

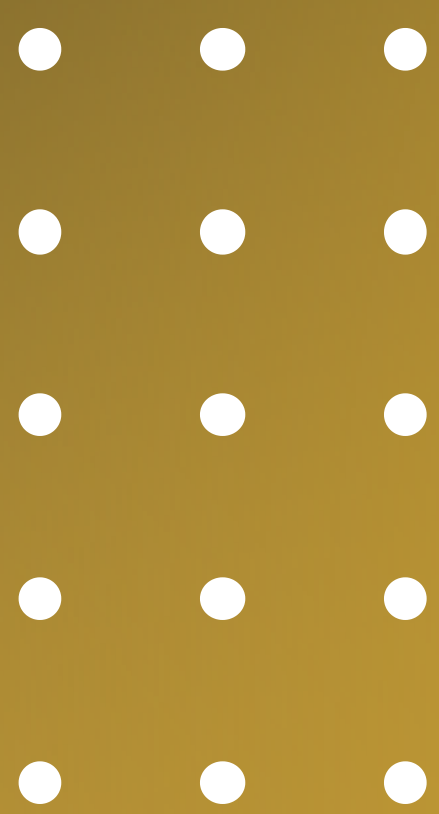


Smart Contract Security Audit Report

BleuFi

January 2023

Security Status



Audit Details



Audited project

BleuFi



Deployer address

0xea502b2f3c015ce6c6c3a1ecd38826e9b26f6988



Client contacts

BleuFi



Blockchain

Binance smart chain



Website

<https://app.bleufi.com/>

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 BleuFi to perform an audit of smart contracts:

- <https://bscscan.com/token/0xFdC00285DDe1f5b5c65C6a963357b4C55d8f601#code>

The purpose of the audit was to achieve the following:

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

The information in this report should be understood 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.

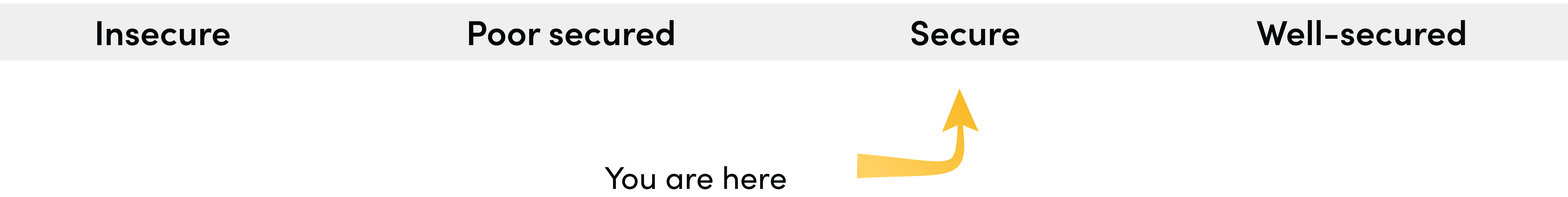
Contract Details

Token contract details for 21.01.2023

Token Type	: DEFI
Contract name	: BLEUFI
Contract address	: 0xFdC00285DDe1f5b5c65C6a963357b4C55d8f601
Total supply	:10,000,000,000
Token ticker	: BLEU
Decimals	: 2
Token Holders	: 13,721
Transactions count	: 52,036
Liquidity fee	: 0
marketing fee	: 0
Total fee	: 0
Pair	: 0x8650a48fd9b0ce49dd3b5b1baa4ded27def070ae
Compiler version	: v0.8.9+commit.e5eed63a
Contract deployer address	: 0xea502b2f3c015ce6c6c3a1ecd38826e9b26f6988
Owner address	: 0xea502b2f3c015ce6c6c3a1ecd38826e9b26f6988

