SOLIDProof

Bring trust into your projects

Blockchain Security | Smart Contract Audits | KYC Development | Marketing

MADE IN GERMANY

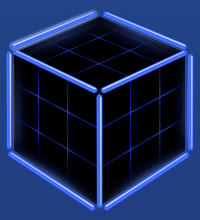
Audit

Security Assessment

15. March 2023

For

BlackBox dApp



SolidProof_io

@solidproof_io

Table of Contents

Introduction

SolidProof.io is a brand of the officially registered company MAKE Network GmbH, based in Germany. We're mainly focused on Blockchain Security such as Smart Contract Audits and KYC verification for project teams.

During the date of 7th March 2023, BlackBox engaged Solidproof.io to assess potential security issues in the smart contracts implementations, review for potential inconsistencies between the code base and the whitepaper/documentation, and provide suggestions for improvement.

Disclaimer

SolidProof.io reports should not be construed as an "endorsement" or "rejection" of any particular project or team. These reports are not, and should not be taken as, an indication of the viability or value of any "product" or "asset" created by any team.

By default, SolidProof.io does not audit integration with external contracts, libraries or services (such as Unicrypt, Uniswap, PancakeSwap, etc.) and is not part of the audit.

SolidProof.io audits do not provide a guarantee or warranty that the technology analyzed is absolutely free of faults, nor do they provide any indication of the owners of the project. SolidProof audits should not be used in any way to make decisions about investing or participating in any particular project. These reports in no way constitute investment advice, nor should they be used as investment advice of any kind. When investing, there is always a risk that you could lose everything.

SolidProof.io reports represent a comprehensive vetting process designed to help our customers increase the quality of their code while mitigating the high risk associated with cryptographic tokens and blockchain technology. Blockchain technology and cryptographic assets carry a high level of risk.

SolidProof takes the position that each company and individual is responsible for their own due diligence and ongoing security. SolidProof makes no claim to guarantee the security or functionality of the technology we have audited.

The tests are a snapshot and may be vulnerable to as yet unknown attacks in the future.

We constantly train the entire team to be able to detect the latest threats. Of course, we work on every audit to the best of our knowledge.

Blockchain Security - Made in Germany

Codebase

Repository

- https://github.com/devgrayhat/devgrayhat.github.io

Commit

Frontend: 6b25fa0

File Overview

The Team provided us with the files that should be tested in the security assessment. This audit covered the following files listed below with a SHA-1 Hash.

Please note: Files with a different hash value than in this table have been modified after the security check, either intentionally or unintentionally. A different hash value may (but need not) be an indication of a changed state or potential vulnerability that was not the subject of this scan.

Imported packages

Used code from other Frameworks/Smart Contracts (direct imports).

➡ Ethers 5.4 (latest version is 6.1.0)

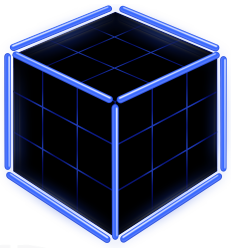
Changelog

A changelog is an overview that contains a chronologically ordered list of changes that have been made to the project. It is often organized by version with the date followed by a list of added, improved and removed features.

#	Date	Description
1.0	08.03.2023	• Layout project • Automated- /Manual-Security Testing • Summary
1.1	15.03.2023	• Updated: scope of work, files
1.2	20.03.2023	• Updated: files

Project Details

We cannot guarantee the completeness and authenticity of the content of descriptions and resources provided by customers. We strongly recommend that you conduct your own research.



Website

https://bbtt.io/

About the project

„In the cyber world, safety, security, freedom is the most valuable and vulnerable thing on the blockchain. So what better than letting BlackBox automation take care of it.“

Twitter	Telegram	E-Mail
https://twitter.com/BBTT_BlackBox	https://t.me/BBTT_PORTAL	tokenblackbox@gmail.com

Vulnerability & Risk Level

Risk represents the probability that a specific threat from a source will exploit a vulnerability and the impact of this event on the organization or system. The risk level is calculated based on CVSS version 3.0.

