MOTECH AUDIT

SMART CONTRACT SECURITY AUDIT

SECURITY ASSESSMENT

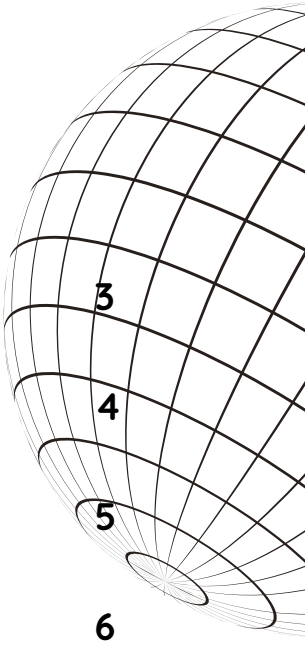
2021

LESS TOKEN AUDIT REPORT

28 NOV 2021

SECURITY ASSESMENT

TABLE OF CONTENTS

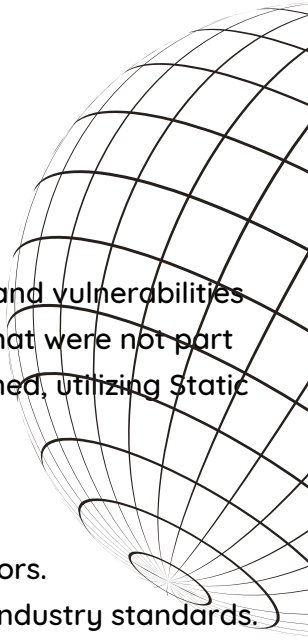


MOTECH AUDIT

SMART CONTRACT SECURITY AUDIT

SECURITY ASSESMENT

SUMMARY



This report has been prepared for Less Token smart contracts, to discover issues and vulnerabilities in the source code of their Smart Contract as well as any contract dependencies that were not part of an officially recognized library. A comprehensive examination has been performed, utilizing Static Analysis and Manual Review techniques.

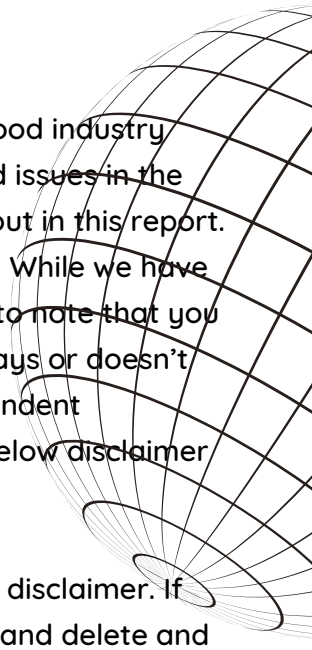
The auditing process pays special attention to the following considerations:

- 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 producedby 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



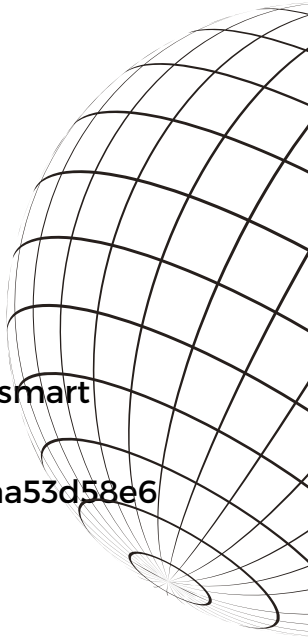
This is a limited report on our findings based on our analysis, in accordance with good industry practice as at the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, the details of which are set out in this report. In 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



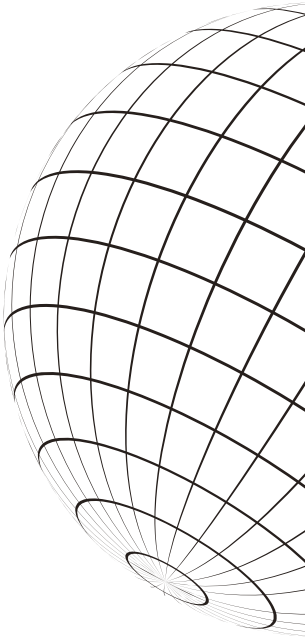
MotechAudit was commissioned by Less Token to perform an audit of smart contracts:
https://bscscan.com/address/0xb698ac9bc82c718d8eba9590564b9a5aa53d58e6
The purpose of the audit was to achieve the following:

- 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

LESS TOKEN

DEPLOYER ADDRESS

0x6b012B20c2075055F87A885d7E7C42586bAF7978

CLIENT CONTACTS:

LESS TOKEN TEAM

BLOCKCHAIN

BSC Project

WEBSITE:

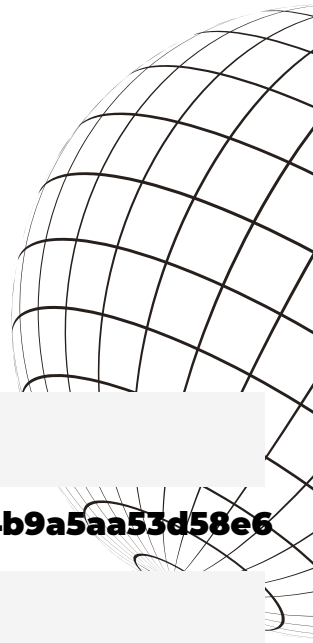
https://less.xyz/

MOTECH AUDIT

SMART CONTRACT SECURITY AUDIT

SECURITY ASSESMENT

CONTRACT DETAILS



Token contract details for May-27-2021

Contract name	**LESS TOKEN**
Contract address	**0xb698ac9bc82c718d8eba9590564b9a5aa53d58e6**
Total supply	**125,000,000 LESS**
Token ticker	**LessToken (LESS)**
Decimals	**18**
Token holders	**2,067**
Transactions count	**18,355**
Top 100 holders dominance	**95.9587%**
Contract deployer address	**0x6b012B20c2075055F87A885d7E7C42586bAF7978**
Contract's current owner address	**0x6b012B20c2075055F87A885d7E7C42586bAF7978**

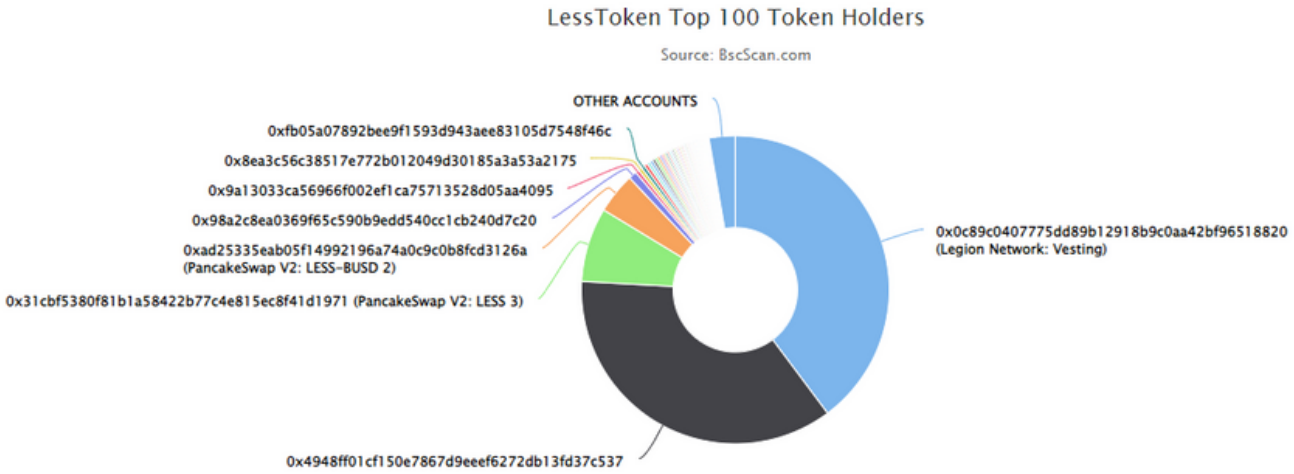
MOTECH AUDIT
SMART CONTRACT SECURITY AUDIT

