HackSafe

Smart Contract Security Audit Report

Decentraland

July 2022

Security Status

★ ★ ★ ★ ⯪

www.hacksafe.io

Audit Details

Audited project
Decentraland

Deployer address
0x6Bf917B4725aD736B33Dbd493Ad7a4B992150DAb

Client contacts
Decentraland team

Blockchain
Ethereum

Website
https://decentraland.org/

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.

Procedure

Step 1 - In-Depth Manual Review

Manual line-by-line code reviews to ensure the logic behind each function is sound and safe from various attack vectors. This is the most important and lengthy portion of the audit process (as automated tools often cannot find the nuances that lead to exploits such as flash loan attacks).

Step 2 - Automated Testing

Simulation of a variety of interactions with your Smart Contract on a test blockchain leveraging a combination of automated test tools and manual testing to determine if any security vulnerabilities exist.

Step 3 – Leadership Review

The engineers assigned to the audit will schedule meetings with our leadership team to review the contracts, any comments or findings, and ask questions to further apply adversarial thinking to discuss less common attack vectors.

Step 4 - Resolution of Issues

Consulting with the team to provide our recommendations to ensure the code's security and optimize its gas efficiency, if possible. We assist project team's in resolving any outstanding issues or implementing our recommendations.

Step 5 - Published Audit Report

Boiling down results and findings into an easy-to-read report tailored to the project. Our audit reports highlight resolved issues and any risks that exist to the project or its users, along with any remaining suggested remediation measures. Diagrams are included at the end of each report to help users understand the interactions which occur within the project.

Background

HackSafe was commissioned by Decentraland to perform an audit of smart contract:

- https://etherscan.io/address/0x0f5d2fb29fb7d3cfee444a200298f468908cc942#code

The purpose of the audit was to achieve the

- Ensutre that the smart contract functions as intended.
- Identify potential security issues with the smart contract.

The information in this report should be 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.

Contract Details

Token contract details for 01.07.2022

Token Type	: ERC20
Contract name	: MANAToken
Contract address	: 0x0F5D2fB29fb7d3CFeE444a200298f468908cC942
Compiler version	: v0.4.11+commit.68ef5810
Max Total supply	: 2,193,628,027
Token Ticker	: MANA
Decimals	: 18
Token Holders	: 252,838
Top 100 token holder's dominance	: 74.29%
Transactions count	: 2,180,761
Contract deployer address	: 0x6Bf917B4725aD736B33Dbd493Ad7a4B992150DAb
Owner address	: 0xA66d83716c7CFE425B44D0f7ef92dE263468fb3d

Social profiles

Twitter Profile	: https://twitter.com/decentraland
Facebook Profile	: https://www.facebook.com/decentraland/
Github Profile	: https://github.com/decentraland
Whitepaper link	: https://decentraland.org/whitepaper.pdf
Coinmarketcap profile	: https://coinmarketcap.com/currencies/decentraland/
Coingecko profile	: https://www.coingecko.com/en/coins/decentraland
Uniswap profile:	https://v2.info.uniswap.org/pair/0x11b1f53204d03e5529f09eb3091939e4fd8c9cf3/
Reddit profile	: https://www.reddit.com/r/decentraland

Claimed Smart Contract Features

Claimed Feature Detail	Our Observation
Tokenomics : • Name : MANA • Symbol : MANA • Decimals : 18 • Protocol : ERC20 • Max Total supply : 2,193,628,027	Yes, This is valid.

Audit Summary

According to the standard audit assessment, Customer`s solidity smart contracts are “Secure”. This token contract does contain owner control, which do not make it fully decentralized as owner does have control over smart contract.

