



SMART CONTRACT AUDIT REPORT

For
DeVestOne



Prepared By: SFI Team

Prepared on: 26/10/2022

Prepared for: DeVest|Finance 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 the DeVestOne smart contract codebase for quality, security, and correctness.

• Introduction

During the period of **October 24, 2022, to October 26, 2022**- SaferICO

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

The project contains approx 469 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: <https://github.com/devest-finance/model-one>

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

#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 ^0.8.12). 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

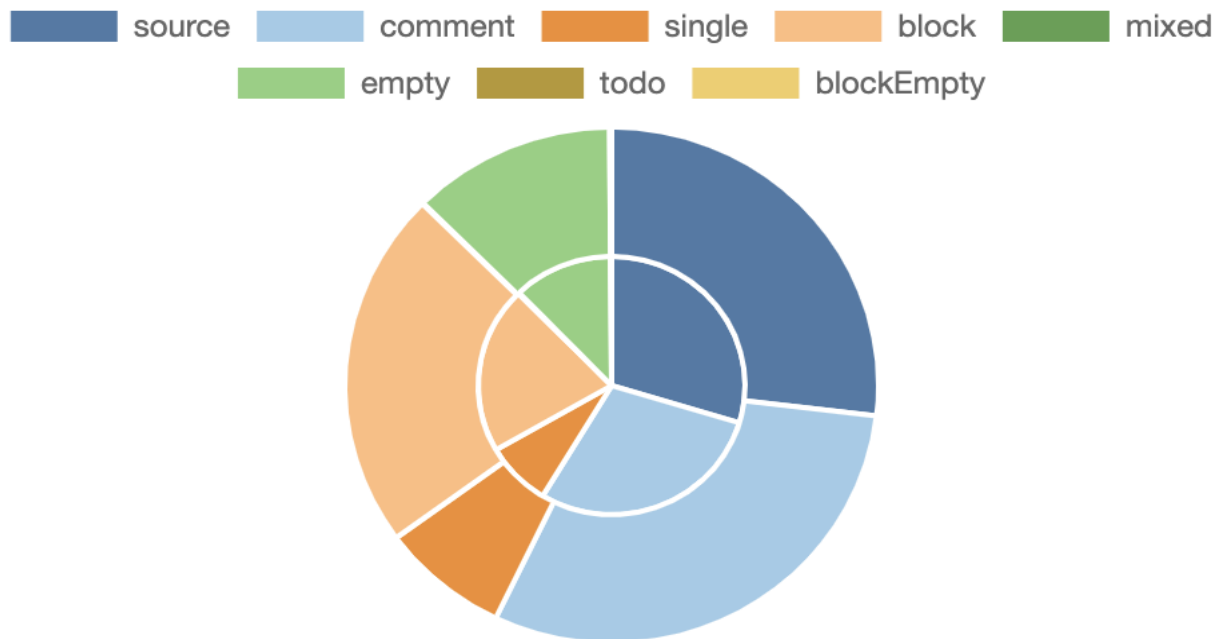
Remove the ^ sign to lock the pragma version.

Status: [Acknowledged](#).

