Smart Contract

Security Assessment

For LinaMeets

25 June 2022

Ascendant

Ascendant
@ascendantproj
www.ascendant.finance.com

Ascendant

Table of Contents

DISCLAIMER

Ascendant Finance ("Ascendant") has conducted an independent audit to verify the integrity of and highlight any vulnerabilities or errors, intentional or unintentional, that may be present in the codes that were provided for the scope of this audit. This audit report does not constitute agreement, acceptance or advocation for the Project that was audited, and users relying on this audit report should not consider this as having any merit for financial advice in any shape, form or nature. The contracts audited do not account for any economic developments that may be pursued by the Project in question, and that the veracity of the findings thus presented in this report relate solely to the proficiency, competence, aptitude and discretion of our independent auditors, who make no guarantees nor assurance that the contracts are completely free of exploits, bugs, vulnerabilities or deprecation of technologies. Further, this audit report shall not be disclosed nor transmitted to any persons or parties on any objective, goal or justification without due written assent, acquiescence or approval by Ascendant.

All information provided in this report does not constitute financial or investment advice, nor should it be used to signal that any persons reading this report should invest their funds without sufficient individual due diligence regardless of the findings presented in this report. Information is provided 'as is', and Ascendant is under no covenant to the completeness, accuracy or solidity of the contracts audited. In no event will Ascendant or its partners, employees, agents or parties related to the provision of this audit report be liable to any parties for, or lack thereof, decisions and/or actions with regards to the information provided in this audit report.

Cryptocurrencies and any technologies by extension directly or indirectly related to cryptocurrencies are highly volatile and speculative by nature. All reasonable due diligence and safeguards may yet be insufficient, and users should exercise considerable caution when participating in any shape or form in this nascent industry.

The audit report has made all reasonable attempts to provide clear and articulate recommendations to the Project team with respect to the rectification, amendment and/or revision of any highlighted issues, vulnerabilities or exploits within the contracts provided. It is the sole responsibility of the Project team to sufficiently test and perform checks, ensuring that the contracts are functioning as intended, specifically that the functions therein contained within said contracts have the desired intended effects, functionalities and outcomes of the Project team.

Ascendant retains full rights over all intellectual property (including expertise and new attack or exploit vectors) discovered during the audit process. Ascendant is therefore allowed and expected to re-use this knowledge in subsequent audits and to inform existing projects that may have similar vulnerabilities. Ascendant may, at its discretion, claim bug bounties from third-parties while doing so.

Executive Summary

Severity	Found
High	1
Medium	1
Low	3
Informational	68
Total	73

We performed an independent technical audit to identify Smart Contracts uncertainties. This shall protect the code from illegitimate authorization attempts or external & internal threats of any type. This also ensures end-to-end proofing of the contract from frauds. The audit was performed semi-manually. We analyzed the Smart Contracts code line-by-line and used an automation tool to report any suspicious code.

The following tools were used:

- Truffle
- Remix IDE
- Slither

Overview

This report has been prepared for LinaMeets on the Polygon network. Ascendant provides a user-centered examination of the smart contracts to look for vulnerabilities, logic errors or other issues from both an internal and external perspective.

Summary

Project Name	LinaMeets
Platform	Polygon
Language	Solidity

Contracts Assessed

Name	Location
linameets.sol	Not deployed
ERC721A.sol	In LinaMeets_NFT Contract
IERC721A.sol	In LinaMeets_NFT Contract
ERC721A_IERC721Receiver.sol	In LinaMeets_NFT Contract
Ownable.sol	In LinaMeets_NFT Contract
Context.sol	In LinaMeets_NFT Contract
Strings.sol	In LinaMeets_NFT Contract

Findings Summary

Severity	Found
High	1
Medium	1
Low	3
Informational	68
Total	73

Classification of Issues

High	Exploits, vulnerabilities or errors that will certainly or probabilistically lead towards loss of funds, control, or impairment of the contract and its functions. Issues under this classification are recommended to be fixed with utmost urgency.
Medium	Bugs or issues that may be subject to exploit, though their impact is somewhat limited. Issues under this classification are recommended to be fixed as soon as possible.
Low	Effects are minimal in isolation and do not pose a significant danger to the project or its users. Issues under this classification are recommended to be fixed nonetheless.
Informational	Consistency, syntax or style best practices, Generally pose a negligible level of risk, if any.

