HackSafe

Smart Contract Security Audit Report

Blockchain Land

May 2022

Security Status

★ ★ ★ ★ ★

www.hacksafe.io

Audit Details

Audited project
Blockchain Land

Deployer address
0x3f21fd58a109CF89237744f6Ad1d0dD64D912cc8

Client contacts
Blockchain Land

Blockchain
Binance Smart Chain

Website
www.blockchain.land

Disclaimer

This is a limited report on our findings based on our analysis, in accordance with good industry practice as at 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 us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the below disclaimer below – please make sure to read it in full.

DISCLAIMER: 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 TechRate and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (HackSafe) owe no duty of care towards you or any other person, nor does HackSafe 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 HackSafe 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, HackSafe hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against HackSafe, 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.

Background

HackSafe was commissioned by Blockchain Land to perform an audit of smart contracts:

Blockchain Land Token :
https://testnet.bscscan.com/address/0x06b14D60d3F979515DD1389d3a5ECd6ae58B8674#code

Blockchain Land NFT :
https://testnet.bscscan.com/address/0xb5066426D9cd6c6fD26fcf8928Ec33B91AFaf695#code

Blockchain Land Marketplace
https://testnet.bscscan.com/address/0x73120781d3BE5E64f572534C7DB45C0F47E24010#code

The purpose of the audit was to achieve the following:

- Ensure that the smart contract functions as intended.
- Identify potential security issue 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.

Contracts Details

Token contract details for 15.05.2022

Contract name	: Token
Contract address	: 0x06b14D60d3F979515DD1389d3a5ECd6ae58B8674
Max. supply	: 10 Billion
Token ticker	: LD
Decimals	: 18
Transactions count	: 1
Token Holders	: 1 addresses
Contract deployer address	: 0x3f21fd58a109CF89237744f6Ad1d0dD64D912cc8
Owner address	: 0x3f21fd58a109CF89237744f6Ad1d0dD64D912cc8

NFT Contract Details for 15.05.2022

Contract name	: ERC721NFT
Contract address	: 0xb5066426D9cd6c6fD26fcf8928Ec33B91AFaf695
Total Type	: ERC721
Contract deployer address	: 0x3f21fd58a109CF89237744f6Ad1d0dD64D912cc8
Owner address	: 0x3f21fd58a109CF89237744f6Ad1d0dD64D912cc8