Audit Summary

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



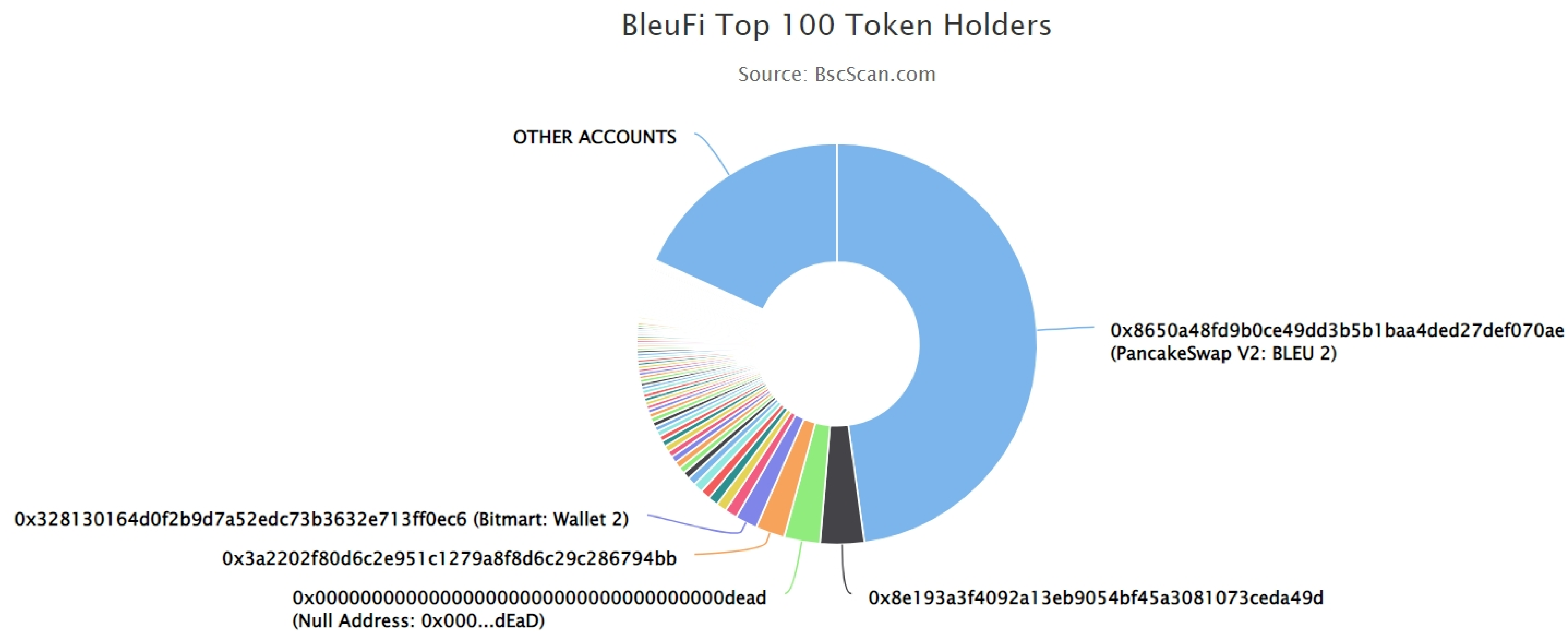
We used various tools like Slither, Mythril and Remix IDE. At the same time this finding is based on critical analysis of the manual audit. All issues found during automated analysis were manually reviewed and applicable vulnerabilities are presented in the issues checking status.

We found 0 critical, 0 high, 1 medium and 0 low.

BleuFi Token Distribution



💡 The top 100 holders collectively own 81.90% (8,190,422,169.41 Tokens) of BleuFi

