Smart Contract
Security Audit
V1

Rootygang Smart Contract

2/8/2022

https://saferico.com/

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

–

Table of Contents

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**: 0x7776c38dee89502FEAEb1588Aa98F3B8636525cB
- **Code:**

https://etherscan.io/address/0x7776c38dee89502FEAEb1588Aa98F3B8636525cB#code

NFT Information

- Name: Rootygang
- MAX Supply: 450
- Holders:
- Total transactions:

Contracts address deployed to test net (Ethereum)

Rootygang smart contract on Ethereum test net to test every function by the auditor.

https://rinkeby.etherscan.io/address/0xbe7f4e04aeacebd3697a22cfdc5a0d7c1563d743

Executive Summary

According to our assessment, the customer`s solidity smart contract is **“WELL SECURED”**. The team has fixed the low-level issues.

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, 3 low, 0 very low-level issues and 0 note in all solidity files of the contract

The files:

Rootygang.sol

File and Function Level Report

File in Scope:

Contract Name	SHA 256 hash	Contract Address
Rootygang.sol	**e38a2e416eb026594a14ae59a75550ed67d3e54ae4708d04e8593d17cadc9f68**	0x7776c38dee89502FEAEb1588Aa98F3B8636525cB

- Contract: Rootygang
- Inherit: ERC721, Ownable
- 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**
cost	✓	Read / public	**Passed**
supportsInterface	✓	Read / public	**Passed**
maxMintAmountPerTx	✓	Read / public	**Passed**
balanceOf	✓	Read / public	**Passed**
Owner	✓	Read / public	**Passed**
addressMintedBalance	✓	Read / public	**Passed**
nftPerAddressLimit	✓	Read / public	**Passed**
getApprovedForAll	✓	Read / public	**Passed**
hiddenMetadataUri	✓	Read / public	**Passed**
getApproved	✓	Read / public	**Passed**

ownerOf	✓	Read / public	**Passed**
tokenURI	✓	Read / public	**Passed**
totalSupply	✓	Read / public	**Passed**
maxSupply	✓	Read / public	**Passed**
revealed	✓	Read / public	**Passed**
paused	✓	Read / public	**Passed**
uriSuffix	✓	Read / public	**Passed**
uriPrefix	✓	Read / public	**Passed**
walletOfOwner	✓	Read / public	**Passed**
mint	✓	Write / payable	**Passed**
approve	✓	Write / public	**Passed**
safeTransferFrom	✓	Write / public	**Passed**
safeTransferFrom	✓	Write / public	**Passed**
setPaused	✓	Write / public	**Passed**
withdraw	✓	Write / public	**Passed**
setRevealed	✓	Write / public	**Passed**
transferOwnership	✓	Write / public	**Passed**
setApprovalForAll	✓	Write / public	**Passed**
transferFrom	✓	Write / public	**Passed**
setHiddenMetadataUri	✓	Write / public	**Passed**
renounceOwnership	✓	Write / public	**Passed**
mintForAddress	✓	Write / public	**Passed**
setMaxMintAmountPerTx	✓	Write / public	**Passed**
setCost	✓	Write / public	**Passed**
setUriPrefix	✓	Write / public	**Passed**
setUriSuffix	✓	Write / public	**Passed**
setNftPerAddressLimit	✓	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:

#Missing zero address validation

Description

When the owner wants to mint NFTs for investors, he has to check for the zero address to make, he didn't mint for the zero address. Otherwise, the mint function will act like burn function.

```
function mintForAddress(uint256 _mintAmount, address _receiver) public
mintCompliance(_mintAmount) onlyOwner {
    _mintLoop(_receiver, _mintAmount);
  }
```

Remediation

Use the require statement to check for zero addresses, require to check if the contract is paused or not, and check the amount + total mint <= Max Supply.

Status: Closed. Fixed in version 2.

