Smart Contract Security Audit V1

Valobit

VALOBIT Token Smart Contract

https://valobit.io/

https://www.valobitdx.io/

28/9/2022

https://saferico.com/
https://github.com/Saferico
business@saferico.com
https://t.me/SFI_ANN

–

Table of Contents

Table of Contents

Background

Project Information

- Token Information
- Executive Summary

File and Function Level Report

- **File in Scope:**

Issues Checking Status

- Severity Definitions
- Audit Findings

Automatic testing

- Testing proves
- Inheritance graph
- Call graph

Unified Modeling Language (UML)

Functions signature

Automatic general report

Conclusion

Disclaimer

Background

The purpose of the audit was to achieve the following:

- Ensure that the smart contract functions as intended.
- Identify potential security issues with the smart contract.

The information in this report should be used to understand the risk exposure of the smart contract, and as a guide to improve the security posture of the smart contract by remediating the issues that were identified.

Project Information

- **Platform**: Ethereum
- **Contract Address**: 0xb8366948b4a3f07bcbf14eb1739daa42a26b07c4
- **Code Source:**

https://etherscan.io/token/0xb8366948b4a3f07bcbf14eb1739daa42a26b07c4#code

Token Information

- Name: VALOBIT
- Total Supply: 1,600,000,000
- Holders: 2415
- Total transactions: 14066

Contracts address deployed to test net (ETH)

VALOBIT Token smart contract on Eth test net by the auditor to test every function (ETH Test Net)

https://rinkeby.etherscan.io/address/0x00805f1790e171ea4a0a3969e8ff24dbd5fda952

Executive Summary

According to our assessment, the customer`s solidity smart contract is **Secured**.

Well Secured	
Secured	✓
Poor Secured	
Insecure	

Automated checks are with remix IDE. All issues were performed by the team, which included the analysis of code functionality, manual audit found during automated analysis were manually reviewed and applicable vulnerabilities are presented in the audit overview section. The general overview is presented in the Project Information section and all issues found are located in the audit overview section.

Team found 0 critical, 0 high, 0 medium, 0 low, 0 very low-level issues and 3 notes in all solidity files of the contract

The files:

VALOBIT.sol

File and Function Level Report

File in Scope:

Contract Name	SHA 256 hash	Contract Address
VALOBIT.sol	**24f8b460314c96068904ca3268b1173d25bf74ea902ce8d212ef6b87a9e8a643**	0xb8366948b4a3f07bcbf14eb1739daa42a26b07c4

- Contract: VALOBIT
- Inherit: StandardToken
- Observation: All passed including security check
- Test Report: passed
- Score: passed
- Conclusion: passed

Function	Test Result	Type / Return Type	Score
name	✓	Read / public	**Passed**
symbol	✓	Read / public	**Passed**
decimals	✓	Read / public	**Passed**
totalSupply	✓	Read / public	**Passed**
allowance	✓	Read / public	**Passed**
balanceOf	✓	Read / public	**Passed**
INITIAL_SUPPLY	✓	Read / public	**Passed**
approve	✓	Write / public	**Passed**
transferFrom	✓	Write / public	**Passed**
decreaseApproval	✓	Write / public	**Passed**
transfer	✓	Write / public	**Passed**
increaseApproval	✓	Write / public	**Passed**

Issues Checking Status

No.	Issue Description	Checking Status
1	Compiler warnings.	**Passed**
2	Race conditions and Reentrancy. Cross-function race conditions.	**Passed**
3	Possible delays in data delivery.	**Passed**
4	Oracle calls.	**Passed**
5	Design Logic.	**Passed**
6	Timestamp dependence.	**Passed**
7	Integer Overflow and Underflow.	**Passed**
8	DoS with Revert.	**Passed**
9	DoS with block gas limit.	**Passed with notes**
10	Methods execution permissions.	**Passed**
11	Economy model. If application logic is based on an incorrect economic model, the application would not function correctly and participants would incur financial losses. This type of issue is most often found in bonus rewards systems, Staking and Farming contracts, Vault and Vesting contracts, etc.	**Passed**
12	The impact of the exchange rate on the logic.	**Passed**
13	Private user data leaks.	**Passed**
14	Malicious Event log.	**Passed**
15	Scoping and Declarations.	**Passed**
16	Uninitialized storage pointers.	**Passed**
17	Arithmetic accuracy.	**Passed**

Severity Definitions

Risk Level	Description
Critical	Critical vulnerabilities are usually straightforward to exploit and can lead to tokens loss etc.
High	High-level vulnerabilities are difficult to exploit; however, they also have significant impact on smart contract execution, e.g. public access to crucial functions
Medium	Medium-level vulnerabilities are important to fix; however, they can’t lead to tokens lose
Low	Low-level vulnerabilities are mostly related to outdated, unused etc. code snippets, that can’t have significant impact on execution
Note	Lowest-level vulnerabilities, code style violations and info statements can’t affect smart contract execution and can be ignored.

