MIDNIGHT6

CODE SECURITY ASSESSMENT

Roko Clan NFT Smart Contract

APRIL 20TH, 2022

https://www.midnight6.com/

Table of Contents

Summary

This report has been prepared for Roko Clan NFT to discover issues and vulnerabilities and to understand the risk exposure in the source code of the Roko Clan NFT Smart Contract.A comprehensive examination has been performed, utilising Static Analysis and Manual Review techniques.

The purpose of the assessment was made to achieve the following:
-Ensure that the smart contract functions as intended.
-Identify potential security issues with the smart contract.

the security assessment will be used as a guidance to improve the security posture of the smart contract by remediating the issues that were identified from critical to note to ensure high level of security standard and to enhance general coding practices

overview

Project summary

PROJECT NAME	ROKO CLAN
BLOCKCHAIN	ETHEREUM
LANGUAGE	Solidity
CONTRACT ADDRESS	0xE42517349ebf890F8899d89edA47b391CD6F545f
CODEBASE	https://etherscan.io/address/0xe42517349ebf890f8899d89eda47b391cd6f545f#code
PROJECT WEBSITE	https://rokoclan.com/

NFT Summary

TOKEN NAME	Roko Clan (DRK)
TOTAL SUPPLY	10,000
HOLDERS	1
TRANSFER	401

OVERVIEW

Audit Summary

DELIVERY DATE	April 20, 2022 UTC
AUDIT TECHNIQUES	Manual Review, Static Analysis

Vulnerability Summary

CARITICAL	HIGH	MEDIUM	LOW	VERY LOW	NOTE
0	0	0	2	0	0

static checks made with remix IDE. All issues were performed by the team, which included the analysis of code functionality, manual audit found during static 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, 2 low, 0 very low-level issues and 0 note in all solidity files of the contract

Contracts address deployed to test net (Ethereum)

Roko Clan NFT contract on ETH test net to test every function by the auditor.

https://rinkeby.etherscan.io/address/0xdcffcf708a2993f3f7f6ebf5a9353825992be6f5

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.

overview

Executive Summary

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

WELL-SECURED	✓
SECURED	
POOR SECURED	
INSECURE	

Audit scope

File and Function Level Report.
file in scope:

CONTRACT NAME	RokoClan.sol
SHA 256 HASH	a235e535ade9c06341d0d54 72ceae29319c4bad2a5aff04 88c87e2d8781a65bb
CONTRACT ADDRESS	0xE42517349ebf890F8899d89edA47b391CD6 F545f

overview

Audit scope

File and Function Level Report.
file in scope:

- Contract: RokoClan
- 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
SYMPOL	✔	Read / public	passed
addressMintCount	✔	Read / public	passed
supportsInterface	✔	Read / public	passed
addressMintAmount	✔	Read / public	passed
balanceOf	✔	Read / public	passed
Owner	✔	Read / public	passed
maxMintPerAddress	✔	Read / public	passed
getTotalwhitelistNFTs	✔	Read / public	passed
getApprovedForAll	✔	Read / public	passed
getOnlyLeftValue	✔	Read / public	passed
getApproved	✔	Read / public	passed

FUNCTION	TEST RESULT	TYPE/ RETURN TYPE	SCORE
ownerOf	✔	Read / public	passed
tokenURI	✔	Read / public	passed
totalSupply	✔	Read / public	passed
baseURI	✔	Read / public	passed
paused	✔	Read / public	passed
balanceOf	✔	Read / public	passed
whitelistStatus	✔	Read / public	passed
whitelistSigner	✔	Read / public	passed
MAX_SUPPLY	✔	Read / public	passed
whitelistCost	✔	Read / public	passed
totalWhitelistMinted	✔	Read / public	passed
publicSaleMinteLimits	✔	Read / public	passed
cost	✔	Read / public	passed
onlyLeftValue	✔	Read / public	passed
publicSaleMinted	✔	Read / public	passed
mint	✔	write / payable	passed

FUNCTION	TEST RESULT	TYPE/ RETURN TYPE	SCORE
approve	✔	write / public	passed
safeTransferFrom	✔	write / public	passed
setPublicSaleMintLimit	✔	write / public	passed
paused	✔	write / public	passed
whitelistMint	✔	write / payable	passed
setMintRate	✔	write / public	passed
transferOwnership	✔	write / public	passed
setApprovalForAll	✔	write / public	passed
transferFrom	✔	write / public	passed
withdraw	✔	write / payable	passed
setBaseURI	✔	write / public	passed
renounceOwnership	✔	write / public	passed
setWhitelistSigner	✔	write / public	passed
toggleWhitelistStatus	✔	write / public	passed

