Guard

Smart contracts security assessment

Final report

Tariff: Standard

MiniVerse

March 2022

0xguard.com

hello@0xguard.com

Contents

1. Introduction 3
2. Contracts checked 3
3. Procedure 4
4. Classification of issue severity 4
5. Issues 5
6. Conclusion 7
7. Disclaimer 8
8. Static code analysis results 9

Introduction

This report has been prepared for the Mini Verse Finance team upon their request.

The audited project is a fork of the Tomb Finance Project.

Further details about Mini Verse Finance are available at the official website: https://mvfinance.club/

Name	MiniVerse
Audit date	2022-03-13 - 2022-03-13
Language	Solidity
Platform	Fantom Network

Contracts checked

Name	Address
MvDollarGenesisPool	https://ftmscan.com/address/0xd486e4Cd0091b31981dB5C0ccD8ba974607d03fc
Land NFT	https://ftmscan.com/address/0xc1E87be1055509081EA73A0FD5D3d70f6573Dc99
Oracle	https://ftmscan.com/address/0xc417d14f3a527cce4a1bfc0ac7ce38f8121c0030
MSHARE	https://ftmscan.com/address/0xb011EC534d9175cD7a69aFBfc1bcc9990862c462
MvBOND	https://ftmscan.com/address/0x4d2df4fdB3E9F57f367B6570eC62642D268D70cD
Boardroom	https://ftmscan.com/address/0x92c102Eab956c8d330709681AE74dc68815fC0bc
Treasury	https://ftmscan.com/address/0xC09BBc9Bc78CA30793334B3AE3565f2a67352169

MvDOLLAR	https://ftmscan.com/address/0x57976c467608983513c9355238dc6de1B1aBbcCA
MvShareRewardPool	https://ftmscan.com/address/0x1D39015cEa46a977cC5752C05fF2Cb3c1a4038E7

Procedure

We perform our audit according to the following procedure:

Automated analysis

- Scanning the project's smart contracts with several publicly available automated Solidity analysis tools
- Manual verification (reject or confirm) all the issues found by the tools

Manual audit

- Comparing the project to the Tomb Finance implementation

Classification of issue severity

High severity	High severity issues can cause a significant or full loss of funds, change of contract ownership, major interference with contract logic. Such issues require immediate attention.
Medium severity	Medium severity issues do not pose an immediate risk, but can be detrimental to the client's reputation if exploited. Medium severity issues may lead to a contract failure and can be fixed by modifying the contract state or redeployment. Such issues require attention.
Low severity	Low severity issues do not cause significant destruction to the contract's functionality. Such issues are recommended to be taken into consideration.

Issues

High severity issues

No issues were found

Medium severity issues

No issues were found

Low severity issues

1. Setting an address as exploiter cannot be undone (MvDollarGenesisPool)

An owner can blacklist address, but can't unset it back in case it was set by mistake.

```
function exploiters(address[] calldata _users) public onlyOperator {
for (uint256 i = 0; i < _users.length; i++){
    exploiter[_users[i]] = true;
}
```

Recommendation: We recommend adding a boolean parameter to the function to be able to set wrongly added address as not exploiter.

2. Exploiter address cannot be unset (Land NFT)

The owner can blacklist an address via setting it as exploiter, but can't undo it.

3. Redundant withdraw function (Land NFT)

No need for withdraw function as its the only function to receive native currency.

```
function withdraw() public payable onlyOwner {

  (bool os, ) = payable(owner()).call{value: address(this).balance}("");
```

```
    require(os);

  }
```

The function will only withdraw the funds that are deposited with it.

Conclusion

The Mini Verse Project was compared with the Tomb Project. Changes in the contracts besides changed parameters:

MvShareRewardPool: removed epochs for reward, effectively leaving only one epoch. For a specific pool pid users can deposit if they have Land NFT on their balance. The pid can be changed by the owner.

MvShare: added ownable function that allows the owner to mint MvShare. No restrictions on the mint amount.

Oracle: added multipliers in consult() and twap() functions.

MvDollarGenesisPool: added blacklist (exploiters). Commission is taken on every deposit.

MvDOLLAR: removed tax, tiers.

Mini Verse team response: There is a 300 day timelock on the function. And we have it left open so in the future if we ever want to increase MShare for more LP rewards or future use case. This is a big issue for even OG Tomb Finance there LP rewards end in April and they can't create more.

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 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 without 0xGuard prior written consent.

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 contracts 0xGuard to perform a security assessment. This report does not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analyzed, 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.

