



MOTECH AUDIT

SMART CONTRACT SECURITY AUDIT

Security Assessment

ZKSWAP V2 PROGRESS REPORT

2021

12 OCT 2021

SECURITY ASSESSMENT

TABLE OF CONTENTS

Summary

Background

Audit Details

Disclaimer

Contract Details

Token Distribution

Contract Interaction Details

Top 10 Token Holders

Finding

VER-01 : Redundant Variable Initialization

ZSS-01 : Redundant Variable Initialization

ZSS-02 : Reusability of code is not observed

Conclusion



MOTECH AUDIT
SMART CONTRACT SECURITY AUDIT

SECURITY ASSESSMENT SUMMARY

This report has been prepared for ZKSwap V2 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 Manual Review and Static Analysis techniques.

This report presents findings from the code delta between commits `5fd4aec99edf725513bb972437767f5bf874f79b` and `72ffa2d5bb803919c52db6b427c49e58e30c84a8` and all the prior code commits have been audited in previous audit iterations.

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.

All of the findings in this delta report are of informational nature related to coding style of the contracts. The team acknowledged the findings but did not apply remediations.



MOTECH AUDIT
SMART CONTRACT SECURITY AUDIT

SECURITY ASSESMENT

BACKGROUND

MotechAudit was commissioned by ZKSwap V2 to perform an audit of smart contracts:

<https://etherscan.io/address/0xe4815AE53B124e7263F08dcDBBB757d41Ed658c6>

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

ZKSwap V2



DEPLOYER ADDRESS

0x6383d169a2353B72097B3862625F50fFb75c42Fe



CLIENT CONTACTS:

ZKSwap V2 team



BLOCKCHAIN

ETHEREUM Project



WEBSITE:

<https://zks.org/en>



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 ASSESMENT

CONTRACT DETAILS

Token contract details for Nov-22-2020

Contract name	ZKSwap V2
Contract address	0xe4815AE53B124e7263F08dcDBBB757d41Ed658c6
Total supply	1,000,000,000
Token ticker	Zks (ZKS)
Decimals	18
Token holders	9,541
Transactions count	144,027
Top 100 holders dominance	98.6932%
Contract deployer address	0x6383d169a2353B72097B3862625F50fFb75c42Fe
Contract's current owner address	0x6383d169a2353B72097B3862625F50fFb75c42Fe

