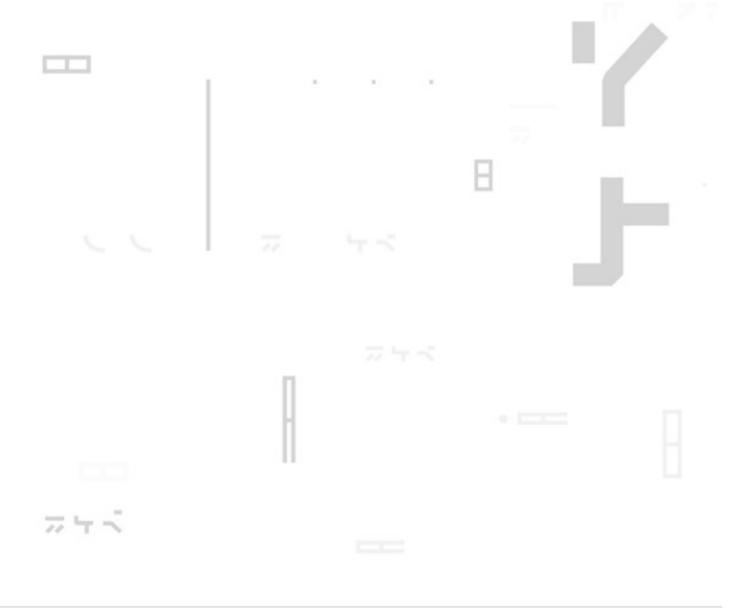


# SMART CONTRACT CODE REVIEW AND SECURITY ANALYSIS REPORT



Customer: Terra Virtua
Date: August 6<sup>th</sup>, 2021

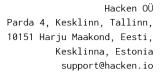


This document may contain confidential information about IT systems and the intellectual property of the Customer as well as information about potential vulnerabilities and methods of their exploitation.

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**

Name	Smart Contract Code Review and Security Analysis Report for Terra Virtua.	
Approved by	Andrew Matiukhin   CTO Hacken OU	
Туре	Balancer	
Platform	Ethereum / Solidity	
Methods	Architecture Review, Functional Testing, Computer-Aided Verification, Manual Review	
Zip archive	tv-balancer-b5350cbc382dff2bb0ea7f13842f5cc69d5953f6.zip	
Technical Documentation	YES	
JS tests	YES	
Timeline	22 JULY 2021 - 06 AUGUST 2021	
Changelog	30 JULY 2021 - INITIAL AUDIT 06 AUGUST 2021 - Second Review	





# Table of contents

Introduction	
Scope	4
Executive Summary	5
Severity Definitions	6
Audit overview	7
Conclusion	7
Disclaimers	9



#### Introduction

Hacken OÜ (Consultant) was contracted by Terra Virtua (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 July  $22^{nd}$ , 2021 - July  $30^{th}$ , 2021. The second review conducted on August  $6^{th}$ , 2021.

## Scope

The scope of the project is smart contracts in the zip archive:

Zip arhive:

tv-balancer-b5350cbc382dff2bb0ea7f13842f5cc69d5953f6.zip

md5 hash:

e451bf25ab1afe5372be363db79ccd91

Technical Documentation: Yes

JS tests: Yes Contracts:

Cooldown.sol Phased.sol

RedeemableERC20.sol RedeemableERC20Pool.sol

SeedERC20.sol Trust.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><li>Reentrancy</li></ul>	
	<ul><li>Ownership Takeover</li></ul>	
	<ul><li>Timestamp Dependence</li></ul>	
	■ Gas Limit and Loops	
	<ul><li>DoS with (Unexpected) Throw</li></ul>	
	<ul><li>DoS with Block Gas Limit</li></ul>	
	<ul> <li>Transaction-Ordering Dependence</li> </ul>	
	Style guide violation	
	<ul><li>Costly Loop</li></ul>	
	<ul><li>ERC20 API violation</li></ul>	
	<ul><li>Unchecked external call</li></ul>	
	<ul><li>Unchecked math</li></ul>	
	<ul><li>Unsafe type inference</li></ul>	
	Implicit visibility level	
	<ul><li>Deployment Consistency</li></ul>	
	<ul><li>Repository Consistency</li></ul>	
	■ Data Consistency	



Functional review	<ul><li>Business Logics Review</li></ul>
	Dusiness Logics Neview
	<ul><li>Functionality Checks</li></ul>
	<ul><li>Access Control &amp; Authorization</li></ul>
	<ul><li>Escrow manipulation</li></ul>
	<ul><li>Token Supply manipulation</li></ul>
	<ul><li>Assets integrity</li></ul>
	<ul><li>User Balances manipulation</li></ul>
	<ul> <li>Data Consistency manipulation</li> </ul>
	<ul><li>Kill-Switch Mechanism</li></ul>

Operation Trails & Event Generation

## **Executive Summary**

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

Insecure	Poor secured	Secured	Well-secured
		You are here	1

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 2 low severity issues which were addressed before the second review.



# **Severity Definitions**

Risk Level	Description	
Critical	Critical vulnerabilities are usually straightforward to exploit and can lead to assets loss or data manipulations.	
High	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	
Medium	Medium-level vulnerabilities are important to fix; however, they can't lead to assets loss or data manipulations.	
Low	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. **Issue**: Maximum line length.

Solidity declares <u>maximum line length</u> that should be followed.

**Recommendation**: Please follow the solidity <u>Code Layout</u> recommendations.

Fixed before the second review.

2. **Issue**: State variable that could be immutable.

State variable which value is initialized in the constructor and never changes should be declared immutable to save gas.

Fixed before the second review.



### 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 2 low severity issues which were addressed before the second review.



#### 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.