ISSUES CHECKING STATUS

NO.	Issue Description	Checking Status
1	Compiler warnings.	passed
2	Race conditions and Reentrancy.	passed
3	Cross-function race conditions.	passed
4	Delays in data delivery.	passed
5	Oracle calls.	passed
6	Design Logic.	passed
7	Timestamp dependence.	passed with notes
8	Integer Overflow and Underflow.	passed
9	Arithmetic accuracy.	passed

ISSUES CHECKING STATUS

NO.	Issue Description	Checking Status
10	DoS with Revert.	passed
11	DoS with block gas limit.	passed with notes
12	Methods execution permissions.	passed
13	Economy model.	passed
14	The impact of the exchange rate on the logic.	passed
15	Private user data leaks.	passed
16	Malicious Event log.	passed
17	Scoping and Declarations.	passed
18	Uninitialized storage pointers.	passed

AUDIT FINDING

CRITICAL	0	(0.0%)
HIGH	0	(0.0%)
MEDIUM	0	(0.0%)
LOW	2	(100%)
VERY LOW	0	(0.0%)
NOTE	0	(0.0%)

CRITICAL:
NO CRITICAL SEVERITY VULNERABILITIES WERE FOUND.
HIGH:
NO HIGH SEVERITY VULNERABILITIES WERE FOUND.
MEDIUM:
NO MEDIUM SEVERITY VULNERABILITIES WERE FOUND

LOW:
PRAGAM VERSION NOT FIXED
USE OF BLOCK.TIMESTAMP FOR COMPARISONS

VERY LOW:
NO VERY LOW SEVERITY VULNERABILITIES WERE FOUND.
NOTES:
NO NOTES VULNERABILITIES WERE FOUND.

AUDIT FINDING

PRAGMA VERSION NOT FIXED

DESCRIPTION:

IT IS A GOOD PRACTICE TO LOCK THE SOLIDITY VERSION FOR A LIVE DEPLOYMENT (USE 0.8.4 INSTEAD OF ^0.8.4). 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.

SEVERITY:

LOW

RECOMMENDATION:

REMOVE THE ^ SIGN TO LOCK THE PRAGMA VERSION.

STATUS:

ACKNOWLEDGED

AUDIT FINDING

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

SEVERITY:

LOW

RECOMMENDATION:

AVOID USE OF BLOCK.TIMESTAMP

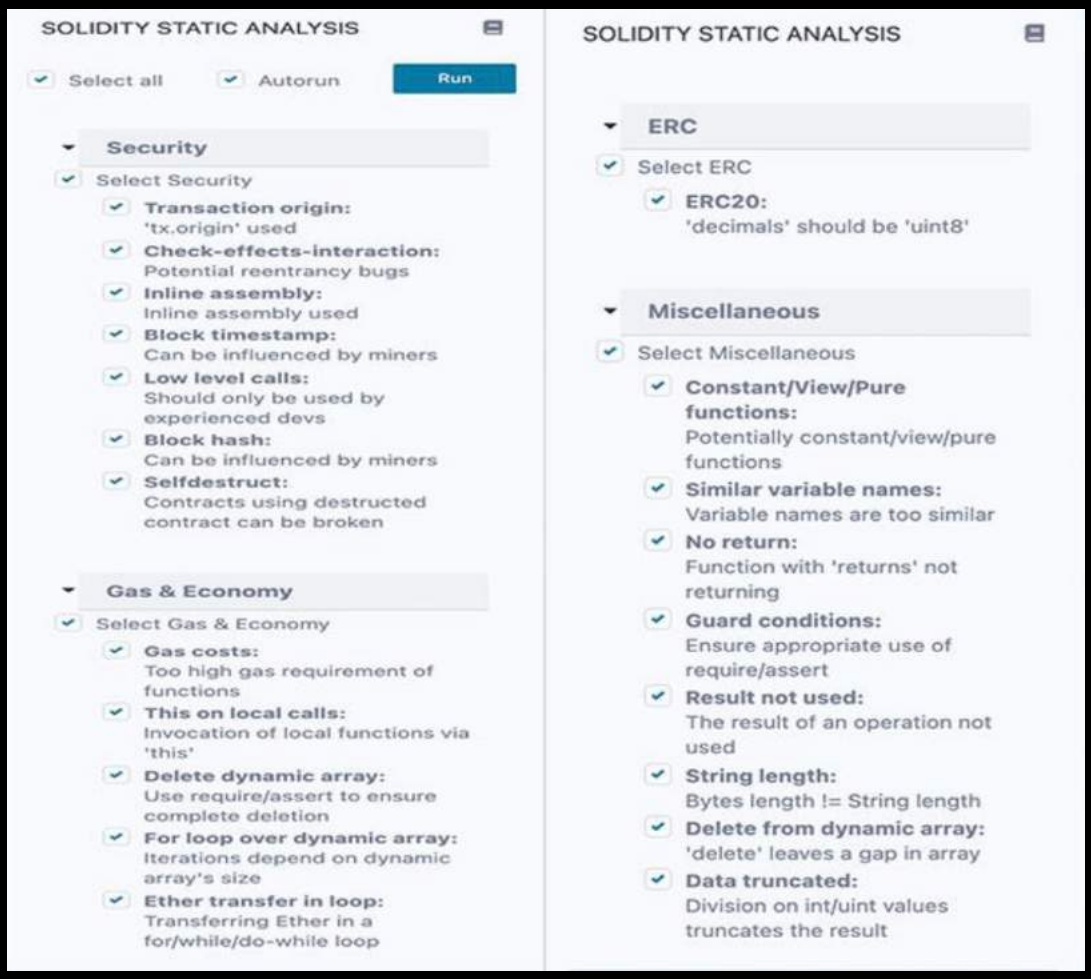
STATUS:

ACKNOWLEDGED

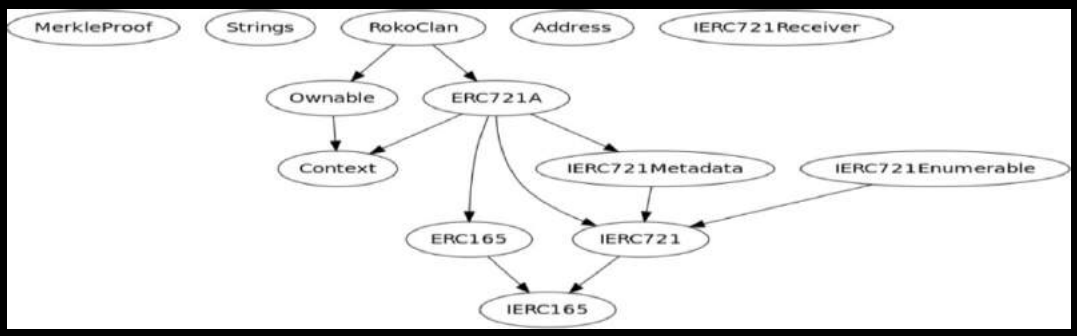
STATIC TESTING

1-CHECK FOR SECURITY

2-SOLIDITY STATIC ANALYSIS

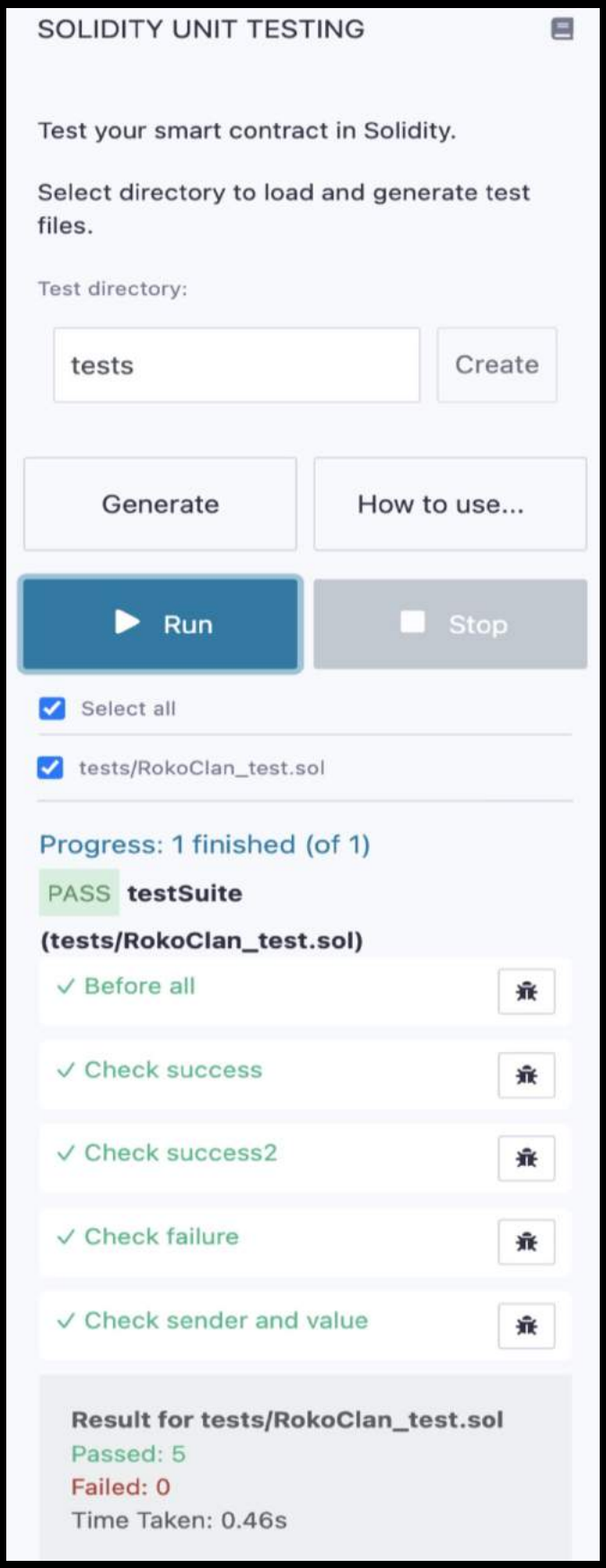


3-INHERITANCE GRAPH



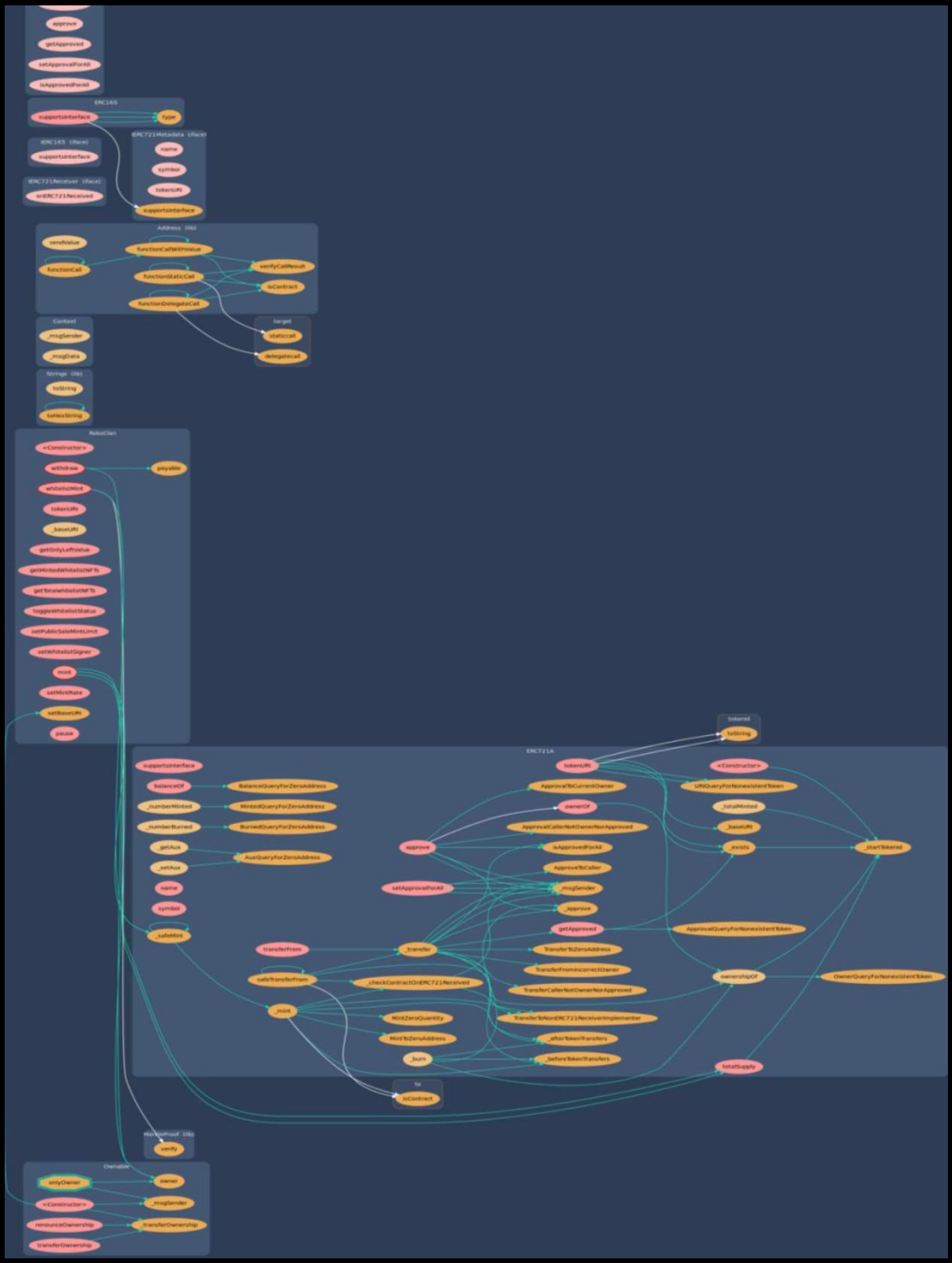
STATIC TESTING

4-SOLIDITY UNIT TESTING

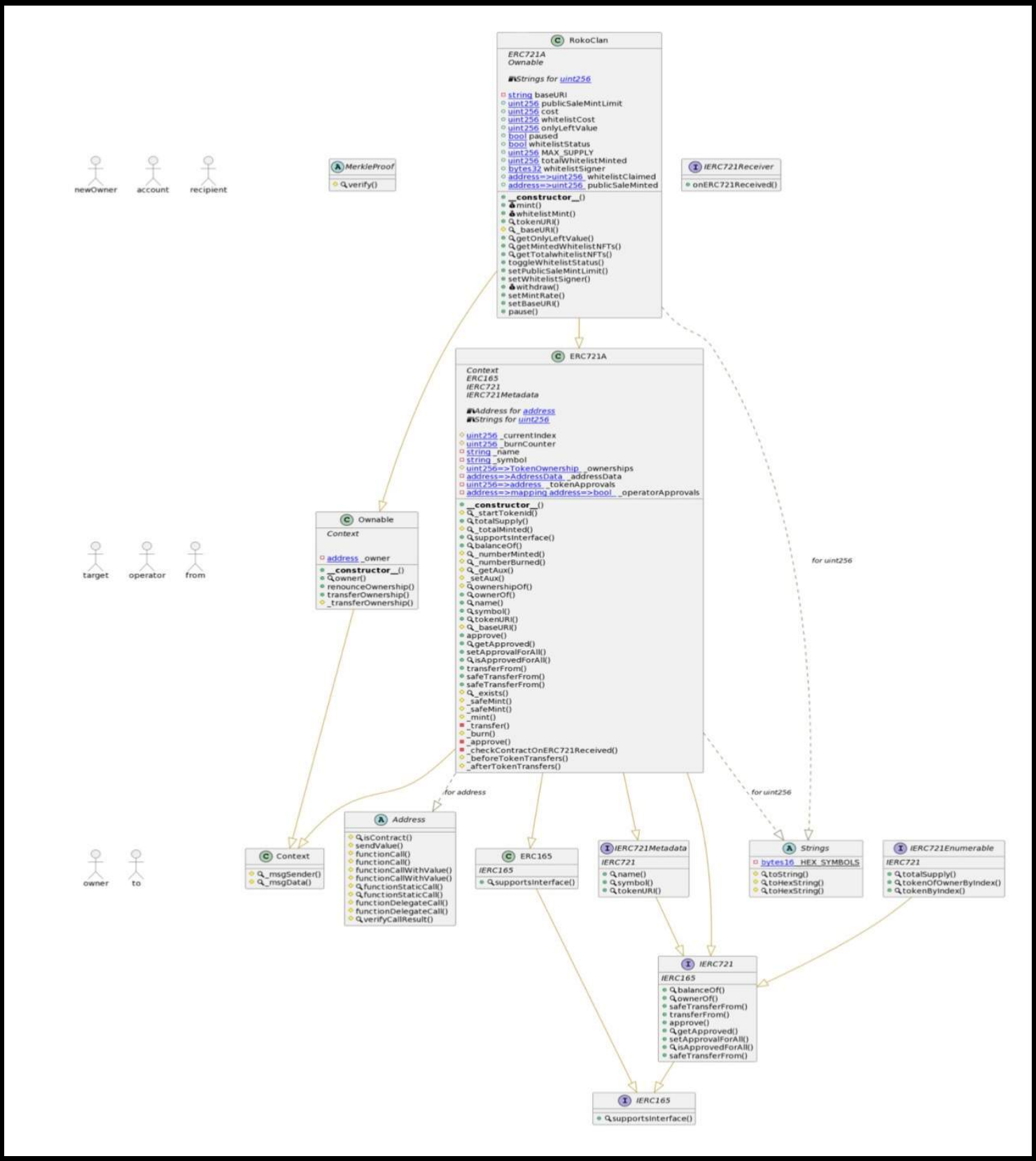


STATIC TESTING

5-CALL GRAPH



UNIFIED MODELING LANGUAGE (UML)



FUNCTIONS SIGNATURE

```
SIGHASH   | FUNCTION SIGNATURE ========================
16279055  => ISCONTRACT(ADDRESS)
25389421  => SETWHITELISTSIGNER(BYTES32)
 5A9A49C7=> VERIFY(BYTES32[],BYTES32,BYTES32)
972A2A62 => VERIFY(BYTES32[],BYTES32)