#Multiple pragma statements

Line	Pragma
11	pragma solidity ^0.8.0;
57	pragma solidity ^0.8.0;
127	pragma solidity ^0.8.0;
154	pragma solidity ^0.8.0;
232	pragma solidity ^0.8.1;
457	pragma solidity ^0.8.0;
487	pragma solidity ^0.8.0;
515	pragma solidity ^0.8.0;
546	pragma solidity ^0.8.0;

691	pragma solidity ^0.8.0;
720	pragma solidity ^0.8.0;
1170	pragma solidity >=0.7.0 <0.9.0;

Description
There are multiple pragma statements in the code. The newest compiler version 0.8.15 will work with the code, but keeping only one pragma statement helps in maintaining readability of the code.

Remediation
Keep a single pragma statement.

Status: Closed. Fixed In version 2

#Owner privileges (In the period when the owner isn't renounced)

Description
The owner can mint the NFT to any address.
The owner can pause and un pause the contract.
The owner can change the price.

```
function mintForAddress(uint256 _mintAmount, address _receiver) public
mintCompliance(_mintAmount) onlyOwner {
    _mintLoop(_receiver, _mintAmount);
  }

function setCost(uint256 _cost) public onlyOwner {
        cost = _cost;
    }
function setPaused(bool _state) public onlyOwner {
        paused = _state;
    }
```

Remediation
Make these functions internal in next version or the team should announce the investors before doing anything to give them time if they want to do anything.
P.S: This issue is common to the majority of NFT smart contracts.

Status: Acknowledged.

Very Low:

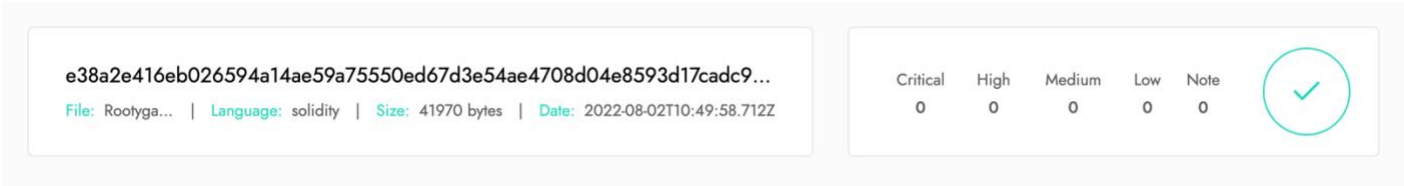
No Very Low severity vulnerabilities were found.

Notes:

No Notes vulnerabilities were found.