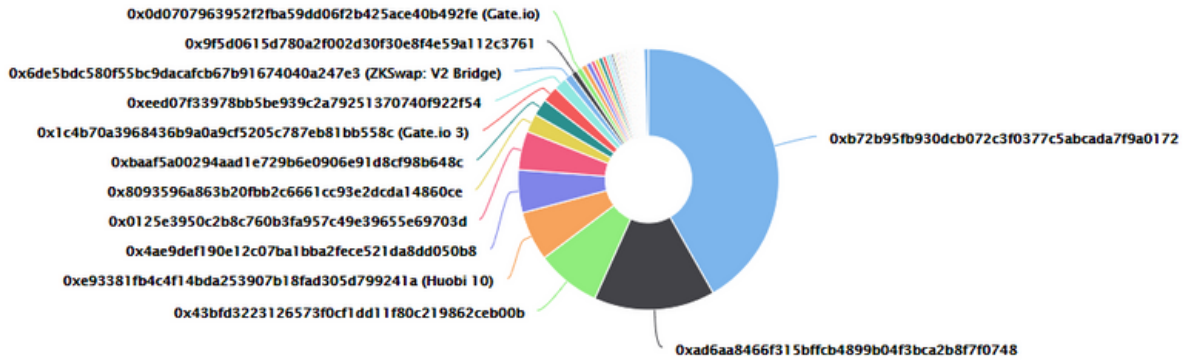
ZKS TOKEN DISTRIBUTION

The top 100 holders collectively own 99.43% (994,288,440.94 Tokens) of Zks

Token Total Supply: 1,000,000,000.00 Token | Total Token Holders: 9,541

Zks Top 100 Token Holders

Source: Etherscan.io



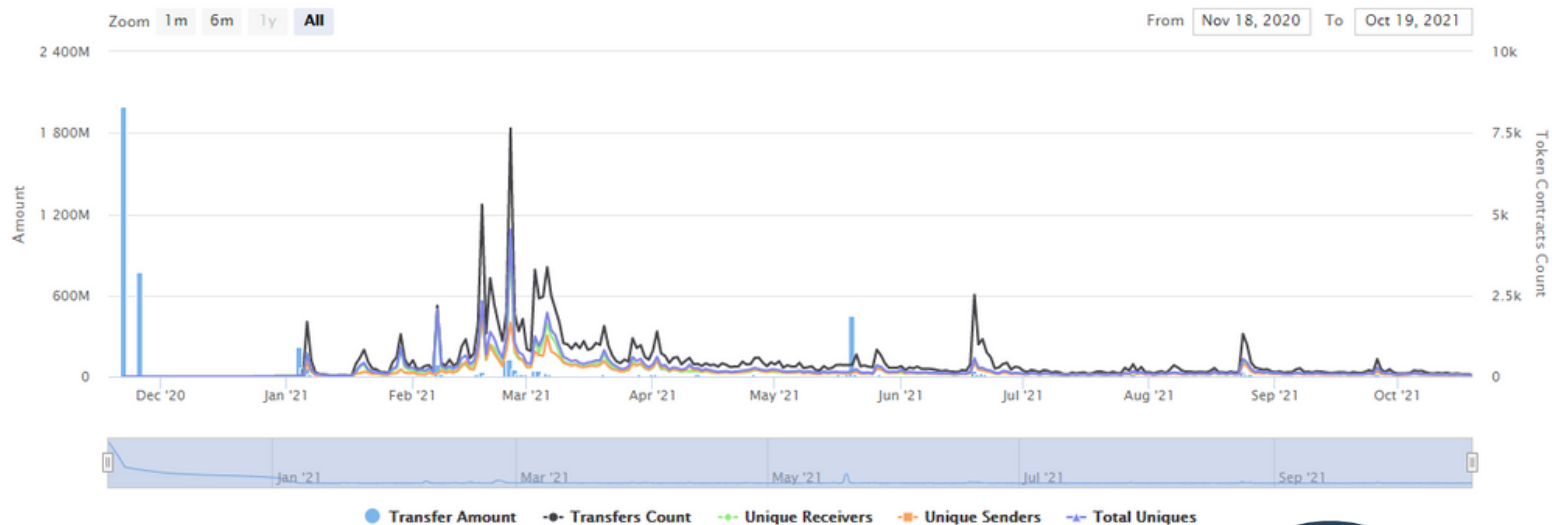
(A total of 994,288,440.94 tokens held by the top 100 accounts from the total supply of 1,000,000,000.00 token)

ZKS TOKEN CONTRACT INTERACTION DETAILS

Time Series: Token Contract Overview

Sun 22, Nov 2020 - Tue 19, Oct 2021















Token Contract 0xe4815AE53B124e7263F08dcDB8B757d41Ed658c6 (Zks)
Source: Etherscan.io



