf | External  | |NO|
|  | safeTransferFrom | External  |  |NO|
|  | safeTransferFrom | External  |  |NO|
|  | transferFrom | External  |  |NO|
|  | approve | External  |  |NO|
|  | setApprovalForAll | External  |  |NO|
|  | getApproved | External  | |NO|
|  | isApprovedForAll | External  | |NO|
|||||
| **Airdrop** | Implementation | Ownable, Pausable |||
|  | <Constructor> | Public  |  |NO|
|  | pause | Public  |  | onlyOwner |
|  | unpause | Public  |  | onlyOwner |
|  | setAdmin | External  |  | onlyOwner |
|  | airDrop | External  |  | whenNotPaused isCallerAllowed isSameLength |
|  | airDropByBatch | Private  |  |
|  | airDropNFT | Private  |  | isAirDropAllowed |

```

Legend

| Symbol | Meaning |

|:-----:|:-----:|

| | Function can modify state |

| | Function is payable |

- **Summary of the Audit**

According to all test, the customer`s solidity smart contract is **Well Secure**.

The general overview is presented in the Project Information section and all issues found are located in the audit overview section.

The test found 0 critical, 0 high, 0 medium, 3 low issues, and 0 notes.