Audit Findings

Critical:

No Critical severity vulnerabilities were found.

High:

No High severity vulnerabilities were found.

Medium:

No Medium severity vulnerabilities were found.

Low:

No Low severity vulnerabilities were found.

Very Low:

No Very Low severity vulnerabilities were found.

Notes:

Unused variables

Description

Unused variables are allowed in Solidity and they do not pose a direct security issue. It is best practice though to avoid them as they can:
- cause an increase in computations (and unnecessary gas consumption)
- indicate bugs or malformed data structures and they are generally a sign of poor code quality
- cause code noise and decrease readability of the code

In this code the initial supply is the total supply so no need to make 2 variables.

```
uint256 public constant INITIAL_SUPPLY = 1600000000 * (10 ** uint256(decimals));

  constructor() public {

    totalSupply_ = INITIAL_SUPPLY;

    balances[msg.sender] = INITIAL_SUPPLY;
```

Status Acknowledged.

#Compiler version is old

Description
The compiler being used was released 4 years – 4 years and half ago. It's recommended to use more recent compiler version, there can be benefits like reduction in bytecode size etc.

Comment: This project from 2018 and this compiler was the best in its time.

Constant calculations in the contract

Description

recalculated initialization will save 2847 units of gas in deployment

```
    uint256 public constant INITIAL_SUPPLY = 1600000000 * (10 **
uint256(decimals));
```

Recommendation

Replace the initialization as

```
        uint256 public constant INITIAL_SUPPLY = 1600000000000000000000000000;
```

Status Acknowledged.

