Smart Contract Code Review And Security Analysis Report

Customer: SOLIDUS AI TECH

Date: 21/02/2024

We express our gratitude to the SOLIDUS AI TECH team for the collaborative engagement that enabled the execution of this Smart Contract Security Assessment.

AITECH introduces the world's first deflationary Artificial Intelligence token, providing Artificial-Intelligence-as-a-Service (AIaaS), Blockchain-as-a-Service (BaaS), and high-performance computing (HPC) power rental through its eco-friendly, secure data center in Europe. The $AITECH utility token is essential for leveraging these cutting-edge tools and services within the AITECH ecosystem.

Platform: EVM

Language: Solidity

Tags: ERC-20

Timeline: 19/02/2024 - 21/02/2024

Methodology: https://hackenio.cc/sc_methodology

Review Scope

Repository	https://github.com/Decubate-com/AITECH/
Commit	704a7dd4f4323a44b7a1bce558a200b4dd1e773e

Audit Summary

10/10	10/10	0%	10/10
Security Score	Code quality score	Test coverage	Documentation quality score

Total 10/10

The system users should acknowledge all the risks summed up in the risks section of the report

0	0	0	0
Total Findings	Resolved	Accepted	Mitigated

Findings by severity

Critical	0
High	0
Medium	0
Low	0

This report may contain confidential information about IT systems and the intellectual property of the Customer, as well as information about potential vulnerabilities and methods of their exploitation.

The report can be disclosed publicly after prior consent by another Party. Any subsequent publication of this report shall be without mandatory consent.

Document

Name	Smart Contract Code Review and Security Analysis Report for SOLIDUS AI TECH
Audited By	Farrukh Odinaev
Approved By	Yves Toiser
Website	https://www.aitech.io/
Changelog	21/02/2024 – Preliminary Report

Table of Contents

System Overview

AITECH is a dApp protocol which contains ERC20 tokens for the interaction with the ecosystem, this audit covers the following contract:

AITECH token — A simple ERC-20 token that mints all the initial supply to a deployer. Additional minting is not allowed. A burnable feature is implemented.

It has the following attributes:

- Name: AITECH
- Symbol: AITECH
- Decimals: 18
- Total supply: 2 billion tokens.

Executive Summary

This report presents an in-depth analysis and scoring of the customer's smart contract project. Detailed scoring criteria can be referenced in the scoring methodology.

Documentation quality

The total Documentation Quality score is **10** out of **10**.

- Functional requirements are provided.
- Technical description is provided.
- NatSpecs are provided.

Code quality

The total Code Quality score is **10** out of **10**.

- The development environment is configured.
- There are no code quality issues.

Test coverage

Code coverage of the project is 0% (branch coverage):

- Tests are not provided (according to our methodology, tests are not mandatory for projects smaller than 250 lines of codes).

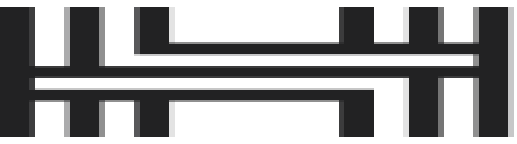
Security score

Upon auditing, the code was found to contain **0** critical, **0** high, **0** medium, and **0** low severity issues, leading to a security score of **10** out of **10**.

All identified issues are detailed in the “Findings” section of this report.

Summary

The comprehensive audit of the customer's smart contract yields an overall score of **10**. This score reflects the combined evaluation of documentation, code quality, test coverage, and security aspects of the project.



Risks

- All the tokens are minted to a single address. The secureness of the supply depends on the secureness of key storage.

Disclaimers

Hacken Disclaimer

The smart contracts given for audit have been analyzed based on best industry practices at the time of the writing of this report, with cybersecurity vulnerabilities and issues in smart contract source code, the details of which are disclosed in this report (Source Code); the Source Code compilation, deployment, and functionality (performing the intended functions).

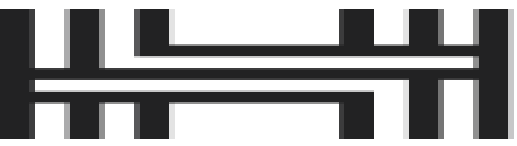
The report contains no statements or warranties on the identification of all vulnerabilities and security of the code. The report covers the code submitted and reviewed, so it may not be relevant after any modifications. Do not consider this report as a final and sufficient assessment regarding the utility and safety of the code, bug-free status, or any other contract statements.

While we have done our best in conducting the analysis and producing this report, it is important to note that you should not rely on this report only — we recommend proceeding with several independent audits and a public bug bounty program to ensure the security of smart contracts.

English is the original language of the report. The Consultant is not responsible for the correctness of the translated versions.

Technical Disclaimer

Smart contracts are deployed and executed on a blockchain platform. The platform, its programming language, and other software related to the smart contract can have vulnerabilities that can lead to hacks. Thus, the Consultant cannot guarantee the explicit security of the audited smart contracts.



Appendix 1. Severity Definitions

When auditing smart contracts, Hacken is using a risk-based approach that considers **Likelihood**, **Impact**, **Exploitability** and **Complexity** metrics to evaluate findings and score severities.

Reference on how risk scoring is done is available through the repository in our Github organization:

[hknio/severity-formula]

Severity	Description
Critical	Critical vulnerabilities are usually straightforward to exploit and can lead to the loss of user funds or contract state manipulation.
High	High vulnerabilities are usually harder to exploit, requiring specific conditions, or have a more limited scope, but can still lead to the loss of user funds or contract state manipulation.
Medium	Medium vulnerabilities are usually limited to state manipulations and, in most cases, cannot lead to asset loss. Contradictions and requirements violations. Major deviations from best practices are also in this category.
Low	Major deviations from best practices or major Gas inefficiency. These issues will not have a significant impact on code execution, do not affect security score but can affect code quality score.

Appendix 2. Scope

The scope of the project includes the following smart contracts from the provided repository:

Scope Details

Repository	https://github.com/Decubate-com/AITECH/
Commit	704a7dd4f4323a44b7a1bce558a200b4dd1e773e
Whitepaper	Not provided
Requirements	Not provided
Technical Requirements	Not provided

Contracts in Scope

./src/AITECH.sol