Level	Value	Vulnerability	Risk
Critical	9 - 10	A vulnerability that can disrupt the contract functioning in a number of scenarios, or creates a risk that the contract may be broken.	Immediate action to reduce risk level.
High	7 – 8.9	A vulnerability that affects the desired outcome when using a contract, or provides the opportunity to use a contract in an unintended way.	Implementation of corrective actions as soon aspossible.
Medium	4 – 6.9	A vulnerability that could affect the desired outcome of executing the contract in a specific scenario.	Implementation of corrective actions in a certain period.
Low	2 – 3.9	A vulnerability that does not have a significant impact on possible scenarios for the use of the contract and is probably subjective.	Implementation of certain corrective actions or accepting the risk.
Informational	0 – 1.9	A vulnerability that have informational character but is not effecting any of the code.	An observation that does not determine a level of risk

Auditing Strategy and Techniques Applied

Throughout the review process, care was taken to check the repository for security-related issues, code quality, and compliance with specifications and best practices. To this end, our team of experienced pentesters and smart contract developers reviewed the code line by line and documented any issues discovered.

We check every file manually. We check every file manually. We use automated tools only so that they help us achieve faster and better results.

Methodology

The auditing process follows a routine series of steps.

1. Code review that includes the following:
    a. Reviewing the specifications, sources, and instructions provided to SolidProof to ensure we understand the size, scope, and functionality of the smart contract.
    b. Manual review of the code, i.e., reading the source code line by line to identify potential vulnerabilities.
    c. Comparison to the specification, i.e., verifying that the code does what is described in the specifications, sources, and instructions provided to SolidProof.

2. Testing and automated analysis that includes the following:
    a. Test coverage analysis, which determines whether test cases actually cover code and how much code is executed when those test cases are executed.
    b. Symbolic execution, which is the analysis of a program to determine what inputs cause each part of a program to execute.

3. Review best practices, i.e., review smart contracts to improve efficiency, effectiveness, clarity, maintainability, security, and control based on best practices, recommendations, and research from industry and academia.

4. Concrete, itemized and actionable recommendations to help you secure your smart contracts.

Overall Security

No critical issues found ✅ dApp is safe to use

The contract does not contain issues of high or medium criticality. This means that no known vulnerabilities were found in the source code.