Static code analysis results

```
INFO:Detectors:
MiniLand.withdraw() (contracts/LandNFT.sol#2409-2414) sends eth to arbitrary user
        Dangerous calls:
        - (os) = address(owner()).call{value: address(this).balance}() (contracts/
LandNFT.sol#2411)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#functions-that-
send-ether-to-arbitrary-destinations
INFO:Detectors:
Reentrancy in MiniLand.mintBronze(uint256) (contracts/LandNFT.sol#2203-2231):
        External calls:
        - IERC20(erc20Address).safeTransferFrom(msg.sender,treasuryAddress,bronzePrice
* _mintAmount) (contracts/LandNFT.sol#2219)
        State variables written after the call(s):
        - whitelistedAddresses[msg.sender] -- (contracts/LandNFT.sol#2224)
Reentrancy in MiniLand.mintBronze(uint256) (contracts/LandNFT.sol#2203-2231):
        External calls:
        - IERC20(erc20Address).safeTransferFrom(msg.sender,treasuryAddress,bronzePrice
* _mintAmount) (contracts/LandNFT.sol#2219)
        - _safeMint(msg.sender,supply + i) (contracts/LandNFT.sol#2226)
                - IERC721Receiver(to).onERC721Received(_msgSender(),from,tokenId,_data)
(contracts/LandNFT.sol#1930-1940)
        State variables written after the call(s):
        - _safeMint(msg.sender,supply + i) (contracts/LandNFT.sol#2226)
                - _allTokens.push(tokenId) (contracts/LandNFT.sol#2083)
                - _allTokens[tokenIndex] = lastTokenId (contracts/LandNFT.sol#2131)
                - _allTokens.pop() (contracts/LandNFT.sol#2136)
        - limit[msg.sender] ++ (contracts/LandNFT.sol#2229)
        - maxMintBronze ++ (contracts/LandNFT.sol#2228)
Reentrancy in MiniLand.mintDiamond(uint256) (contracts/LandNFT.sol#2293-2321):
        External calls:
        - IERC20(erc20Address).safeTransferFrom(msg.sender,treasuryAddress,diamondPrice
* _mintAmount) (contracts/LandNFT.sol#2309)
        State variables written after the call(s):
        - whitelistedAddresses[msg.sender] -- (contracts/LandNFT.sol#2314)
Reentrancy in MiniLand.mintDiamond(uint256) (contracts/LandNFT.sol#2293-2321):
        External calls:
        - IERC20(erc20Address).safeTransferFrom(msg.sender,treasuryAddress,diamondPrice
```

```
* _mintAmount) (contracts/LandNFT.sol#2309)
        - _safeMint(msg.sender,supply + i) (contracts/LandNFT.sol#2316)
                - IERC721Receiver(to).onERC721Received(_msgSender(),from,tokenId,_data)
(contracts/LandNFT.sol#1930-1940)
        State variables written after the call(s):
        - _safeMint(msg.sender,supply + i) (contracts/LandNFT.sol#2316)
                - _allTokens.push(tokenId) (contracts/LandNFT.sol#2083)
                - _allTokens[tokenIndex] = lastTokenId (contracts/LandNFT.sol#2131)
                - _allTokens.pop() (contracts/LandNFT.sol#2136)
        - limit[msg.sender] ++ (contracts/LandNFT.sol#2319)
        - maxMintDiamond ++ (contracts/LandNFT.sol#2318)
Reentrancy in MiniLand.mintGold(uint256) (contracts/LandNFT.sol#2263-2291):
        External calls:
        - IERC20(erc20Address).safeTransferFrom(msg.sender,treasuryAddress,goldPrice *
_mintAmount) (contracts/LandNFT.sol#2279)
        State variables written after the call(s):
        - whitelistedAddresses[msg.sender] -- (contracts/LandNFT.sol#2284)
Reentrancy in MiniLand.mintGold(uint256) (contracts/LandNFT.sol#2263-2291):
        External calls:
        - IERC20(erc20Address).safeTransferFrom(msg.sender,treasuryAddress,goldPrice *
_mintAmount) (contracts/LandNFT.sol#2279)
        - _safeMint(msg.sender,supply + i) (contracts/LandNFT.sol#2286)
                - IERC721Receiver(to).onERC721Received(_msgSender(),from,tokenId,_data)
(contracts/LandNFT.sol#1930-1940)
        State variables written after the call(s):
        - _safeMint(msg.sender,supply + i) (contracts/LandNFT.sol#2286)
                - _allTokens.push(tokenId) (contracts/LandNFT.sol#2083)
                - _allTokens[tokenIndex] = lastTokenId (contracts/LandNFT.sol#2131)
                - _allTokens.pop() (contracts/LandNFT.sol#2136)
        - limit[msg.sender] ++ (contracts/LandNFT.sol#2289)
        - maxMintGold ++ (contracts/LandNFT.sol#2288)
Reentrancy in MiniLand.mintSilver(uint256) (contracts/LandNFT.sol#2233-2261):
        External calls:
        - IERC20(erc20Address).safeTransferFrom(msg.sender,treasuryAddress,silverPrice
