



# MOTECH AUDIT

SMART CONTRACT SECURITY AUDIT

**SECURITY ASSESSMENT**

## BARREL TOKEN AUDIT REPORT

2021

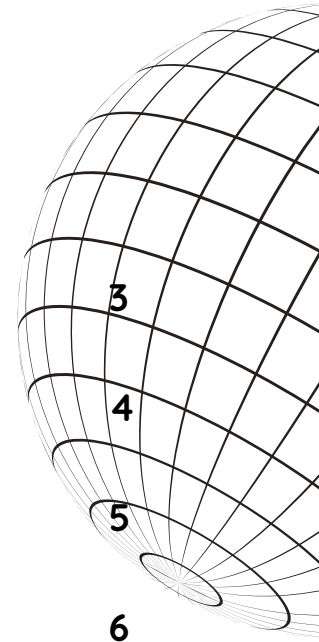


11 DEV 2021

## SECURITY ASSESSMENT

# TABLE OF CONTENTS

Summary	3
Disclaimer	4
Background	5
Audit Details	6
Contract Details	7
BARREL Token Distribution	8
BARREL Token Contract Interaction Details	8
Top 10 Token Holders	9
Finding	10
BAR-01 : Initial token distribution	11
BAR-02 : Missing zero address validation	12
BAR-03 : No restrict of `changeFeePercentage`	13
BAR-04 : Boolean equality	14
Conclusion	15



# SECURITY ASSESMENT

## SUMMARY

This report has been prepared for Bernard.finance to discover issues and vulnerabilities in the source code of the BARREL project as well as any contract dependencies that were not part of an officially recognized library. A comprehensive examination has been performed, utilizing Static Analysis techniques.

The auditing process pays special attention to the following considerations:

- Testing the smart contracts against both common and uncommon attack vectors.
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Ensuring contract logic meets the specifications and intentions of the client.
- Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- Thorough line-by-line manual review of the entire codebase by industry experts.

The security assessment resulted in findings that ranged from critical to informational. We recommend addressing these findings to ensure a high level of security standards and industry practices. We suggest recommendations that could better serve the project from the security perspective:

- Enhance general coding practices for better structures of source codes;
- Add enough unit tests to cover the possible use cases given they are currently missing in the repository;
- Provide more comments per each function for readability, especially contracts that are verified in public;
- Provide more transparency on privileged activities once the protocol is live.



**MOTECH AUDIT**  
SMART CONTRACT SECURITY AUDIT

# SECURITY ASSESSMENT

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



**MOTECH AUDIT**  
SMART CONTRACT SECURITY AUDIT

# SECURITY ASSESSMENT BACKGROUND

MotechAudit was commissioned by BARREL to perform an audit of smart contracts:

<https://bscscan.com/address/0xdb1b7a685e6876d508de3c5160764b56577a83ae>

The purpose of the audit was to achieve the following:

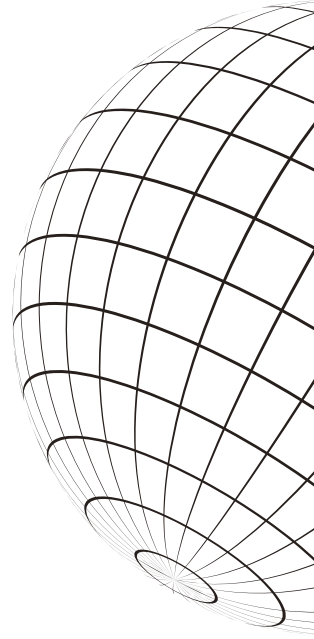
- Ensure that the smart contract functions as intended.
- Identify potential security issues with the smart contract.

The information in this report should be 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.