Comment: N/A

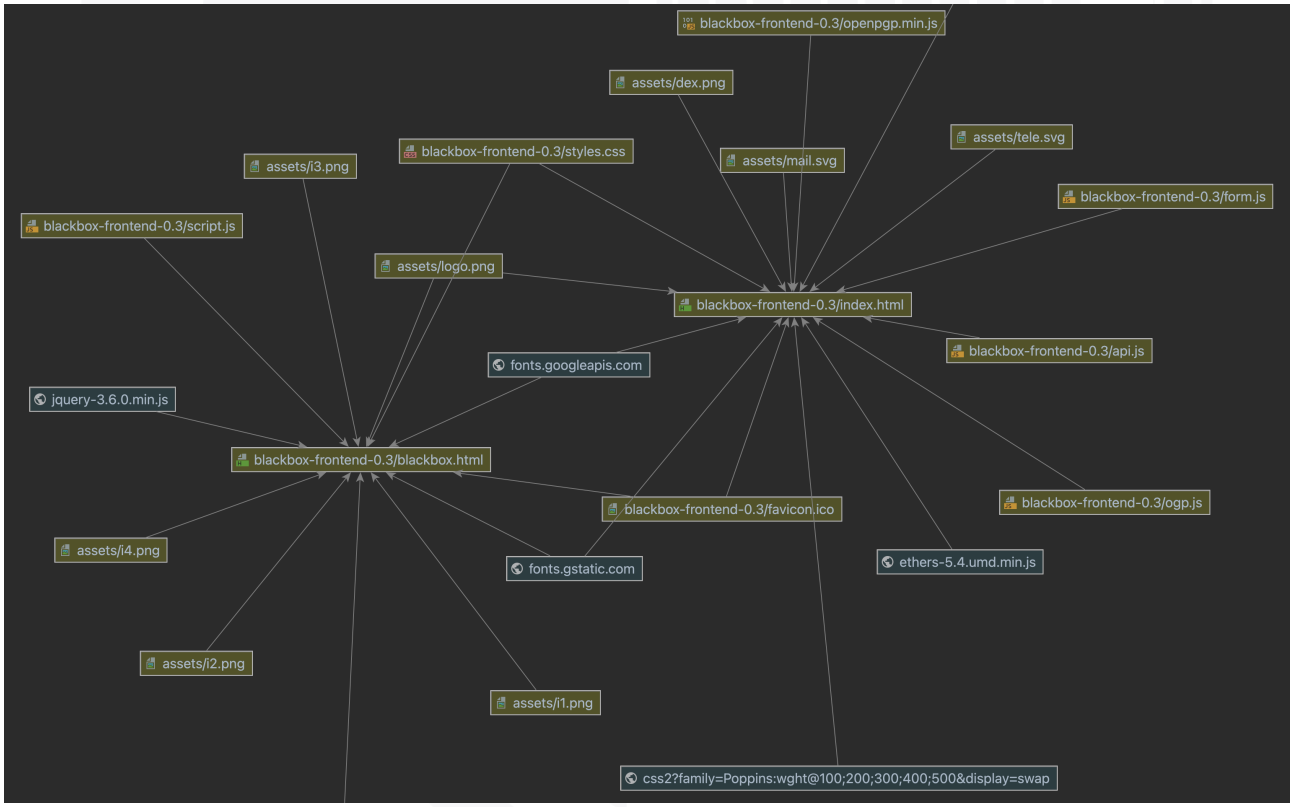
Components

The Scope of Work contains the following types.

JavaScript	Libraries	HTML	Other
4	2	2	15

Visualization

The files in the Scope of Work have the following dependencies to each other.



Audit Results

Critical issues

No critical issues

High issues

No high issues

Medium issues

#2 File: ogp.js Lines: /

Description
It is possible to send less than the required 0.5 Eth.

Comment
The corresponding checks for the minimum quantity must be adjusted.

Low issues

#1 File: index.html Lines: 75, 120

Description
Invalid id reference

Comment
Align the label for attribute with the input id

Informational issues

#1 File: ogp.js Lines: 64, 118, 134, 144, 145

Description
Unused constants: network, encrypted, encMessage, usdcAddress, usdtAddress

Comment
Delete unused constants

#2 File: ogp.js Lines: 165, 176, 182

Description
'return' is unnecessary as the last statement in a function with no return value

Comment
Delete return statements

#3 File: index.html Lines: -

Description
No dynamic update of the Wallet Balance while changing the network or account on MetaMask.

Comment
We recommend to listen to events and update the logic.

#4 File: api.js Lines: -

Description
Unused function getBalance

Comment
api.js is not used yet. You can remove the import and function.

Commented Code exist

There are some instances of code being commented out in the following files that should be removed:

File	Line
form.js	10-19
ogp.js	9-14
ogp.js	29, 30
ogp.js	80-85
ogp.js	148-159

Recommendation

Remove the commented code, or address them properly.

Audit Comments

- There are several not allowed HTML elements in the index.html. This is not an security or functional issue, just a break of the implementation.
- We recommend to separate the whole process into more functions to improve the readability and maintenance.
- The latest version of the ethers library is 6.1.0. We recommend to use the latest version.
- Production deployment was tested on https://devgrayhat.github.io/
- It is advisable to retrieve the values directly from the input box and then calculate them. This can be repeated during a transfer and is better than getting them from a span element and taking these values for the transfer/calculation.
- In general, you should consider a uniform naming convention for variables and functions.