



**HACKEN**

# SMART CONTRACT CODE REVIEW AND SECURITY ANALYSIS REPORT

**Customer:** Crypto Stake Token

**Date:** November 11<sup>th</sup>, 2021



This document 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 containing confidential information can be used internally by the Customer, or it can be disclosed publicly after all vulnerabilities are fixed – upon a decision of the Customer.

## Document

<b>Name</b>	Smart Contract Code Review and Security Analysis Report for Crypto Stake Token.
<b>Approved by</b>	Andrew Matiukhin   CTO Hacken OU
<b>Type</b>	BEP20 token
<b>Platform</b>	Binance Smart Chain / Solidity
<b>Methods</b>	Architecture Review, Functional Testing, Computer-Aided Verification, Manual Review
<b>Repository</b>	<a href="https://github.com/Cryptostaketoken/CryptoStakeToken/blob/main/CryptoStakeToken.sol">https://github.com/Cryptostaketoken/CryptoStakeToken/blob/main/CryptoStakeToken.sol</a>
<b>Commit</b>	ec6c56263f2b90fd07080f595433c9cd236fbf72
<b>Technical Documentation</b>	NO
<b>JS tests</b>	NO
<b>Website</b>	crypto-stake.org
<b>Timeline</b>	08 NOVEMBER 2021 - 11 NOVEMBER 2021
<b>Changelog</b>	11 NOVEMBER 2021 - INITIAL AUDIT



## Table of contents

Introduction	4
Scope	4
Executive Summary	5
Severity Definitions	7
Audit overview	8
Conclusion	10
Disclaimers	11

## Introduction

Hacken OÜ (Consultant) was contracted by Crypto Stake Token (Customer) to conduct a Smart Contract Code Review and Security Analysis. This report presents the findings of the security assessment of the Customer's smart contract and its code review conducted between November 8<sup>th</sup>, 2021 - November 11<sup>th</sup>, 2021.

## Scope

The scope of the project is smart contracts in the repository:

**Repository:**

<https://github.com/Cryptostaketoken/CryptoStakeToken/blob/main/CryptoStakeToken.sol>

**Commit:**

[ec6c56263f2b90fd07080f595433c9cd236fbf72](https://github.com/Cryptostaketoken/CryptoStakeToken/commit/ec6c56263f2b90fd07080f595433c9cd236fbf72)

**Technical Documentation:** No

**JS tests:** No

**Contracts:**

[CryptoStakeToken.sol](#)

We have scanned this smart contract for commonly known and more specific vulnerabilities. Here are some of the commonly known vulnerabilities that are considered:

Category	Check Item
Code review	<ul style="list-style-type: none"><li>▪ Reentrancy</li><li>▪ Ownership Takeover</li><li>▪ Timestamp Dependence</li><li>▪ Gas Limit and Loops</li><li>▪ DoS with (Unexpected) Throw</li><li>▪ DoS with Block Gas Limit</li><li>▪ Transaction-Ordering Dependence</li><li>▪ Style guide violation</li><li>▪ Costly Loop</li><li>▪ ERC20 API violation</li><li>▪ Unchecked external call</li><li>▪ Unchecked math</li><li>▪ Unsafe type inference</li><li>▪ Implicit visibility level</li><li>▪ Deployment Consistency</li><li>▪ Repository Consistency</li><li>▪ Data Consistency</li></ul>

Functional review	<ul style="list-style-type: none"> <li>▪ Business Logics Review</li> <li>▪ Functionality Checks</li> <li>▪ Access Control &amp; Authorization</li> <li>▪ Escrow manipulation</li> <li>▪ Token Supply manipulation</li> <li>▪ Assets integrity</li> <li>▪ User Balances manipulation</li> <li>▪ Data Consistency manipulation</li> <li>▪ Kill-Switch Mechanism</li> <li>▪ Operation Trails &amp; Event Generation</li> </ul>
-------------------	---

