Smart Contract
Security Audit
V1

CHI NFT Smart Contract

20/3/2022

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**: 0x541DDB0de848A15AFb552E3B9ff72A4A4ae57815
- **Code:**

https://github.com/Saferico/Smart-Contracts-for-Projects/blob/main/CHI.sol

NFT Information

- Name: CHI
- MAX Supply: 5000
- Holders:
- Total transactions:

Contracts address deployed to test net (Ethereum)

Crypto Yachts NFT contract on ETH test net to test every function by the auditor.

https://rinkeby.etherscan.io/address/0x541ddb0de848a15afb552e3b9ff72a4a4ae57815

Executive Summary

According to our assessment, the customer`s solidity smart contract is **Well-Secured**. Because the team fix all high and low 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 1 critical, 1 high, 0 medium, 2 low, 0 very low-level issues and 1 note in all solidity files of the contract

The files:

CHI.sol
ERC721A.sol

File and Function Level Report

File in Scope:

Contract Name	SHA 256 hash	Contract Address
CHI.sol	**56a5cb21eba837f3eba447e09453b4c9a6c42d7675d669f382053578bdbf7e20**	0x541DDB0de848A15AFb552E3B9ff72A4A4ae57815

- Contract: CHI
- Inherit: ERC721A, 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**
MAX_PER_MINT	✓	Read / public	**Passed**
supportsInterface	✓	Read / public	**Passed**
merkleRoot	✓	Read / public	**Passed**
balanceOf	✓	Read / public	**Passed**
Owner	✓	Read / public	**Passed**
MAX_TOKENS	✓	Read / public	**Passed**
tokenOfOwnerByIndex	✓	Read / public	**Passed**
getApprovedForAll	✓	Read / public	**Passed**
isRevealed	✓	Read / public	**Passed**
getApproved	✓	Read / public	**Passed**

ownerOf	✓	Read / public	**Passed**
tokenURI	✓	Read / public	**Passed**
totalSupply	✓	Read / public	**Passed**
maxBatchSize	✓	Read / public	**Passed**
nextOwnerToExplicitlySet	✓	Read / public	**Passed**
presaleMaxPerWallet	✓	Read / public	**Passed**
presalePrice	✓	Read / public	**Passed**
notRevealedUri	✓	Read / public	**Passed**
presaleStarted	✓	Read / public	**Passed**
publicSalePrice	✓	Read / public	**Passed**
publicSaleStarted	✓	Read / public	**Passed**
baseExtension	✓	Read / public	**Passed**
baseURI	✓	Read / public	**Passed**
tokenByIndex	✓	Read / public	**Passed**
mintPresale	✓	Write / payable	**Passed**
approve	✓	Write / public	**Passed**
safeTransferFrom	✓	Write / public	**Passed**
safeTransferFrom	✓	Write / public	**Passed**
setPrice	✓	Write / public	**Passed**
setnotRevealedUri	✓	Write / public	**Passed**
mint	✓	Write / payable	**Passed**
setPresalePrice	✓	Write / public	**Passed**
transferOwnership	✓	Write / public	**Passed**
setApprovalForAll	✓	Write / public	**Passed**
transferFrom	✓	Write / public	**Passed**
withdrawAll	✓	Write / public	**Passed**

setMarketRoot	✓	Write / public	**Passed**
renounceOwnership	✓	Write / public	**Passed**
setBaseURI	✓	Write / public	**Passed**
ownerMint	✓	Write / public	**Passed**
setPresaleMaxPerWallet	✓	Write / public	**Passed**
toggleReveal	✓	Write / public	**Passed**
togglePresaleStarted	✓	Write / public	**Passed**
togglePublicSaleStarted	✓	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:

#Possibility of losing all funds

Description

The return value of a message call has not been checked; the developer Makes the return value as private function. Execution will resume even if the called contract throws an exception. If the call fails accidentally or an attacker forces the call to fail, this may cause unexpected behavior in the subsequent program logic, in this case could cause losing the funds

```
function withdrawAll() public onlyOwner {
        uint256 balance = address(this).balance;
        require(balance > 0);
        _widthdraw(creatorAddress, address(this).balance);
    }

    function _widthdraw(address _address, uint256 _amount) private {
        (bool success, ) = _address.call{value: _amount}("");
        require(success, "Transfer failed.");
    }
```

Remediation

Remove these functions and add a simple withdraw function only the owner can control it with require statement.

Status: Closed. Fixed in version 2.

