HackSafe

Smart Contract Security Audit Report

Bifrost

April **2022**

Security Status

★★★★½

www.hacksafe.io

Audit Details

Audited project
Bifrost

Deployer address
0x509F6180bc2B195c2864Ce7EE920D3Ac08943F17

Client contacts
Bifrost team

Blockchain
Ethereum

Website
https://thebifrost.io/

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

HeckSafe was commissioned by Bifrost to perform an audit of smart contracts:

- https://etherscan.io/address/0x0c7D5ae016f806603CB1782bEa29AC69471CAb9c#code

Contract Details

Token contract details for 19.04.2022

Contract name	: ERC20
Contract address	: 0x0c7D5ae016f806603CB1782bEa29AC69471CAb9c
Total supply	: 4 billion
Token Ticker	: BFC
Decimals	: 18
Token Holders	: 2,889
Transactions count	: 76, 375
Contract deployer address	: 0x509F6180bc2B195c2864Ce7EE920D3Ac08943F17
Owner address	: 0x509F6180bc2B195c2864Ce7EE920D3Ac08943F17

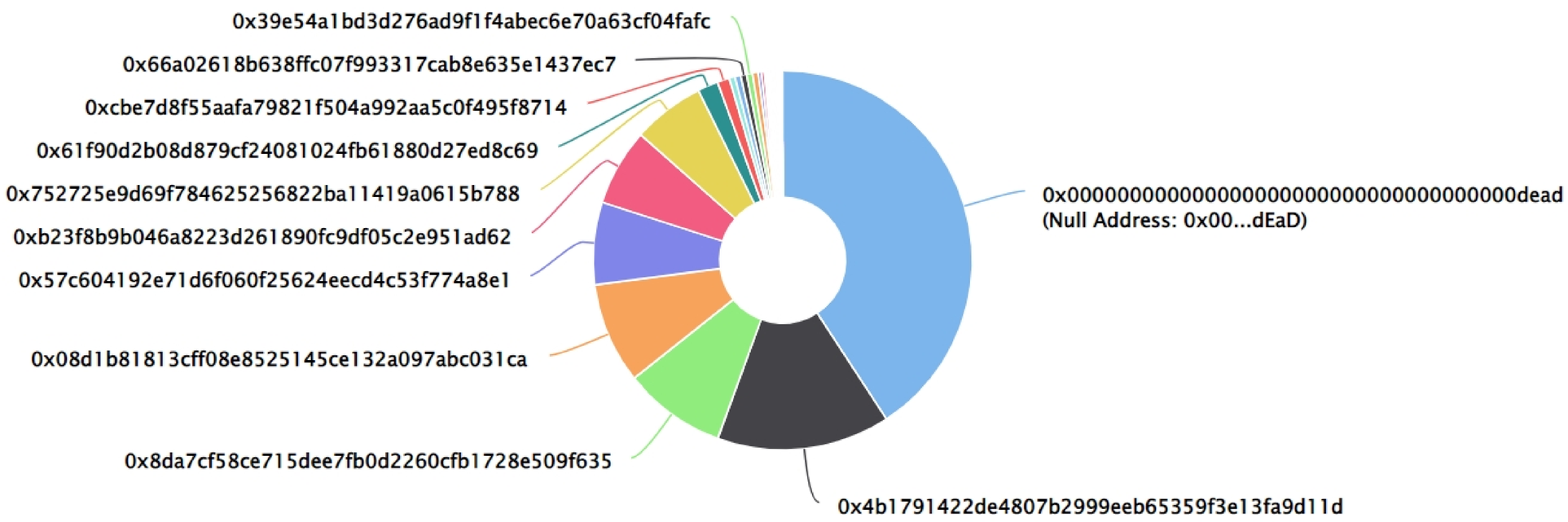
Bifrost Token Distribution

The top 500 holders collectively own 99.96% (3,998,511,540.38 Tokens) of Bifrost

Token Total Supply: 4,000,000,000.00 Token | Total Token Holders: 2,889

Bifrost Top 500 Token Holders

Source: Etherscan.io



Bifrost Top 10 Token Holders

(A total of 3,838,073,295.70 tokens held by the top 10 accounts from the total supply of 4,000,000,000.00 token)

Rank	Address	Quantity (Token)	Percentage
1	Null Address: 0x00...dEaD	1,631,415,927	40.7854%
2	0x4b1791422de4807b2999eeb65359f3e13fa9d11d	591,620,931.594869195957841602	14.7905%
3	0x8da7cf58ce715dee7fb0d2260cfb1728e509f635	350,000,000	8.7500%
4	0x08d1b81813cff08e8525145ce132a097abc031ca	344,000,000	8.6000%
5	0x57c604192e71d6f060f25624eecd4c53f774a8e1	282,005,415.939852161597305368	7.0501%
6	0xb23f8b9b046a8223d261890fc9df05c2e951ad62	262,209,800	6.5552%
7	0x752725e9d69f784625256822ba11419a0615b788	245,931,331.259691837799788608	6.1483%
8	0x61f90d2b08d879cf24081024fb61880d27ed8c69	69,515,615.903391763844821746	1.7379%
9	0xcbe7d8f55aafa79821f504a992aa5c0f495f8714	41,374,274	1.0344%
10	0xab6af9a773f9cba6b15db625ac51daa2f1a894e7	20,000,000	0.5000%

Contract functions details

+ Context
    -[Int] _msgSender
    -[Int] _msgData

+ Pausable (Context)
    -[Int] <Constructor> #
    -[Pub] paused
    -[Int] _pause #
      -modifiers: whenNotPaused
    -[Pub] _unpause #
      -modifiers: whenPaused

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

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

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

+ [Lib] Address
    -[Int] isContract
    -[Int] sendValue

Contract functions details

+ ERC20 (Context, IERC20, Pausable, Ownable)
    -[Pub] <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] _burn #
    -[Int] _approve #
    -[Pub] burn #
    -[Pub] burnFrom #
    -[Pub] pause #
      -modifiers: onlyOwner
    -[Pub] unpause #
      -modifiers: onlyOwner
    -[Int] _beforeTokenTransfer #

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.	Low issue
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 issues found.

✓ **Low Severity Issues**

Two low severity issues 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 differences in the generated bytecode between compilations due to differing compiler version numbers. This can lead to ambiguity when debugging as compiler-specific bugs may occur in the codebase that would be difficult to identify over a span of multiple compiler versions rather than a specific 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 v0.6.0 the contract should contain the following line:

  pragma solidity 0.6.0;

2. Scoping and Declarations.

Unused function.

- **Description**

  The div, mod, _msgData functions do nothing.
  Library Address does nothing.

- **Location**

  div, mod, _msgData functions.

- **Recommendation**

  We advise to remove unused code which can help you to develop clean coding style and save some computational gas too.

Owner Privileges

Owner Privileges (in the period when the owner is not renounced) :

- Bifrost Contract:
    - Owner can transfer ownership.
    - Owner can renounce ownership.
    - Owner can pause and unpause transfer of tokens.

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.