MOTECH AUDIT

SMART CONTRACT SECURITY AUDIT

SECURITY ASSESSMENT

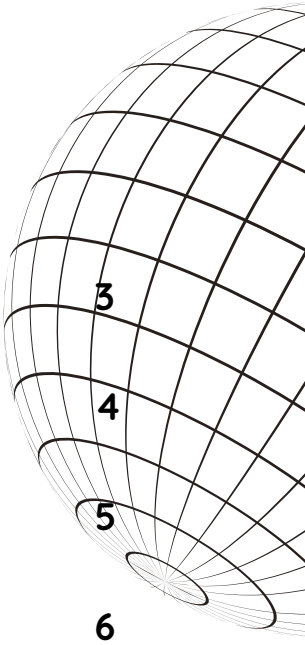
2021

BROKOLI TOKEN AUDIT REPORT

7 DEC 2021

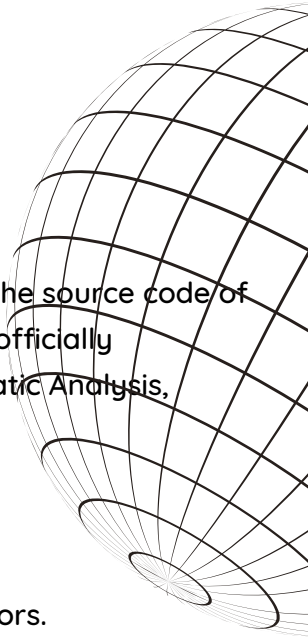
SECURITY ASSESMENT

TABLE OF CONTENTS



SECURITY ASSESMENT

SUMMARY



This report has been prepared for Brokoli to discover issues and vulnerabilities in the source code of the Brokoli 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, Manual Review, and Testnet Deployment techniques.

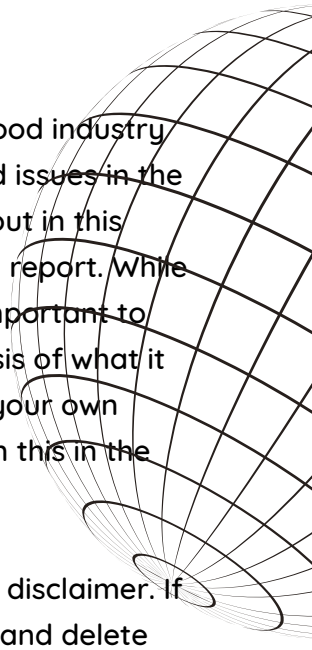
The auditing process pays special attention to the following considerations:

- 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 are verified in public;
- Provide more transparency on privileged activities once the protocol is live.

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.

SECURITY ASSESMENT

BACKGROUND

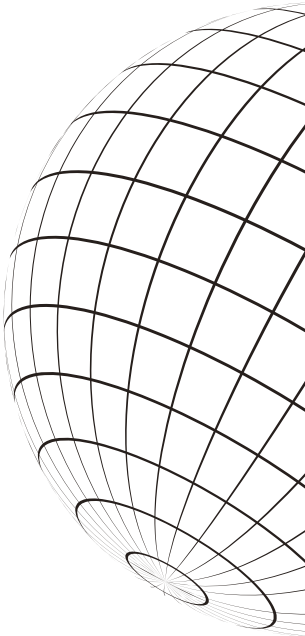
MotechAudit was commissioned by Brokoli to perform an audit of smart contracts:
https://etherscan.io/address/0x4674a4f24c5f63d53f22490fb3a08eaaad739ff8
The purpose of the audit was to achieve the following:

- 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.

SECURITY ASSESMENT

AUDIT DETAILS



AUDITED PROJECT

BROKOLI

DEPLOYER ADDRESS

0x333273259d6a4F5Ebd938fCa45c57F104061E26d

CLIENT CONTACTS:

BROKOLI Team

BLOCKCHAIN

Ethereum Project

WEBSITE:

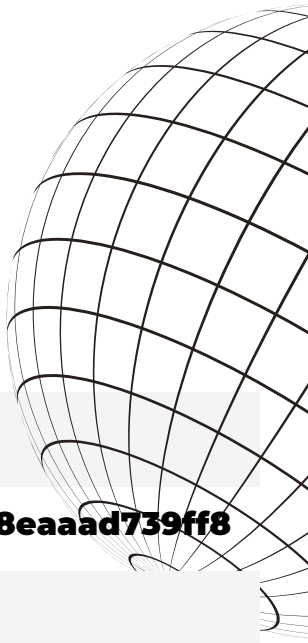
https://brokoli.network

MOTECH AUDIT

SMART CONTRACT SECURITY AUDIT

SECURITY ASSESMENT

CONTRACT DETAILS



Token contract details for Sep-23-2021

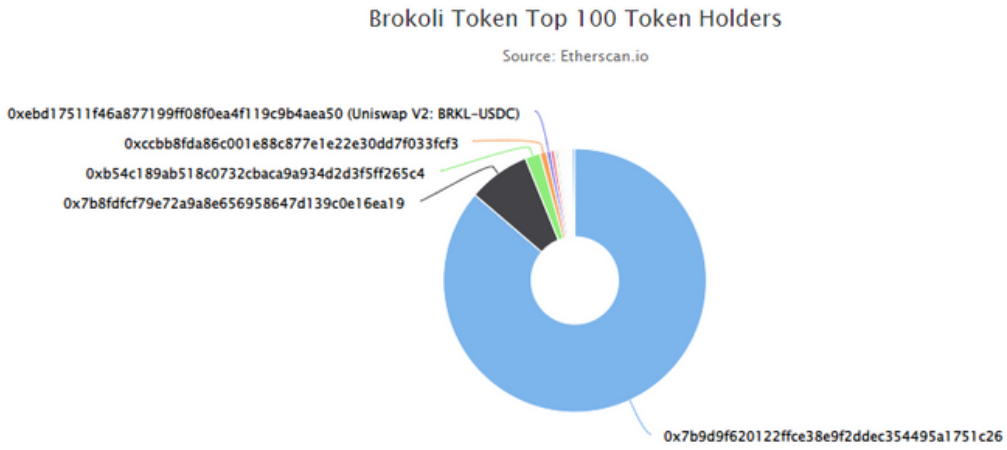
Contract name	**BROKOLI**
Contract address	**0x4674a4f24c5f63d53f22490fb3a08eaaad739ff8**
Total supply	**125,000,000 BRK**
Token ticker	**Brokoli Token (BRKL)**
Decimals	**18**
Token holders	**485**
Transactions count	**3,911**
Top 100 holders dominance	**99.39%**
Contract deployer address	**0x333273259d6a4F5Ebd938fCa45c57F104061E26d**
Contract's current owner address	**0x333273259d6a4F5Ebd938fCa45c57F104061E26d**

SECURITY ASSESMENT

THE TRUTH TOKEN DISTRIBUTION

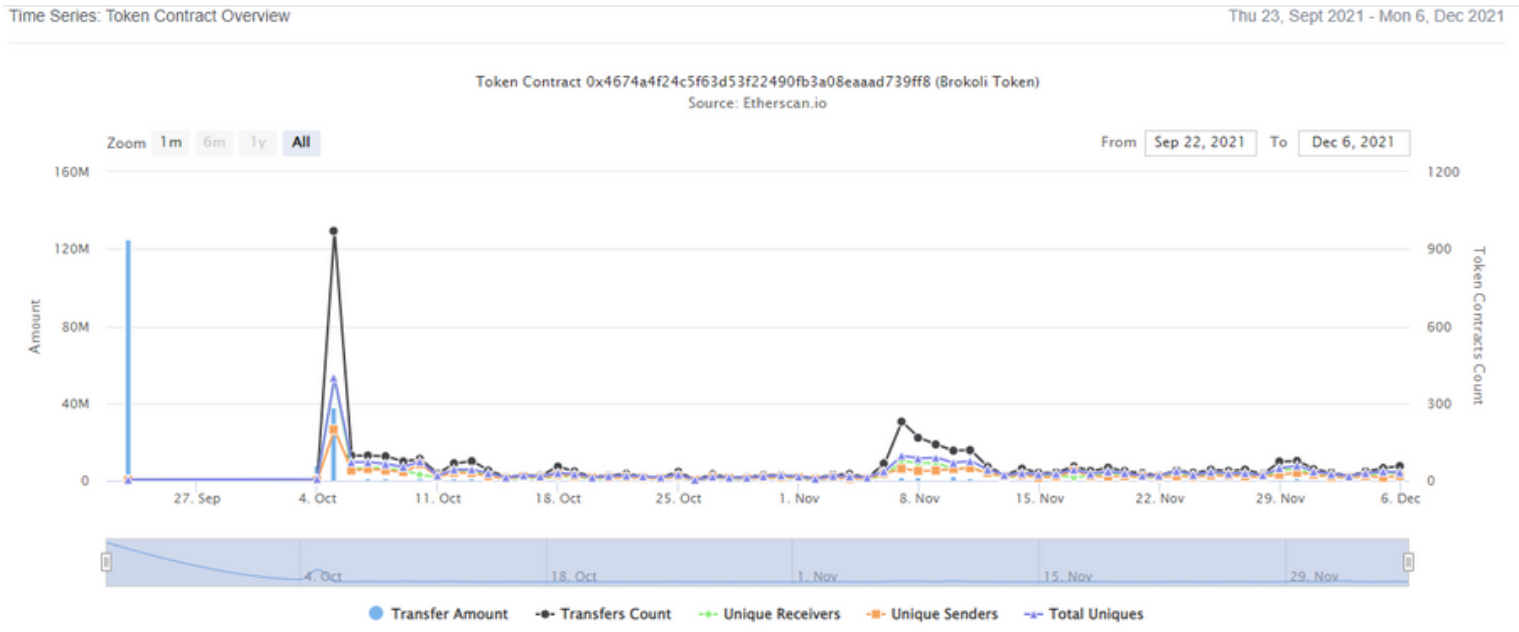
The top 100 holders collectively own 99.69% (124,614,396.56 Tokens) of Brokoli Token