High:

#The new public sale price will be multiply in 1 ETH

Description

Normally the price of token or NFT = $$ wei , 1 ETH = 10**18 wei so when we want to make the new price 0.1 ETH we will add 10**17 wei, the developer make huge mistake by multiply the new price * 1ETH so now with this function if the owner want to change the price of NFT to let say 0.008 ETH with this function the new price will 10**15 ETH.

```
function setPrice(uint256 _newPrice) external onlyOwner {
        price = _newPrice * (1 ether);
    }
```

Remediation

Remove multiply in 1 ETH to keep the price in wei.

Status: Closed. Fixed in version 2.

Medium:

No Medium severity vulnerabilities were found

Low:

#Pragam version not fixed

Description

It is a good practice to lock the solidity version for a live deployment (use 0.8.10 instead of ^0.8.10). 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.

#Missing zero address validation

Description

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

```
function ownerMint(address to, uint256 tokens) external onlyOwner {
        require(totalSupply() + tokens <= MAX_TOKENS, "Minting would exceed max
supply");

        require(tokens > 0, "Must mint at least one token");

        _safeMint(to, tokens);
    }
```

Remediation

Use the require statement to check for zero addresses.

```
require(to != address(0), "Not Mint for the zero address");
```

Status: Closed. Fixed in version2.

Very Low:

No Very Low severity vulnerabilities were found.

Notes:

#Unnecessary import of SafeMath, and string libraries

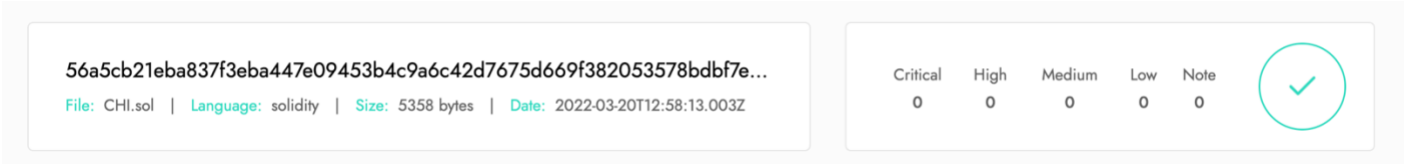
Description
The main contract inherits: ERC721A, and Ownable, and ERC721A is already import String library, And for SafeMath library, Solidity version 0.8 was released with SafeMath checks inbuilt, we can avoid using an explicit safe math library so no need to import it again in the main contract.

Remediation
Remove unnecessary libraries from the main contract save some gas fees.

Status: Closed. Fixed in version2.