**MOTECH AUDIT**  
SMART CONTRACT SECURITY AUDIT

# AUDIT DETAILS



## AUDITED PROJECT

BARREL



## DEPLOYER ADDRESS

0x8256F1B68054d4bE1Fa9f60498d565E7A90cB923



## CLIENT CONTACTS:

BARREL Team



## BLOCKCHAIN

BSC Project



## WEBSITE:

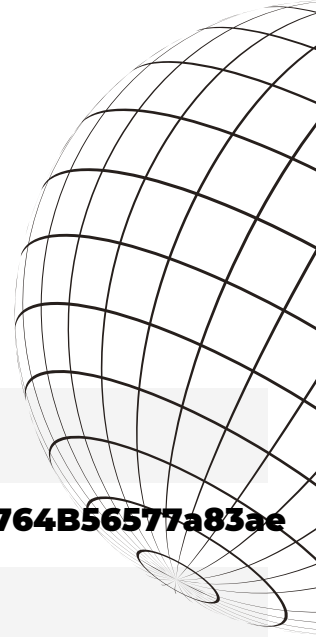
<https://bernard.finance/barrel>



## SECURITY ASSESSMENT

# CONTRACT DETAILS

### Token contract details for Jul-05-2021



<b>Contract name</b>	<b>BARREL</b>
<b>Contract address</b>	<b>0xDB1B7a685e6876d508DE3c5160764B56577a83ae</b>
<b>Total supply</b>	<b>517,496 BARREL</b>
<b>Token ticker</b>	<b>BARREL by bernard.finance (BARREL)</b>
<b>Decimals</b>	<b>18</b>
<b>Token holders</b>	<b>1,214</b>
<b>Transactions count</b>	<b>5,215</b>
<b>Top 100 holders dominance</b>	<b>98.64%</b>
<b>Contract deployer address</b>	<b>0x8256F1B68054d4bE1Fa9f60498d565E7A90cB923</b>
<b>Contract's current owner address</b>	<b>0x8256F1B68054d4bE1Fa9f60498d565E7A90cB923</b>



## SECURITY ASSESSMENT

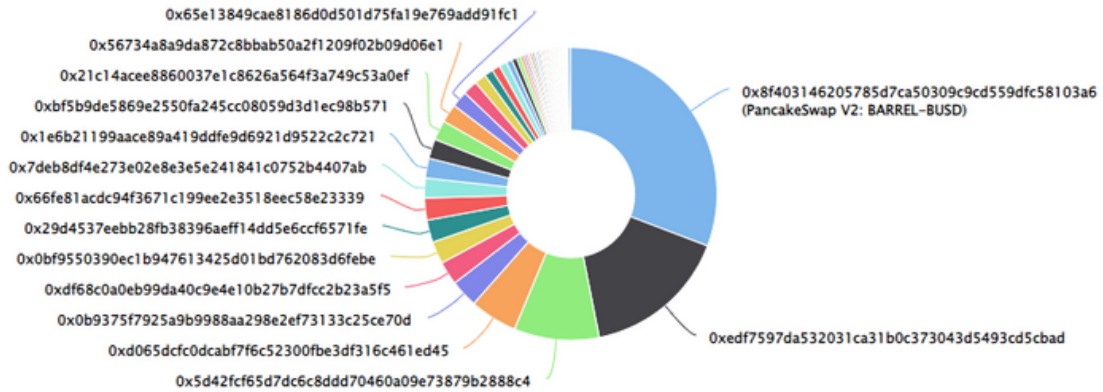
# BARREL TOKEN DISTRIBUTION

The top 100 holders collectively own 99.67% (515,787.21 Tokens) of BARREL by bernard.finance

Token Total Supply: 517,496.00 Token | Total Token Holders: 1,214

### BARREL by bernard.finance Top 100 Token Holders

Source: BscScan.com



(A total of 515,787.21 tokens held by the top 100 accounts from the total supply of 517,496.00 token)

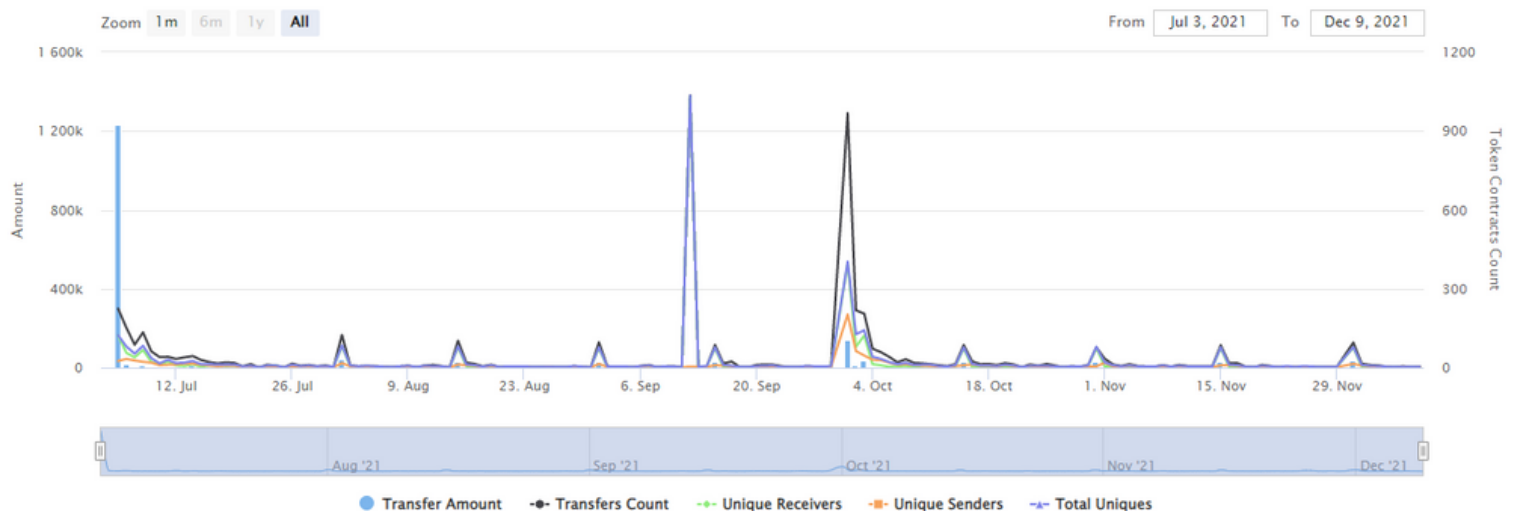
## BARREL TOKEN CONTRACT INTERACTION DETAILS