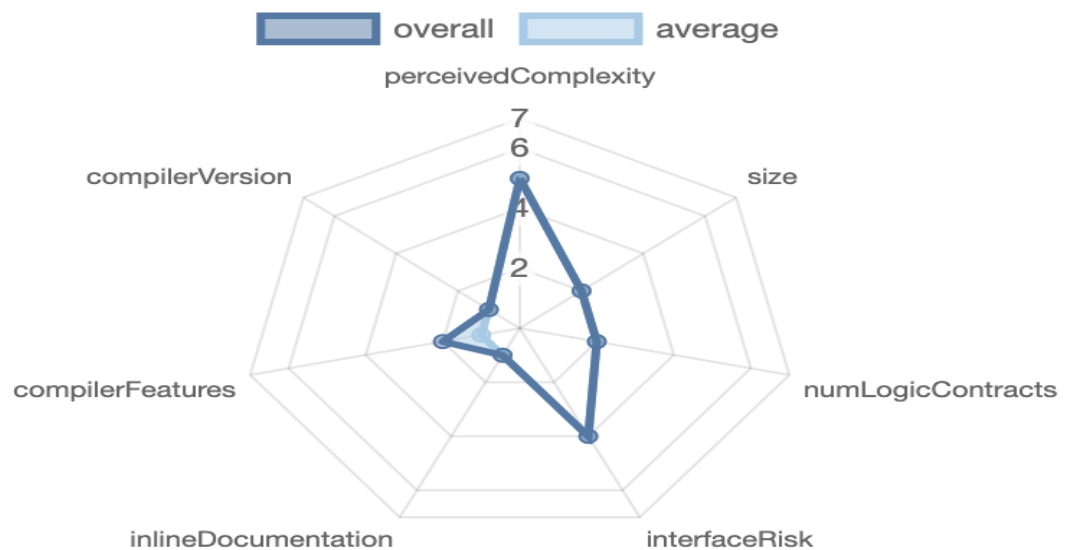
Informational issues

There are no Informational issues found.

- Source Lines




- Risk Level



- Testing proves
- Check for security

fbef1014028c9c3bd494517de16ebd99747b6869e8fa3a521fba3db75e0662c4
 File: Devest... | Language: solidity | Size: 16425 bytes | Date: 2022-10-25T14:41:06.267Z

Critical	High	Medium	Low	Note
0	0	0	0	0



- Solidity Static Analysis

SOLIDITY STATIC ANALYSIS

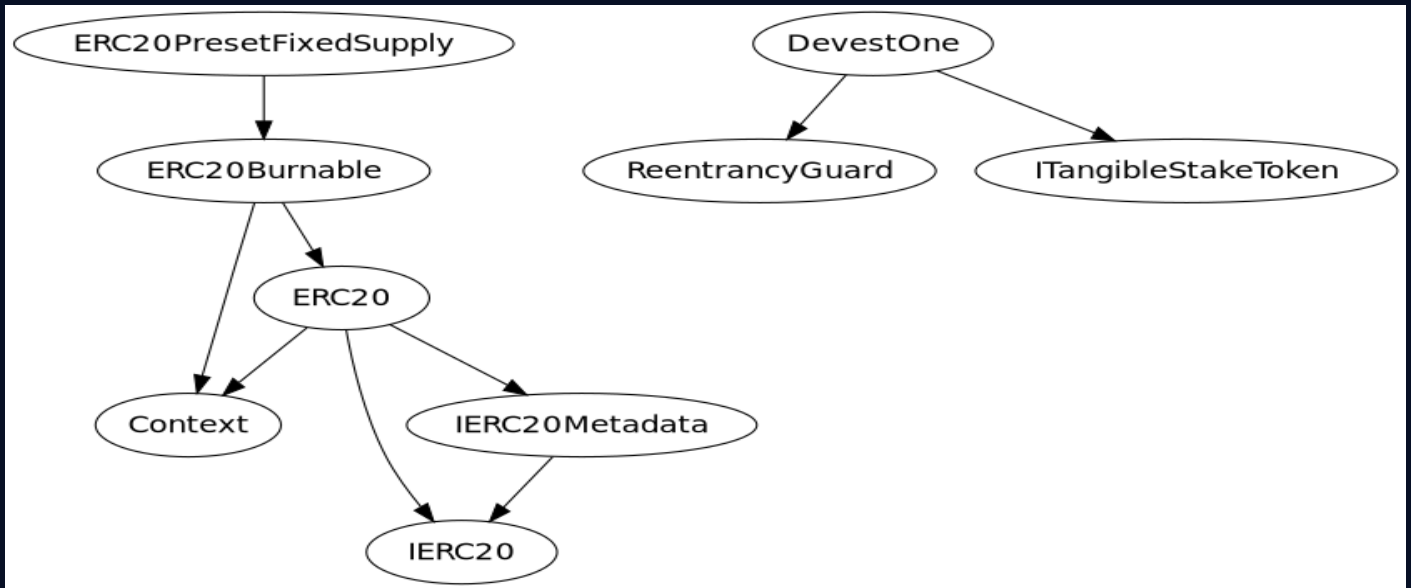
- ▼ ERC
 - ☒ Select ERC
 - ☒ ERC20: 'decimals' should be 'uint8'
- ▼ Miscellaneous
 - ☒ Select Miscellaneous
 - ☒ Constant/View/Pure functions: Potentially constant/view/pure functions
 - ☒ Similar variable names: Variable names are too similar
 - ☒ No return: Function with 'returns' not returning
 - ☒ 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

