MOTECH AUDIT

SMART CONTRACT SECURITY AUDIT

SECURITY ASSESSMENT

2021

ASI FI LTD TOKEN AUDIT REPORT

14 NOV 2021

MOTECH AUDIT
SMART CONTRACT SECURITY AUDIT

SECURITY ASSESMENT
SUMMARY

This report has been prepared for ASI FI LTD to discover issues and vulnerabilities in the source code of the ASI FI LTD 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.

MOTECH AUDIT
SMART CONTRACT SECURITY AUDIT

SECURITY ASSESMENT
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

BACKGROUND

MotechAudit was commissioned by Asi Fi Ltd to perform an audit of smart contracts:
https://etherscan.io/address/0x705d6cbf5352b29b4f4ee0bbe0788721f961abcd
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

Asi Fi Ltd

DEPLOYER ADDRESS

0x79f7c0A6fB99303104BFf1c01165Cce110bb4778
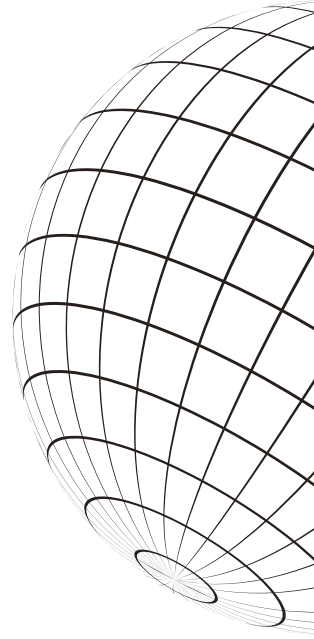
CLIENT CONTACTS:

Asi Fi Ltd team

BLOCKCHAIN
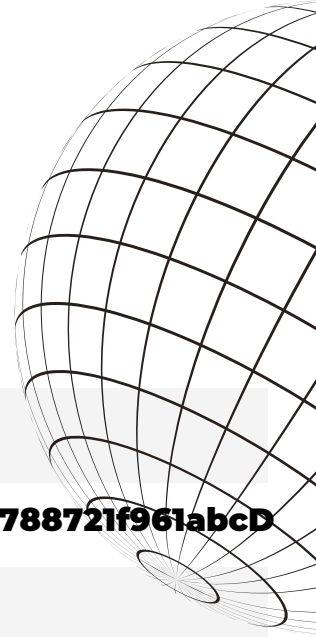
Ethereum Project

WEBSITE:

https://asi.finance/

MOTECH AUDIT
SMART CONTRACT SECURITY AUDIT

SECURITY ASSESMENT
CONTRACT DETAILS

Token contract details for Feb-18-2021

Contract name	**Monsters Clan**
Contract address	**0x705d6CBF5352B29b4f4eE0bBe0788721f961abcD**
Total supply	**10,000,000 ASI**
Token ticker	**asi.finance (ASI)**
Decimals	**18**
Token holders	**282**
Transactions count	**1,863**
Top 100 holders dominance	**89.9206%**
Contract deployer address	**0x79f7c0A6fB99303104BFf1c01165Cce110bb4778**
Contract's current owner address	**0x79f7c0A6fB99303104BFf1c01165Cce110bb4778**