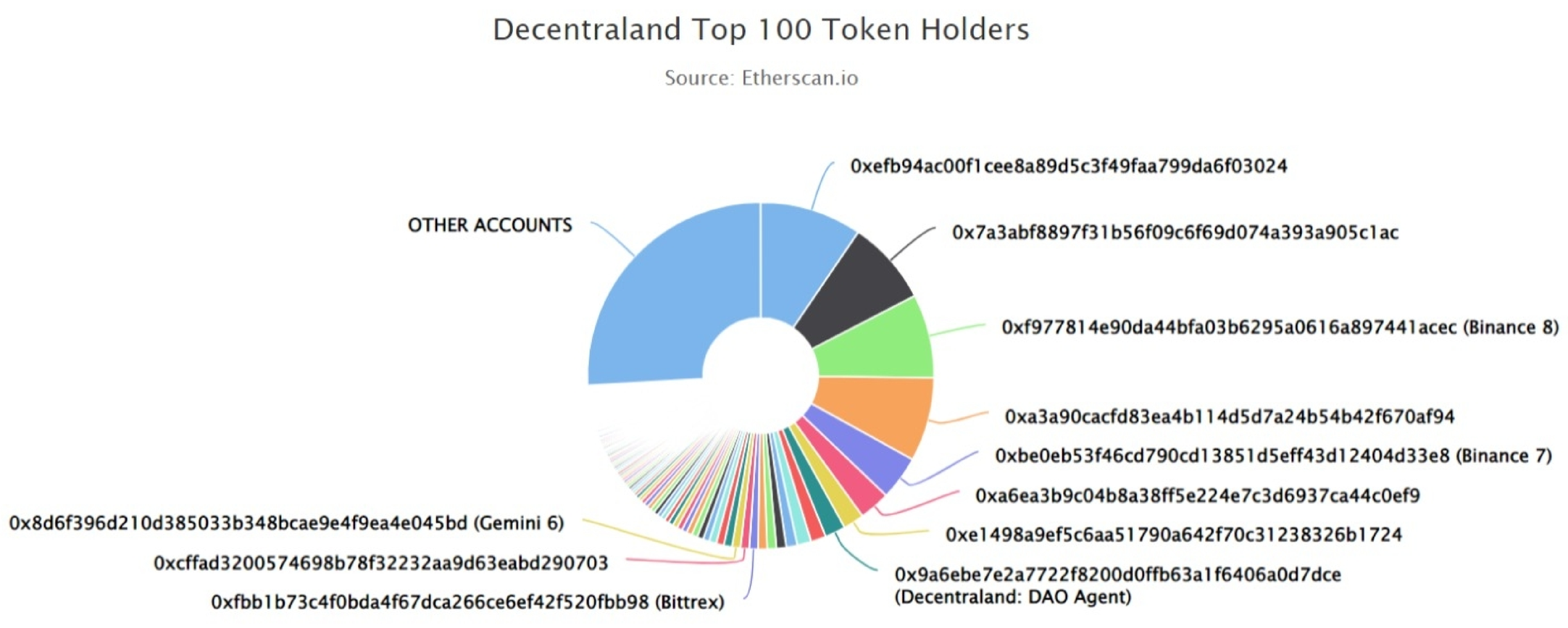
Insecure	Poor secured	Secure	Well-secured

You are here

We used various tools like Slither, Mythril and Remix IDE. At the same time this finding is based on critical analysis of the manual audit. All issues found during analysis were manually reviewed and applicable vulnerabilities are presented in the issues checking status.

We found 0 critical, 0 high, 0 medium and 2 low and some very low-level issues. These issues are not critical ones.