SECURITY ASSESMENT

LESS TOKEN DISTRIBUTION

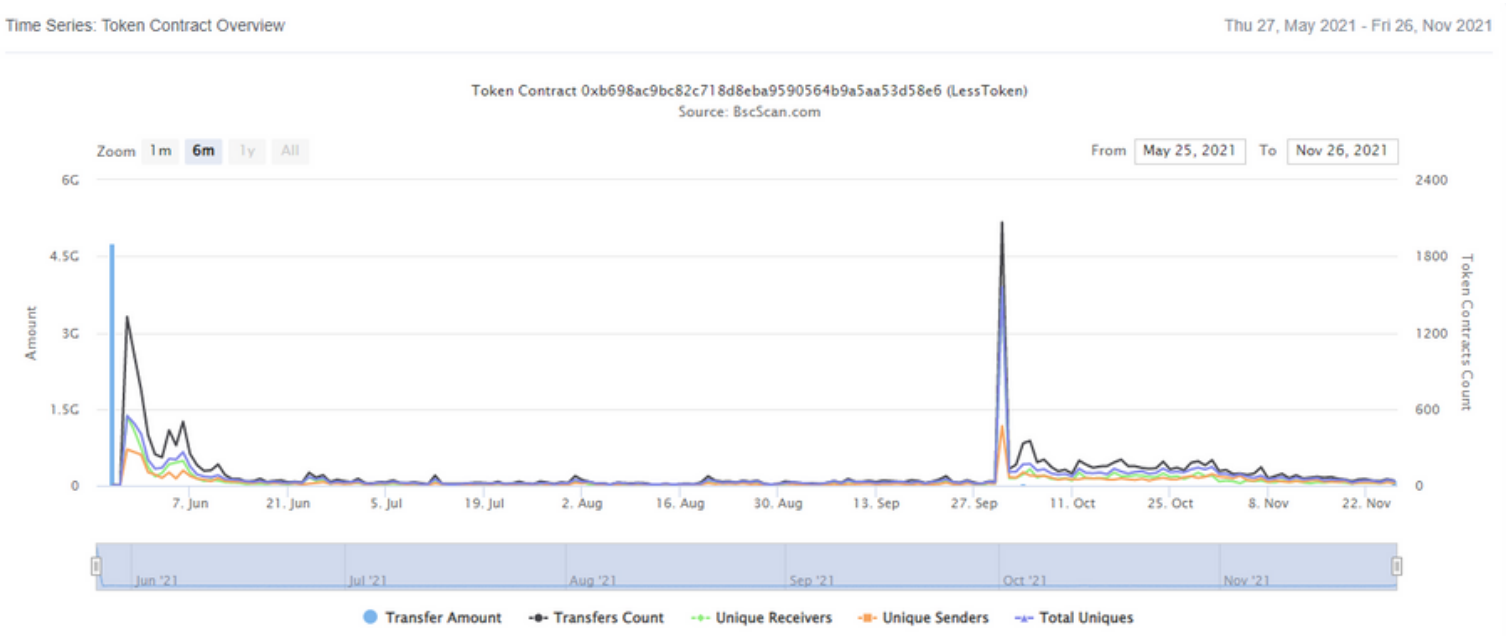
The top 100 holders collectively own 97.26% (121,573,813.70 Tokens) of LessToken

Token Total Supply: 125,000,000.00 Token | Total Token Holders: 2,067



(A total of 121,573,813.70 tokens held by the top 100 accounts from the total supply of 125,000,000.00 token)