* _mintAmount) (contracts/LandNFT.sol#2249)
        State variables written after the call(s):
        - whitelistedAddresses[msg.sender] -- (contracts/LandNFT.sol#2254)
Reentrancy in MiniLand.mintSilver(uint256) (contracts/LandNFT.sol#2233-2261):
        External calls:
        - IERC20(erc20Address).safeTransferFrom(msg.sender,treasuryAddress,silverPrice
* _mintAmount) (contracts/LandNFT.sol#2249)
```

```
        - _safeMint(msg.sender,supply + i) (contracts/LandNFT.sol#2256)
                - IERC721Receiver(to).onERC721Received(_msgSender(),from,tokenId,_data)
(contracts/LandNFT.sol#1930-1940)
        State variables written after the call(s):
        - _safeMint(msg.sender,supply + i) (contracts/LandNFT.sol#2256)
                - _allTokens.push(tokenId) (contracts/LandNFT.sol#2083)
                - _allTokens[tokenIndex] = lastTokenId (contracts/LandNFT.sol#2131)
                - _allTokens.pop() (contracts/LandNFT.sol#2136)
        - limit[msg.sender] ++ (contracts/LandNFT.sol#2259)
        - maxMintSilver ++ (contracts/LandNFT.sol#2258)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#reentrancy-
vulnerabilities-1
INFO:Detectors:
MiniLand.walletOfOwner(address).i (contracts/LandNFT.sol#2330) is a local variable
never initialized
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#uninitialized-
local-variables
INFO:Detectors:
ERC721._checkOnERC721Received(address,address,uint256,bytes) (contracts/
LandNFT.sol#1923-1944) ignores return value by
IERC721Receiver(to).onERC721Received(_msgSender(),from,tokenId,_data) (contracts/
LandNFT.sol#1930-1940)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#unused-return
INFO:Detectors:
MiniLand.constructor(string,string,address,address,string,string,string,string)._name
(contracts/LandNFT.sol#2172) shadows:
        - ERC721._name (contracts/LandNFT.sol#1559) (state variable)
MiniLand.constructor(string,string,address,address,string,string,string,string)._symbol
(contracts/LandNFT.sol#2173) shadows:
        - ERC721._symbol (contracts/LandNFT.sol#1562) (state variable)
MiniLand.walletOfOwner(address)._owner (contracts/LandNFT.sol#2323) shadows:
        - Ownable._owner (contracts/LandNFT.sol#46) (state variable)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#local-variable-
shadowing
INFO:Detectors:
MiniLand.constructor(string,string,address,address,string,string,string,string)._erc20Ad
dress (contracts/LandNFT.sol#2174) lacks a zero-check on :
                - erc20Address = _erc20Address (contracts/LandNFT.sol#2185)
MiniLand.constructor(string,string,address,address,string,string,string,string)._treasur
yAddress (contracts/LandNFT.sol#2175) lacks a zero-check on :
                - treasuryAddress = _treasuryAddress (contracts/LandNFT.sol#2186)
```

```
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#missing-zero-
address-validation
INFO:Detectors:
Variable 'ERC721._checkOnERC721Received(address,address,uint256,bytes).retval
(contracts/LandNFT.sol#1930)' in
ERC721._checkOnERC721Received(address,address,uint256,bytes) (contracts/
LandNFT.sol#1923-1944) potentially used before declaration: retval ==
IERC721Receiver.onERC721Received.selector (contracts/LandNFT.sol#1931)
Variable 'ERC721._checkOnERC721Received(address,address,uint256,bytes).reason
(contracts/LandNFT.sol#1932)' in
ERC721._checkOnERC721Received(address,address,uint256,bytes) (contracts/
LandNFT.sol#1923-1944) potentially used before declaration: reason.length == 0
(contracts/LandNFT.sol#1933)
Variable 'ERC721._checkOnERC721Received(address,address,uint256,bytes).reason
(contracts/LandNFT.sol#1932)' in
ERC721._checkOnERC721Received(address,address,uint256,bytes) (contracts/
LandNFT.sol#1923-1944) potentially used before declaration: revert(uint256,uint256)(32
+ reason,mload(uint256)(reason)) (contracts/LandNFT.sol#1937)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#pre-
declaration-usage-of-local-variables
INFO:Detectors:
Reentrancy in MiniLand.mintBronze(uint256) (contracts/LandNFT.sol#2203-2231):
        External calls:
        - IERC20(erc20Address).safeTransferFrom(msg.sender,treasuryAddress,bronzePrice
* _mintAmount) (contracts/LandNFT.sol#2219)
        - _safeMint(msg.sender,supply + i) (contracts/LandNFT.sol#2226)
                - IERC721Receiver(to).onERC721Received(_msgSender(),from,tokenId,_data)