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)
98995F77   =>  _STARTTOKENID()
736BF591   =>  _TOTALMINTED()
4D388A98 =>  _NUMBERMINTED(ADDRESS)
6BA1B8D0  =>  _NUMBERBURNED(ADDRESS)
F4A540C5   =>  _GETAUX(ADDRESS)
4FF8C452   =>  _SETAUX(ADDRESS,UINT64)
140364A1   =>  OWNERSHIPOF(UINT256)
743976A0   =>  _BASEURI()
F8E76CC0   =>  _EXISTS(UINT256)
B3E1C718   =>  _SAFEMINT(ADDRESS,UINT256)
6A4F832B  =>  _SAFEMINT(ADDRESS,UINT256,BYTES)
```

FUNCTIONS SIGNATURE

```
SIGHASH    |    FUNCTION SIGNATURE ========================
DE0D9900 => _MINT(ADDRESS,UINT256,BYTES,BOOL)
30E0789E => _TRANSFER(ADDRESS,ADDRESS,UINT256)
9B1F9E74 => _BURN(UINT256)
F272404D => _APPROVE(ADDRESS,UINT256,ADDRESS)
D88343E2 => _CHECKCONTRACTONERC721RECEIVED(ADDRESS,ADDRESS,UINT256,BYTES)
EF435773 => _BEFORETOKENTRANSFERS(ADDRESS,ADDRESS,UINT256,UINT256)
08C018F7 => _AFTERTOKENTRANSFERS(ADDRESS,ADDRESS,UINT256,UINT256)
A0712D68 => MINT(UINT256)
2904E6D9 => WHITELISTMINT(BYTES32[],UINT256)
A6458ECB => GETONLYLEFTVALUE()
D0C039D7 => GETMINTEDWHITELISTNFTS()
49E8C1E0 => GETTOTALWHITELISTNFTS()
48A99793 => TOGGLEWHITELISTSTATUS()
80DBCA8B => SETPUBLICSALEMINTLIMIT(UINT256)
3CCFD60B => WITHDRAW()
DBE2193F => SETMINTRATE(UINT256)
55F804B3 => SETBASEURI(STRING)
02329A29 => PAUSE(BOOL)
```

STATIC GENERAL REPORT

```
Files Description Table

|  File Name  |  SHA-1 Hash  |
|-------------|--------------|
| /Users/macbook/Desktop/smart contracts/RokoClan.sol |
bcdaaf2fcfb4972a436d0f7947b6a5a3f5ebfefa |

 Contracts Description Table

|  Contract  |         Type        |       Bases      |                  |
|
|:----------:|:-------------------:|:----------------:|:----------------:|:--------
-------:|
|     └      |  **Function Name**  |  **Visibility**  |  **Mutability**  |
**Modifiers**  |
||||||
| **MerkleProof** | Library |  |||
| └ | verify | 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 |  |||
```