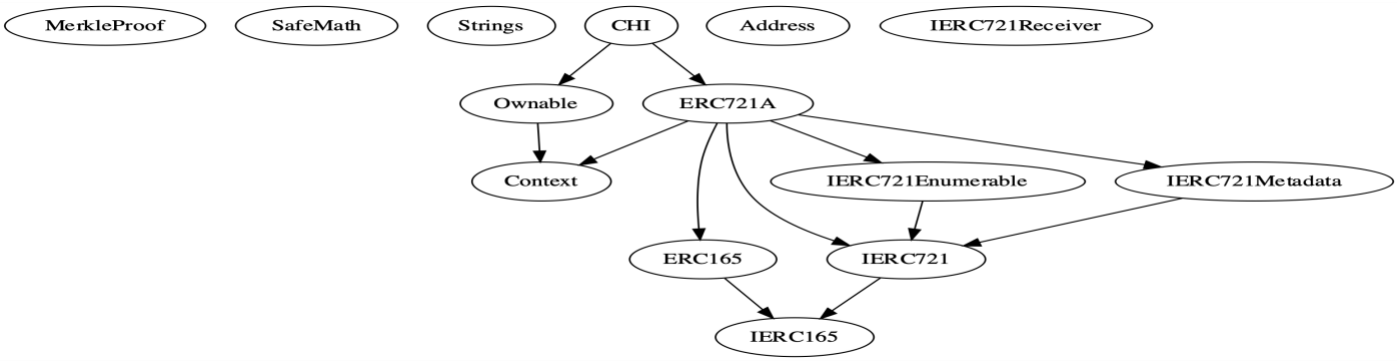
Automatic Testing

1- Check for security

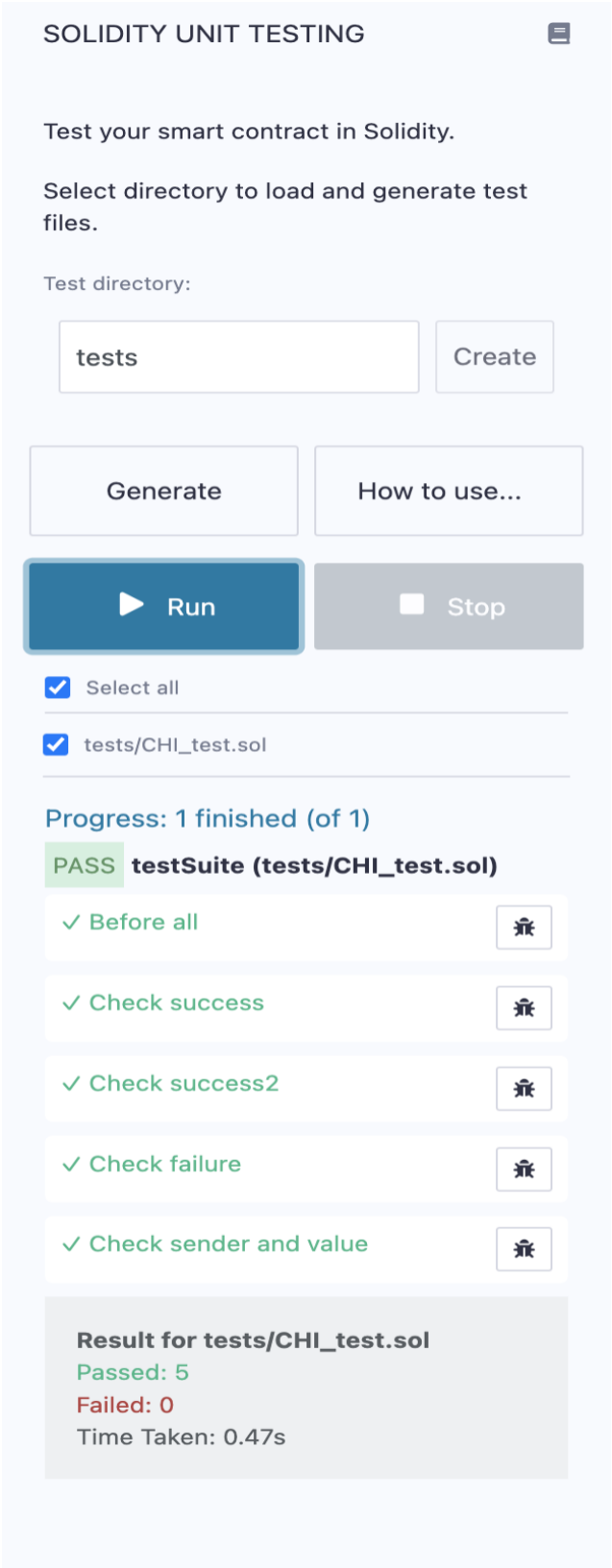


2- SOLIDITY STATIC ANALYSIS

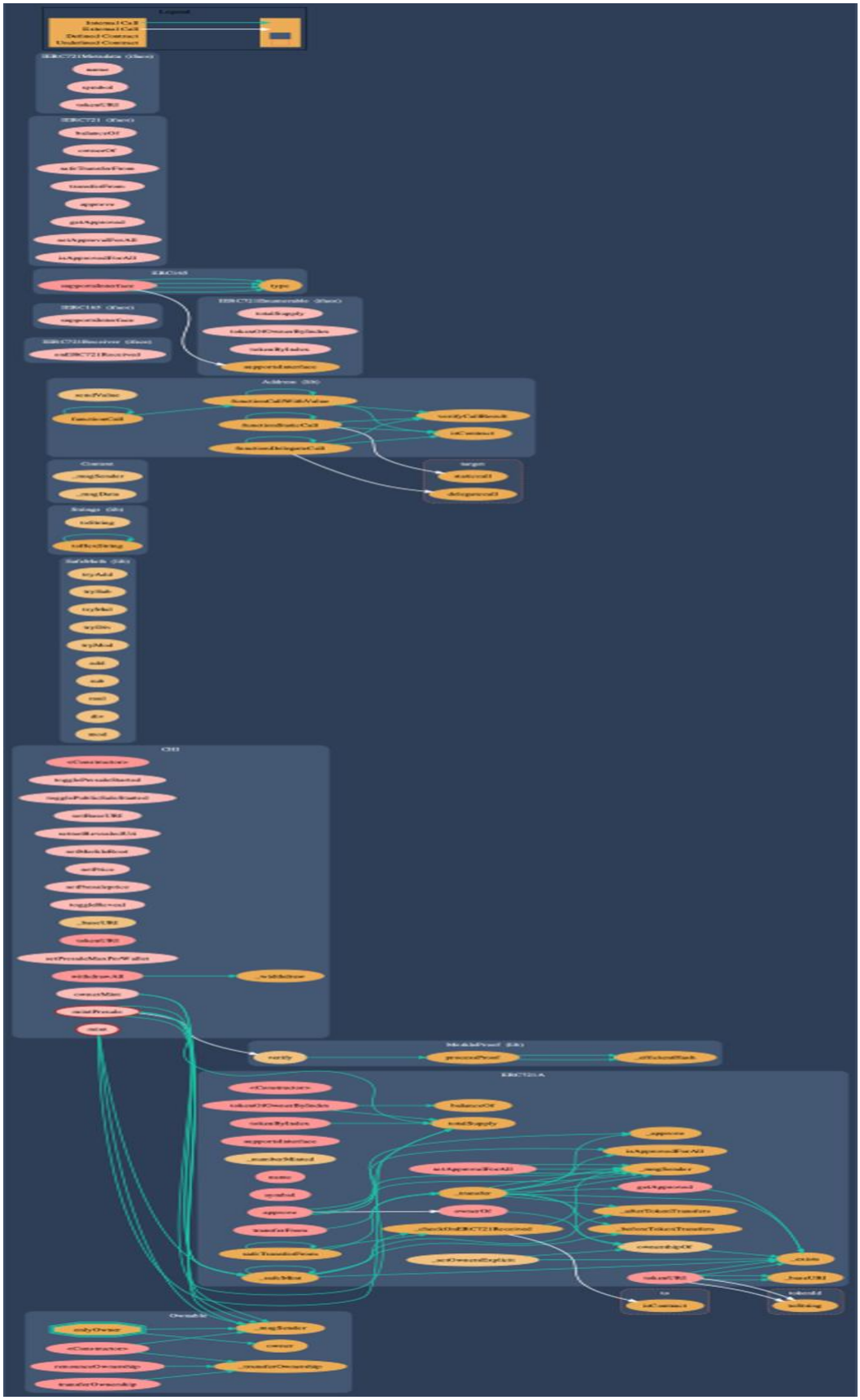
3- Inheritance graph



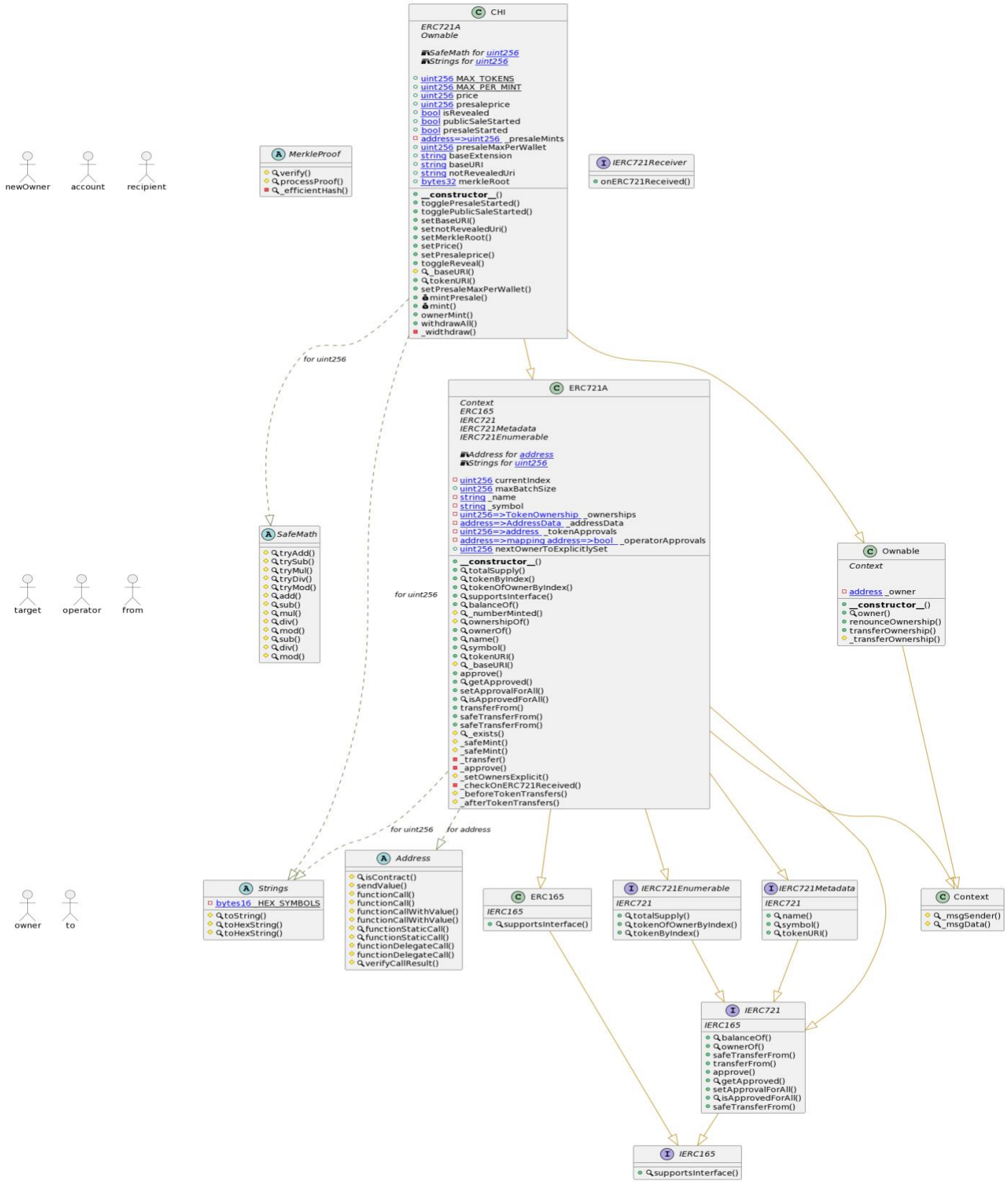
4- SOLIDITY UNIT TESTING



5- Call graph



Unified Modeling Language (UML)



Functions signature

```
Sighash   |   Function Signature
========================
16279055  =>  isContract(address)
5a9a49c7  =>  verify(bytes32[],bytes32,bytes32)
62702a6b  =>  processProof(bytes32[],bytes32)
41ed615b  =>  _efficientHash(bytes32,bytes32)
884557bf  =>  tryAdd(uint256,uint256)
a29962b1  =>  trySub(uint256,uint256)
6281efa4  =>  tryMul(uint256,uint256)
736ecb18  =>  tryDiv(uint256,uint256)
38dc0867  =>  tryMod(uint256,uint256)
771602f7  =>  add(uint256,uint256)
b67d77c5  =>  sub(uint256,uint256)
c8a4ac9c  =>  mul(uint256,uint256)
a391c15b  =>  div(uint256,uint256)