💡 Token Total Supply: 10,000,000,000.00 Token | Total Token Holders: 13,721



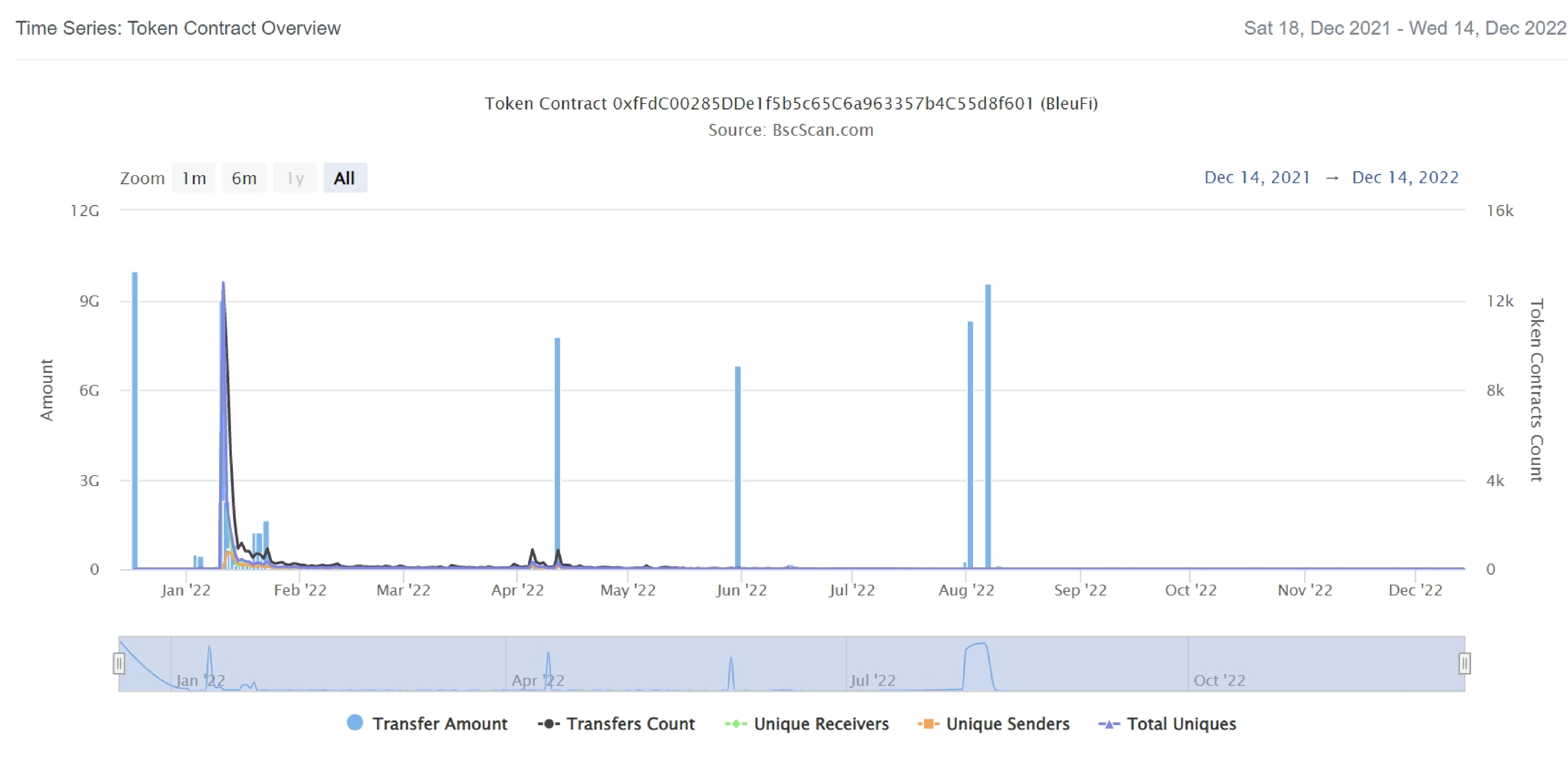
BleuFi Top 20 Token Holders

(A total of 8,190,422,169.41 tokens held by the top 100 accounts from the total supply of 10,000,000,000.00 token)

Rank	Address	Quantity (Token)	Percentage
1	 PancakeSwap V2: BLEU 2	4,782,569,499.78	47.8257%
2	 0x8e193a3f4092a13eb9054bf45a3081073ceda49d	355,020,749.79	3.5502%
3	Null Address: 0x000...dEaD	289,297,694.48	2.8930%
4	0x3a2202f80d6c2e951c1279a8f8d6c29c286794bb	234,785,283.48	2.3479%
5	Bitmart: Wallet 2	178,429,855.99	1.7843%
6	0xf2117527e25cb59b0b32737f1a9010d3b7190b61	100,391,487.16	1.0039%
7	0xaf0ecffa0a86323eefe2c49a5714129c7fec39c0	84,919,594.34	0.8492%
8	0x235ea6e206e79b30a630e050e2e47018f999ffa0	81,604,900	0.8160%
9	0x42e415b05ef84951eabb439c39fd2e40f29c11fc	79,000,100	0.7900%
10	0xfc156b33ddc82dcb9b63b90946310d4ede839a83	77,497,800	0.7750%
11	0xf0e0dc8b276f0c777e1e984504ad060619d625e6	67,700,000	0.6770%
12	0xc3cd61ede5809d521acb1080c5ddb7e13098bfcc	56,147,400	0.5615%
13	0x16f5758a2764efd31a4837379ca80f06d343a3b0	53,492,800	0.5349%
14	0xb939304eb2b93c9c95150f816a7c9d0958f0fb5a	53,198,509.25	0.5320%
15	0xa992f7d625f3074a445d2ff1631a3c4b369e4652	52,789,400	0.5279%
16	0x08f660b846a2dbf24e9873298320d0a22bb5a67c	50,114,800	0.5011%
17	0xc9f0786630343aad04d5a5ca103edca9c3324355	49,927,438.71	0.4993%
18	0xbeb332a157ecec13e3086954fef8a28fdd3cb5b	46,397,100	0.4640%
19	0xdeb209b94dfd57fad6793dbd1e6553cba9acc618	43,930,300	0.4393%
20	0x3008b434dd39ace0f3e513c245698991ab47c962	43,408,700	0.4341%