Automatic Testing

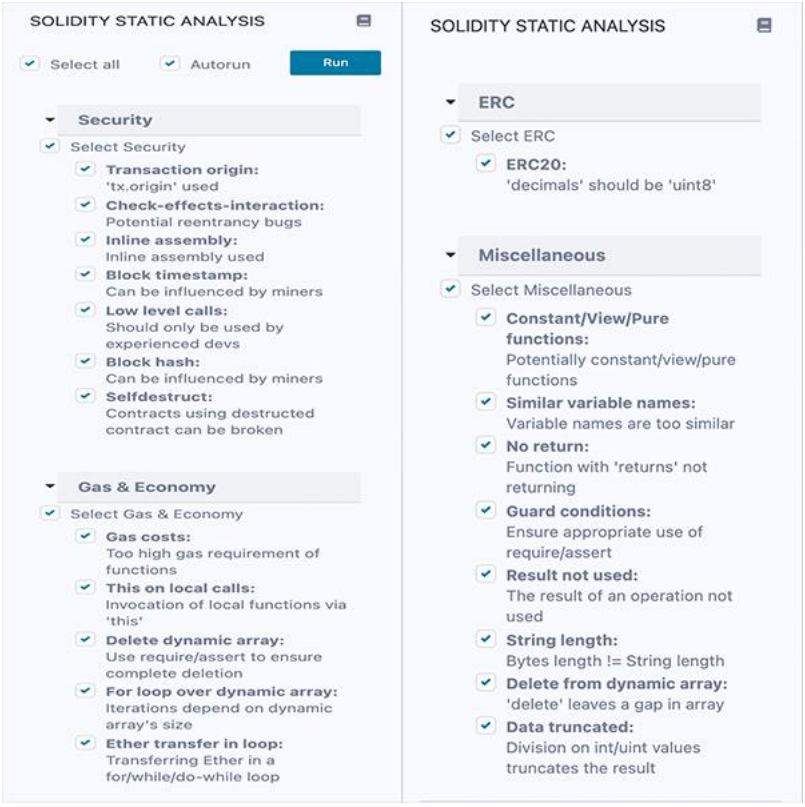
1- Check for security

24f8b460314c96068904ca3268b1173d25bf74ea902ce8d212ef6b87a9e8a643

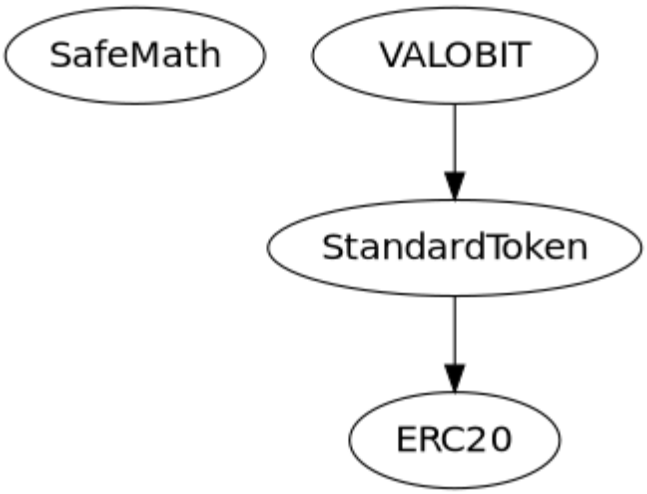
File: VALOBIT.... | Language: solidity | Size: 7141 bytes | Date: 2022-09-28T09:03:56.858Z