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 destructured 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 "../DevestOne.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'
```

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/DevestOne_test.sol

Progress: 1 finished (of 1)

PASS testSuite (tests/DevestOne_test.sol)

✓ Before all



✓ Check success



✓ Check success2



✓ Check failure



✓ Check sender and value



Result for tests/DevestOne_test.sol

Passed: 5

Failed: 0

Time Taken: 0.43s

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

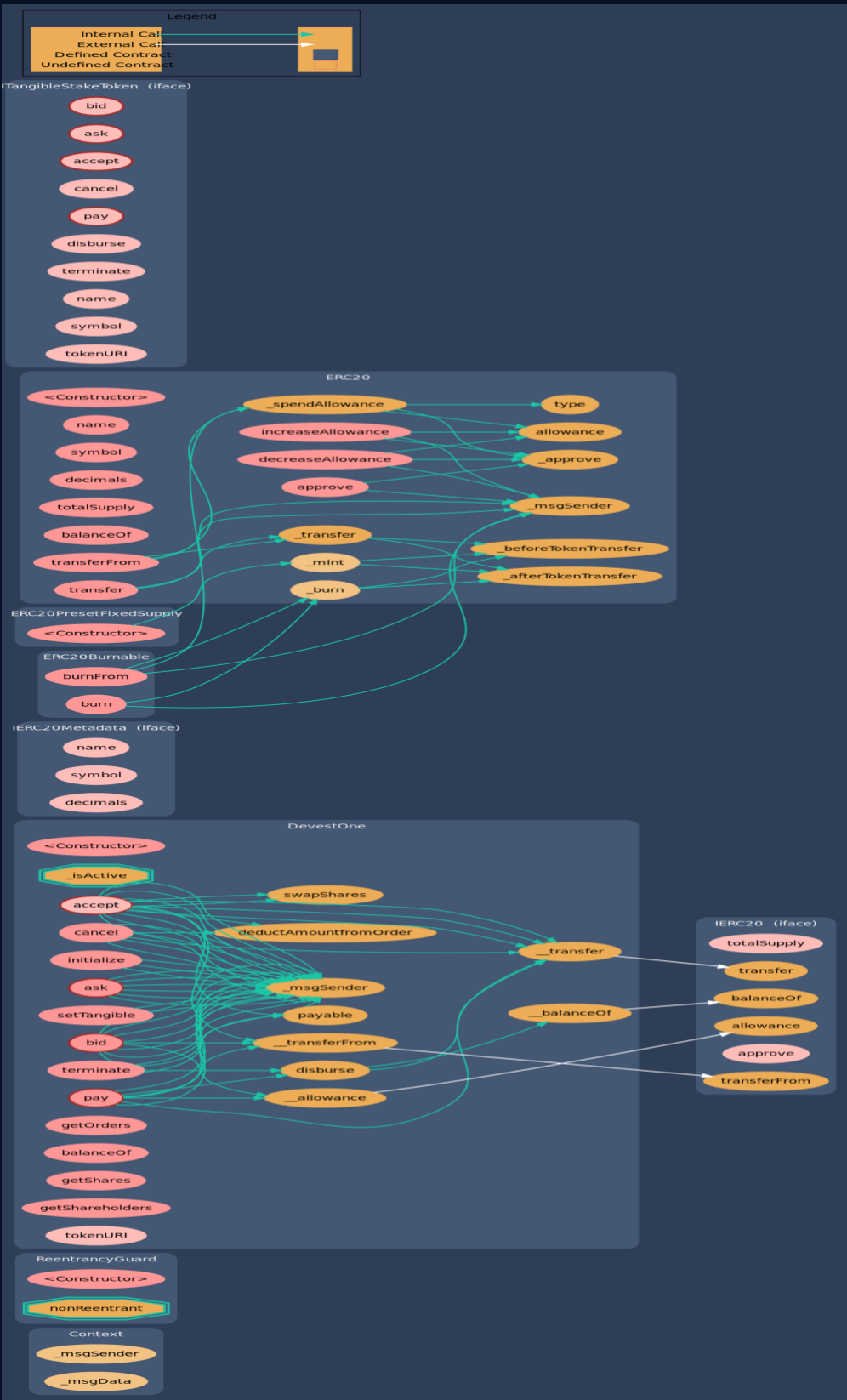
function checkSuccess() public {
    // Use 'Assert' methods: https://remix-
    ide.readthedocs.io/en/latest/assert_library.html
    Assert.ok(2 == 2, 'should be true');
    Assert.greaterThan(uint(2), uint(1), "2 should be greater than to
1");
    Assert.lesserThan(uint(2), uint(3), "2 should be lesser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

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

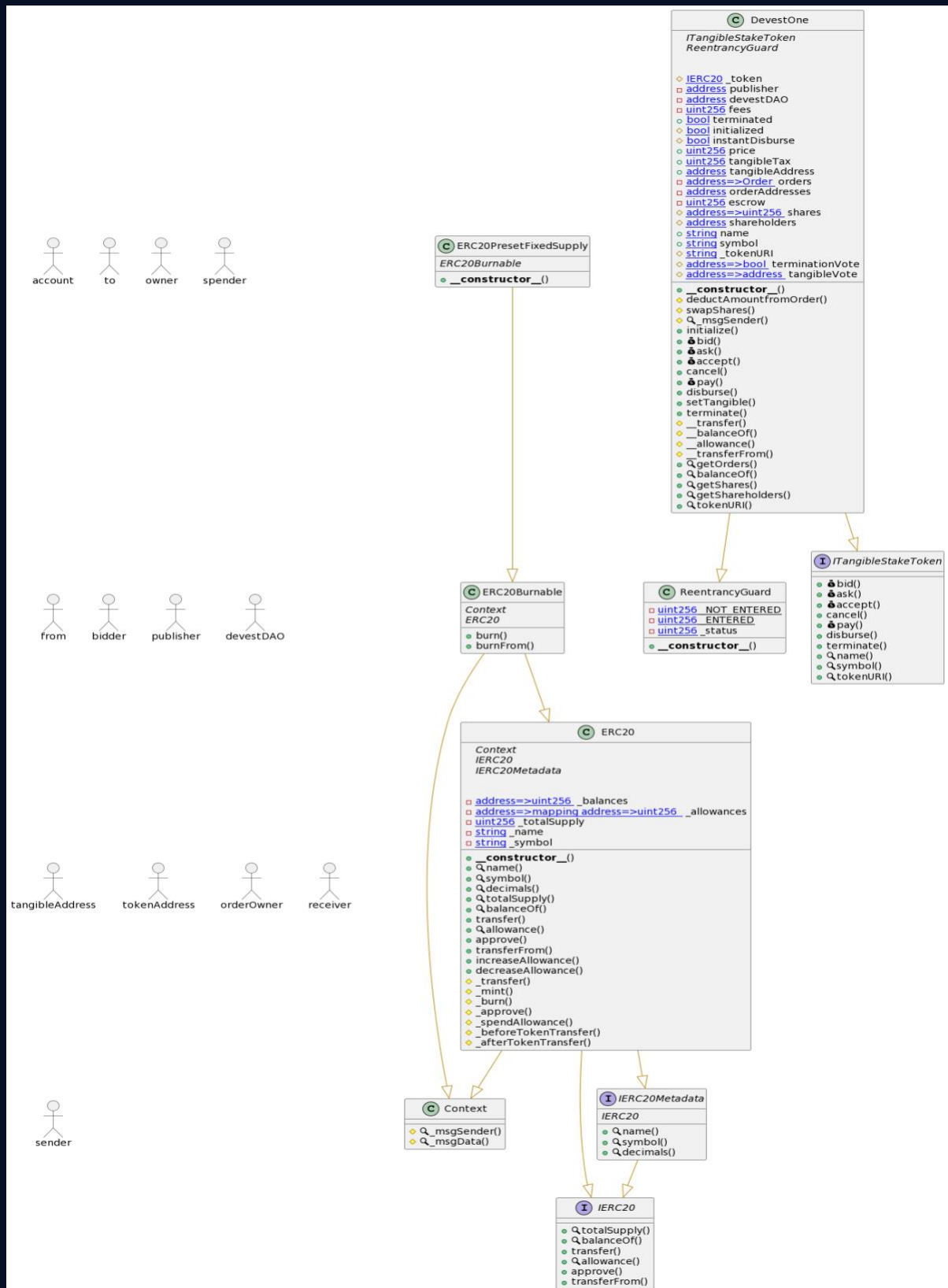
function checkFailure() public {
    Assert.notEqual(uint(1), uint(2), "1 should not be equal to 1");
}

/// 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
3	0	3	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
46	8

External	Internal	Private	Pure	View
21	51	0	0	23

StateVariables

Total	 Public
28	6

Capabilities

Solidity Versions observed	✔ Experimental Features	👛 Can Receive Funds	📜 Uses Assembly	🔥 Has Destroyable Contracts	
<div>^0.8.0</div> <div>^0.8.4</div> <div>^0.8.12</div>		yes			
📡 Transfers ETH	⚡ Low-Level Calls	👥 DelegateCall	📦 Uses Hash Functions	🔧 ECRrecover	🔗 New/Create/Create2
yes					
🌿 TryCatch	Σ Unchecked				
	yes				

• 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
	DevestOne.sol	6	3	1184	1035	435	516	410	
	Totals	6	3	1184	1035	435	516	410	

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

=====