Decentraland Distribution



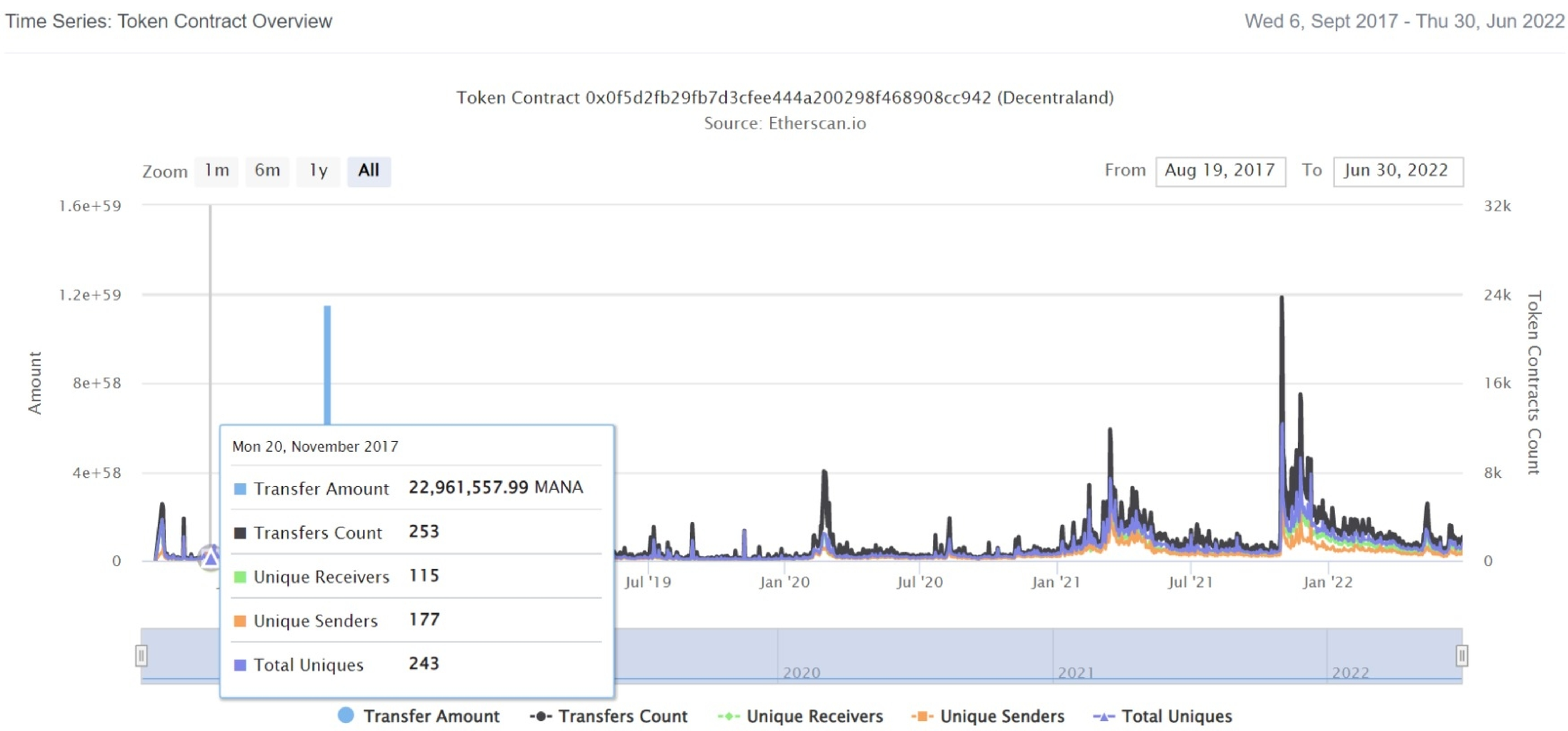
Decentraland Distribution

Decentraland Top 20 Token Holders

Rank	Address	Quantity	Percentage	Value	Analytics
1	0xefb94ac00f1cee8a89d5c3f49faa799da6f03024	208,570,187.444403031150693956	9.5080%	$175,941,438.35	
2	0x7a3abf8897f31b56f09c6f69d074a393a905c1ac	173,129,202.568493150684931507	7.8924%	$146,044,846.07	
3	Binance 8	171,761,754	7.8300%	$144,891,321.35	
4	0xa3a90cacfd83ea4b114d5d7a24b54b42f670af94	171,283,883.885083713850837139	7.8082%	$144,488,209.30	
5	Binance 7	90,000,000	4.1028%	$75,920,387.50	
6	0xa6ea3b9c04b8a38ff5e224e7c3d6937ca44c0ef9	63,254,948.249230596499182438	2.8836%	$53,359,335.36	
7	0xe1498a9ef5c6aa51790a642f70c31238326b1724	43,071,167.248793748178070947	1.9635%	$36,333,107.86	
8	Decentraland: DAO Agent	41,607,739.074984563777692532	1.8968%	$35,098,618.59	
9	Decentraland: wMANA Token	31,218,720.937222222	1.4232%	$26,334,859.90	
10	0x2ee555c9006a9dc4674f01e0d4dfc58e013708f0	28,496,316.210924596	1.2990%	$24,038,348.54	
11	Binance US 2	22,926,986.883993909546685787	1.0452%	$19,340,285.87	
12	0x90c8161ade96fc4c11295d012a20bdfd88eb039f	19,669,314.762115585915901629	0.8967%	$16,592,244.43	
13	Crypto.com	18,944,167.325415037471683718	0.8636%	$15,980,539.16	
14	0xadf023a014462fdced0557c42454989ef102ec86	18,635,999.289508938017089381	0.8496%	$15,720,580.97	
15	Bittrex	17,801,297.87171179	0.8115%	$15,016,460.36	
16	0xcffad3200574698b78f32232aa9d63eabd290703	17,740,986	0.8088%	$14,965,583.69	
17	Gemini 6	17,250,001	0.7864%	$14,551,408.45	
18	0xcc30c767f5d8e859de902ad39223ca387c79bb70	16,559,136.4968181001	0.7549%	$13,968,622.88	
19	OKEx	15,908,837.108756579927658843	0.7252%	$13,420,056.42	
20	0xe19499512f0fb4b1378175c1d5756e0197ff9351	14,999,225.76559835270610687	0.6838%	$12,652,744.80	