(contracts/LandNFT.sol#1930-1940)
        State variables written after the call(s):
        - deedType[supply + i] = bronze (contracts/LandNFT.sol#2227)
Reentrancy in MiniLand.mintDiamond(uint256) (contracts/LandNFT.sol#2293-2321):
        External calls:
        - IERC20(erc20Address).safeTransferFrom(msg.sender,treasuryAddress,diamondPrice
* _mintAmount) (contracts/LandNFT.sol#2309)
        - _safeMint(msg.sender,supply + i) (contracts/LandNFT.sol#2316)
                - IERC721Receiver(to).onERC721Received(_msgSender(),from,tokenId,_data)
(contracts/LandNFT.sol#1930-1940)
        State variables written after the call(s):
        - deedType[supply + i] = diamond (contracts/LandNFT.sol#2317)
Reentrancy in MiniLand.mintGold(uint256) (contracts/LandNFT.sol#2263-2291):
        External calls:
```

```
        - IERC20(erc20Address).safeTransferFrom(msg.sender,treasuryAddress,goldPrice *
_mintAmount) (contracts/LandNFT.sol#2279)
        - _safeMint(msg.sender,supply + i) (contracts/LandNFT.sol#2286)
                - IERC721Receiver(to).onERC721Received(_msgSender(),from,tokenId,_data)
(contracts/LandNFT.sol#1930-1940)
        State variables written after the call(s):
        - deedType[supply + i] = gold (contracts/LandNFT.sol#2287)
Reentrancy in MiniLand.mintSilver(uint256) (contracts/LandNFT.sol#2233-2261):
        External calls:
        - IERC20(erc20Address).safeTransferFrom(msg.sender,treasuryAddress,silverPrice
* _mintAmount) (contracts/LandNFT.sol#2249)
        - _safeMint(msg.sender,supply + i) (contracts/LandNFT.sol#2256)
                - IERC721Receiver(to).onERC721Received(_msgSender(),from,tokenId,_data)
(contracts/LandNFT.sol#1930-1940)
        State variables written after the call(s):
        - deedType[supply + i] = silver (contracts/LandNFT.sol#2257)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#reentrancy-
vulnerabilities-2
INFO:Detectors:
Reentrancy in MiniLand.mintBronze(uint256) (contracts/LandNFT.sol#2203-2231):
        External calls:
        - IERC20(erc20Address).safeTransferFrom(msg.sender,treasuryAddress,bronzePrice
* _mintAmount) (contracts/LandNFT.sol#2219)
        - _safeMint(msg.sender,supply + i) (contracts/LandNFT.sol#2226)
                - IERC721Receiver(to).onERC721Received(_msgSender(),from,tokenId,_data)
(contracts/LandNFT.sol#1930-1940)
        Event emitted after the call(s):
        - Transfer(address(0),to,tokenId) (contracts/LandNFT.sol#1824)
                - _safeMint(msg.sender,supply + i) (contracts/LandNFT.sol#2226)
Reentrancy in MiniLand.mintDiamond(uint256) (contracts/LandNFT.sol#2293-2321):
        External calls:
        - IERC20(erc20Address).safeTransferFrom(msg.sender,treasuryAddress,diamondPrice
* _mintAmount) (contracts/LandNFT.sol#2309)
        - _safeMint(msg.sender,supply + i) (contracts/LandNFT.sol#2316)
                - IERC721Receiver(to).onERC721Received(_msgSender(),from,tokenId,_data)
(contracts/LandNFT.sol#1930-1940)
        Event emitted after the call(s):
        - Transfer(address(0),to,tokenId) (contracts/LandNFT.sol#1824)
                - _safeMint(msg.sender,supply + i) (contracts/LandNFT.sol#2316)
Reentrancy in MiniLand.mintGold(uint256) (contracts/LandNFT.sol#2263-2291):
        External calls:
```

```
        - IERC20(erc20Address).safeTransferFrom(msg.sender,treasuryAddress,goldPrice *
_mintAmount) (contracts/LandNFT.sol#2279)
        - _safeMint(msg.sender,supply + i) (contracts/LandNFT.sol#2286)
                - IERC721Receiver(to).onERC721Received(_msgSender(),from,tokenId,_data)
(contracts/LandNFT.sol#1930-1940)
        Event emitted after the call(s):
        - Transfer(address(0),to,tokenId) (contracts/LandNFT.sol#1824)
                - _safeMint(msg.sender,supply + i) (contracts/LandNFT.sol#2286)
Reentrancy in MiniLand.mintSilver(uint256) (contracts/LandNFT.sol#2233-2261):
        External calls:
        - IERC20(erc20Address).safeTransferFrom(msg.sender,treasuryAddress,silverPrice
* _mintAmount) (contracts/LandNFT.sol#2249)
        - _safeMint(msg.sender,supply + i) (contracts/LandNFT.sol#2256)
                - IERC721Receiver(to).onERC721Received(_msgSender(),from,tokenId,_data)
(contracts/LandNFT.sol#1930-1940)
        Event emitted after the call(s):
        - Transfer(address(0),to,tokenId) (contracts/LandNFT.sol#1824)