```
39509351 => increaseAllowance(address,uint256)
119df25f => _msgSender()
8b49d47e => _msgData()
18160ddd => totalSupply()
70a08231 => balanceOf(address)
a9059cbb => transfer(address,uint256)
dd62ed3e => allowance(address,address)
095ea7b3 => approve(address,uint256)
23b872dd => transferFrom(address,address,uint256)
06fdde03 => name()
95d89b41 => symbol()
313ce567 => decimals()
a457c2d7 => decreaseAllowance(address,uint256)
30e0789e => _transfer(address,address,uint256)
4e6ec247 => _mint(address,uint256)
6161eb18 => _burn(address,uint256)
104e81ff => _approve(address,address,uint256)
1532335e => _spendAllowance(address,address,uint256)
cad3be83 => _beforeTokenTransfer(address,address,uint256)
8f811a1c => _afterTokenTransfer(address,address,uint256)
42966c68 => burn(uint256)
79cc6790 => burnFrom(address,uint256)
598647f8 => bid(uint256,uint256)
6f941083 => ask(uint256,uint256)
cd67571c => accept(address,uint256)
ea8a1af0 => cancel()
c290d691 => pay(uint256)
abc6fd0b => disburse()
0c08bf88 => terminate()
3c130d90 => tokenURI()
09b9726f => deductAmountfromOrder(address,uint256)
0f69944c => swapShares(address,address,uint256)
525bd7b6 => initialize(uint256,uint256,bool)
```