BleuFi Token Distribution

BleuFi Contract Overview



Contract functions details

+ [Lib] SafeMath

- [Int] add
- [Int] sub
- [Int] sub
- [Int] mul
- [Int] div
- [Int] div

+ [Int] BEP20

- [Ext] totalSupply
- [Ext] decimals
- [Ext] symbol
- [Ext] name
- [Ext] getOwner
- [Ext] balanceOf
- [Ext] transfer #
- [Ext] allowance
- [Ext] approve #
- [Ext] transferFrom #

+ Auth

- [Pub] <Constructor> #
- [Pub] authorize #
 - modifiers: onlyOwner
- [Pub] unauthorize #
 - modifiers: onlyOwner
- [Pub] isOwner
- [Pub] isAuthorized
- [Pub] transferOwnership #
 - modifiers: onlyOwner

+ [Int] PCSFactory

- [Ext] createPair #

+ [Int] PCSv2Router

- [Ext] factory
- [Ext] WETH
- [Ext] addLiquidityETH (\$)
- [Ext] swapExactTokensForETHSupportingFeeOnTransferTokens #

Contract functions details

+BLEUFI (BEP20, Auth)

-[Pub] < Constructor >#

- modifiers: Auth

-[Ext] (\$)

-[Ext] totalSupply

-[Ext] decimals

-[Ext] symbol

-[Ext] name

-[Ext] getOwner

-[Pub] balanceOf

-[Ext] allowance

-[Pub] approve #

-[Ext] approveMax #

-[Ext] transfer #

-[Ext] transferFrom #

-[Pub] setMaxWalletPercent_base10000 #

- modifiers: onlyOwner

-[Pub] setMaxTxPercent_base10000 #

- modifiers: onlyOwner

-[Pub] setMaxTxAbsolute #

- modifiers: authorized

-[Int] _transferFrom #

-[Int] _basicTransfer #

-[Int] takeFee #

-[Ext] clearStuckBalance #

- modifiers: authorized

-[Ext] set_sell_multiplier #

- modifiers: onlyOwner

-[Pub] tradingStatus #

- modifiers: onlyOwner

-[Pub] launchStatus #

- modifiers: onlyOwner

-[Int] swapBack #

- modifiers: swapping

-[Pub] enable_blacklist #

- modifiers: onlyOwner

-[Pub] manage_blacklist #

- modifiers: onlyOwner

-[Ext] setIsFeeExempt #

- modifiers: authorized

Contract functions details

- [Ext] setIsTxLimitExempt #
 - modifiers: authorized
- [Ext] setFees #
 - modifiers: authorized
- [Ext] setFeeReceivers #
 - modifiers: authorized
- [Ext] setSwapBackSettings #
 - modifiers: authorized
- [Ext] setTargetLiquidity #
 - modifiers: authorized
- [Pub] getCirculatingSupply
- [Pub] getLiquidityBacking
- [Pub] isOverLiquified
- [Ext] multiTransfer #
 - modifiers: onlyOwner

(\$) = payable function

= non-constant function

Issues Checking Status

No.	Title	Status
1.	Compiler error	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.	Medium Issue
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
20.	Too old version	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

One medium severity issue found.

1. Out of gas

- **Issue:**

The function `manage_blacklist()` uses the loop to change blacklist status of addresses. It also could be aborted with `OUT_OF_GAS` exception if there will be a long addresses list.

- **Recommendation**

Check that the array length is not too big.

✓ Low Severity Issues

No low severity issue found.

- **Notes:**

There is sending tokens to burn address, instead of real burning (decreasing total supply).

Centralization

Owner privileges :

- BleuFi Contract:
 - owner can authorize addresses.
 - owner can change `_maxwallettoken` and `_maxtxamount`.
 - owner can change `sellmultiplier`.
 - owner can change launch status.
 - owner can change trading status.
 - owner can change blacklist mode.
 - owner can multitransfer listed token amounts (started from 1).
 - authorized addresses can change `_maxtxamount`.
 - authorized addresses can withdraw contract bnbs.
 - authorized addresses can include in and exclude from fee and transaction amount.
 - authorized addresses can change fees.
 - authorized addresses can change fee receivers.
 - authorized addresses can change swap threshold and disable/enable swap.
 - authorized addresses can change `targetliquidity`.

This smart contract has some functions which can be executed by the admin (Owner) only. If the admin wallet private key would be compromised, then it would create trouble, as smart contract ownership has not been renounced.

Conclusion

Smart contract contains medium 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.