STATIC GENERAL REPORT

```
| └ | 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 |||
| └ | <Constructor> | Public ❗ | 🔴    |NO❗ |
| └ | _startTokenId | Internal 🔒 |    | |
| └ | totalSupply | Public ❗ |    |NO❗ |
| └ | _totalMinted | Internal 🔒 |    | |
| └ | supportsInterface | Public ❗ |    |NO❗ |
| └ | balanceOf | Public ❗ |    |NO❗ |
| └ | _numberMinted | Internal 🔒 |    | |
| └ | _numberBurned | Internal 🔒 |    | |
| └ | _getAux | Internal 🔒 |    | |
| └ | _setAux | 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 🔒 | 🔴    | |
| └ | _mint | Internal 🔒 | 🔴    | |
| └ | _transfer | Private 🔐 | 🔴    | |
```

STATIC GENERAL REPORT

```
| └ | _burn | Internal 🔒 | 🛑 | |
| └ | _approve | Private 🔒 | 🛑 | |
| └ | _checkContractOnERC721Received | Private 🔒 | 🛑 | |
| └ | _beforeTokenTransfers | Internal 🔒 | 🛑 | |
| └ | _afterTokenTransfers | Internal 🔒 | 🛑 | |
||||||
| **RokoClan** | Implementation | ERC721A, Ownable |||
| └ | <Constructor> | Public ❗ | 🛑 | ERC721A |
| └ | mint | Public ❗ | 💵 |NO❗ |
| └ | whitelistMint | Public ❗ | 💵 |NO❗ |
| └ | tokenURI | Public ❗ |  |NO❗ |
| └ | _baseURI | Internal 🔒 |  | |
| └ | getOnlyLeftValue | Public ❗ |  |NO❗ |
| └ | getMintedWhitelistNFTs | Public ❗ |  |NO❗ |
| └ | getTotalwhitelistNFTs | Public ❗ |  |NO❗ |
| └ | toggleWhitelistStatus | Public ❗ | 🛑 | onlyOwner |
| └ | setPublicSaleMintLimit | Public ❗ | 🛑 | onlyOwner |
| └ | setWhitelistSigner | Public ❗ | 🛑 | onlyOwner |
| └ | withdraw | Public ❗ | 💵 | onlyOwner |
| └ | setMintRate | Public ❗ | 🛑 | onlyOwner |
| └ | setBaseURI | Public ❗ | 🛑 | onlyOwner |
| └ | pause | Public ❗ | 🛑 | onlyOwner |

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, AND NO NEED TO REDEPLOY THE CONTRACT.

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 HIGH SEVERITY ISSUES WERE FOUND.

DISCLAIMER

THIS REPORT IS SUBJECT TO THE TERMS AND CONDITIONS (INCLUDING WITHOUT LIMITATION, DESCRIPTION OF SERVICES,CONFIDENTIALITY, DISCLAIMER AND LIMITATION OF LIABILITY) SET FORTH IN THE SERVICES AGREEMENT, OR THE SCOPE OF SERVICES, AND TERMS AND CONDITIONS PROVIDED TO YOU ("CUSTOMER" OR THE "COMPANY") IN CONNECTION WITH THE AGREEMENT. THIS REPORT PROVIDED IN CONNECTION WITH THE SERVICES SET FORTH IN THE AGREEMENT SHALL BE USED BY THE COMPANY ONLY TO THE EXTENT PERMITTED UNDER THE TERMS AND CONDITIONS SET FORTH IN THE AGREEMENT.THIS REPORT MAY NOT BE TRANSMITTED, DISCLOSED, REFERRED TO OR RELIED UPON BY ANY PERSON FOR ANY PURPOSES,NOR MAY COPIES BE DELIVERED TO ANY OTHER PERSON OTHER THAN THE COMPANY, WITHOUT MIDNIGHT6 PRIOR WRITTEN CONSENT IN EACH INSTANCE.