```
f9bee225 => setTangible(address)
f9c00549 => __transfer(address,uint256)
eca68bf9 => __balanceOf(address)
0c03f6a5 => __allowance(address,uint256)
ba3f71a9 => __transferFrom(address,address,uint256)
2e2dc43e => getOrders()
f04da65b => getShares(address)
41ca641e => getShareholders()
```


• Automatic General Report

Files Description Table

File Name	SHA-1 Hash
/Users/macbook/Desktop/smart contracts/DevestOne.sol	99f3cefb0b3e32ef13e96ac5ef67a74d2b4a24b4

Contracts Description Table

Contract	Type	Bases		
↳	**Function Name**	**Visibility**	**Mutability**	**Modifiers**
Context Implementation				
↳	_msgSender	Internal	🔒	
↳	_msgData	Internal	🔒	
ReentrancyGuard Implementation				
↳	<Constructor>	Public	🔓	🚫 NO 🔒
IERC20 Interface				
↳	totalSupply	External	🔓	🚫 NO 🔒
↳	balanceOf	External	🔓	🚫 NO 🔒
↳	transfer	External	🔓	🚫 NO 🔒
↳	allowance	External	🔓	🚫 NO 🔒
↳	approve	External	🔓	🚫 NO 🔒
↳	transferFrom	External	🔓	🚫 NO 🔒
IERC20Metadata Interface IERC20				
↳	name	External	🔓	🚫 NO 🔒
↳	symbol	External	🔓	🚫 NO 🔒
↳	decimals	External	🔓	🚫 NO 🔒
ERC20 Implementation Context, IERC20, IERC20Metadata				