Decentraland Distribution

Decentraland Contract Overview



Contract functions details

+ ERC20Basic
    - balanceOf
    - transfer

+ Ownable
    Ownable
    TransferOwnership #
    -modifiers: onlyOwner

+ Pausable (Ownable)
    - pause
      -modifiers: onlyOwner whenNotPaused
    - unpause
      -modifiers: onlyOwner whenPaused

+ ERC20 (ERC20Basic)
    - allowance
    - transferFrom
    - approve

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

+BasicToken (ERC20Basic)
    - transfer
    - balanceOf

+ StandardToken (ERC20, BasicToken)
    - transferFrom
    - approve
    - allowance

+ MintableToken (StandardToken, Ownable)
    - mint
      - modifiers: onlyOwner, canMint
    - finishMinting
      -modifiers: onlyOwner

Contract functions details

+ PausableToken (StandardToken, Pausable)
    - transfer
      -modifiers: whenNotPaused
    - transferFrom
      -modifiers: whenNotPaused

+ BurnableToken (StandardToken)
    -[Pub] burn

+ MANAToken (BurnableToken, PausableToken, MintableToken)
    -[Pub] burn
      -modifiers: whenNotPaused

($) = payable function
= non-constant function

Issues Checking Status

No.	Title	Status
1.	Unlocked Compiler Version	Low issue
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.	Low issue
18.	Safe Open Zeppelin contracts implementation and usage.	Passed
19.	Incorrect Naming State Variable	Passed
20.	Compiler version too old	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 issues found.
- **Low Severity Issues**
  Two low severity issue found.

1. Unlocked Compiler Version.

- **Description**
  The contract utilizes an unlocked compiler version. An unlocked compiler version in the contract's source code permits the user to compile it at or above a particular version. This, in turn, leads to diffffferences in the generated bytecode between compilations due to diffffering compiler version numbers. This can lead to ambiguity when debugging as compiler-specifific bugs may occur in the codebase that would be diffiffifficult to identify over a span of multiple compiler versions rather than a specifific one.
- **Recommendation**
  It is advisable that the compiler version is alternatively locked at the lowest version possible so that the contract can be compiled. For example, for version v0^0.4.11 the contract should contain the following line:

  pragma solidity 0.4.11;

2. Design logic

Unused function.

- **Description**
  Transfer, transferFrom function do not check if the receiver's address is zero address or not.
- **Location:**
  Transfer, transferFrom function
- **Recommendation**
  We advise you to add require condition in both of the function checking that if receiver's address is not zero address as this can end to sending tokens to zero address which can not be return back.

Centralization

Owner Privileges :

- Decentraland Contract:
    - Owner can transfer ownership.
    - Owner can mint new tokens.
    - Owner can pause and unpause transfers.
    - Owner can finish minting.

This smart contract has some functions which can be executed by the pauser addresses only. If their wallet private key would be compromised, then it would create trouble. The ownership of the smart contract can't renounced for the token, which means admin is able to modify contract behavior (for example: mint new tokens, freeze and unfreeze contract). Please exercise with extra caution if you are investing in this asset. Following are Admin functions:

- Transferownership
- Unpause
- Pause
- Mint
- Finishminting

Conclusion

Smart contract contains low 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.