Critical	High	Medium	Low	Note
0	0	0	0	0

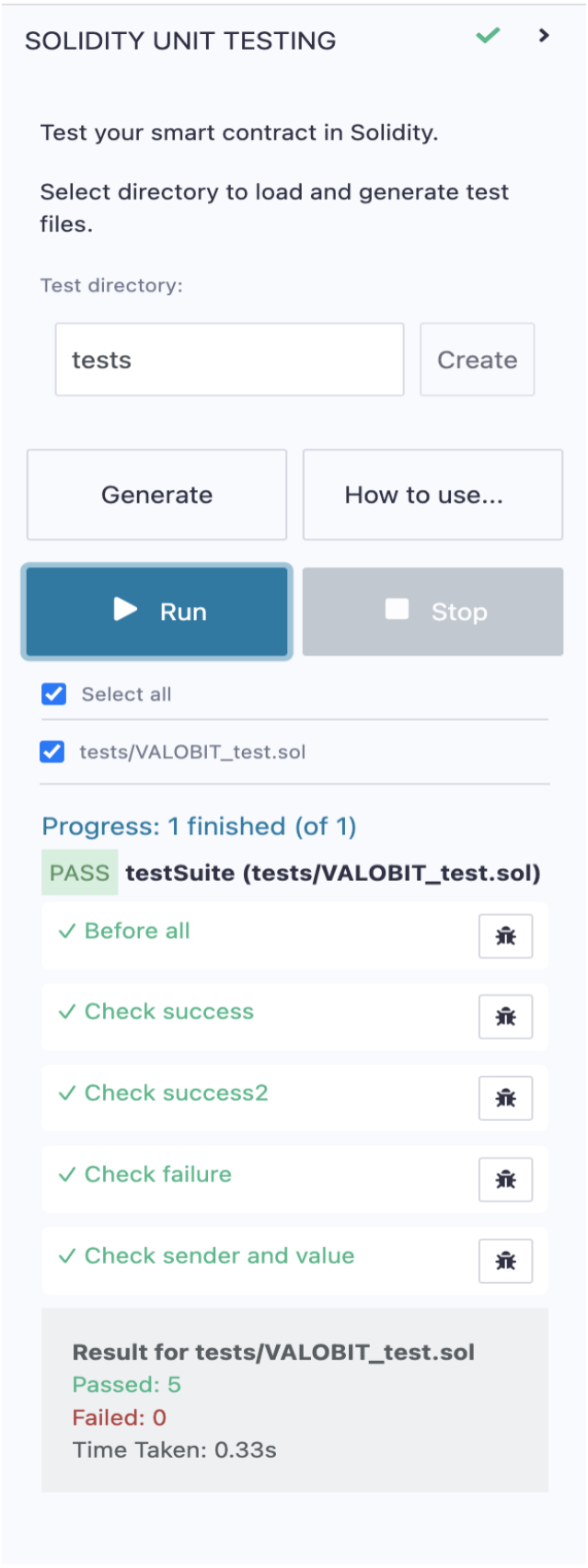
2- SOLIDITY STATIC ANALYSIS



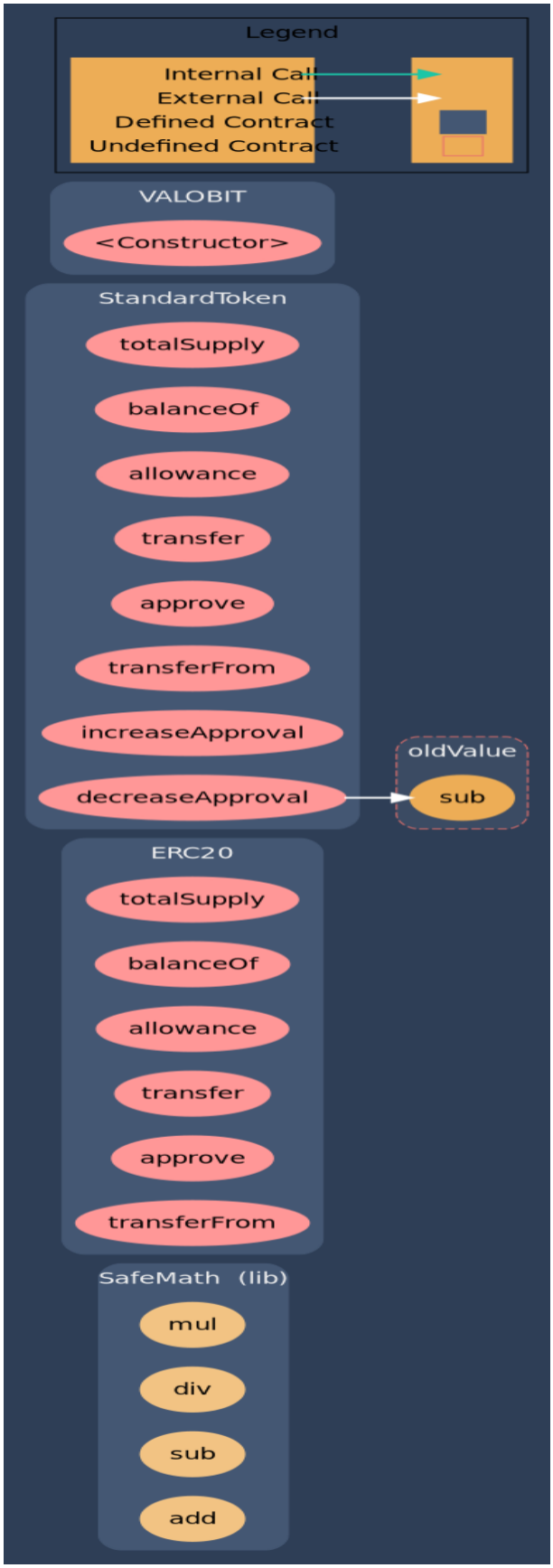
3- Inheritance graph



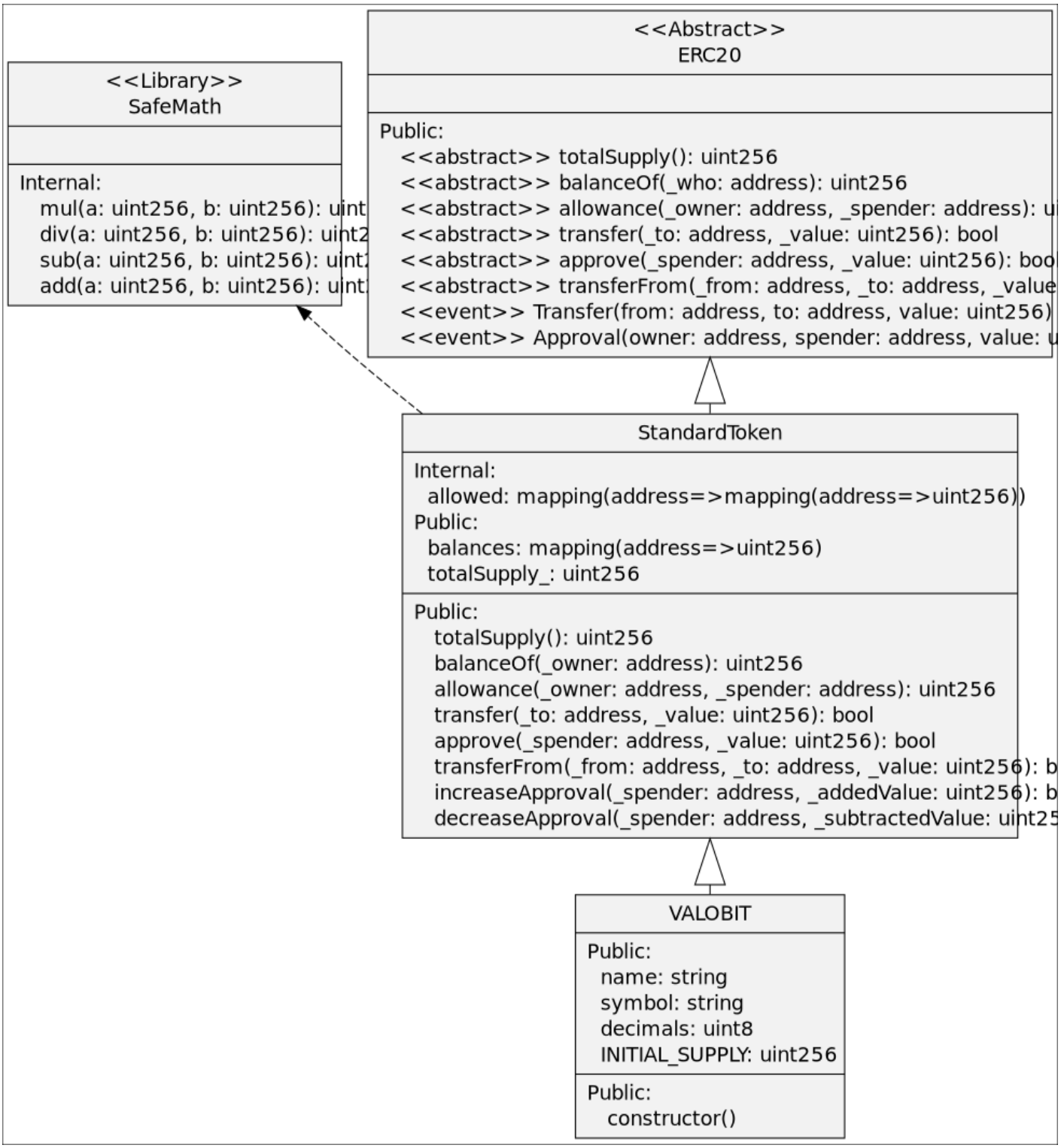
4- SOLIDITY UNIT TESTING



5- Call graph


Legend
Internal Call
External Call
Defined Contract
Undefined Contract
VALOBIT
<Constructor>
StandardToken
totalSupply
balanceOf
allowance
transfer
approve
transferFrom
increaseApproval
decreaseApproval
oldValue
sub
ERC20
totalSupply
balanceOf
allowance
transfer
approve
transferFrom
SafeMath (lib)
mul
div
sub
add

Unified Modeling Language (UML)



Functions signature

```
Sighash   |   Function Signature
========================
66188463  =>  decreaseApproval(address,uint256)
c8a4ac9c  =>  mul(uint256,uint256)
a391c15b  =>  div(uint256,uint256)
b67d77c5  =>  sub(uint256,uint256)
771602f7  =>  add(uint256,uint256)
18160ddd  =>  totalSupply()
70a08231  =>  balanceOf(address)
dd62ed3e  =>  allowance(address,address)
a9059cbb  =>  transfer(address,uint256)
095ea7b3  =>  approve(address,uint256)
23b872dd  =>  transferFrom(address,address,uint256)
d73dd623  =>  increaseApproval(address,uint256)
```

Automatic general report

Files Description Table

File Name	SHA-1 Hash
/Users/macbook/Desktop/smart contracts/VALOBIT.sol	92b0748f4886aec4da30025db4a594b27ff6151e

Contracts Description Table

Contract	Type	Bases			
└	**Function Name**	**Visibility**	**Mutability**	**Modifiers**
