



AUDIT REPORT

2023

Security Assessment AI DogeX

June 3, 2023
Audit Status: Pass

Project Overview

Token Summary

Parameter	Result
Address	0x246fCdC18bF3781B4c5100B3A6DEcEf8DBcC8a31
Name	AI DogeX
Ticker	AIDOGEX
Decimals	18
Supply	420,000,000,000,000
Platform	Ethereum Chain
Deployer	0xdcaf11423c955b8f8055e5d1c38defbc2424742c
Compiler	v0.8.17+commit.8df45f5f
Contract Name	AIDOGEX
Optimization	Yes with 200 runs
License Type	MIT
Language	Solidity
Code Base	https://etherscan.io/address/0x246fCdC18bF3781B4c5100B3A6DEcEf8DBcC8a31#code

Risk Analysis

Classifications of Manual Risk Results

Classification	Description
● Critical	Danger or Potential Problems
● Major	Be Careful
● Minor	Pass, Not-Detected or Sale Item
● Informational	Function Detected

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 we were identified.

The following quick summary it's added to the project overview; however, there are more details about the audit and its results. Please read every detail.

Manual Code Review Risk Results

Contract Privilege	Description
● Can Mint?	Passed
● Edit taxes over 25%?	Passed
● Max TX?	Passed
● Max Wallet?	Passed
● Has to enable trading?	Passed
● Modify Tax?	Yes
● Can Blacklist?	Passed
● Is Honeypot?	Passed
● Trading Cool down?	Not Detected
● Can Pause Trade?	Passed
● Pause Transfer?	Not Detected
● Is Proxy?	Not Detected
● Is Anti Whale?	Not Detected
● Is Anta Bot?	Not Detected
● Is Blacklist?	Not Detected
● Blacklist Check	Passed
● Is Whitelist?	Not Detected
● Buy Tax	0
● Sell Tax	10
● Can Take Ownership?	Not Detected
● Hidden Owner?	Not Detected
● Owner	0xBe2681A431B79C692A0AB0256b274c6EC63f6532
● Self-Destruct?	Not Detected
● Holders	1
● Audit Confidence	Medium
● Other?	Not Detected

Assessment Summary

This report has been prepared for AI DogeX Token on the Ethereum Chain network. Aterand provides both client-centered and usercentered examination of the smart contracts and their current status when applicable. This report represents the security assessment made to find issues and vulnerabilities on the source code along with the current liquidity and token holder statistics of the protocol.

A comprehensive examination has been performed, utilizing Cross Referencing, Static Analysis, In-House Security Tools, and line-by-line Manual Review.

The auditing process pays special attention to the following considerations:

- Testing the smart contracts against both common and uncommon attack vectors.
- Inspecting liquidity and holders statistics to inform the current status to both users and client when applicable.
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Verifying contract functions that allow trusted and/or untrusted actors to mint, lock, pause, and transfer assets.
- 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.

Issues Checking Status

Issue Description	Checking Status
Compiler errors.	Passed
Race conditions and Reentrancy.	Passed
Possible delays in data delivery.	Passed
Oracle calls.	Passed
Front running.	Passed
Timestamp dependence.	Passed
Integer Overflow and Underflow.	Passed
DoS with revert.	Passed
DoS with block gas limit.	Passed
Methods execution permissions.	Passed
Economy model of the contract.	Passed
The impact of the exchange rate on the logic.	Passed
Private user data leaks.	Passed
Malicious Event log.	Passed
Scoping and Declarations.	Passed
Uninitialized storage pointers.	Passed
Arithmetic accuracy.	Passed
Design Logic.	Passed
Cross-function race conditions.	Passed
Safe Open Zeppelin contracts implementation and usage.	Passed
Fallback function security.	Passed

Security Issues



High Severity Issues

No high severity issues found.



Medium Severity Issues

No medium severity issues found.



Low Severity Issues

No low severity issues found.

Conclusion

Smart contracts do not contain high severity issues! Liquidity pair contract's security is not checked due to out of scope. The further transfers and operations with the funds raise are not related to this particular contract.

Social & Links

Website: <https://www.aidogex.com/>

Twitter: <https://twitter.com/aidogex>

Telegram: https://t.me/AIDogeX_Official

Discord: N/A at the time of audit.

Github: <https://ai-dogex.gitbook.io/docs/>

Facebook: N/A at the time of audit.

Youtube: <https://www.youtube.com/watch?v=6FG72NsluII>

Instagram: <https://www.instagram.com/aidogex/>

Reddit: N/A at the time of audit.

Logo



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