Token Total Supply: 125,000,000.00 Token | Total Token Holders: 485



(A total of 124,614,396.56 tokens held by the top 100 accounts from the total supply of 125,000,000.00 token)

THE TRUTH TOKEN CONTRACT INTERACTION DETAILS



MOTECH AUDIT
SMART CONTRACT SECURITY AUDIT

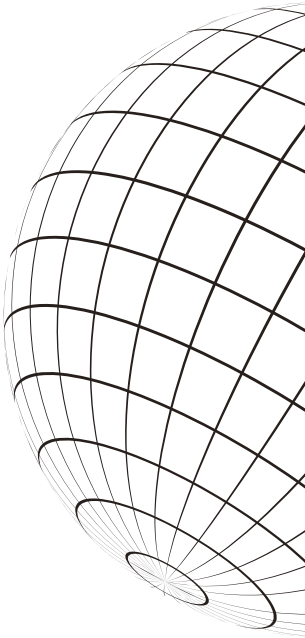
SECURITY ASSESMENT

TOP 10 TOKEN HOLDERS

Rank	Address	Quantity	Percentage	Value	Analytics
1	0x7b9d9f620122ffce38e9f2ddec354495a1751c26	107,850,558	86.2804%	$131,577,680.76	
2	0x7b8fdfcf79e72a9a8e656958647d139c0e16ea19	9,474,502.99999999999606784	7.5796%	$11,558,893.66	
3	0xb54c189ab518c0732cbaca9a934d2d3f5ff265c4	2,343,755	1.8750%	$2,859,381.10	
4	0xccbb8fda86c001e88c877e1e22e30dd7f033fcf3	1,000,000	0.8000%	$1,220,000.00	
5	Uniswap V2: BRKL-USDC	644,734.931083748298310339	0.5158%	$786,576.62	
6	Gate.io	512,913.267145787007620793	0.4103%	$625,754.19	
7	0x6e50d3c6b659db780f21da84fa8194f437239ca6	299,870	0.2399%	$365,841.40	
8	0x90a8825da4c8cf6d7e14c765fe2c411ce33ff117	260,937.5	0.2088%	$318,343.75	
9	0x9953794f39786b540c3c6a49e27bba5bf3520598	185,149.929409428281696698	0.1481%	$225,882.91	
10	0x08a3ac8dff839daefaa13945f2e88aa3128488fd	156,250	0.1250%	$190,625.00	

source:https://etherscan.io/

SECURITY ISSUES



Critical Severity Issues

No high severity issues found.

High Severity Issues

No high severity issues found.

Medium Severity Issues

The owner could withdraw rewards token

The owner account could withdraw any tokens from the IDO contract, including the reward tokens before users will receive their reward allocations.

Recommendation: Please add the “require” statement to check that emergency withdrawal is requested not for the rewards token.

Lines: BaseClaim.sol#101-106

```
function emergencyWithdrawToken(ERC20 tokenAddress) external onlyOwner {
    tokenAddress.safeTransfer(
        msg.sender,
        tokenAddress.balanceOf(address(this))
    );
}
```

SECURITY ASSESMENT

SECURITY ISSUES

Low Severity Issues

1. Boolean equality Boolean constants can be used directly and do not need to be compared to true or false.

Recommendation: Remove the equality to the boolean constant

Fixed before the second review

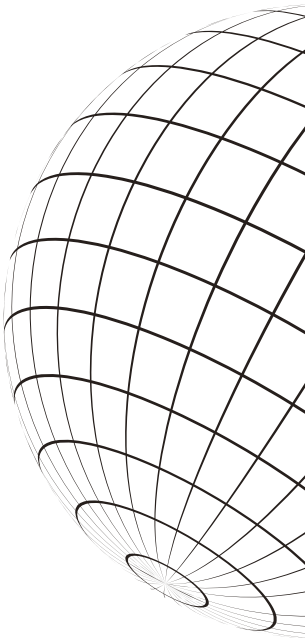
2. Dust amounts could be left on percentage Because of finding percentage for before 90 days and after (20 and 80) there could be dust amount of tokens left. It's better to just subtract the unlockedOnClaim amount from the total to get the rest 80% instead of doing calculations

Recommendation: Please consider subtracting the unlockedOnClaim value from the total

Fixed before the second review.

SECURITY ASSESMENT

TOKEN LOGO

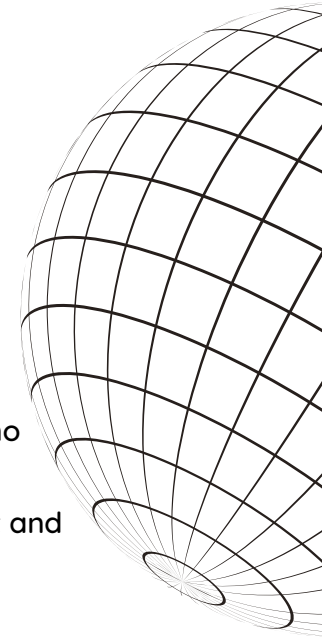


MOTECH AUDIT

SMART CONTRACT SECURITY AUDIT

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.