MOTECH AUDIT
SMART CONTRACT SECURITY AUDIT

SECURITY ASSESSMENT

TOP 10 TOKEN HOLDERS

Rank	Address	Quantity	Percentage	Value	Analytics
1	 0xb72b95fb930dcb072c3f0377c5abcada7f9a0172	417,610,000	41.7610%	\$206,668,114.30	
2	0xad6aa8466f315bffc4899b04f3bca2b8f7f0748	150,000,000	15.0000%	\$74,232,458.86	
3	0x43bfd3223126573f0cf1dd11f80c219862ceb00b	80,000,000	8.0000%	\$39,590,644.73	
4	Huobi 10	61,186,152.966350678	6.1186%	\$30,279,990.55	
5	0x4ae9def190e12c07ba1bba2fece521da8dd050b8	53,000,000	5.3000%	\$26,228,802.13	
6	0x0125e3950c2b8c760b3fa957c49e39655e69703d	48,100,000	4.8100%	\$23,803,875.14	
7	 0x8093596a863b20fbb2c6661cc93e2dcda14860ce	22,916,605.15375611449483272	2.2917%	\$11,341,039.66	
8	 0xbaaf5a00294aad1e729b6e0906e91d8cf98b648c	20,827,517.837103949068780198	2.0828%	\$10,307,185.74	
9	Gate.io 3	20,000,000.00000000000000000015	2.0000%	\$9,897,661.18	
10	 0xeed07f33978bb5be939c2a79251370740f922f54	15,798,579.000433535355437461	1.5799%	\$7,818,449.10	

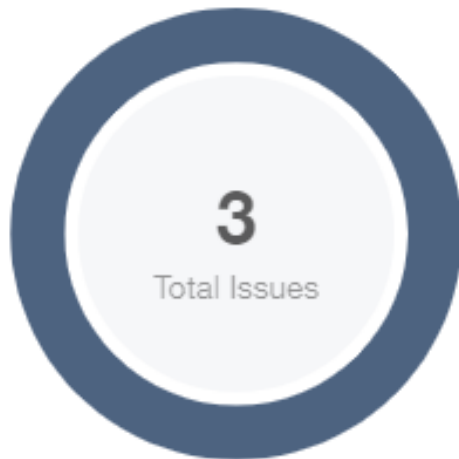
source:etherscan.io



MOTECH AUDIT
SMART CONTRACT SECURITY AUDIT

SECURITY ASSESMENT

FINDINGS



■ Critical	0 (0.00%)
■ Major	0 (0.00%)
■ Medium	0 (0.00%)
■ Minor	0 (0.00%)
■ Informational	3 (100.00%)
■ Discussion	0 (0.00%)

ID	Title	Category	Severity	Status
VER-01	Redundant Variable Initialization	Coding Style	● Informational	ⓘ Acknowledged
ZSS-01	Redundant Variable Initialization	Coding Style	● Informational	ⓘ Acknowledged
ZSS-02	Reusability of code is not observed	Coding Style	● Informational	ⓘ Acknowledged



SECURITY ASSESMENT

VER-01 | REDUNDANT VARIABLE INITIALIZATION

Category	Severity	Location	Status
Coding Style	<div><div></div> Informational</div>	Verifier.sol: 9	<div><div></div> Acknowledged</div>

Description

The aforementioned line redundantly initializes bool type variable to false as the default value of a booltype variable is false.

Recommendation

We advise that the linked initialization statement is removed from the codebase to increase legibility.



SECURITY ASSESMENT

ZSS-01 | REDUNDANT VARIABLE INITIALIZATION

Category	Severity	Location	Status
Coding Style	● Informational	ZkSync.sol: 349, 369	ⓘ Acknowledged

Description

The aforementioned lines redundantly initialize uint16 type variable to 0 as the default value of a uint16type variable is 0.

Recommendation

We advise that the linked initialization statement is removed from the codebase to increase legibility.



SECURITY ASSESMENT

ZSS-02 | REUSABILITY OF CODE IS NOT OBSERVED

Category	Severity	Location	Status
Coding Style	● Informational	ZkSync.sol: 347, 366	ⓘ Acknowledged

Description

The functions `withdrawERC20` and `withdrawERC20WithAddress` on the aforementioned lines contain the same functionality with the difference being one registers withdrawal on `msg.sender` and the other registers withdrawal on parameter `_to`.

Recommendation

We advise to introduce a private function containing functionality from `withdrawERC20WithAddress` that is called by both of the aforementioned functions to increase code legibility.



SECURITY ASSESSMENT

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