Contracts Details

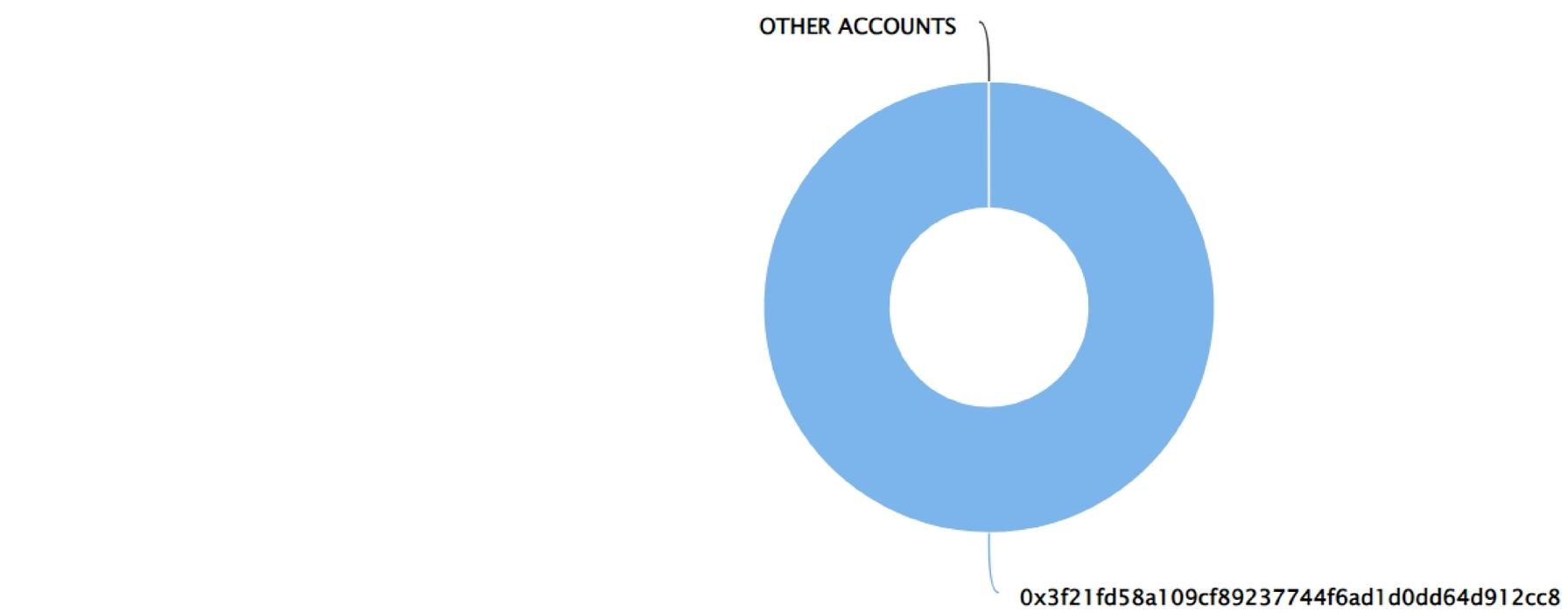
NFT Marketplace Contract for 15.05.2022

Contract name	: Marketplace
Contract address	: 0x73120781d3BE5E64f572534C7DB45C0F47E24010
Marketplace commission	: 10% (Commision), 15% (Nativecommision)
Contract deployer address	: 0x3f21fd58a109CF89237744f6Ad1d0dD64D912cc8
Owner address	: 0x3f21fd58a109CF89237744f6Ad1d0dD64D912cc8

Land Token Distribution

The top 100 holders collectively own 100.00% (1,000,000,000.00 Tokens) of land

Token Total Supply: 1,000,000,000.00 Token | Total Token Holders: 1



Land Token Top Holders

(A total of 1,000,000,000.00 tokens held by the top 100 accounts from the total supply of 1,000,000,000.00 token)

Rank	Address	Quantity (Token)	Percentage
1	0x3f21fd58a109cf89237744f6ad1d0dd64d912cc8	1,000,000,000	100.0000%

Contract Function details

Token contract function details

+ [Int] IERC20
    -[Ext]totalSupply
    -[Ext]balanceOf
    -[Ext]transfer
    -[Ext]allowance
    -[Ext]approve
    -[Ext]transferFrom

+ [Int] IERC20Metadata
    -[Ext] name
    -[Ext] symbol
    -[Ext] decimals

+ Context
    -[Int] _msgSender

+ ERC20 (Context, IERC20, IERC20Metadata)
    <Constructor>#
    -[Pub] name
    -[Pub] symbol
    -[Pub] decimals
    -[Pub] totalsupply
    -[Pub] balanceOf
    -[Pub] transfer#
    -[Pub] allowance
    -[Pub] approve#
    -[Pub] transferFrom#
    -[Pub] increaseAllowance#
    -[Pub] decreaseAllowance#
    -[Int] _transfer #
    -[Int] _mint #
    -[Int] _burn #
    -[Int] _approve #
    -[Int] _spendAllowance #
    -[Int] _beforeTokenTransfer
    -[Int] _afterTokenTransfer

Contract Function details

+ Token (ERC20)
    - <constructor> #
    - [Pub] mint #
        - modifier: onlyOwner
    - [Pub] burn #

NFT contract function details

+ [Int] IERC165
    -[Ext]supportsInterface

+[Int] IERC721 (IERC165)
    -[Ext] balanceOf
    -[Ext] ownerOf
    -[Ext] safeTransferFrom #
    -[Ext] safeTransferFrom #
    -[Ext] transferFrom #
    -[Ext] approve #
    -[Ext] setApprovalForAll #
    -[Ext] getApproved #
    -[Ext] isApprovedForAll

+ [Int] IERC721Receiver
    - [Ext] onERC721Received

+ [Int] IERC721Metadata (IERC721)
    - [Ext] name
    - [Ext] symbol
    - [Ext] tokenURI

+ [Lib] Address
    - [Int] isContract #

+ Context
    - [Int] _msgSender

Contract Function details

+ ERC165 (IERC165)
    - [Pub] supportsInterface

+ ERC721 (Context, ERC165, IERC721, IERC721Metadata)
    - < constructor>
    - [Pub] supportsInterface
    - [Pub] balanceOf
    - [Pub] ownerOf
    - [Pub] name
    - [Pub] symbol
    - [Pub] tokenURI
    - [Pub] approve #
    - [Pub] getApproved
    - [Pub] setApprovalForAll #
    - [Pub] isApprovedForAll
    - [Pub] transferFrom #
    - [Pub] safeTransferFrom #
    - [Pub] safeTransferFrom #
    - [Int] _safeTransfer #
    - [Int] _exists
    - [Int] _isApprovedOrOwner
    - [Int] _safeMint #
    - [Int] _safeMint #
    - [Int] _mint #
    - [Int] _burn #
    - [Int] _transfer #
    - [Int] _approve #
    - [Int] _setApprovalForAll #
    - [Pvt] _checkOnERC721Received #
    - [Int] _beforeTokenTransfer
    - [Int] _afterTokenTransfer

- [Lib] Counters
    - [Int] current
    - [Int] increment
    - [Int] decrement

Contract Function details

- [Lib] SafeMath
    - [Int] add
    - [Int] sub
    - [Int] mul
    - [Int] div
    - [Int] mod
    - [Int] sub
    - [Int] div
    - [Int] mod