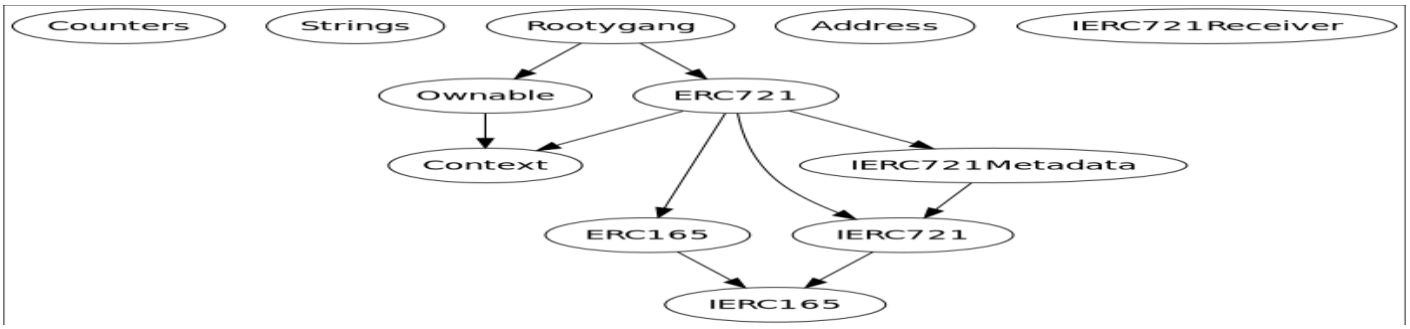
Automatic Testing

1- Check for security

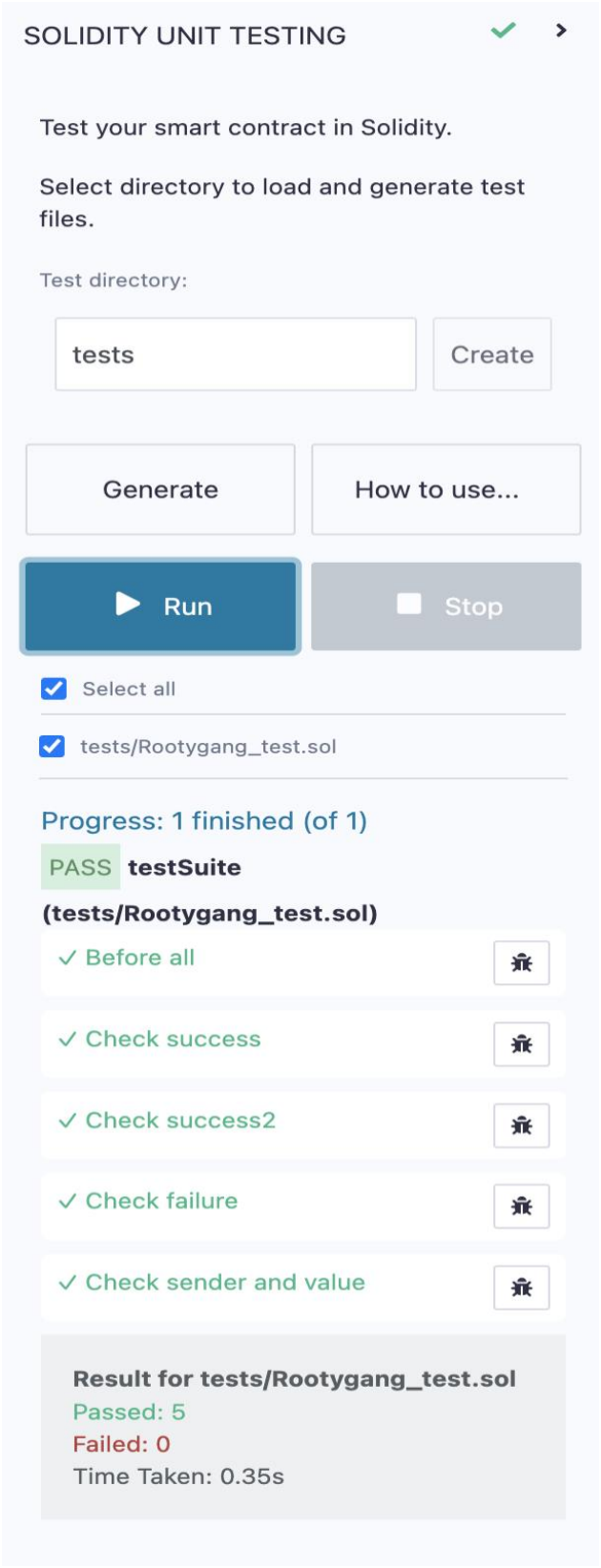


2- SOLIDITY STATIC ANALYSIS

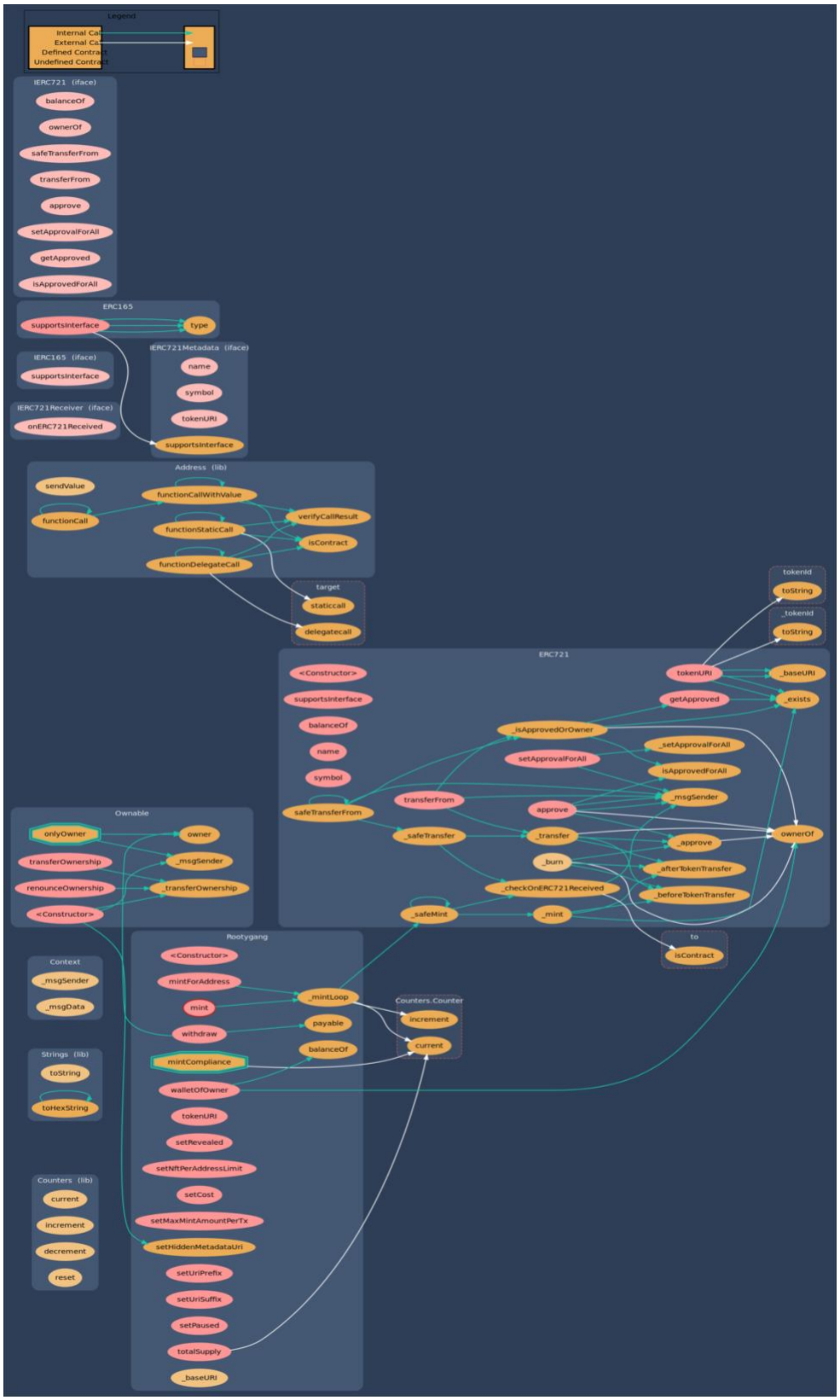
3- Inheritance graph



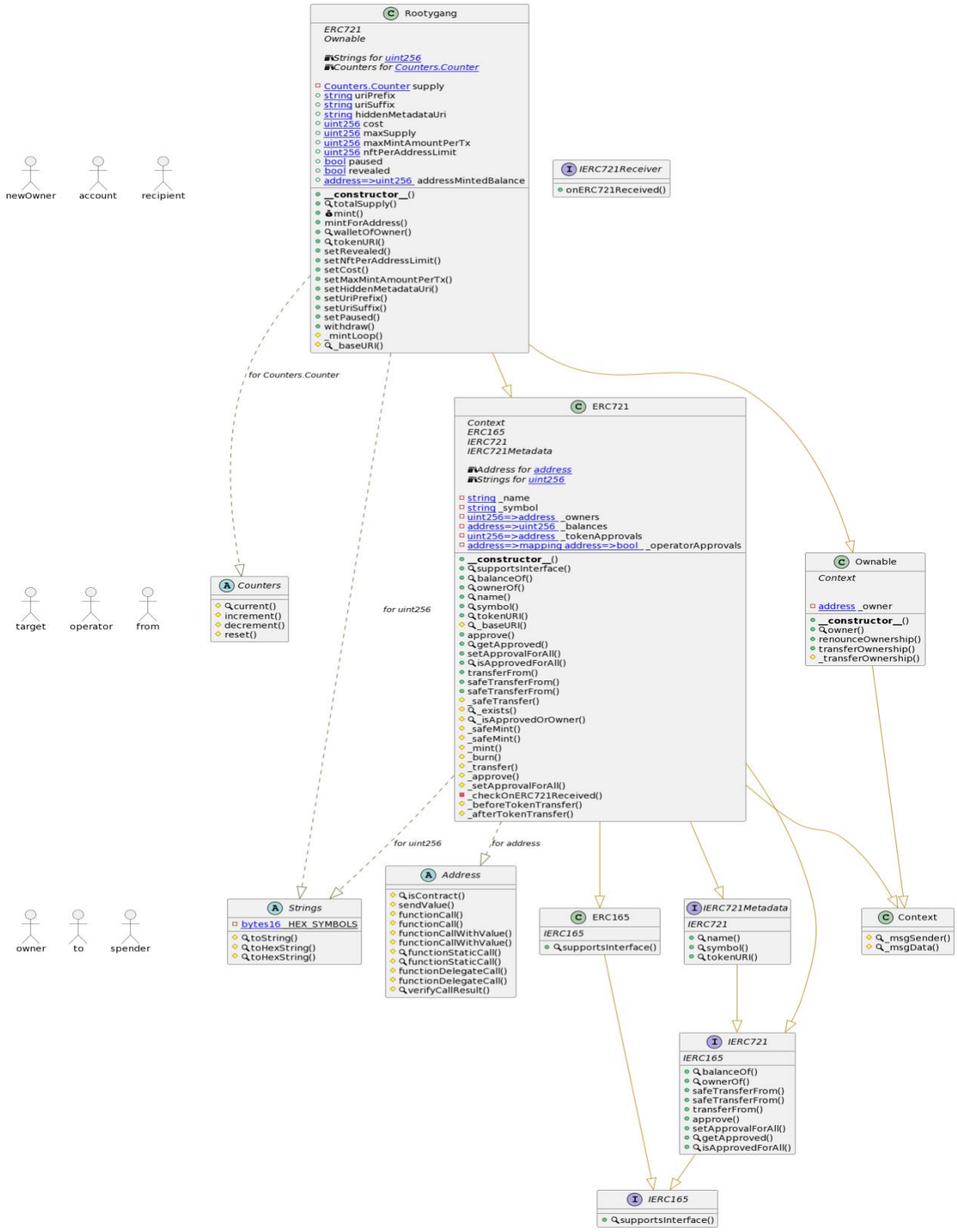
4- SOLIDITY UNIT TESTING



5- Call graph


Legend
Internal Call
External Call
Defined Contract
Undefined Contract
IERC721 (iface)
balanceOf
ownerOf
safeTransferFrom
transferFrom
approve
setApprovalForAll
getApproved
isApprovedForAll
ERC165
supportsInterface
type
IERC165 (iface)
supportsInterface
IERC721Metadata (iface)