MOTECH AUDIT
SMART CONTRACT SECURITY AUDIT

SECURITY ASSESMENT

ASI FI LTD TOKEN DISTRIBUTION

The top 100 holders collectively own 94.19% (9,419,066.56 Tokens) of asi.finance

Token Total Supply: 10,000,000.00 Token | Total Token Holders: 282

asi.finance Top 100 Token Holders
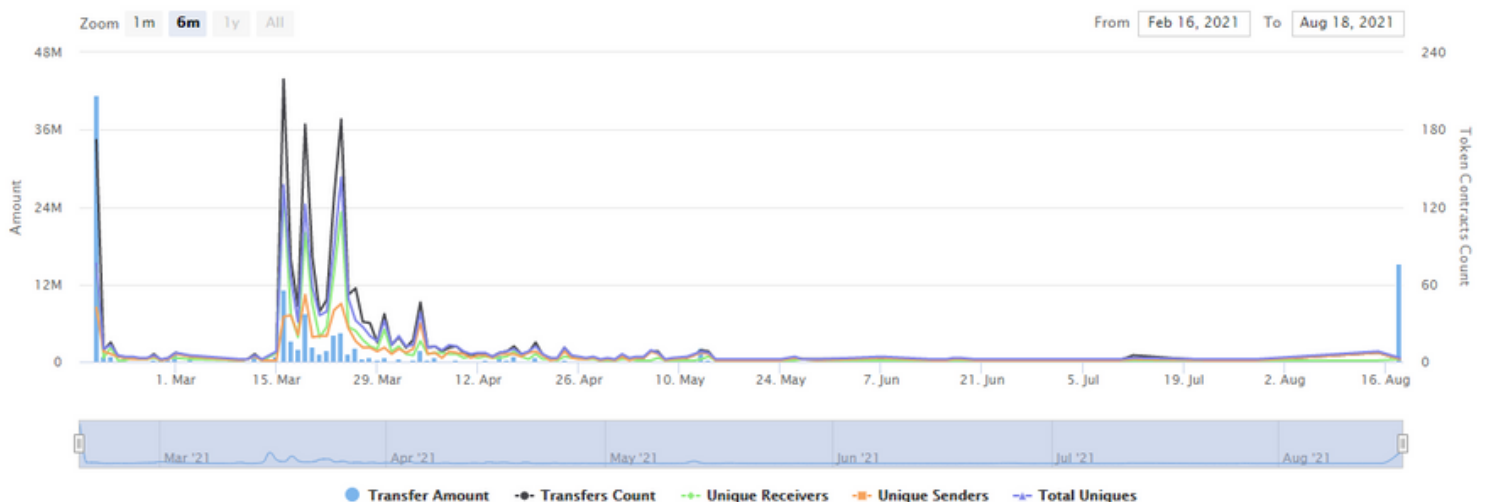Source: Etherscan.io

OTHER ACCOUNTS

0x6d7e810affcff12749f0c33753b1fd9c7ac76c42
0xf93fdbc76889a0f02168523d6f8763769fd7923e
0x1f64b1da953421248b93bf25c97e75d344b8b532
0xfc7fa94473c13e61b15e36f75566009d2f20e3ec
0xf0f67b3c8588b62cecfc8223f3890b4de5709cf3
0x9177ee01aa0abe22ad0b03d43265a99590de68ff

0x79f7c0a6fb99303104bff1c01165cce110bb4778 (ASI Finance: Deployer)

(A total of 9,419,066.56 tokens held by the top 100 accounts from the total supply of 10,000,000.00 token)

ASI FI LTD TOKEN CONTRACT INTERACTION DETAILS

Time Series: Token Contract Overview

Thu 18, Feb 2021 - Wed 18, Aug 2021

Token Contract 0x705d6cbf5352b29b4f4ee0bbe0788721f961abcd (asi.finance)
Source: Etherscan.io

Zoom 1m **6m** 1y All

From Feb 16, 2021 To Aug 18, 2021

Amount

48M

36M

24M

12M

0

Token Contracts Count

240

180

120

60

0

1. Mar   15. Mar   29. Mar   12. Apr   26. Apr   10. May   24. May   7. Jun   21. Jun   5. Jul   19. Jul   2. Aug   16. Aug

Mar '21   Apr '21   May '21   Jun '21   Jul '21   Aug '21

● Transfer Amount   -●- Transfers Count   -●- Unique Receivers   -■- Unique Senders   -▲- Total Uniques

MOTECH AUDIT
SMART CONTRACT SECURITY AUDIT

TOP 10 TOKEN HOLDERS

Rank	Address	Quantity	Percentage	Value	Analytics
1	ASI Finance: Deployer	7,287,702.203815840422806833	72.8770%	$85,873.93	📈
2	0x9177ee01aa0abe22ad0b03d43265a99590de68ff	216,795.039128327079734836	2.1680%	$2,554.58	📈
3	0xf0f67b3c8588b62cecfc8223f3890b4de5709cf3	98,906.988148903717836003	0.9891%	$1,165.46	📈
4	0xfc7fa94473c13e61b15e36f75566009d2f20e3ec	85,318.115742129975320862	0.8532%	$1,005.34	📈
5	0x1f64b1da953421248b93bf25c97e75d344b8b532	79,371.9718646266871206	0.7937%	$935.27	📈
6	0xf93fdbc76889a0f02168523d6f8763769fd7923e	77,049.6021217228911263309	0.7705%	$907.91	📈
7	0x6d7e810affcff12749f0c33753b1fd9c7ac76c42	68,975.632600192987852345	0.6898%	$812.77	📈
8	0x12d6f056cc022c84cf91e8d66541b62757073dd6	61,145.32098872582773625	0.6115%	$720.50	📈
9	0x28778064153d242f0655e0a9bf58fd846c65f316	56,576.041437878597190454	0.5658%	$666.66	📈
10	0xf2e911734f88c18854989ad86e0f1e8fadc80752	53,874.2583464963358230098	0.5387%	$634.82	📈