Time Series: Token Contract Overview

Mon 5, Jul 2021 - Thu 9, Dec 2021

Token Contract 0xdb1b7a685e6876d508de3c5160764b56577a83ae (BARREL by bernard.finance)

Source: BscScan.com














**MOTECH AUDIT**  
SMART CONTRACT SECURITY AUDIT



## SECURITY ASSESSMENT

# TOP 10 TOKEN HOLDERS

Rank	Address	Quantity	Percentage	Analytics
1	 PancakeSwap V2: BARREL-BUSD	159,354.48460656350293394	30.7934%	
2	0xedf7597da532031ca31b0c373043d5493cd5cbad	83,259.0000009999999999	16.0888%	
3	0x5d42fcf65d7dc6c8ddd70460a09e73879b2888c4	48,663.71588	9.4037%	
4	0xd065dcfc0dcabf7f6c52300f6e3df316c461ed45	27,175.6	5.2514%	
5	0x0b9375f7925a9b9988aa298e2ef73133c25ce70d	15,865.723374186782998152	3.0659%	
6	0xdf68c0a0eb99da40c9e4e10b27b7dfcc2b23a5f5	13,397	2.5888%	
7	0x0bf9550390ec1b947613425d01bd762083d6febe	12,754	2.4646%	
8	0x29d4537eebb28fb38396aeff14dd5e6ccf6571fe	12,754	2.4646%	
9	0x66fe81acdc94f3671c199ee2e3518eec58e23339	12,638.880202219748177573	2.4423%	
10	0x7deb8df4e273e02e8e3e5e241841c0752b4407ab	11,278	2.1793%	

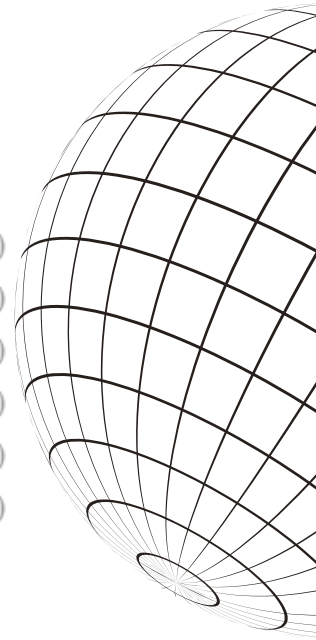
source:<https://bscscan.com/>



# SECURITY ASSESSMENT FINDINGS



Critical	0 (0.00%)
Major	0 (0.00%)
Medium	1 (25.00%)
Minor	0 (0.00%)
Informational	3 (75.00%)
Discussion	0 (0.00%)



ID	Title	Category	Severity	Status
BAR-01	Initial token distribution	Centralization / Privilege	● Medium	✓ Resolved
BAR-02	Missing zero address validation	Coding Style	● Informational	ⓘ Acknowledged
BAR-03	No restrict of <code>changeFeePercentage</code>	Coding Style	● Informational	ⓘ Acknowledged
BAR-04	Boolean equality	Coding Style	● Informational	ⓘ Acknowledged



# SECURITY ASSESSMENT

## BAR-01 | INITIAL TOKEN DISTRIBUTION

Type	Severity	Location	Status
Centralization / Privilege	● Medium	BARREL.sol: 765	✓ Resolved

### Description

All of the initialSupply tokens are sent to the contract deployer when deploying the contract.