## Executive Summary

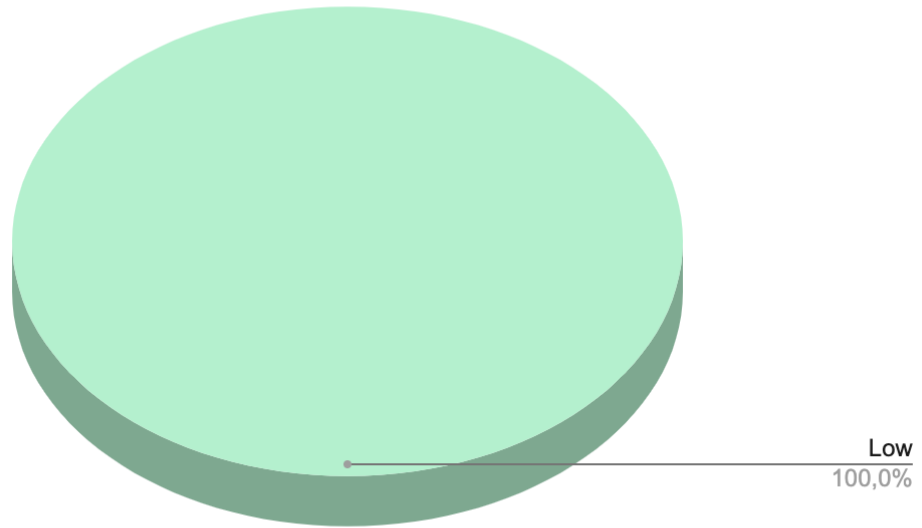
According to the assessment, the Customer's smart contracts are well-secured.



Our team performed an analysis of code functionality, manual audit, and automated checks with Mythril and Slither. All issues found during automated analysis were manually reviewed, and important vulnerabilities are presented in the Audit overview section. All found issues can be found in the Audit overview section.

As a result of the audit, security engineers found **4** low severity issues.

*Graph 1. The distribution of vulnerabilities after the audit.*



## Severity Definitions

Risk Level	Description
<b>Critical</b>	Critical vulnerabilities are usually straightforward to exploit and can lead to assets loss or data manipulations.
<b>High</b>	High-level vulnerabilities are difficult to exploit; however, they also have a significant impact on smart contract execution, e.g., public access to crucial functions
<b>Medium</b>	Medium-level vulnerabilities are important to fix; however, they can't lead to assets loss or data manipulations.
<b>Low</b>	Low-level vulnerabilities are mostly related to outdated, unused, etc. code snippets that can't have a significant impact on execution

## Audit overview

### ■ ■ ■ ■ Critical

No critical issues were found.

### ■ ■ ■ High

No high severity issues were found.

### ■ ■ Medium

No medium severity issues were found.

### ■ Low

#### 1. Using contracts with empty functions

In the code, we've found several contracts (ERC20Basic, ERC20) which have all functions unimplemented. Those look like interfaces but are declared as contracts.

**Contracts:** ERC20Basic, ERC20

**Recommendation:** We'd recommend doing the following:

- move "totalSupply" variable declaration from ERC20Basic to StandardToken;
- declare functions of ERC20Basic, ERC20 external instead of public;
- remove the inheritance from the ERC20 and put two inheritances into the StandardToken (contract StandardToken is ERC20, ERC20Basic);
- declare both ERC20Basic and ERC20 as interfaces instead of contracts

#### 2. Unlimited minting token

The owner of the contract is able to mint an unlimited amount of the token at any time. If it is correct behavior, please make sure this is stated in the whitelist and the community is acknowledged.

**Contracts:** CoinToken

**Function:** mint

**Recommendation:** Please either restrict minting by some hard cap, or add vesting time, or inform the community that the minting is unlimited and unrestricted for the owner.

#### 3. Boolean equality

Boolean constants can be used directly and do not need to be compared to **true** or **false**.

**Contracts:** StandardToken





**Function:** transfer, transferFrom

**Recommendation:** Remove the equality to the boolean constant.

4. A public function that could be declared external

**public** functions that are never called by the contract should be declared **external** to save gas.

**Contracts:** OwnableToken, Pausable, ERC20Basic, StandardToken, ERC20, CoinToken

**Function:** OwnableToken.transferOwnership, Pausable.pause,  
Pausable.unpause, ERC20Basic.balanceOf, StandardToken.balanceOf,  
ERC20.allowance, StandardToken.allowance,  
PausableToken.blackListAddress, CoinToken.burn, CoinToken.mint

**Recommendation:** Use the external attribute for functions never called from the contract.



## Conclusion

Smart contracts within the scope were manually reviewed and analyzed with static analysis tools.

The audit report contains all found security vulnerabilities and other issues in the reviewed code.

As a result of the audit, security engineers found **4** low severity issues.



## Disclaimers

### **Hacken Disclaimer**

The smart contracts given for audit have been analyzed in accordance with the best industry practices at the date of this report, in relation to 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 audit makes no statements or warranties on the security of the code. It also cannot be considered as a sufficient assessment regarding the utility and safety of the code, bug-free status, or any other statements of the contract. 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.

### **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 audit can't guarantee the explicit security of the audited smart contracts.