                - _safeMint(msg.sender,supply + i) (contracts/LandNFT.sol#2256)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#reentrancy-
vulnerabilities-3
INFO:Detectors:
EnumerableSet.values(EnumerableSet.AddressSet) (contracts/LandNFT.sol#792-801) uses
assembly
        - INLINE ASM (contracts/LandNFT.sol#796-798)
EnumerableSet.values(EnumerableSet.UintSet) (contracts/LandNFT.sol#865-874) uses
assembly
        - INLINE ASM (contracts/LandNFT.sol#869-871)
Address.verifyCallResult(bool,bytes,string) (contracts/LandNFT.sol#1328-1348) uses
assembly
        - INLINE ASM (contracts/LandNFT.sol#1340-1343)
ERC721._checkOnERC721Received(address,address,uint256,bytes) (contracts/
LandNFT.sol#1923-1944) uses assembly
        - INLINE ASM (contracts/LandNFT.sol#1936-1938)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#assembly-usage
INFO:Detectors:
MiniLand.mintBronze(uint256) (contracts/LandNFT.sol#2203-2231) compares to a boolean
constant:
        -require(bool,string)(exploiter[msg.sender] == false,EXPLOITER GIVE ME MY
MONEY) (contracts/LandNFT.sol#2204)
MiniLand.mintBronze(uint256) (contracts/LandNFT.sol#2203-2231) compares to a boolean
constant:
```

```
        -onlyWhitelisted == true (contracts/LandNFT.sol#2215)
MiniLand.mintSilver(uint256) (contracts/LandNFT.sol#2233-2261) compares to a boolean
constant:
        -require(bool,string)(exploiter[msg.sender] == false,EXPLOITER GIVE ME MY
MONEY) (contracts/LandNFT.sol#2234)
MiniLand.mintSilver(uint256) (contracts/LandNFT.sol#2233-2261) compares to a boolean
constant:
        -onlyWhitelisted == true (contracts/LandNFT.sol#2245)
MiniLand.mintGold(uint256) (contracts/LandNFT.sol#2263-2291) compares to a boolean
constant:
        -onlyWhitelisted == true (contracts/LandNFT.sol#2275)
MiniLand.mintGold(uint256) (contracts/LandNFT.sol#2263-2291) compares to a boolean
constant:
        -require(bool,string)(exploiter[msg.sender] == false,EXPLOITER GIVE ME MY
MONEY) (contracts/LandNFT.sol#2264)
MiniLand.mintDiamond(uint256) (contracts/LandNFT.sol#2293-2321) compares to a boolean
constant:
        -onlyWhitelisted == true (contracts/LandNFT.sol#2305)
MiniLand.mintDiamond(uint256) (contracts/LandNFT.sol#2293-2321) compares to a boolean
constant:
        -require(bool,string)(exploiter[msg.sender] == false,EXPLOITER GIVE ME MY
MONEY) (contracts/LandNFT.sol#2294)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#boolean-
equality
INFO:Detectors:
Different versions of Solidity is used:
        - Version used: ['>=0.7.0<0.9.0', '^0.8.0']
        - ^0.8.0 (contracts/LandNFT.sol#10)
        - >=0.7.0<0.9.0 (contracts/LandNFT.sol#2141)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#different-
pragma-directives-are-used
INFO:Detectors:
MiniLand.mintBronze(uint256) (contracts/LandNFT.sol#2203-2231) has costly operations
inside a loop:
        - maxMintBronze ++ (contracts/LandNFT.sol#2228)
MiniLand.mintSilver(uint256) (contracts/LandNFT.sol#2233-2261) has costly operations
inside a loop:
        - maxMintSilver ++ (contracts/LandNFT.sol#2258)
MiniLand.mintGold(uint256) (contracts/LandNFT.sol#2263-2291) has costly operations
inside a loop:
        - maxMintGold ++ (contracts/LandNFT.sol#2288)
```

```
MiniLand.mintDiamond(uint256) (contracts/LandNFT.sol#2293-2321) has costly operations
inside a loop:
        - maxMintDiamond ++ (contracts/LandNFT.sol#2318)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#costly-
operations-inside-a-loop
INFO:Detectors:
Address.functionCall(address,bytes) (contracts/LandNFT.sol#1212-1214) is never used and
should be removed
Address.functionCallWithValue(address,bytes,uint256) (contracts/LandNFT.sol#1241-1247)
is never used and should be removed
Address.functionDelegateCall(address,bytes) (contracts/LandNFT.sol#1301-1303) is never
used and should be removed
Address.functionDelegateCall(address,bytes,string) (contracts/LandNFT.sol#1311-1320) is
never used and should be removed
Address.functionStaticCall(address,bytes) (contracts/LandNFT.sol#1274-1276) is never
used and should be removed
Address.functionStaticCall(address,bytes,string) (contracts/LandNFT.sol#1284-1293) is
never used and should be removed
Address.sendValue(address,uint256) (contracts/LandNFT.sol#1187-1192) is never used and
should be removed
Context._msgData() (contracts/LandNFT.sol#29-31) is never used and should be removed