+ Ownable (Context)
    - <constructor> #
    - [Pub] owner
    - [Pub] renounceOwnership #
      -modifiers: onlyOwner
    - [Pub] transferOwnership #
      -modifiers: onlyOwner
    - [Int] _transferOwnership #

+ERC721NFT (ERC721, Ownable)
    - <constructor> #
    - [Pub] addAdmin #
      -modifier: onlyOwner
    - [Pub] addMinter #
    - [Pub] mint #
    - [Pub] batchMint #
    - [Pub] royaltyOf
    - [Pub] creatorOf
    - [Pub] totalSupply

Marketplace contract function details

+[Int] IERC165
    -[Ext] supportsInterface

+[Int] IERC721 (IERC165)
    -[Ext] balanceOf
    -[Ext] ownerOf

Contract Function details

- [Ext] safeTransferFrom #
- [Ext] transferFrom #
- [Ext] approve #
- [Ext] setApprovalForAll #
- [Ext] getApproved #
- [Ext] isApprovedForAll
- [Ext] totalSupply
- [Ext] royaltyOf
- [Ext] creatorOf

+ [Int] IERC20
  - [Ext] balanceOf
  - [Ext] transfer #
  - [Ext] approve #
  - [Ext] transferFrom #

+ Context
  - [Int] _msgSender

+ [Lib] Address
  - [Int] isContract #

+ Ownable (Context)
  - <constructor> #
  - [Pub] owner
  - [Pub] renounceOwnership #
    -modifiers: onlyOwner
  - [Pub] transferOwnership #
    -modifiers: onlyOwner
  - [Int] _transferOwnership #

+ [Lib] Counters
  - [Int] current
  - [Int] increment
  - [Int] decrement

Contract Function details

+ [Lib] SafeMath
    - [Int] add
    - [Int] sub
    - [Int] mul
    - [Int] div

+ Marketplace (Ownable)
    - <constructor>
    - [Pvt] callOptionalReturn
    - [Pub] sell #
    - [Pub] buy #
    - [Pub] nativeBuy $
    - [Pub] createAuction #
    - [Pub] bid #
    - [Pub] nativeBid $
    - [Pub] auctionFinalize #
    - [Pub] makeOffer #
    - [Pub] makeNativeOffer $
    - [Pub] fillOffer #
    - [Pub] withdrawOffer #
    - [Pub] listOfBidder
    - [Pub] listOfNativeBidder
    - [Pub] listofOwner
    - [Pub] updateCommission #
      - modifier: onlyOwner
    - [Pub] updateNativeCommission #
      - modifier: onlyOwner
    - [Ext] removeAuction #
    - [Pub] removeSell#
    - [Pub] auctionDetail
    - [Pub] sellDetail
    - [Pub] openSell
    - [Pub] openAuction

($) = payable function

= non-constant function

Issues Checking Status

No.	Title	Status
1.	Unlocked Compiler Version	Passed
2.	Missing Input Validation	Passed
3.	Race conditions and Reentrancy. Cross-function race conditions.	Passed
4.	Possible delays in data delivery	Passed
5.	Oracle calls.	Passed
6.	Timestamp dependence.	Passed
7.	Integer Overflow and Underflow	Passed
8.	DoS with Revert.	Passed
9.	DoS with block gas limit.	Passed
10.	Methods execution permissions.	Passed
11.	Economy model of the contract.	Passed
12.	Private use data leaks.	Passed
13.	Malicious Event log.	Passed
14.	Scoping and Declarations.	Passed
15.	Uninitialized storage pointers.	Passed
16.	Arithmetic accuracy.	Passed
17.	Design Logic.	Passed
18.	Safe Open Zeppelin contracts implementation and usage.	Passed
19.	Incorrect Naming State Variable	Passed

Severity Definitions

Risk Level	Description
Critical	Critical vulnerabilities are usually straightforward to exploit and can lead to assets loss or data manipulations.
High	High-level vulnerabilities are difficult to exploit; however, they also have a 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 assets loss or data manipulations.
Low	Low-level vulnerabilities are mostly related to outdated, unused, etc. code snippets that can't have a significant impact on execution.

Security Issues

- **Critical Severity Issues**
  No Critical severity issue found.

- **High Severity Issues**
  No high severity issue found.

- **Medium Severity Issues**
  No medium severity issue found.

- **Low Severity Issues**
  No low severity issue found.

Owner Privileges

Owner Privileges :

- Token contract :
    - Owner can mint maximum 10 billion tokens.

- NFT Contract :
    - Owner can add admin.
    - Owner can renounce ownership.
    - Owner can transfer ownership.
    - Owner can mint NFTs.

- NFT Marketplace :
    - Owner can renounce ownership.
    - Owner can transfer ownership.
    - Owner can update commission rates.

Conclusion

Smart contracts contain no severity issues! The further transfer and operations with the fund raised are not related to this particular contract.

HackSafe note: 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.