name
symbol
tokenURI
supportsInterface
IERC721Receiver (iface)
onERC721Received
Address (lib)
sendValue
functionCallWithValue
functionCall
functionStaticCall
functionDelegateCall
verifyCallResult
isContract
target
staticcall
delegatecall
tokenId
toString
_tokenId
toString
ERC721
<Constructor>
supportsInterface
balanceOf
name
symbol
safeTransferFrom
transferFrom
_safeTransfer
_isApprovedOrOwner
setApprovalForAll
approve
_transfer
_burn
_checkOnERC721Received
_safeMint
_mint
tokenURI
getApproved
_setApprovalForAll
isApprovedForAll
_msgSender
_approve
_afterTokenTransfer
_beforeTokenTransfer
_baseURI
_exists
ownerOf
to
isContract
Ownable
onlyOwner
transferOwnership
renounceOwnership
<Constructor>
owner
_msgSender
_transferOwnership
Rootygang
<Constructor>
mintForAddress
mint
withdraw
mintCompliance
walletOfOwner
tokenURI
setRevealed
setNftPerAddressLimit
setCost
setMaxMintAmountPerTx
setHiddenMetadataUri
setUriPrefix
setUriSuffix
setPaused
totalSupply
_baseURI
_mintLoop
payable
balanceOf
Counters.Counter
increment
current
Context
_msgSender
_msgData
Strings (lib)
toString
toHexString
Counters (lib)
current
increment
decrement
reset

