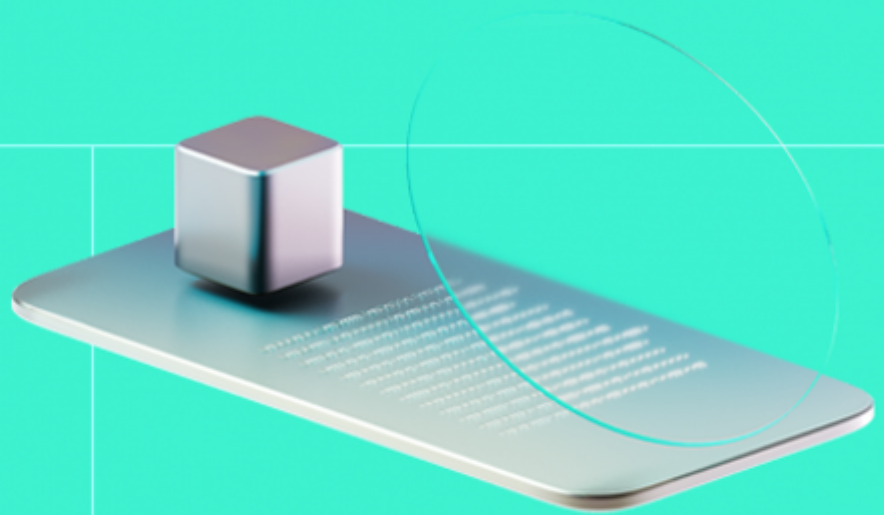




Smart Contract Code Review And Security Analysis Report

Customer: BlackCardCoin

Date: 17/04/2024



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

BlackCard Coin is a groundbreaking BEP20 token.

Platform: BEP

Language: Solidity

Tags: ERC20

Timeline: 15/04/2024 - 17/04/2024

Methodology: https://hackenio.cc/sc_methodology.

Review

Scope

Deployed	
Link	https://bscscan.com/address/0x2940566Eb50F15129238f4Dc599ADC4F742D7d8E#code
Commit	n/a

Audit Summary

10/10

Security Score

6/10

Code quality score

100%

Test coverage

7/10

Documentation quality score

Total 8.8/10

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

0

Total Findings

0

Resolved

0

Accepted

0

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 BlackCardCoin
Audited By	Turgay Arda Usman
Approved By	Grzegorz Trawinski
Website	https://blackcardcoin.com
Changelog	16/04/2024 - Preliminary Report

Table of Contents

System Overview	6
Privileged Roles	6
Executive Summary	7
Documentation Quality	7
Code Quality	7
Test Coverage	7
Security Score	7
Summary	7
Risks	8
Findings	9
Vulnerability Details	9
Observation Details	9
Disclaimers	10
Appendix 1. Severity Definitions	11
Appendix 2. Scope	12

System Overview

Black Card Coin is a BEP20 token with the following contracts:

BlackCardCoin — simple ERC-20 token. Additional minting is not allowed.

It has the following attributes:

- Name: BlackCardCoin
- Symbol: TST
- Decimals: BCCoin
- Total supply: 150m tokens.

Privileged roles

- No roles defined.

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 **6** out of **10**.

- Functional requirements are partially provided.
- Technical description is mostly provided.

Code quality

The total Code Quality score is **6** out of **10**.

- The code duplicates commonly known contracts instead of reusing them.
- Several template code patterns were found.

Test coverage

Code coverage of the project is **0.0%** (branch coverage)..

- The code is already deployed.
- Tests are not required with the projects with LoCs less than 250.

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 **8.8**. This score reflects the combined evaluation of documentation, code quality, test coverage, and security aspects of the project.

Risks

- The project concentrates on minting tokens in a single address, raising the risk of fund mismanagement or theft, especially if key storage security is compromised.
- The current implementation does not strictly follow the ERC20 standard, this may cause some risks in future interactions.

Findings

Vulnerability Details

Observation Details

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](https://github.com/hacken/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://bscscan.com/address/0x2940566Eb50F15129238f4Dc599ADC4F742D7d8E#code
Commit	n/a
Whitepaper	https://download.blackcardcoin.com/Whitepaper.pdf
Requirements	https://download.blackcardcoin.com/Whitepaper.pdf
Technical Requirements	Natspec

Contracts in Scope

BlackCardCoin.sol