### Recommendation

We recommend the team to be transparent regarding the initial token distribution process.

### Alleviation

[BARREL Team]: For the total supply, we have explained the distribution in medium articles and also on the website. The wallets of the address checks are known by the community so everything is transparent. Reference:

<https://bernardfinance.medium.com/bernard-finance-barrel-is-live-21e374eb05e6>



**MOTECH AUDIT**  
SMART CONTRACT SECURITY AUDIT

## SECURITY ASSESSMENT

### BAR-02 | MISSING ZERO ADDRESS VALIDATION

Type	Severity	Location	Status
Coding Style	● Informational	BARREL.sol: 784	ⓘ Acknowledged

## Description

Detect missing zero address validation.

## Recommendation

Consider adding zero address check, for example:

```
constructor(..., address feeAccount) ERC20PresetFixedSupply(...) {  
    _transferFeePercentage = 10;  
    require(feeAccount != address(0), "No Zero Address");  
    _feeAccount = feeAccount;  
}
```

## Alleviation

The team acknowledged the finding, and given the deployed contract cannot be updated, decided to retain the code base unchanged.



**MOTECH AUDIT**  
SMART CONTRACT SECURITY AUDIT

## SECURITY ASSESSMENT

### BAR-03 | NO RESTRICT OF CHANGEFEEPERCENTAGE

Type	Severity	Location	Status
Coding Style	● Informational	BARREL.sol: 835~838	ⓘ Acknowledged

## Description

The value of newFeePercentage should be restricted and the function should be defined with eventdeclarations.

## Recommendation

The following is for reference only:

```
event _changeFeePercentage(uint newFeePercentage);
function changeFeePercentage(uint newFeePercentage) external onlyOwner
{
    require(newFeePercentage <= 10, "newFeePercentage is inappropriate");
    _transferFeePercentage = newFeePercentage;
    emit _changeFeePercentage(newFeePercentage);
}
```

## Alleviation

The team acknowledged the finding, and given the deployed contract cannot be updated, decided to retain the code base unchanged.



**MOTECH AUDIT**  
SMART CONTRACT SECURITY AUDIT

## SECURITY ASSESSMENT

### BAR-04 | BOOLEAN EQUALITY

Type	Severity	Location	Status
Coding Style	● Informational	BARREL.sol: 863	ⓘ Acknowledged

### Description

Performs comparison with a boolean literal false which can be replaced with the negation of the expression to increase the legibility of the codebase.

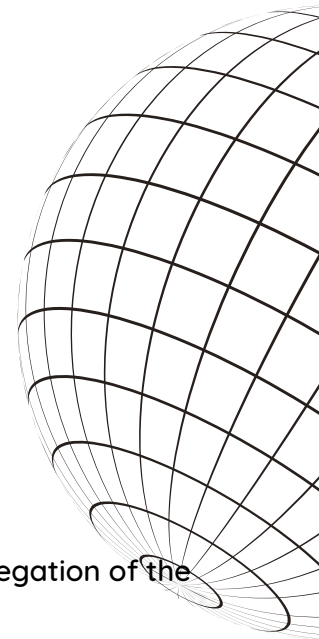
### Recommendation

Consider modifying like below:

```
863  if (!_fromFees[sender] || _toFees[recipient])
```

### Alleviation

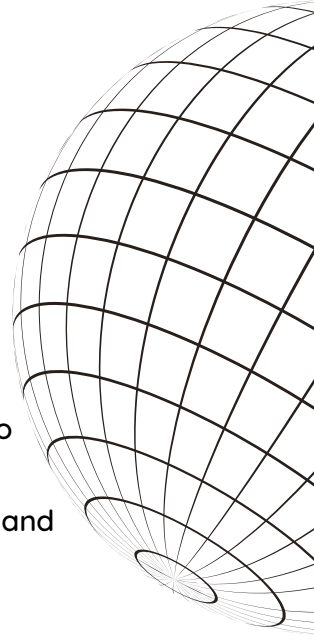
The team acknowledged the finding, and given the deployed contract cannot be updated, decided to retain the code base unchanged.



# SECURITY ASSESMENT CONCLUSION

Smart contracts contain owner privileges!

Motech Audit 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.



**MOTECH AUDIT**  
SMART CONTRACT SECURITY AUDIT