Unified Modeling Language (UML)



Functions signature

```
Sighash   |   Function Signature
========================
16279055  =>  isContract(address)
ad04a8d1  =>  current(Counter)
e2bee435  =>  increment(Counter)
854ec98e  =>  decrement(Counter)
440d212a  =>  reset(Counter)
6900a3ae  =>  toString(uint256)
8fba8d5c  =>  toHexString(uint256)
63e1cbea  =>  toHexString(uint256,uint256)
119df25f  =>  _msgSender()
8b49d47e  =>  _msgData()
8da5cb5b  =>  owner()
715018a6  =>  renounceOwnership()
f2fde38b  =>  transferOwnership(address)
d29d44ee  =>  _transferOwnership(address)
24a084df  =>  sendValue(address,uint256)
a0b5ffb0  =>  functionCall(address,bytes)
241b5886  =>  functionCall(address,bytes,string)
2a011594  =>  functionCallWithValue(address,bytes,uint256)
d525ab8a  =>  functionCallWithValue(address,bytes,uint256,string)
c21d36f3  =>  functionStaticCall(address,bytes)
dbc40fb9  =>  functionStaticCall(address,bytes,string)
ee33b7e2  =>  functionDelegateCall(address,bytes)
57387df0  =>  functionDelegateCall(address,bytes,string)
946b5793  =>  verifyCallResult(bool,bytes,string)
150b7a02  =>  onERC721Received(address,address,uint256,bytes)
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)
06fdde03  =>  name()
95d89b41  =>  symbol()
c87b56dd  =>  tokenURI(uint256)
743976a0  =>  _baseURI()
24b6b8c0  =>  _safeTransfer(address,address,uint256,bytes)
f8e76cc0  =>  _exists(uint256)
4cdc9549  =>  _isApprovedOrOwner(address,uint256)
b3e1c718  =>  _safeMint(address,uint256)
6a4f832b  =>  _safeMint(address,uint256,bytes)
4e6ec247  =>  _mint(address,uint256)
9b1f9e74  =>  _burn(uint256)
30e0789e  =>  _transfer(address,address,uint256)
7b7d7225  =>  _approve(address,uint256)
8c4e3f32  =>  _setApprovalForAll(address,address,bool)
1fd01de1  =>  _checkOnERC721Received(address,address,uint256,bytes)
cad3be83  =>  _beforeTokenTransfer(address,address,uint256)
```

```
8f811a1c  =>  _afterTokenTransfer(address,address,uint256)
18160ddd  =>  totalSupply()
a0712d68  =>  mint(uint256)
efbd73f4  =>  mintForAddress(uint256,address)
438b6300  =>  walletOfOwner(address)
e0a80853  =>  setRevealed(bool)
d0eb26b0  =>  setNftPerAddressLimit(uint256)
44a0d68a  =>  setCost(uint256)
b071401b  =>  setMaxMintAmountPerTx(uint256)
4fdd43cb  =>  setHiddenMetadataUri(string)
7ec4a659  =>  setUriPrefix(string)
16ba10e0  =>  setUriSuffix(string)
16c38b3c  =>  setPaused(bool)
3ccfd60b  =>  withdraw()
0d43db94  =>  _mintLoop(address,uint256)
```

Automatic general report

Files Description Table

File Name	SHA-1 Hash
/Users/macbook/Desktop/smart contracts/Rootygang.sol	f0f3f0ac948320d138d681c3ff92bd2bd2f5b81f