SafeMath	Library				
└	mul	Internal 🔒			
└	div	Internal 🔒			
└	sub	Internal 🔒			
└	add	Internal 🔒			
ERC20	Implementation				
└	totalSupply	Public ❗		NO❗	
└	balanceOf	Public ❗		NO❗	
└	allowance	Public ❗		NO❗	
└	transfer	Public ❗	🛑	NO❗	
└	approve	Public ❗	🛑	NO❗	
└	transferFrom	Public ❗	🛑	NO❗	
StandardToken	Implementation	ERC20			
└	totalSupply	Public ❗		NO❗	
└	balanceOf	Public ❗		NO❗	
└	allowance	Public ❗		NO❗	
└	transfer	Public ❗	🛑	NO❗	
└	approve	Public ❗	🛑	NO❗	
└	transferFrom	Public ❗	🛑	NO❗	
└	increaseApproval	Public ❗	🛑	NO❗	
└	decreaseApproval	Public ❗	🛑	NO❗	
VALOBIT	Implementation	StandardToken			
└	<Constructor>	Public ❗	🛑	NO❗	

Legend

Symbol	Meaning
🛑	Function can modify state
💵	Function is payable

Conclusion

The contracts are written systematically. Team found no critical issues. So, it is good to go for production.

Since possible test cases can be unlimited and developer level documentation (code flow diagram with function level description) not provided, for such an extensive smart contract protocol, we provide no such guarantee of future outcomes. We have used all the latest static tools and manual observations to cover maximum possible test cases to scan Everything.

Security state of the reviewed contract is “Secured”.

✓ No mint function.
✓ No volatile code.
✓ No high severity issues were found.

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 s) 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.