Manual Review

Ascendant

Issues Checking Status

Issue Description	Checking Status
Compiler errors	PASS
Race conditions and Reentrancy. Cross-function race conditions.	PASS
Possible delays in data delivery.	PASS
Oracle calls.	PASS
Front running.	PASS
Timestamp dependence.	PASS
Integer Overflow and Underflow.	PASS
DoS with Revert.	PASS
DoS with block gas limit.	PASS
Methods execution permissions.	PASS
Economy model of the contract.	PASS
The impact of the exchange rate on the logic.	PASS
Private user data leaks.	PASS
Malicious Event log.	PASS
Scoping and Declarations.	PASS
Uninitialized storage pointers.	PASS

Arithmetic accuracy.	PASS
Design Logic.	PASS
Cross-function race conditions.	PASS
Safe Open Zeppelin contracts implementation and usage.	PASS
Fallback function security.	PASS

Audit Findings

Severity	**High**
Contract	linameets.sol
Description	IPFS hash visible in comments
Code Snippet	1510: //QmVJZya8rKExh5qw14QEqo92WbPKgtZrpf5sJPadSevuny
Recommendation	Delete the comment containing the ipfs hash on line 1510

Severity	**Medium**
Contract	linameets.sol
Description	string baseURI declared public
Code Snippet	1407: string public baseURI;
Recommendation	When the baseURI is public, this means that even before the reveal function is called, any person can read the baseURI variable, which in the best case scenario, makes the reveal pointless, but in the worse case scenario, a bad actor can use the hash to locate your stored images, download them, and sell them on their own without paying for them. Make the baseURI a private variable.

Functional Test Status

Function Name	Type/Return Type	Score
baseURI	read/public	PASS
unrevURI	read/public	PASS
baseExtension	read/public	PASS
cost	read/public	PASS
maxSupply	read/public	PASS
public_paused	read/public	PASS
revealed	read/public	PASS
_baseURI	internal	PASS
mint	payable/public	PASS
ownerMint	write/public	PASS
tokenURI	read/public	PASS
setCost	write/public	PASS
setBaseURI	write/public	PASS
setUnrevURI	write/public	PASS
setBaseExtension	write/public	PASS
startPublicSale	write/public	PASS
stopPublicSale	write/public	PASS
revealNFT	write/public	PASS