ERC721._baseURI() (contracts/LandNFT.sol#1640-1642) is never used and should be removed
ERC721._burn(uint256) (contracts/LandNFT.sol#1839-1853) is never used and should be
removed
EnumerableSet._add(EnumerableSet.Set,bytes32) (contracts/LandNFT.sol#572-582) is never
used and should be removed
EnumerableSet._at(EnumerableSet.Set,uint256) (contracts/LandNFT.sol#648-650) is never
used and should be removed
EnumerableSet._contains(EnumerableSet.Set,bytes32) (contracts/LandNFT.sol#627-629) is
never used and should be removed
EnumerableSet._length(EnumerableSet.Set) (contracts/LandNFT.sol#634-636) is never used
and should be removed
EnumerableSet._remove(EnumerableSet.Set,bytes32) (contracts/LandNFT.sol#590-622) is
never used and should be removed
EnumerableSet._values(EnumerableSet.Set) (contracts/LandNFT.sol#660-662) is never used
and should be removed
EnumerableSet.add(EnumerableSet.AddressSet,address) (contracts/LandNFT.sol#742-744) is
never used and should be removed
EnumerableSet.add(EnumerableSet.Bytes32Set,bytes32) (contracts/LandNFT.sol#676-678) is
never used and should be removed
EnumerableSet.add(EnumerableSet.UintSet,uint256) (contracts/LandNFT.sol#815-817) is
```

```
never used and should be removed
EnumerableSet.at(EnumerableSet.AddressSet,uint256) (contracts/LandNFT.sol#780-782) is
never used and should be removed
EnumerableSet.at(EnumerableSet.Bytes32Set,uint256) (contracts/LandNFT.sol#714-716) is
never used and should be removed
EnumerableSet.at(EnumerableSet.UintSet,uint256) (contracts/LandNFT.sol#853-855) is
never used and should be removed
EnumerableSet.contains(EnumerableSet.AddressSet,address) (contracts/
LandNFT.sol#759-761) is never used and should be removed
EnumerableSet.contains(EnumerableSet.Bytes32Set,bytes32) (contracts/
LandNFT.sol#693-695) is never used and should be removed
EnumerableSet.contains(EnumerableSet.UintSet,uint256) (contracts/LandNFT.sol#832-834)
is never used and should be removed
EnumerableSet.length(EnumerableSet.AddressSet) (contracts/LandNFT.sol#766-768) is never
used and should be removed
EnumerableSet.length(EnumerableSet.Bytes32Set) (contracts/LandNFT.sol#700-702) is never
used and should be removed
EnumerableSet.length(EnumerableSet.UintSet) (contracts/LandNFT.sol#839-841) is never
used and should be removed
EnumerableSet.remove(EnumerableSet.AddressSet,address) (contracts/LandNFT.sol#752-754)
is never used and should be removed
EnumerableSet.remove(EnumerableSet.Bytes32Set,bytes32) (contracts/LandNFT.sol#686-688)
is never used and should be removed
EnumerableSet.remove(EnumerableSet.UintSet,uint256) (contracts/LandNFT.sol#825-827) is
never used and should be removed
EnumerableSet.values(EnumerableSet.AddressSet) (contracts/LandNFT.sol#792-801) is never
used and should be removed
EnumerableSet.values(EnumerableSet.Bytes32Set) (contracts/LandNFT.sol#726-728) is never
used and should be removed
EnumerableSet.values(EnumerableSet.UintSet) (contracts/LandNFT.sol#865-874) is never
used and should be removed
Math.average(uint256,uint256) (contracts/LandNFT.sol#956-959) is never used and should
be removed
Math.ceilDiv(uint256,uint256) (contracts/LandNFT.sol#967-970) is never used and should
be removed
Math.max(uint256,uint256) (contracts/LandNFT.sol#941-943) is never used and should be
removed
Math.min(uint256,uint256) (contracts/LandNFT.sol#948-950) is never used and should be
removed
Pausable._pause() (contracts/LandNFT.sol#1039-1042) is never used and should be removed
Pausable._unpause() (contracts/LandNFT.sol#1051-1054) is never used and should be
removed
```

```
SafeERC20.safeApprove(IERC20,address,uint256) (contracts/LandNFT.sol#1386-1399) is
never used and should be removed
SafeERC20.safeDecreaseAllowance(IERC20,address,uint256) (contracts/
LandNFT.sol#1410-1421) is never used and should be removed
SafeERC20.safeIncreaseAllowance(IERC20,address,uint256) (contracts/
LandNFT.sol#1401-1408) is never used and should be removed
SafeERC20.safeTransfer(IERC20,address,uint256) (contracts/LandNFT.sol#1362-1368) is
never used and should be removed
SafeMath.add(uint256,uint256) (contracts/LandNFT.sol#189-191) is never used and should
be removed
SafeMath.div(uint256,uint256) (contracts/LandNFT.sol#231-233) is never used and should
be removed
SafeMath.div(uint256,uint256,string) (contracts/LandNFT.sol#287-296) is never used and