LESS TOKEN CONTRACT INTERACTION DETAILS



MOTECH AUDIT
SMART CONTRACT SECURITY AUDIT

SECURITY ASSESMENT

TOP 10 TOKEN HOLDERS

Rank	Address	Quantity	Percentage	Value	Analytics
1	Legion Network: Vesting	49,740,806.511275053538896332	39.7926%	$1,321,815.67	
2	0x4948ff01cf150e7867d9eeef6272db13fd37c537	45,104,868.95973745514	36.0839%	$1,198,619.95	
3	PancakeSwap V2: LESS 3	9,755,563.845684246420863927	7.8045%	$259,245.04	
4	PancakeSwap V2: LESS-BUSD 2	5,345,296.957625084726469724	4.2762%	$142,046.30	
5	0x98a2c8ea0369f65c590b9edd540cc1cb240d7c20	1,060,897.889934632522891405	0.8487%	$28,192.37	
6	0x9a13033ca56966f002ef1ca75713528d05aa4095	478,570.601033441782372104	0.3829%	$12,717.57	
7	0x8ea3c56c38517e772b012049d30185a3a53a2175	467,399	0.3739%	$12,420.69	
8	0xfb05a07892bee9f1593d943aee83105d7548f46c	467,115.32224033366135522	0.3737%	$12,413.16	
9	0x8e4b6d8a141d10801eaefd07b658aefa34765fae	458,435.379758291493804081	0.3667%	$12,182.49	
10	0x7f7db5716239e9d87b373d580522fc728b26270c	424,619.790365137155995289	0.3397%	$11,283.88	

source:https://bscscan.com/

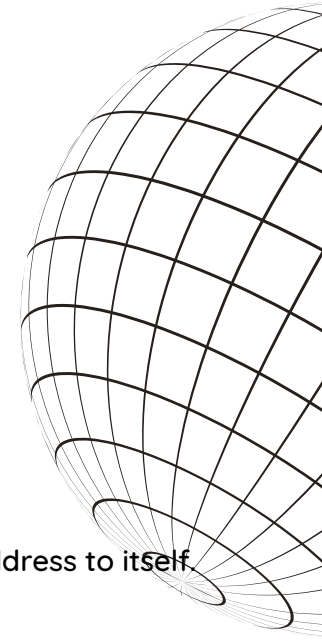
SECURITY ASSESMENT

FINDINGS

Critical	0 (0.00%)
Major	2 (66.67%)
Medium	0 (0.00%)
Minor	0 (0.00%)
Informational	1 (33.33%)
Discussion	0 (0.00%)

ID	Title	Category	Severity	Status
TCK-01	Centralized Risk	Centralization / Privilege	Major	Resolved
TCK-02	Centralized Risk	Centralization / Privilege	Major	Resolved
TCK-03	Proper Usage of `public` and `external` type	Gas Optimization	Informational	Pending

SECURITY ASSESMENT
TCK-01 | CENTRALIZED RISK



Category	Severity	Location	Status
Centralization / Privilege	Major	lessToken.sol: 623consult()	Resolved

Description

In function extractLostToken, the owner of the contract owner could transferIERC20(token.balanceOf(address(this))) amount of tokens from _tokenAddress to itself.

Recommendation

We advise the client to carefully manage the owner account's private key and avoid any potential risks of being hacked. In general, we strongly recommend centralized privileges or roles in the protocol to be improved via a decentralized mechanism or via smart-contract-based accounts with enhanced security practices, f.e. Multisignature wallets.

Indicatively, here are some feasible solutions that would also mitigate the potential risk:

- Time-lock with reasonable latency, i.e. 48 hours, for awareness on privileged operations;
- Assignment of privileged roles to multi-signature wallets to prevent a single point of failure due to theprivate key;
- Introduction of a DAO/governance/voting module to increase transparency and user involvement.

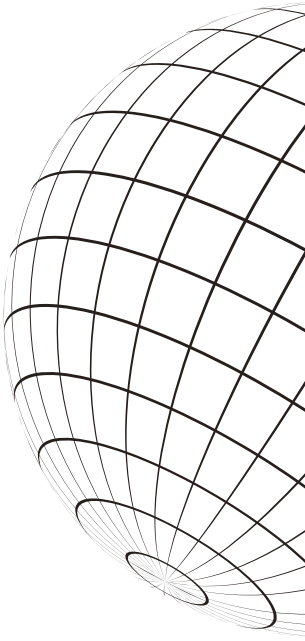
Alleviation

[LESS]: The team decided to use Gnosis-Safe multi-signature solution for remediating the private keymanagement.

The less team provides the below information for the multi-signature wallet address, deployers address,and the transfer ownership on-chain record.