f43f523a  =>  mod(uint256,uint256)
e31bdc0a  =>  sub(uint256,uint256,string)
b745d336  =>  div(uint256,uint256,string)
71af23e8  =>  mod(uint256,uint256,string)
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)
42842e0e  =>  safeTransferFrom(address,address,uint256)
23b872dd  =>  transferFrom(address,address,uint256)
095ea7b3  =>  approve(address,uint256)
081812fc  =>  getApproved(uint256)
a22cb465  =>  setApprovalForAll(address,bool)
e985e9c5  =>  isApprovedForAll(address,address)
b88d4fde  =>  safeTransferFrom(address,address,uint256,bytes)
18160ddd  =>  totalSupply()
2f745c59  =>  tokenOfOwnerByIndex(address,uint256)
4f6ccce7  =>  tokenByIndex(uint256)
06fdde03  =>  name()
```

```
95d89b41  =>  symbol()
c87b56dd  =>  tokenURI(uint256)
4d388a98  =>  _numberMinted(address)
140364a1  =>  ownershipOf(uint256)
743976a0  =>  _baseURI()
f8e76cc0  =>  _exists(uint256)
b3e1c718  =>  _safeMint(address,uint256)
6a4f832b  =>  _safeMint(address,uint256,bytes)
30e0789e  =>  _transfer(address,address,uint256)
f272404d  =>  _approve(address,uint256,address)
55adf19f  =>  _setOwnersExplicit(uint256)
1fd01de1  =>  _checkOnERC721Received(address,address,uint256,bytes)
ef435773  =>  _beforeTokenTransfers(address,address,uint256,uint256)
08c018f7  =>  _afterTokenTransfers(address,address,uint256,uint256)
ed1fc2a2  =>  togglePresaleStarted()
2f814575  =>  togglePublicSaleStarted()
55f804b3  =>  setBaseURI(string)
0188541d  =>  setnotRevealedUri(string)
7cb64759  =>  setMerkleRoot(bytes32)
91b7f5ed  =>  setPrice(uint256)
578c7201  =>  setPresaleprice(uint256)
5b8ad429  =>  toggleReveal()
4c0770f0  =>  setPresaleMaxPerWallet(uint256)
0c0a6b5e  =>  mintPresale(uint256,bytes32[])
a0712d68  =>  mint(uint256)
484b973c  =>  ownerMint(address,uint256)
853828b6  =>  withdrawAll()
b4e380d5  =>  _widthdraw(address,uint256)
```