should be removed
SafeMath.mod(uint256,uint256) (contracts/LandNFT.sol#247-249) is never used and should
be removed
SafeMath.mod(uint256,uint256,string) (contracts/LandNFT.sol#313-322) is never used and
should be removed
SafeMath.mul(uint256,uint256) (contracts/LandNFT.sol#217-219) is never used and should
be removed
SafeMath.sub(uint256,uint256) (contracts/LandNFT.sol#203-205) is never used and should
be removed
SafeMath.sub(uint256,uint256,string) (contracts/LandNFT.sol#264-273) is never used and
should be removed
SafeMath.tryAdd(uint256,uint256) (contracts/LandNFT.sol#118-124) is never used and
should be removed
SafeMath.tryDiv(uint256,uint256) (contracts/LandNFT.sol#160-165) is never used and
should be removed
SafeMath.tryMod(uint256,uint256) (contracts/LandNFT.sol#172-177) is never used and
should be removed
SafeMath.tryMul(uint256,uint256) (contracts/LandNFT.sol#143-153) is never used and
should be removed
SafeMath.trySub(uint256,uint256) (contracts/LandNFT.sol#131-136) is never used and
should be removed
Strings.toHexString(uint256) (contracts/LandNFT.sol#1520-1531) is never used and should
be removed
Strings.toHexString(uint256,uint256) (contracts/LandNFT.sol#1536-1546) is never used
and should be removed
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#dead-code
INFO:Detectors:
Pragma version^0.8.0 (contracts/LandNFT.sol#10) necessitates a version too recent to be
```

```
trusted. Consider deploying with 0.6.12/0.7.6
Pragma version>=0.7.0<0.9.0 (contracts/LandNFT.sol#2141) is too complex
solc-0.8.4 is not recommended for deployment
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#incorrect-
versions-of-solidity
INFO:Detectors:
Low level call in Address.sendValue(address,uint256) (contracts/LandNFT.sol#1187-1192):
        - (success) = recipient.call{value: amount}() (contracts/LandNFT.sol#1190)
Low level call in Address.functionCallWithValue(address,bytes,uint256,string)
(contracts/LandNFT.sol#1255-1266):
        - (success,returndata) = target.call{value: value}(data) (contracts/
LandNFT.sol#1264)
Low level call in Address.functionStaticCall(address,bytes,string) (contracts/
LandNFT.sol#1284-1293):
        - (success,returndata) = target.staticcall(data) (contracts/LandNFT.sol#1291)
Low level call in Address.functionDelegateCall(address,bytes,string) (contracts/
LandNFT.sol#1311-1320):
        - (success,returndata) = target.delegatecall(data) (contracts/LandNFT.sol#1318)
Low level call in MiniLand.withdraw() (contracts/LandNFT.sol#2409-2414):
        - (os) = address(owner()).call{value: address(this).balance}() (contracts/
LandNFT.sol#2411)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#low-level-
calls
INFO:Detectors:
Parameter ERC721.safeTransferFrom(address,address,uint256,bytes)._data (contracts/
LandNFT.sol#1714) is not in mixedCase
Parameter MiniLand.mintBronze(uint256)._mintAmount (contracts/LandNFT.sol#2203) is not
in mixedCase
Parameter MiniLand.mintSilver(uint256)._mintAmount (contracts/LandNFT.sol#2233) is not
in mixedCase
Parameter MiniLand.mintGold(uint256)._mintAmount (contracts/LandNFT.sol#2263) is not in
mixedCase
Parameter MiniLand.mintDiamond(uint256)._mintAmount (contracts/LandNFT.sol#2293) is not
in mixedCase
Parameter MiniLand.walletOfOwner(address)._owner (contracts/LandNFT.sol#2323) is not in
mixedCase
Parameter MiniLand.setmaxMintAmount(uint256)._newmaxMintAmount (contracts/
LandNFT.sol#2357) is not in mixedCase
Parameter MiniLand.setBaseURIDiamond(string)._newBaseURI (contracts/LandNFT.sol#2361)
is not in mixedCase
Parameter MiniLand.setBaseURIGold(string)._newBaseURI (contracts/LandNFT.sol#2365) is
```

```
not in mixedCase
Parameter MiniLand.setBaseURISilver(string)._newBaseURI (contracts/LandNFT.sol#2369) is
not in mixedCase
Parameter MiniLand.setBaseURIBronze(string)._newBaseURI (contracts/LandNFT.sol#2373) is
not in mixedCase
Parameter MiniLand.setBaseExtension(string)._newBaseExtension (contracts/
LandNFT.sol#2377) is not in mixedCase
Parameter MiniLand.pause(bool)._state (contracts/LandNFT.sol#2381) is not in mixedCase
Parameter MiniLand.setOnlyWhitelisted(bool)._state (contracts/LandNFT.sol#2385) is not
in mixedCase
Parameter MiniLand.whitelistUsers(address[],uint256[])._users (contracts/
LandNFT.sol#2389) is not in mixedCase