```



| L | <Constructor> | Public | | | NO |
| L | name | Public | | | NO |
| L | symbol | Public | | | NO |
| L | decimals | Public | | | NO |
| L | totalSupply | Public | | | NO |
| L | balanceOf | Public | | | NO |
| L | transfer | Public | | | NO |
| L | allowance | Public | | | NO |
| L | approve | Public | | | NO |
| L | transferFrom | Public | | | NO |
| L | increaseAllowance | Public | | | NO |
| L | decreaseAllowance | Public | | | NO |
| L | _transfer | Internal | | | |
| L | _mint | Internal | | | |
| L | _burn | Internal | | | |
| L | _approve | Internal | | | |
| L | _spendAllowance | Internal | | | |
| L | _beforeTokenTransfer | Internal | | | |
| L | _afterTokenTransfer | Internal | | | |
|||||
| **ERC20Burnable** | Implementation | Context, ERC20 |||
| L | burn | Public | | | NO |
| L | burnFrom | Public | | | NO |
|||||
| **ERC20PresetFixedSupply** | Implementation | ERC20Burnable |||
| L | <Constructor> | Public | | | ERC20 |
|||||
| **ITangibleStakeToken** | Interface | |||
| L | bid | External | | | NO |
| L | ask | External | | | NO |
| L | accept | External | | | NO |
| L | cancel | External | | | NO |
| L | pay | External | | | NO |
| L | disburse | External | | | NO |
| L | terminate | External | | | NO |
| L | name | External | | | NO |
| L | symbol | External | | | NO |
| L | tokenURI | External | | | NO |



```


|||||

| ****DevestOne**** | Implementation | ITangibleStakeToken, ReentrancyGuard |||



| ^L | <Constructor> | Public |  |  | NO |



| ^L | deductAmountfromOrder | Internal |  |  | |



| ^L | swapShares | Internal |  |  | |



| ^L | _msgSender | Internal |  | | |


| ^L | initialize | Public |  |  | NO |


| ^L | bid | Public |  |  | nonReentrant _isActive |



| ^L | ask | Public |  |  | nonReentrant _isActive |

| ^L | accept | External |  |  | _isActive |



| ^L | cancel | Public |  |  | _isActive |

| ^L | pay | Public |  |  | _isActive |



| ^L | disburse | Public |  |  | _isActive |



| ^L | setTangible | Public |  |  | _isActive |


| ^L | terminate | Public |  |  | _isActive |


| ^L | __transfer | Internal |  |  | |


| ^L | __balanceOf | Internal |  |  | |

| ^L | __allowance | Internal |  |  | |

| ^L | __transferFrom | Internal |  |  | |

| ^L | getOrders | Public |  | | NO |

| ^L | balanceOf | Public |  | | NO |

| ^L | getShares | Public |  | | NO |


| ^L | getShareholders | Public |  | | NO |


| ^L | tokenURI | External |  | | NO |

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, 1 low issues, and 0 notes.