- Multi-Sig Wallet Created: 0x109169C8bF29Dee206cd8c2728367Af93443B45f
- Deployer: 0x9f751906f858fc881960bc0d71e66478FE6E16E5,0xa0b5C5176A04017Be839e729A8B8160dD9E52789
- Transfer Ownership TX hash:0x82fa8d2e1e5f690a1aa4c58a2469fd390fe39eecfe74c7bb9efdc135cd7ffcc4

SECURITY ASSESMENT
TCK-02 | CENTRALIZED RISK



Category	Severity	Location	Status
Centralization / Privilege	Major	lessToken.sol: 619	Resolved

Description

In function extractLostCrypto, the owner of the contract owner could transferowner()).transfer(address(this).balance amount to the owner address

Recommendation

We advise the client to carefully manage the owner account's private key and avoid any potential risks ofbeing hacked. In general, we strongly recommend centralized privileges or roles in the protocol to beimproved via a decentralized mechanism or via smart-contract based accounts with enhanced securitypractices, f.e. Multisignature wallets

Indicatively, here are some feasible solutions that would also mitigate the potential risk:

- Time-lock with reasonable latency, i.e. 48 hours, for awareness on privileged operations;
- Assignment of privileged roles to multi-signature wallets to prevent single point of failure due to theprivate key;
- Introduction of a DAO / governance / voting module to increase transparency and user involvement.

Alleviation

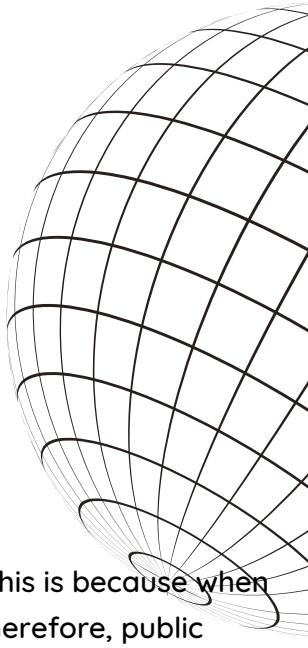
[LESS]: The team decided to use Gnosis-Safe multi-signature solution for remediating the private key management.

The less team provides the below information for the multi-signature wallet address, deployers address,and the transfer ownership on-chain record.

- Multi-Sig Wallet Created: 0x109169C8bF29Dee206cd8c2728367Af93443B45f
- Deployer: 0x9f751906f858fc881960bc0d71e66478FE6E16E5,0xa0b5C5176A04017Be839e729A8B8160dD9E52789
- Transfer Ownership TX hash:0x82fa8d2e1e5f690a1aa4c58a2469fd390fe39eecfe74c7bb9efdc135cd7ffcc4

SECURITY ASSESMENT

TCK-03 | PROPER USAGE OF PUBLIC AND EXTERNAL TYPE



Category	Severity	Location	Status
Gas Optimization	Informational	lessToken.sol: 189, 197, 214, 221, 228, 240, 248, 259, 277, 299, 315	Pending

Description

Public functions that are never called by the contract could be declared external. This is because when theinputs are arrays, external functions are more efficient than public functions. Therefore, public functionsthat are never called by the contract could be declared external.

Example functions :

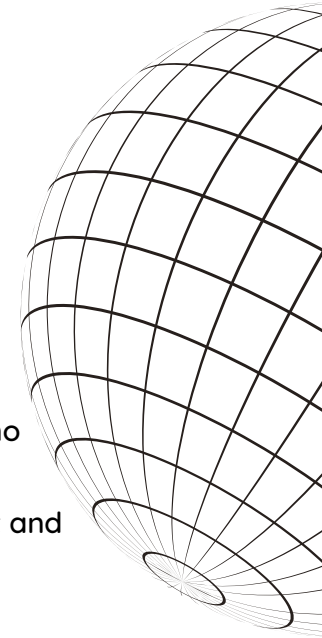
- name()
- symbol()
- decimals()
- totalSupply()
- balanceOf()
- transfer()
- allowance()
- approve()
- transferFrom()
- increaseAllowance()
- decreaseAllowance()

Recommendation

Consider using the external attribute for functions never called from the contract.

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.