



**HACKEN**

# SMART CONTRACT CODE REVIEW AND SECURITY ANALYSIS REPORT

**Customer:** Fantohm

**Date:** August 04<sup>th</sup>, 2022

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

<b>Name</b>	Smart Contract Code Review and Security Analysis Report for Fantohm
<b>Approved By</b>	Evgeniy Bezuglyi   SC Audits Department Head at Hacken OU
<b>Type</b>	Lending
<b>Platform</b>	EVM
<b>Network</b>	Ethereum
<b>Language</b>	Solidity
<b>Methods</b>	Manual Review, Automated Review, Architecture Review
<b>Website</b>	<a href="https://www.balance.capital/">https://www.balance.capital/</a>
<b>Timeline</b>	01.08.2022 - 04.08.2022
<b>Changelog</b>	04.08.2022 - Initial Review



## Table of contents

Introduction	4
Scope	4
Severity Definitions	5
Executive Summary	6
Checked Items	7
System Overview	10
Findings	11
Disclaimers	12

## Introduction

Hacken OÜ (Consultant) was contracted by Fantohm (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 contracts.

## Scope

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

### Initial review scope

#### Repository:

<https://github.com/FantOHM-DAO/usdb-nft-lending-contract>

#### Commit:

9dde8f4a54d562ee1812e1ee10872241f0a2b2a0

#### Technical Documentation:

[Project documentation](#)

#### Integration and Unit Tests: Yes

#### Contracts:

File: ./contracts/UsdbLending.sol

SHA3: c125672846a04855182c05e4ac64d7d88bd190adb883766ba3dbdc404983287d

File: ./contracts/UsdbLendingCore.sol

SHA3: c2f3ad9dbecbfd4a38b9da7cc27be0f8724a3e5f3e9f8680f32f57df724521c6

## 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 cannot lead to assets loss or data manipulations.
Low	Low-level vulnerabilities are mostly related to outdated, unused, etc. code snippets that cannot have a significant impact on execution.

## Executive Summary

The score measurement details can be found in the corresponding section of the [methodology](#).

### Documentation quality

The total Documentation Quality score is **10** out of **10**. Functional and technical requirements are provided in the project's documentation. Code is followed by NatSpec comments.

### Code quality

The total CodeQuality score is **8** out of **10**. Code violates Style guide. All the contract's custom functionality is covered with tests. **Total test coverage is 71%.**

### Architecture quality

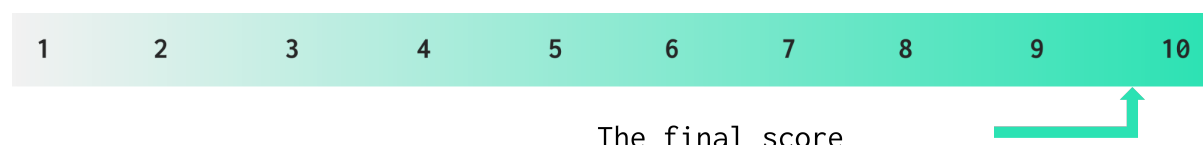
The architecture quality score is **10** out of **10**. Code follows best practices.

### Security score

As a result of the audit, the code contains **no** issues. The security score is **10** out of **10**.

### Summary

According to the assessment, the Customer's smart contract has the following score: **9.8**.



*Table. The distribution of issues during the audit*

Review date	Low	Medium	High	Critical
4 August 2022	0	0	0	0

## Checked Items

We have audited provided smart contracts for commonly known and more specific vulnerabilities. Here are some of the items that are considered:

Item	Type	Description	Status
Default Visibility	<a href="#">SWC-100</a> <a href="#">SWC-108</a>	Functions and state variables visibility should be set explicitly. Visibility levels should be specified consciously.	Passed
Integer Overflow and Underflow	<a href="#">SWC-101</a>	If unchecked math is used, all math operations should be safe from overflows and underflows.	Not Relevant
Outdated Compiler Version	<a href="#">SWC-102</a>	It is recommended to use a recent version of the Solidity compiler.	Passed
Floating Pragma	<a href="#">SWC-103</a>	Contracts should be deployed with the same compiler version and flags that they have been tested thoroughly.	Passed
Unchecked Call Return Value	<a href="#">SWC-104</a>	The return value of a message call should be checked.	Passed
Access Control & Authorization	<a href="#">CWE-284</a>	Ownership takeover should not be possible. All crucial functions should be protected. Users could not affect data that belongs to other users.	Passed
SELFDESTRUCT Instruction	<a href="#">SWC-106</a>	The contract should not be self-destructible while it has funds belonging to users.	Not Relevant
Check-Effect-Interaction	<a href="#">SWC-107</a>	Check-Effect-Interaction pattern should be followed if the code performs ANY external call.	Passed
Assert Violation	<a href="#">SWC-110</a>	Properly functioning code should never reach a failing assert statement.	Passed
Deprecated Solidity Functions	<a href="#">SWC-111</a>	Deprecated built-in functions should never be used.	Passed
Delegatecall to Untrusted Callee	<a href="#">SWC-112</a>	Delegatecalls should only be allowed to trusted addresses.	Not Relevant
DoS (Denial of Service)	<a href="#">SWC-113</a> <a href="#">SWC-128</a>	Execution of the code should never be blocked by a specific contract state unless it is required.	Passed
Race Conditions	<a href="#">SWC-114</a>	Race Conditions and Transactions Order Dependency should not be possible.	Passed
Authorization	<a href="#">SWC-115</a>	tx.origin should not be used for	Not Relevant