Parameter MiniLand.whitelistUsers(address[],uint256[])._amount (contracts/
LandNFT.sol#2389) is not in mixedCase
Parameter MiniLand.exploiters(address[])._users (contracts/LandNFT.sol#2395) is not in
mixedCase
Parameter MiniLand.setMintPrice(uint256[])._prices (contracts/LandNFT.sol#2401) is not
in mixedCase
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#conformance-to-
solidity-naming-conventions
INFO:Detectors:
MiniLand.maxSupply (contracts/LandNFT.sol#2151) should be constant
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#state-
variables-that-could-be-declared-constant
INFO:Detectors:
renounceOwnership() should be declared external:
        - Ownable.renounceOwnership() (contracts/LandNFT.sol#79-81)
transferOwnership(address) should be declared external:
        - Ownable.transferOwnership(address) (contracts/LandNFT.sol#87-90)
name() should be declared external:
        - ERC721.name() (contracts/LandNFT.sol#1614-1616)
symbol() should be declared external:
        - ERC721.symbol() (contracts/LandNFT.sol#1621-1623)
tokenURI(uint256) should be declared external:
        - ERC721.tokenURI(uint256) (contracts/LandNFT.sol#1628-1633)
        - MiniLand.tokenURI(uint256) (contracts/LandNFT.sol#2336-2347)
approve(address,uint256) should be declared external:
        - ERC721.approve(address,uint256) (contracts/LandNFT.sol#1647-1657)
setApprovalForAll(address,bool) should be declared external:
        - ERC721.setApprovalForAll(address,bool) (contracts/LandNFT.sol#1671-1673)
transferFrom(address,address,uint256) should be declared external:
```

```
        - ERC721.transferFrom(address,address,uint256) (contracts/
LandNFT.sol#1685-1694)
safeTransferFrom(address,address,uint256) should be declared external:
        - ERC721.safeTransferFrom(address,address,uint256) (contracts/
LandNFT.sol#1699-1705)
tokenByIndex(uint256) should be declared external:
        - ERC721Enumerable.tokenByIndex(uint256) (contracts/LandNFT.sol#2027-2030)
mintBronze(uint256) should be declared external:
        - MiniLand.mintBronze(uint256) (contracts/LandNFT.sol#2203-2231)
mintSilver(uint256) should be declared external:
        - MiniLand.mintSilver(uint256) (contracts/LandNFT.sol#2233-2261)
mintGold(uint256) should be declared external:
        - MiniLand.mintGold(uint256) (contracts/LandNFT.sol#2263-2291)
mintDiamond(uint256) should be declared external:
        - MiniLand.mintDiamond(uint256) (contracts/LandNFT.sol#2293-2321)
walletOfOwner(address) should be declared external:
        - MiniLand.walletOfOwner(address) (contracts/LandNFT.sol#2323-2334)
setmaxMintAmount(uint256) should be declared external:
        - MiniLand.setmaxMintAmount(uint256) (contracts/LandNFT.sol#2357-2359)
setBaseURIDiamond(string) should be declared external:
        - MiniLand.setBaseURIDiamond(string) (contracts/LandNFT.sol#2361-2363)
setBaseURIGold(string) should be declared external:
        - MiniLand.setBaseURIGold(string) (contracts/LandNFT.sol#2365-2367)
setBaseURISilver(string) should be declared external:
        - MiniLand.setBaseURISilver(string) (contracts/LandNFT.sol#2369-2371)
setBaseURIBronze(string) should be declared external:
        - MiniLand.setBaseURIBronze(string) (contracts/LandNFT.sol#2373-2375)
setBaseExtension(string) should be declared external:
        - MiniLand.setBaseExtension(string) (contracts/LandNFT.sol#2377-2379)
pause(bool) should be declared external:
        - MiniLand.pause(bool) (contracts/LandNFT.sol#2381-2383)
setOnlyWhitelisted(bool) should be declared external:
        - MiniLand.setOnlyWhitelisted(bool) (contracts/LandNFT.sol#2385-2387)
whitelistUsers(address[],uint256[]) should be declared external:
        - MiniLand.whitelistUsers(address[],uint256[]) (contracts/
LandNFT.sol#2389-2393)
exploiters(address[]) should be declared external:
        - MiniLand.exploiters(address[]) (contracts/LandNFT.sol#2395-2399)
setMintPrice(uint256[]) should be declared external:
        - MiniLand.setMintPrice(uint256[]) (contracts/LandNFT.sol#2401-2407)
withdraw() should be declared external:
```

```
        - MiniLand.withdraw() (contracts/LandNFT.sol#2409-2414)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#public-
function-that-could-be-declared-external
INFO:Slither:contracts/LandNFT.sol analyzed (20 contracts with 75 detectors), 157
result(s) found
```

0x Guard