sourcehttps://etherscan.io/

MOTECH AUDIT
SMART CONTRACT SECURITY AUDIT

SECURITY ISSUES

✓ High Severity Issues

No high severity issues found.

✓ Medium Severity Issues

No medium severity issues found.

Low Severity Issues

1. Add 0x0 address validation in function setExchange in ASI.sol

2. Default value of uint type in solidity is 0, so code construction in function ASI. _calculateBalance could be simplified.

Lowest / Code style / Best Practice

1. Functions decreaseAllowance in both contracts throw an error while decreasing amount is higher than already allowed. It is not an issue, but it will be better to set allowance to 0. To simplify the user journey.
2. It is a good practice to move repeatable requires operations to modifiers due to DRY principles.
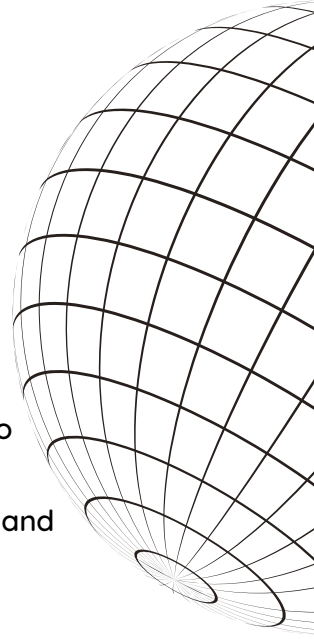
MOTECH AUDIT
SMART CONTRACT SECURITY AUDIT

MOTECH AUDIT

SMART CONTRACT SECURITY AUDIT
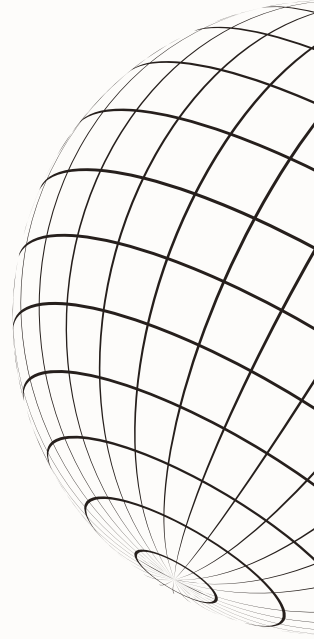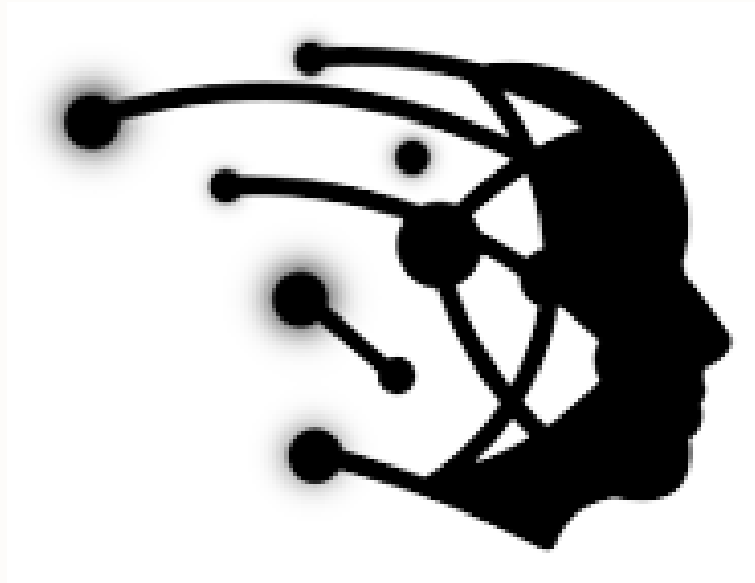
SECURITY ASSESMENT
CONCLUSION

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.

MOTECH AUDIT
SMART CONTRACT SECURITY AUDIT