Automatic general report

Files Description Table

File Name	SHA-1 Hash
/Users/macbook/Desktop/smart contracts/CHI.sol	0f4d07eb5f2b7679650fc194a3c48cbbb200e936

Contracts Description Table

Contract	Type	Bases		
└	**Function Name**	**Visibility**	**Mutability**	**Modifiers**
MerkleProof	Library			
└	verify	Internal 🔒		
└	processProof	Internal 🔒		
└	_efficientHash	Private 🔐		
SafeMath	Library			
└	tryAdd	Internal 🔒		
└	trySub	Internal 🔒		
└	tryMul	Internal 🔒		
└	tryDiv	Internal 🔒		
└	tryMod	Internal 🔒		
└	add	Internal 🔒		
└	sub	Internal 🔒		
└	mul	Internal 🔒		
└	div	Internal 🔒		
└	mod	Internal 🔒		
└	sub	Internal 🔒		
└	div	Internal 🔒		
└	mod	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❗
└	transferFrom	External ❗	🛑	NO❗
└	approve	External ❗	🛑	NO❗
└	getApproved	External ❗		NO❗
└	setApprovalForAll	External ❗	🛑	NO❗
└	isApprovedForAll	External ❗		NO❗
└	safeTransferFrom	External ❗	🛑	NO❗
IERC721Enumerable	Interface	IERC721		
└	totalSupply	External ❗		NO❗
└	tokenOfOwnerByIndex	External ❗		NO❗
└	tokenByIndex	External ❗		NO❗
IERC721Metadata	Interface	IERC721		
└	name	External ❗		NO❗
└	symbol	External ❗		NO❗
└	tokenURI	External ❗		NO❗
ERC721A	Implementation	Context, ERC165, IERC721, IERC721Metadata, IERC721Enumerable		
└	<Constructor>	Public ❗	🛑	NO❗
└	totalSupply	Public ❗		NO❗
└	tokenByIndex	Public ❗		NO❗
└	tokenOfOwnerByIndex	Public ❗		NO❗
└	supportsInterface	Public ❗		NO❗
└	balanceOf	Public ❗		NO❗
└	_numberMinted	Internal 🔒		
└	ownershipOf	Internal 🔒		
└	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❗
└	_exists	Internal 🔒		
└	_safeMint	Internal 🔒	🛑	
└	_safeMint	Internal 🔒	🛑	
└	_transfer	Private 🔐	🛑	
└	_approve	Private 🔐	🛑	
└	_setOwnersExplicit	Internal 🔒	🛑	
└	_checkOnERC721Received	Private 🔐	🛑	
└	_beforeTokenTransfers	Internal 🔒	🛑	
└	_afterTokenTransfers	Internal 🔒	🛑	
CHI	Implementation	ERC721A, Ownable	
└	<Constructor>	Public ❗	🛑	ERC721A
└	togglePresaleStarted	External ❗	🛑	onlyOwner
└	togglePublicSaleStarted	External ❗	🛑	onlyOwner
└	setBaseURI	External ❗	🛑	onlyOwner
└	setnotRevealedUri	External ❗	🛑	onlyOwner
└	setMerkleRoot	External ❗	🛑	onlyOwner
└	setPrice	External ❗	🛑	onlyOwner
└	setPresaleprice	External ❗	🛑	onlyOwner
└	toggleReveal	External ❗	🛑	onlyOwner
└	_baseURI	Internal 🔒		
└	tokenURI	Public ❗		NO❗
└	setPresaleMaxPerWallet	External ❗	🛑	onlyOwner
└	mintPresale	External ❗	💰	NO❗
└	mint	External ❗	💰	NO❗
└	ownerMint	External ❗	🛑	onlyOwner
└	withdrawAll	Public ❗	🛑	onlyOwner
└	_widthdraw	Private 🔐	🛑	

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.
✓ Not many 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.