through tx.origin		authorization.	
Block values as a proxy for time	<a href="#">SWC-116</a>	Block numbers should not be used for time calculations.	Passed
Signature Unique Id	<a href="#">SWC-117</a> <a href="#">SWC-121</a> <a href="#">SWC-122</a> <a href="#">EIP-155</a>	Signed messages should always have a unique id. A transaction hash should not be used as a unique id. Chain identifier should always be used. All parameters from the signature should be used in signer recovery	Passed
Shadowing State Variable	<a href="#">SWC-119</a>	State variables should not be shadowed.	Passed
Weak Sources of Randomness	<a href="#">SWC-120</a>	Random values should never be generated from Chain Attributes or be predictable.	Not Relevant
Incorrect Inheritance Order	<a href="#">SWC-125</a>	When inheriting multiple contracts, especially if they have identical functions, a developer should carefully specify inheritance in the correct order.	Passed
Calls Only to Trusted Addresses	<a href="#">EEA-Leve1-2</a> <a href="#">SWC-126</a>	All external calls should be performed only to trusted addresses.	Passed
Presence of unused variables	<a href="#">SWC-131</a>	The code should not contain unused variables if this is not <a href="#">justified</a> by design.	Passed
EIP standards violation	<a href="#">EIP</a>	EIP standards should not be violated.	Passed
Assets integrity	Custom	Funds are protected and cannot be withdrawn without proper permissions.	Not Relevant
User Balances manipulation	Custom	Contract owners or any other third party should not be able to access funds belonging to users.	Not Relevant
Data Consistency	Custom	Smart contract data should be consistent all over the data flow.	Passed
Flashloan Attack	Custom	When working with exchange rates, they should be received from a trusted source and not be vulnerable to short-term rate changes that can be achieved by using flash loans. Oracles should be used.	Not Relevant
Token Supply manipulation	Custom	Tokens can be minted only according to rules specified in a whitepaper or any other documentation provided by the customer.	Not Relevant
Gas Limit and Loops	Custom	Transaction execution costs should not depend dramatically on the amount of	Not Relevant



		data stored on the contract. There should not be any cases when execution fails due to the block Gas limit.	
<b>Style guide violation</b>	<b>Custom</b>	Style guides and best practices should be followed.	<b>Failed</b>
<b>Requirements Compliance</b>	<b>Custom</b>	The code should be compliant with the requirements provided by the Customer.	<b>Passed</b>
<b>Environment Consistency</b>	<b>Custom</b>	The project should contain a configured development environment with a comprehensive description of how to compile, build and deploy the code.	<b>Failed</b>
<b>Secure Oracles Usage</b>	<b>Custom</b>	The code should have the ability to pause specific data feeds that it relies on. This should be done to protect a contract from compromised oracles.	Not Relevant
<b>Tests Coverage</b>	<b>Custom</b>	The code should be covered with unit tests. Test coverage should be 100%, with both negative and positive cases covered. Usage of contracts by multiple users should be tested.	<b>Passed</b>
<b>Stable Imports</b>	<b>Custom</b>	The code should not reference draft contracts, that may be changed in the future.	<b>Passed</b>

## System Overview

*FantOHM* is a lending system with the following contracts:

- *UsdbLendingCore* – core contract with data containers, signature mechanism, function to add new supported currencies and functionality to calculate and set new fee.
- *UsdbLending* – lending contract with methods for loan creation, repayment, and liquidation of loan.

### Privileged roles

- The project owner can change the duration unit, exit loan status, set platform fee, and remove currency.

## Findings

### ■ ■ ■ ■ Critical

No critical severity issues were found.

### ■ ■ ■ High

No high severity issues were found.

### ■ ■ Medium

No medium severity issues were found.

### ■ Low

No low severity issues were found.

## Disclaimers

### Hacken Disclaimer

The smart contracts given for audit have been analyzed by the best industry practices at the date 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 to 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, Consultant cannot guarantee the explicit security of the audited smart contracts.