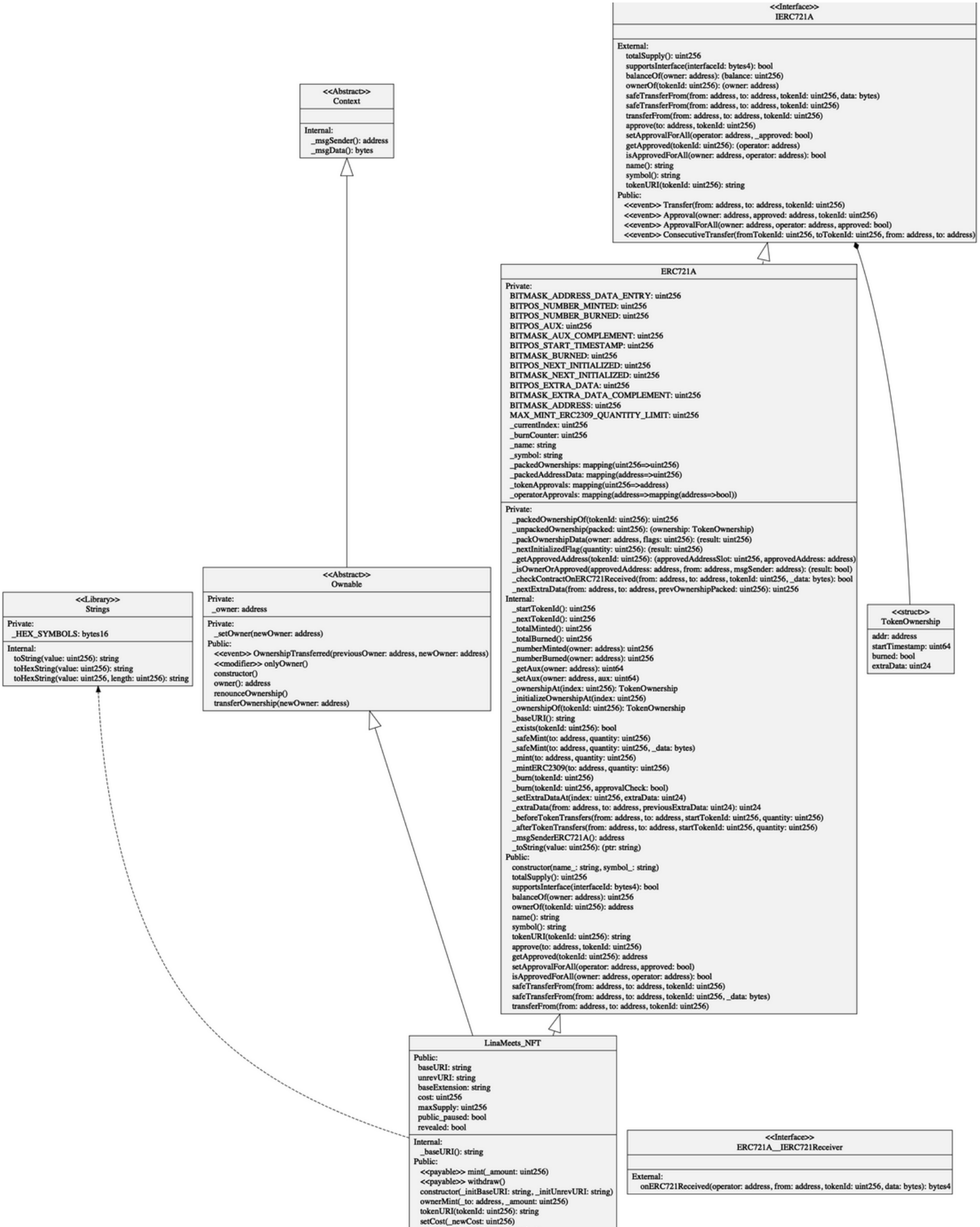
withdraw	payable/public	PASS

Automated Review

Ascendant

Inheritance Graph

Unified Modeling Language(UML)



Function ID Report

ERC721A__IERC721Receiver:

Name	ID
onERC721Received(address,address,uint256,bytes)	0x150b7a02

LinaMeets_NFT:

Name	ID
owner()	0x8da5cb5b
renounceOwnership()	0x715018a6
transferOwnership(address)	0xf2fde38b
constructor(string,string)	0xd4d8c5c3
totalSupply()	0x18160ddd
supportsInterface(bytes4)	0x01ffc9a7
balanceOf(address)	0x70a08231
ownerOf(uint256)	0x6352211e
name()	0x06fdde03
symbol()	0x95d89b41
tokenURI(uint256)	0xc87b56dd
approve(address,uint256)	0x095ea7b3
getApproved(uint256)	0x081812fc
setApprovalForAll(address,bool)	0xa22cb465
isApprovedForAll(address,address)	0xe985e9c5
safeTransferFrom(address,address,uint256)	0x42842e0e
safeTransferFrom(address,address,uint256,bytes)	0xb88d4fde
transferFrom(address,address,uint256)	0x23b872dd
totalSupply()	0x18160ddd
supportsInterface(bytes4)	0x01ffc9a7
balanceOf(address)	0x70a08231
ownerOf(uint256)	0x6352211e
safeTransferFrom(address,address,uint256,bytes)	0xb88d4fde
safeTransferFrom(address,address,uint256)	0x42842e0e
transferFrom(address,address,uint256)	0x23b872dd
approve(address,uint256)	0x095ea7b3
setApprovalForAll(address,bool)	0xa22cb465
getApproved(uint256)	0x081812fc
isApprovedForAll(address,address)	0xe985e9c5
name()	0x06fdde03
symbol()	0x95d89b41

```
| tokenURI(uint256)                    | 0xc87b56dd |
| constructor(string,string)           | 0xd4d8c5c3 |
| mint(uint256)                        | 0xa0712d68 |
| ownerMint(address,uint256)           | 0x484b973c |
| tokenURI(uint256)                    | 0xc87b56dd |
| setCost(uint256)                     | 0x44a0d68a |
| setBaseURI(string)                   | 0x55f804b3 |
| setUnrevURI(string)                  | 0x841bfb27 |
| setBaseExtension(string)             | 0xda3ef23f |
| startPublicSale()                    | 0x0c1c972a |
| stopPublicSale()                     | 0xda1b91c3 |
| revealNFT()                          | 0x04b4bba9 |
| withdraw()                           | 0x3ccfd60b |
| baseURI()                            | 0x6c0360eb |
| unrevURI()                           | 0x580b1c8d |
| baseExtension()                      | 0xc6682862 |
| cost()                               | 0x13faede6 |
| maxSupply()                          | 0xd5abeb01 |
| public_paused()                      | 0x5c6331bd |
| revealed()                           | 0x51830227 |
+--------------------------------------------------+------------+
```

Conclusion

The smart contracts reviewed in this audit contain no critical severity issues and all High to Medium issues have either been corrected or acknowledged.

Please check the disclaimer above and note, the audit makes no statements or warranties on business model, investment attractiveness or code sustainability. The report is provided for the only contract mentioned in the report and does not include any other potential contracts deployed by Owner.

Ascendant

Ascendant

@ascendantproj

www.ascendant.finance.com

Ascendant