THIS REPORT IS NOT, NOR SHOULD BE CONSIDERED, AN "ENDORSEMENT" OR "DISAPPROVAL" OF ANY PARTICULAR PROJECT OR TEAM. THIS REPORT IS NOT, NOR SHOULD BE CONSIDERED, AN INDICATION OF THE ECONOMICS OR VALUE OF ANY"PRODUCT" OR "ASSET" CREATED BY ANY TEAM OR PROJECT THAT CONTACTS MIDNIGHT6 TO PERFORM A CODE ASSESSMENT. THIS REPORT DOES NOT PROVIDE ANY WARRANTY OR GUARANTEE REGARDING THE ABSOLUTE BUG-FREE NATURE OF THE TECHNOLOGY ANALYSED, NOR DO THEY PROVIDE ANY INDICATION OF THE TECHNOLOGIES PROPRIETORS,BUSINESS, BUSINESS MODEL OR LEGAL COMPLIANCE

THIS REPORT SHOULD NOT BE USED IN ANY WAY TO MAKE DECISIONS AROUND INVESTMENT OR INVOLVEMENT WITH ANY PARTICULAR PROJECT. THIS REPORT IN NO WAY PROVIDES INVESTMENT ADVICE, NOR SHOULD BE LEVERAGED AS INVESTMENT ADVICE OF ANY SORT. THIS REPORT REPRESENTS AN EXTENSIVE ASSESSING PROCESS INTENDING TO HELP OUR CUSTOMERS INCREASE THE QUALITY OF THEIR CODE WHILE REDUCING THE HIGH LEVEL OF RISK PRESENTED BY CRYPTOGRAPHIC TOKENS AND BLOCKCHAIN TECHNOLOGY

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. BLOCKCHAIN TECHNOLOGY AND CRYPTOGRAPHIC ASSETS PRESENT A HIGH LEVEL OF ONGOING RISK. MIDNIGHT6 POSITION IS THAT EACH COMPANY AND INDIVIDUAL ARE RESPONSIBLE FOR THEIR OWN DUE DILIGENCE AND CONTINUOUS SECURITY.THIS REPORT IS PROVIDED FOR INFORMATION PURPOSES ONLY AND ON A NON-RELIANCE BASIS, AND DOES NOT CONSTITUTE INVESTMENT ADVICE. MIDNIGHT6 VISION ON THIS REPORT MADE TO HELP REDUCE THE ATTACK VECTORS AND THE HIGH LEVEL OF VARIANCE ASSOCIATED WITH UTILISING NEW AND CONSISTENTLY CHANGING TECHNOLOGIES, AND IN NO WAY CLAIMS ANY GUARANTEE OF SECURITY OR FUNCTIONALITY OF THE TECHNOLOGY WE AGREE TO ANALYSE.NO ONE SHALL HAVE ANY RIGHT TO RELY ON THE REPORT OR ITS CONTENTS, AND MIDNIGHT6 AND ITS AFFILIATES AND/OR THIRD PARTIES (INCLUDING HOLDING COMPANIES, SHAREHOLDERS, SUBSIDIARIES, EMPLOYEES, DIRECTORS, OFFICERS AND OTHER REPRESENTATIVES)

THE ASSESSMENT SERVICES PROVIDED BY MIDNIGHT6 OR ITS THIRD PARTY IS SUBJECT TO DEPENDENCIES AND UNDER CONTINUING DEVELOPMENT. YOU AGREE THAT YOUR ACCESS AND/OR USE, INCLUDING BUT NOT LIMITED TO ANY SERVICES, REPORTS,AND MATERIALS, WILL BE AT YOUR OWN RISK ON AN AS-IS, WHERE-IS, AND AS-AVAILABLE. CRYPTOGRAPHIC TOKENS ARE EMERGENT TECHNOLOGIES AND CARRY WITH THEM HIGH LEVELS OF TECHNICAL RISK AND UNCERTAINTY. THE ASSESSMENT REPORT COULD INCLUDE FALSE POSITIVES, FALSE NEGATIVES, AND OTHER UNPREDICTABLE RESULTS. THE SERVICES MAY ACCESS, AND DEPEND UPON, MULTIPLE LAYERS OF THIRD PARTIE.

MIDNIGHT6 OWE NO DUTY OF CARE TOWARDS YOU OR ANY OTHER PERSON, NOR DOES MIDNIGH6 MAKE ANY WARRANTY OR REPRESENTATION TO ANY PERSON ON THE ACCURACY OR COMPLETENESS OF THE REPORT. THE REPORT IS PROVIDED "AS IS", "WHERE-IS", AND "AS AVAILABLE" WITHOUT ANY CONDITIONS, WARRANTIES OR OTHER TERMS OF ANY KIND EXCEPT AS SET OUT IN THIS DISCLAIMER,

MIDNIGHT6

Contact us.

www.midnight6.com

hello@midnight6.com

https://twitter.com/_midnight6_