Contracts Description Table

Contract	Type	Bases		
└	**Function Name**	**Visibility**	**Mutability**	**Modifiers**
Counters	Library			
└	current	Internal 🔒		
└	increment	Internal 🔒	🛑	
└	decrement	Internal 🔒	🛑	
└	reset	Internal 🔒	🛑	
Strings	Library			
└	toString	Internal 🔒		
└	toHexString	Internal 🔒		
└	toHexString	Internal 🔒		
Context	Implementation			
└	_msgSender	Internal 🔒		
└	_msgData	Internal 🔒		
Ownable	Implementation	Context		
└	<Constructor>	Public ❗	🛑	NO❗
└	owner	Public ❗		NO❗
└	renounceOwnership	Public ❗	🛑	onlyOwner
└	transferOwnership	Public ❗	🛑	onlyOwner
└	_transferOwnership	Internal 🔒	🛑	
Address	Library			
└	isContract	Internal 🔒		
└	sendValue	Internal 🔒	🛑	
└	functionCall	Internal 🔒	🛑	
└	functionCall	Internal 🔒	🛑	
└	functionCallWithValue	Internal 🔒	🛑	
└	functionCallWithValue	Internal 🔒	🛑	
└	functionStaticCall	Internal 🔒		
└	functionStaticCall	Internal 🔒		
└	functionDelegateCall	Internal 🔒	🛑	
└	functionDelegateCall	Internal 🔒	🛑	
└	verifyCallResult	Internal 🔒		
IERC721Receiver	Interface			


└	onERC721Received	External ❗	🔘	NO❗
IERC165	Interface			
└	supportsInterface	External ❗		NO❗
ERC165	Implementation	IERC165		
└	supportsInterface	Public ❗		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❗
IERC721Metadata	Interface	IERC721		
└	name	External ❗		NO❗
└	symbol	External ❗		NO❗
└	tokenURI	External ❗		NO❗
ERC721	Implementation	Context, ERC165, IERC721, IERC721Metadata		
└	<Constructor>	Public ❗	🔘	NO❗
└	supportsInterface	Public ❗		NO❗
└	balanceOf	Public ❗		NO❗
└	ownerOf	Public ❗		NO❗
└	name	Public ❗		NO❗
└	symbol	Public ❗		NO❗
└	tokenURI	Public ❗		NO❗
└	_baseURI	Internal 🔒		
└	approve	Public ❗	🔘	NO❗
└	getApproved	Public ❗		NO❗
└	setApprovalForAll	Public ❗	🔘	NO❗
└	isApprovedForAll	Public ❗		NO❗
└	transferFrom	Public ❗	🔘	NO❗
└	safeTransferFrom	Public ❗	🔘	NO❗
└	safeTransferFrom	Public ❗	🔘	NO❗
└	_safeTransfer	Internal 🔒	🔘	
└	_exists	Internal 🔒		
└	_isApprovedOrOwner	Internal 🔒		
└	_safeMint	Internal 🔒	🔘	
└	_safeMint	Internal 🔒	🔘	
└	_mint	Internal 🔒	🔘	
└	_burn	Internal 🔒	🔘	
└	_transfer	Internal 🔒	🔘	
└	_approve	Internal 🔒	🔘	
└	_setApprovalForAll	Internal 🔒	🔘	
└	_checkOnERC721Received	Private 🔐	🔘	
└	_beforeTokenTransfer	Internal 🔒	🔘	
└	_afterTokenTransfer	Internal 🔒	🔘	
Rootygang	Implementation	ERC721, Ownable		

└	<Constructor>	Public ❗	🛑	ERC721
└	totalSupply	Public ❗		NO❗
└	mint	Public ❗	💵	mintCompliance
└	mintForAddress	Public ❗	🛑	mintCompliance onlyOwner
└	walletOfOwner	Public ❗		NO❗
└	tokenURI	Public ❗		NO❗
└	setRevealed	Public ❗	🛑	onlyOwner
└	setNftPerAddressLimit	Public ❗	🛑	onlyOwner
└	setCost	Public ❗	🛑	onlyOwner
└	setMaxMintAmountPerTx	Public ❗	🛑	onlyOwner
└	setHiddenMetadataUri	Public ❗	🛑	onlyOwner
└	setUriPrefix	Public ❗	🛑	onlyOwner
└	setUriSuffix	Public ❗	🛑	onlyOwner
└	setPaused	Public ❗	🛑	onlyOwner
└	withdraw	Public ❗	🛑	onlyOwner
└	_mintLoop	Internal 🔒	🛑	
└	_baseURI	Internal 🔒		

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 “ Well Secured”.

✓ No volatile code.

✓ No many high severity issues were found.

✓ Low (or very low) level issues have been fixed.

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.